



## Firepower Management Center バージョン 6.1 コンフィギュレーションガイド

初版：2016年8月29日

最終更新：2017年12月4日

### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

**【注意】** シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークボロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2016–2017 Cisco Systems, Inc. All rights reserved.



## 目次

### 第 1 章

#### Firepower の概要 1

##### 管理対象デバイスの概要 1

7000 および 8000 シリーズ 管理対象デバイス 2

NGIPSv 3

Cisco ASA with FirePOWER Services 3

Firepower Threat Defense 4

Firepower Threat Defense Virtual 4

##### Firepower Management Center の概要 4

Firepower Management Center の機能 5

##### Firepower システムのコンポーネント 6

冗長性およびリソース共有 6

7000 & 8000 シリーズ デバイスのためのネットワーク トラフィック管理 6

マルチテナント機能 8

検出とアイデンティティ 8

アクセス制御 8

SSL インспекション 9

侵入検知と防御 9

Cisco Advanced Malware Protection およびファイル制御 10

アプリケーションプログラミング インターフェイス 12

##### Firepower のオンライン ヘルプとドキュメンテーション 13

ドキュメンテーションのライセンス ステートメント 13

ドキュメント内のサポート対象デバイスに関する記述 13

ドキュメント内のアクセス ステートメント 14

##### Firepower システムの IP アドレス表記法 14

---

第 1 部 :	<b>ユーザ アカウント 15</b>
第 2 章	<b>Firepower システムへのログイン 17</b>
	Firepower システムのユーザ アカウント 17
	Firepower システムのユーザ インターフェイス 19
	Web インターフェイスに関する考慮事項 23
	セッションのタイムアウト (Session Timeout) 24
	Web インターフェイスによる Firepower Management Center へのログイン 24
	Web インターフェイスによる管理対象デバイスへのログイン 25
	CAC クレデンシヤルを使用した Firepower Management Center へのログイン 26
	CAC クレデンシヤルを使用した管理対象デバイスへのログイン 27
	従来型デバイスでのコマンドライン インターフェイスへのログイン 28
	Firepower Threat Defense デバイスのコマンドライン インターフェイスへのログイン 29
	Web インターフェイスでの基本システム情報の表示 31
	Firepower Management Center のドメインの切り替え 31
	Firepower システム Web インターフェイスからのログアウト 32
	コンテキスト メニュー 32
第 3 章	<b>ユーザ設定の指定 35</b>
	ユーザ設定の概要 35
	パスワードの変更 35
	失効パスワードの変更 36
	ホームページの指定 37
	イベント ビュー設定の設定 37
	イベント ビュー設定 38
	ファイル ダウンロード設定 40
	デフォルト時間枠 41
	デフォルトワークフロー 43
	デフォルト タイム ゾーンの設定 43
	デフォルトのダッシュボードの指定 44

---

## 第 11 部 :

**Firepower システムの管理 45**

## 第 4 章

**Firepower システム ユーザ管理 47**

## ユーザの役割 47

定義済みのユーザ ロール 48

カスタム ユーザ ロール 50

例 : カスタム ユーザ ロールとアクセス制御 51

## ユーザ アカウントの権限 51

[概要 (Overview) ]メニュー 51

[分析 (Analysis) ]メニュー 55

ポリシー メニュー 62

[デバイス (Devices) ]メニュー 68

[オブジェクト マネージャ (Object Manager) ]メニュー 69

Cisco AMP 69

デバイスへの設定の展開 69

[システム (System) ]メニュー 70

[REST VDI] メニュー 76

[ヘルプ (Help) ]メニュー 77

## ユーザ ロールの管理 77

ユーザ ロールのアクティブおよび非アクティブの設定 78

カスタム ユーザ ロールの作成 79

ユーザ ロールのコピー 80

カスタム ユーザ ロールの編集 81

## ユーザ ロールのエスカレーション 82

エスカレーション ターゲット ロールの設定 82

エスカレーションに使用するカスタム ユーザ ロールの設定 83

ユーザ ロールのエスカレーション 84

## ユーザ アカウント 84

ユーザ アカウントの管理 85

ユーザ アカウントの作成 86

ユーザ アカウントの編集	87
複数のドメインでのユーザ ロールの割り当て	88
内部認証から外部認証へのユーザの変換	88
ユーザ アカウント ログイン オプション	89
コマンドラインのアクセス レベル	91
Firepower Threat Defense の CLI ユーザ アカウントの作成	92
Firepower システムのユーザ認証	94
内部認証	95
外部認証 (External Authentication)	96
LDAP 認証	97
LDAP 認証オブジェクトを作成するために必要な情報	97
CAC 認証	99
CAC 認証の設定	100
基本 LDAP 認証オブジェクトの作成	101
拡張 LDAP 認証オブジェクトの作成	104
LDAP 認証サーバのフィールド	108
LDAP 認証サーバの特定	109
LDAP 固有フィールド	110
LDAP 固有パラメータの設定	114
LDAP グループ フィールド	116
グループによるアクセス権の設定	117
LDAP シェル アクセスのフィールド	119
LDAP シェル アクセスの設定	119
LDAP 認証接続のテスト	121
LDAP 認証接続のトラブルシューティング	122
RADIUS 認証	124
RADIUS 認証オブジェクトの作成	124
RADIUS 接続の設定	127
RADIUS ユーザ ロールの設定	129
RADIUS シェル アクセスの設定	131
カスタム RADIUS 属性の定義	132

RADIUS 認証接続のテスト	133
シングル サインオン (SSO)	134
SSO の設定	135

---

**第 5 章**

<b>Firepower システムのライセンス</b>	<b>137</b>
Firepower の機能ライセンスについて	137
Firepower 機能のサービス サブスクリプション	138
Firepower システムのスマート ライセンス	139
Smart Software Manager	139
ライセンス認証局との定期通信	140
スマート ライセンスのステータス	140
スマート ライセンスの移転	141
スマート ライセンスのタイプと制約事項	141
基本ライセンス	143
Firepower Threat Defense デバイスのマルウェア ライセンス	143
脅威ライセンス	144
Firepower Threat Defense デバイスの URL フィルタリング ライセンス	145
Firepower Management Center Virtual ライセンス	145
Cisco Smart Software Manager での Firepower Management Center の登録	146
スマート ライセンスおよびスマート ライセンス ステータスの表示	147
スマート ライセンスの編集	147
Cisco Smart Software Manager から Firepower Management Center の登録解除	148
Cisco Smart Software Manager と Firepower Management Center の同期	149
Smart Software Satellite Server の設定	149
Firepower システムのクラシック ライセンス	150
製品ライセンス登録ポータル	150
従来のライセンスのタイプと制約事項	150
プロテクションライセンス	152
制御ライセンス	153
従来のデバイスの URL フィルタリング ライセンス	154
従来のデバイスのマルウェア ライセンス	155

VPN ライセンス	156
デバイス スタックおよびハイ アベイラビリティ ペアのクラシック ライセンス	156
従来型ライセンスの表示	156
ライセンス キーの特定	157
Firepower Management Center への従来型ライセンスの追加	158
管理対象デバイスへのライセンスの割り当て	159

## 第 6 章

<b>システム ソフトウェア更新</b>	<b>161</b>
システム ソフトウェア アップデートの概要	161
Firepower システムのソフトウェア アップデート	164
Firepower システムのソフトウェア アップデートの準備	164
Firepower システムのソフトウェア アップデート プロセス	165
Firepower システム ソフトウェア アップデートに関する注意事項	168
Firepower Management Center でのソフトウェアの更新	169
Firepower システムのソフトウェア更新のダウンロード	170
Firepower Management Center にソフトウェア更新をアップロードする	171
管理対象デバイスでのソフトウェア更新	172
主要な Firepower システム ソフトウェア更新のモニタリング	173
Firepower システムのソフトウェア アップデートのアンインストール	174
Firepower システムのソフトウェア更新のアンインストール	176
脆弱性データベースの更新	177
脆弱性データベースの更新	178
侵入ルールの更新	179
侵入ルールのワンタイム手動更新	182
侵入ルールのワンタイム自動更新	182
定期的な侵入ルール更新の設定	183
ローカル侵入ルール ファイル インポート	184
ローカル侵入ルール ファイルのインポート	185
ルールの更新ログ	186
侵入ルール更新のログ テーブル	186
侵入ルールの更新ログの表示	187



ルールアップデートのインポート ログの詳細ビュー	188
侵入ルールの更新インポート ログの詳細の表示	191
地理位置情報データベースの更新	192
手動による GeoDB の更新（インターネット接続）	193
地理位置情報データベース（GeoDB）の手動更新：インターネット接続なし	193
GeoDB 更新のスケジューリング	194

---

**第 7 章**

<b>バックアップと復元</b>	<b>197</b>
バックアップと復元の概要	197
バックアップと復元に関する制限事項	197
バックアップ ファイル	199
Firepower Management Center のバックアップ	200
管理対象デバイスのローカルでのバックアップ	201
Firepower Management Center からの管理対象デバイスのバックアップ	203
バックアップ プロファイルの作成	204
ローカル ホストからのバックアップのアップロード	205
[バックアップ管理（Backup Management）] ページ	206
バックアップ ファイルからのアプライアンスの復元	207

---

**第 8 章**

<b>コンフィギュレーションのインポートとエクスポート</b>	<b>211</b>
コンフィギュレーションのインポート/エクスポートについて	211
インポート/エクスポートをサポートする構成	212
設定のインポート/エクスポートに関する特別な考慮事項	212
設定のエクスポート	214
設定のインポート	214
インポート競合の解決	216

---

**第 9 章**

<b>タスクのスケジューリング</b>	<b>219</b>
タスクのスケジューリングの概要	219
定期タスクの設定	219
バックアップ タスクの自動化	221

Firepower Management Center のバックアップの自動化	221
管理対象デバイスのバックアップの自動化	222
証明書失効リストのダウンロードの設定	223
ポリシー展開の自動化	224
Nmap スキャンの自動化	225
Nmap スキャンのスケジュール	226
レポートの生成の自動化	227
スケジュールされたレポート生成設定の指定	228
Firepower の推奨ルールの自動化	229
ソフトウェア更新の自動化	231
ソフトウェア ダウンロードの自動化	232
ソフトウェア プッシュの自動化	233
ソフトウェア インストールの自動化	234
脆弱性データベースの更新の自動化	235
VDB 更新のダウンロードの自動化	236
VDB 更新のインストールの自動化	237
URL フィルタリング更新の自動化	238
スケジュール済みタスクの確認	239
タスク一覧の詳細	240
カレンダーのスケジュール済みタスクの表示	241
スケジュール済みタスクの編集	241
スケジュール済みタスクの削除	242

---

第 10 章	Management Center データベースの消去	243
	Management Center データベースからのデータの消去	243

---

第 III 部 :	システム モニタリングとトラブルシューティング	245
-----------	-------------------------	-----

---

第 11 章	ダッシュボード	247
	ダッシュボードについて	247
	Firepower システムのダッシュボード ウィジェット	248

ウィジェットの使用可能性	249
ユーザ ロール別のダッシュボード ウィジェットの可用性	250
定義済みダッシュボード ウィジェット	251
[アプライアンス情報 (Appliance Information) ] ウィジェット	252
[アプライアンス ステータス (Appliance Status) ] ウィジェット	252
[関連イベント (Correlation Events) ] ウィジェット	253
[現在のインターフェイス ステータス (Current Interface Status) ] ウィジェット	253
[現在のセッション (Current Sessions) ] ウィジェット	254
[カスタム分析 (Custom Analysis) ] ウィジェット	254
[ディスク使用量 (Disk Usage) ] ウィジェット	259
[インターフェイス トラフィック (Interface Traffic) ] ウィジェット	260
[侵入イベント (Intrusion Events) ] ウィジェット	261
[ネットワーク コンプライアンス (Network Compliance) ] ウィジェット	261
[製品ライセンス (Product Licensing) ] ウィジェット	262
[製品更新 (Product Updates) ] ウィジェット	263
[RSS フィード (RSS Feed) ] ウィジェット	263
[システム負荷 (System Load) ] ウィジェット	264
[システム時刻 (System Time) ] ウィジェット	264
[ホワイトリスト イベント (White List Events) ] ウィジェット	264
ダッシュボードの管理	265
ダッシュボード タブの追加	266
ダッシュボードへのウィジェットの追加	266
ウィジェットの設定	268
カスタム ダッシュボードの作成	268
カスタム ダッシュボード オプション	269
ウィジェット表示のカスタマイズ	271
ダッシュボード オプションの編集	271
ダッシュボードの時刻設定の変更	272
ダッシュボード タブの名前の変更	273
ダッシュボードの表示	274

## 第 12 章

**ヘルス モニタリング 275**

- ヘルス モニタリングについて 275
  - ヘルス モジュール 276
  - ヘルス モニタリングの設定 284
- 正常性ポリシー 284
  - デフォルトの正常性ポリシー 285
  - 正常性ポリシーの作成 285
  - 正常性ポリシーの適用 286
  - 正常性ポリシーの編集 287
  - 正常性ポリシーの削除 288
- ヘルス モニタ ブラックリスト 289
  - アプライアンスのブラックリスト登録 290
  - 正常性ポリシー モジュールのブラックリスト登録 291
- ヘルス モニタ アラート 292
  - ヘルス モニタ アラート情報 292
  - ヘルス モニタ アラートの作成 293
  - ヘルス モニタ アラートの編集 294
  - ヘルス モニタ アラートの削除 294
- ヘルス モニタの使用 295
  - ヘルス モニタ ステータスのカテゴリ 296
- アプライアンス ヘルス モニタの表示 297
  - アプライアンスのすべてのモジュールの実行 298
  - 特定のヘルス モジュールの実行 299
  - ヘルス モジュール アラート グラフの生成 300
- ヘルス イベント ビュー 300
  - ヘルス イベントの表示 301
  - モジュールとアプライアンス別のヘルス イベントの表示 302
  - ヘルス イベント テーブルの表示 302
  - 7000 および 8000 シリーズ デバイスのハードウェア アラートの詳細 303
  - [ヘルス イベント (Health Events) ] テーブル 306

---

第 13 章	<b>システムのモニタリング</b>	<b>309</b>
	システム統計	309
	システム統計が使用できるアプライアンス	309
	[ホスト統計情報 (Host Statistics) ]セクション	310
	[ディスク使用量 (Disk Usage) ]セクション	311
	[プロセス (Processes) ]セクション	311
	プロセス使用状況フィールド	311
	システム デーモン	313
	実行可能ファイルおよびシステム ユーティリティ	315
	[SFDataCorrelator プロセス統計情報 (SFDataCorrelator Process Statistics) ]セクション	319
	[侵入イベント情報 (Intrusion Event Information) ]セクション	320
	システム統計情報の表示	320
第 14 章	<b>システムのトラブルシューティング</b>	<b>323</b>
	システム メッセージ	323
	メッセージタイプ	324
	メッセージ管理	326
	システム メッセージの管理	327
	展開メッセージの表示	328
	ヘルス メッセージの表示	329
	タスク メッセージの表示	330
	タスク メッセージの管理	331
	通知動作の設定	332
	トラブルシューティング用のヘルス モニタ レポート	332
	特定のシステム機能のトラブルシューティング ファイルの作成	333
	高度なトラブルシューティング ファイルのダウンロード	334
	Web インターフェイスからの Firepower Threat Defense CLI の使用	335
	機能固有のトラブルシューティング	336
第 IV 部 :	<b>導入管理</b>	<b>337</b>

---

---

第 15 章	<b>ドメイン管理</b>	<b>339</b>
	ドメインを使用したマルチテナンシーの概要	339
	ドメインの用語	340
	ドメインのプロパティ	341
	ドメインの管理	343
	新しいドメインの作成	344
	ドメイン間のデータの移動	345
	ドメイン間のデバイスの移動	346

---

第 16 章	<b>ポリシー管理</b>	<b>349</b>
	ポリシーの導入	349
	設定変更の導入	350
	デバイスへの強制導入	352
	設定変更の展開に関する注意事項	353
	Snort® の再起動シナリオ	354
	ポリシー適用中のトラフィックの検査	355
	Snort® の再起動によるトラフィックの動作	356
	展開またはアクティブ化された際に Snort プロセスを再起動する設定	357
	変更により Snort プロセスがただちに再起動する場合	360
	ポリシーの比較	360
	ポリシーの比較	361
	ポリシー レポート	362
	現在のポリシー レポートの生成	363
	失効ポリシー	363
	限定的な導入のパフォーマンスに関する考慮事項	364
	侵入防御のない検出	365
	ディスカバリのない侵入防御	366

---

第 17 章	<b>ルール管理：共通の特性</b>	<b>369</b>
	ルールの概要	369

ルール条件タイプ	371
ルール条件の仕組み	373
インターフェイス条件	374
インターフェイス条件の設定	376
ネットワーク条件	377
ネットワーク条件の設定	379
トンネルエンドポイント条件	380
トンネルエンドポイント条件の設定	381
VLAN 条件	382
ポートおよび ICMP コードの条件	382
ポート条件の設定	384
カプセル化の条件	385
アプリケーション条件 (アプリケーション制御)	386
アプリケーション条件とフィルタの設定	387
アプリケーションの特性	390
アプリケーション制御の制限	391
URL 条件 (URL フィルタリング)	393
レピュテーションベースの URL フィルタリング	393
手動 URL フィルタリング	395
URL 条件の設定	396
HTTPS トラフィックのフィルタリング	398
URL フィルタリングの制限	399
ユーザ条件、レルム条件、および ISE 属性条件 (ユーザ制御)	401
ユーザ制御の前提条件	402
ユーザおよびレルム条件の設定	403
ISE 属性条件の設定	404
ユーザ制御のトラブルシューティング	405
カスタム SGT 条件	406
ISE SGT とカスタム SGT ルール条件との比較	406
カスタム セキュリティ グループ タグ (SGT) から ISE セキュリティ グループ タグ (SGT) への自動遷移	407

カスタム SGT 条件の設定	408
カスタム SGT 条件のトラブルシューティング	408
ルールの検索	409
デバイス別のフィルタリングルール	410
ルールとその他のポリシーの警告	411
ルールのパフォーマンスに関するガイドライン	412
ルールの簡素化および絞り込みのガイドライン	413
ルールの順序指定のガイドライン	413
ルールのプリエンブション	413
ルールのアクションとルールの順序	415
コンテンツ規制ルールの順序	416
SSL ルールの順序	416
URL ルールの順序	417
侵入ポリシーの急増を回避するためのガイドライン	417
大規模接続（フロー）のオフロード	418
フロー オフロードの制限事項	419

## 第 18 章

再利用可能なオブジェクト	421
再利用可能オブジェクトの概要	422
オブジェクト マネージャ	424
オブジェクトの編集	424
オブジェクトまたはオブジェクト グループのフィルタ処理	425
オブジェクトのソート	426
オブジェクト グループ	426
再利用可能オブジェクトのグループ化	427
オブジェクトのオーバーライド	429
オブジェクト オーバーライドの管理	430
オブジェクトのオーバーライドの許可	431
オブジェクトのオーバーライドの追加	431
オブジェクト オーバーライドの編集	432
ネットワーク オブジェクト	433



ネットワーク オブジェクトの作成	434
ポート オブジェクト	435
ポート オブジェクトの作成	436
インターフェイス オブジェクト：インターフェイスグループとセキュリティゾーン	437
セキュリティゾーンおよびインターフェイス グループ オブジェクトの作成	438
トンネルゾーン	439
アプリケーションフィルタ	439
VLAN タグ オブジェクト	440
VLAN タグ オブジェクトの作成	440
セキュリティ グループ タグ オブジェクト	441
セキュリティ グループ タグ オブジェクトの作成	441
URL オブジェクト	442
URL オブジェクトの作成	442
地理位置情報オブジェクト	443
地理位置情報オブジェクトの作成	444
変数セット	444
侵入ポリシー内の変数セット	446
変数	446
定義済みデフォルト変数	447
ネットワーク変数	450
ポート変数	452
拡張変数	453
変数のリセット	454
セットに変数を追加する	455
変数のネスト	457
変数セットの管理	459
変数セットの作成	460
変数の管理	460
変数の追加	462
変数の編集	463
セキュリティ インテリジェンスのリストとフィード	464

セキュリティ インテリジェンス オブジェクトのクイック リファレンス	466
[今すぐブラックリストに登録 (Blacklist Now) ]、[今すぐホワイトリストに登録 (Whitelist Now) ]、およびグローバル リスト	466
セキュリティ インテリジェンス リストとマルチテナンシー	468
セキュリティ インテリジェンス フィードの更新頻度の変更	470
カスタム セキュリティ インテリジェンス フィード	470
セキュリティ インテリジェンス フィードの作成	471
手動によるセキュリティ インテリジェンス フィードの更新	472
カスタム セキュリティ インテリジェンス リスト	472
新しいセキュリティ インテリジェンス リストの Firepower Management Center へのアップロード	474
セキュリティ インテリジェンス リストの更新	475
シンクホール オブジェクト	475
シンクホール オブジェクトの作成	476
ファイル リスト	476
ファイル リストのソース ファイル	477
ファイル リスト別の SHA-256 値の追加	478
ファイル リストへの個々のファイルのアップロード	479
ファイル リストへのソース ファイルのアップロード	480
ファイル リストの SHA-256 値の編集	481
ファイル リストからのソース ファイルのダウンロード	483
暗号スイート リスト	483
暗号スイート リストの作成	484
識別名オブジェクト	484
識別名オブジェクトの作成	486
PKI オブジェクト	487
内部認証局オブジェクト	488
CA 証明書と秘密キーのインポート	489
CA 証明書と秘密キーのインポート	489
CA 証明書および秘密キーの生成	490
新しい署名付き証明書	491

未署名の CA 証明書と CSR の作成	491
CSR への応答として発行された署名付き証明書のアップロード	492
CA 証明書および秘密キーのダウンロード	493
CA 証明書と秘密キーのダウンロード	493
信頼できる認証局オブジェクト	494
信頼できる CA オブジェクト	494
信頼できる CA オブジェクトの追加	495
信頼できる CA オブジェクトの証明書失効リスト	495
信頼できる CA オブジェクトへの証明書失効リストの追加	496
外部証明書オブジェクト	497
外部証明書オブジェクトの追加	497
内部証明書オブジェクト	498
内部証明書オブジェクトの追加	499
SLA モニタ オブジェクト	499
プレフィックス リスト	501
IPv6 プレフィックス リストの設定	501
IPv4 プレフィックス リストの設定	502
ルート マップ	504
アクセス リスト	508
拡張 ACL オブジェクトの設定	509
標準 ACL オブジェクトの設定	510
AS パスのオブジェクト	511
コミュニティ リスト	512
ポリシー リスト	514
VPN オブジェクト	516
Firepower Threat Defense IKE ポリシー	516
IKEv1 ポリシー オブジェクトの設定	516
IKEv2 ポリシー オブジェクトの設定	518
Firepower Threat Defense IPsec プロポーザル	520
IKEv1 IPsec プロポーザル オブジェクトの設定	521
IKEv2 IPsec プロポーザル オブジェクトの設定	522

---

第 V 部 :	<b>アプライアンス管理の基本</b>	<b>523</b>
---------	---------------------	------------

---

第 19 章	<b>Firepower Management Center の基礎</b>	<b>525</b>
	Firepower Management Center	525
	デバイス管理	525
	Firepower Management Center で管理できるデバイス	526
	ポリシーとイベント以外の機能	527
	NAT 環境	527

---

第 20 章	<b>Firepower Management Center ハイ アベイラビリティ</b>	<b>529</b>
	Firepower Management Center のハイ アベイラビリティについて	529
	Firepower Management Center のシステム要件	530
	ハードウェア要件	530
	ソフトウェア要件	530
	ライセンス要件	530
	高可用性 Firepower Management Center での役割とステータス	531
	Firepower Management Center ハイ アベイラビリティ ペアのデバイス登録	531
	Firepower Management Center のハイ アベイラビリティ ペアでのイベント処理	532
	AMP クラウド接続とマルウェア情報	532
	URL フィルタリングとセキュリティ インテリジェンス	532
	Firepower Management Center のフェールオーバー中のユーザ データの処理	533
	Firepower Management Center ハイ アベイラビリティ ペアの構成管理	533
	バックアップ中の Firepower Management Center の高可用性動作	533
	Firepower Management Center ハイ アベイラビリティのスプリットブレイン	533
	ハイ アベイラビリティ ペアでの Firepower Management Center のアップグレード	534
	Firepower Management Center のハイ アベイラビリティのトラブルシューティング	535
	Firepower Management Center の高可用性の設定	536
	Firepower Management Center ハイ アベイラビリティ ステータスの表示	538
	ハイ アベイラビリティ中に Firepower Management Center 間で同期された設定データ	539

Firepower Management Center のハイ アベイラビリティにおけるデバイス登録を解決するための CLI の使用	540
Firepower Management Center ハイ アベイラビリティ ペアにおけるピアの切り替え	540
Firepower Management Center ペア間の通信の一時停止	541
Firepower Management Center ペア間の通信の再開	542
高可用性ペアの Firepower Management Center の IP アドレスの変更	542
ハイ アベイラビリティ ペアでの Firepower Management Center のアップグレード	543
Firepower Management Center ハイ アベイラビリティの無効化	544

---

 第 21 章

**デバイスの管理の基本 547**

[デバイス管理 (Device Management) ] ページ	547
管理対象デバイスのフィルタリング	548
リモート管理の設定	549
Firepower Management Center へのデバイスの追加	550
Firepower Management Center からのデバイスの削除	552
デバイス コンフィギュレーションの設定	553
一般的なデバイスの設定	553
デバイス ライセンスの設定	553
デバイス システムの設定	554
デバイス ヘルスの設定	554
デバイス管理設定	555
デバイスの詳細設定	555
デバイス情報の表示	556
デバイス管理設定の編集	556
一般的なデバイス設定の編集	557
デバイス ライセンスの有効化と無効化	558
詳細なデバイス設定の編集	559
自動アプリケーションバイパスの設定	559
ローカルルータ トラフィックの検査	561
高速パス ルールの設定 (8000 シリーズ)	561
システム シャットダウンの管理	563

インターフェイス テーブル ビュー 564

デバイス グループ管理 568

    デバイス グループの追加 568

    デバイス グループの編集 569

---

第 VI 部 :           **クラシック デバイス設定の基本 571**

---

第 22 章           **従来型デバイスの管理の基本 573**

    リモート管理の設定 573

        管理対象デバイス上のリモート管理の設定 574

        管理対象デバイスでのリモート管理の編集 575

        管理ポートの変更 576

    インターフェイス構成時の設定 576

        物理的なハードウェア ビュー 577

        インターフェイス アイコン 577

        物理ハードウェア ビューの使用 578

        センシング インターフェイスの設定 579

        HA リンク インターフェイスの設定 580

        インターフェイスの無効化 582

        Cisco ASA FirePOWER インターフェイスの管理 583

        7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 584

        セキュリティ ゾーン オブジェクトのリビジョンの同期 584

---

第 23 章           **IPS デバイスの展開と設定 587**

    IPS デバイスの展開と設定の概要 587

    パッシブ IPS 展開 587

        Firepower システムのパッシブ インターフェイス 588

        パッシブ インターフェイスの設定 588

    インライン IPS 展開 590

        Firepower システムのインライン インターフェイス 592

        インライン インターフェイスの設定 592

Firepower システムのインライン セット	593
インライン セットの表示	595
インライン セットの追加	595
インライン セットの詳細オプション	597
高度なインライン セット オプションの設定	599
インライン セットの削除	599

## 第 VII 部 :

## クラシック デバイスのハイ アベイラビリティと拡張性 601

## 第 24 章

## 7000 および 8000 シリーズ デバイスのハイ アベイラビリティ 603

7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて	603
デバイスのハイ アベイラビリティ要件	604
デバイス ハイ アベイラビリティ フェールオーバーとメンテナンス モード	605
デバイスの高可用性ペアでのポリシーの導入と更新	606
展開タイプとデバイス ハイ アベイラビリティ	606
デバイスのハイ アベイラビリティ設定	608
デバイスのハイ アベイラビリティの確立	609
デバイスのハイ アベイラビリティの編集	610
高可用性ペアの個々のデバイスの設定	611
高可用性ペアの個々のデバイス スタックの設定	612
高可用性ペアのデバイスでのインターフェイスの設定	613
デバイスのハイ アベイラビリティ ペアにおけるアクティブ ピアの切り替え	613
高可用性ピアのメンテナンス モードへの切り替え	614
高可用性ペアのスタック内のデバイスの交換	615
デバイスのハイ アベイラビリティ状態共有	616
デバイスのハイ アベイラビリティ状態共有の確立	618
トラブルシューティングのためのデバイスのハイ アベイラビリティの状態共有統計情報	619
デバイス ハイ アベイラビリティの状態共有統計情報の表示	621
デバイス高可用性ペアの分離	622

---

第 25 章	<b>8000 シリーズ デバイスのスタック構成</b>	<b>625</b>
	デバイス スタックについて	625
	デバイス スタック 設定	627
	デバイス スタックの確立	628
	デバイス スタックの編集	630
	スタック内のデバイスの交換	630
	高可用性ペアのスタック内のデバイスの交換	631
	スタックに含まれる個々のデバイスの設定	632
	スタック構成のデバイスでのインターフェイスの設定	633
	スタック構成のデバイスの分離	634
	スタック内のデバイスの交換	635

---

第 VIII 部 :	<b>Firepower Threat Defense の設定の基本</b>	<b>637</b>
------------	--	------------

---

第 26 章	<b>Firepower Threat Defense 用のトランスペアレントまたはルーテッド ファイアウォール モード</b>	<b>639</b>
	ファイアウォール モードについて	639
	ルーテッド ファイアウォール モードについて	640
	トランスペアレント ファイアウォール モードについて	640
	ネットワークでのトランスペアレント ファイアウォールの使用	640
	ブリッジグループについて	641
	ルーテッド モード機能のためのトラフィックの通過	646
	デフォルト設定	646
	ファイアウォール モードのガイドライン	646
	ファイアウォール モードの設定	647

---

第 27 章	<b>Firepower Threat Defense のインターフェイス</b>	<b>649</b>
	Firepower Threat Defense インターフェイスについて	649
	管理/診断インターフェイスとネットワーク 配置	649
	管理インターフェイス	649



診断インターフェイス	650
ルーテッドモードの導入	650
トランスペアレントモードの展開	651
インターフェイスモードとタイプ	652
セキュリティゾーンとインターフェイスグループ	654
Auto-MDI/MDIX 機能	654
通常の（ファイアウォール）モードインターフェイスの設定	654
物理インターフェイスの有効化およびイーサネット設定の構成	655
EtherChannel インターフェイスと冗長インターフェイス	657
EtherChannel インターフェイスと冗長インターフェイスについて	657
EtherChannel インターフェイスと冗長インターフェイスのガイドライン	660
冗長インターフェイスの設定	662
EtherChannel の設定	664
VLAN サブインターフェイスと 802.1Q トランッキングの設定	666
ルーテッドモードインターフェイスおよびトランスペアレントモードインターフェイス	668
ルーテッドモードインターフェイスとトランスペアレントモードインターフェイスについて	668
ルーテッドモードおよびトランスペアレントモードのインターフェイスのガイドライン	671
ルーテッドモードのインターフェイスの設定	672
トランスペアレントモードのブリッジグループインターフェイスの設定	674
IPv6 アドレッシングの設定	678
インターフェイスの詳細設定	683
インターフェイスの詳細設定について	683
デフォルト設定	687
ARP インスペクションと MAC アドレス テーブルのガイドライン	687
MTU の設定	687
MAC アドレスの設定	688
スタティック ARP エントリの追加	689
静的 MAC アドレスの追加とトランスペアレントモードのブリッジグループの MAC 学習の無効化	690

セキュリティの設定パラメータの設定	691
IPS のみ対応のインターフェイスの設定	694
インラインセットのハードウェアバイパスについて	694
ハードウェアバイパス トリガー	694
ハードウェアバイパスのスイッチオーバー	695
フェールセーフとハードウェアバイパス	695
ハードウェアバイパスのステータス	695
インラインセットの前提条件	695
IPS 専用インターフェイスのガイドライン	696
パッシブ IPS 専用インターフェイスの設定	697
IPS 専用インターフェイスのインラインセットの設定	699
インターフェイスと Firepower Management Center の同期	702

---

**第 28 章**

<b>Threat Defense 用の DHCP および DDNS サービス</b>	<b>705</b>
DHCP サービスと DDNS サービスについて	705
DHCPv4 サーバについて	705
DHCP オプション	706
DHCP リレー エージェントについて	706
DDNS について	707
DDNS 更新設定	707
UDP パケット サイズ	707
DHCP サービスと DDNS サービスのガイドライン	708
DHCP サーバの設定	709
DHCP リレー エージェントの設定	711
DDNS の設定	713

---

**第 29 章**

<b>Firepower Threat Defense 用の Quality of Service (QoS)</b>	<b>717</b>
QoS の概要	717
QoS ポリシーについて	718
QoS ポリシーによるレートの制限	719
QoS ポリシーの作成	720

QoS ポリシーのターゲット デバイスの設定 721

QoS ルールの設定 722

QoS ルール コンポーネント 723

---

第 IX 部 :

**Firepower Threat Defense のハイ アベイラビリティと拡張性 725**

---

第 30 章

**Firepower Threat Defense ハイ アベイラビリティ 727**

ハイ アベイラビリティ Firepower Threat Defense について 727

ハイ アベイラビリティ のシステム要件 728

ハードウェア要件 728

ソフトウェア要件 728

ライセンス要件 728

フェールオーバー リンクとステートフル フェールオーバー リンク 729

フェールオーバー リンク 729

ステートフル フェールオーバー リンク 730

フェールオーバー リンクとデータ リンクの中断の回避 731

フェールオーバーでの MAC アドレスおよび IP アドレス 734

ステートフル フェールオーバー 735

サポートされる機能 735

サポートされない機能 737

フェールオーバーのトランスペアレント ファイアウォール モードブリッジ グループ要件  
738

フェールオーバーのヘルス モニタリング 738

装置のヘルス モニタリング 738

インターフェイス モニタリング 739

フェールオーバー トリガーおよび検出タイミング 741

アクティブ/スタンバイ フェールオーバーについて 741

プライマリ/セカンダリの役割とアクティブ/スタンバイ ステータス 741

起動時のアクティブ装置の判別 742

フェールオーバー イベント 742

ハイ アベイラビリティ のガイドライン 744

Firepower Threat Defense ハイ アベイラビリティ ペアの追加	745
オプションの高可用性パラメータの設定	747
インターフェイス モニタリングの設定	747
ハイ アベイラビリティ フェールオーバー条件の編集	748
仮想 MAC アドレスの設定	749
ハイ アベイラビリティ の管理	750
Firepower Threat Defense ハイ アベイラビリティ ペアにおけるアクティブ ピアの切り替え	750
ハイ アベイラビリティ の中断と再開	750
ユニットの交換	751
プライマリ ユニットの交換	751
セカンダリ ユニットの交換	752
ハイ アベイラビリティ ペアにおけるユニットの分離	753
ハイ アベイラビリティ ペアの登録解除	753
ハイ アベイラビリティ のモニタリング	754
フェールオーバー履歴の表示	754
ステートフル フェールオーバーの統計情報の表示	755

## 第 31 章

<b>Firepower 9300 の Firepower Threat Defense クラスタ</b>	<b>757</b>
Firepower 9300 シャーシでのクラスタリングについて	757
パフォーマンス スケーリング係数	758
ブートストラップ コンフィギュレーション	758
クラスタ メンバー	759
マスターおよびスレーブ ユニットのロール	759
マスター ユニット選定	759
クラスタ インターフェイス	759
VSS または vPC への接続	760
クラスタ制御リンク	760
クラスタ制御リンク ネットワーク	760
クラスタ内のハイ アベイラビリティ	760
シャーシアプリケーションのモニタリング	760

装置のヘルス モニタリング	761
インターフェイス モニタリング	761
障害後のステータス	761
クラスタへの再参加	762
データ パス接続状態の複製	762
コンフィギュレーションの複製	763
管理インターフェイス	763
クラスタが接続を管理する方法	764
接続ロール	764
新しい接続の所有権	765
サンプル データ フロー	765
Firepower Threat Defense の機能とクラスタリング	766
クラスタリングでサポートされない機能	766
クラスタリングの中央集中型機能	766
ダイナミック ルーティングとクラスタリング	767
NAT とクラスタリング	767
SIP インспекションとクラスタリング	768
syslog とクラスタリング	768
SNMP とクラスタリング	769
FTP とクラスタリング	769
Cisco TrustSec とクラスタリング	769
Firepower 9300 シャーシ でのクラスタ化前提条件	769
Firepower 9300 シャーシ 上のクラスタリングのガイドライン	769
Firepower 9300 シャーシ でのクラスタリングのデフォルト	770
Firepower 4100/9300 シャーシ のクラスタリング設定	770
Firepower 4100/9300 シャーシ スーパーバイザからのクラスタの展開	770
Management Center へのクラスタの追加	771
クラスタ メンバーの追加	773
スレーブ メンバーの削除	774
クラスタへの再参加	774
クラスタリングの履歴	775

---

第 X 部 :	<b>Firepower Threat Defense のルーティング</b>	<b>777</b>
第 32 章	<b>Firepower Threat Defense のルーティングの概要</b>	<b>779</b>
	パスの決定	779
	サポートされるルート タイプ	780
	スタティックとダイナミックの比較	780
	シングルパスとマルチパスの比較	781
	フラットと階層型の比較	781
	リンクステートと距離ベクトル型の比較	781
	<b>Firepower Threat Defense 内でのルーティングの仕組み</b>	<b>782</b>
	出力インターフェイスの決定	782
	ネクスト ホップの選択プロセス	783
	ECMP ルーティング	784
	ルーティングでサポートされるインターネット プロトコル	784
	着信サービス一覧 (Routing Table)	785
	ルーティング テーブルへの入力方法	785
	ルートのアドミニストレーティブ ディスタンス	786
	バックアップ ルート	787
	転送の決定方法	788
	ダイナミック ルーティングおよびハイ アベイラビリティ	789
	クラスタリングでのダイナミック ルーティング	789
	管理トラフィック用ルーティングテーブル	790
	ルート マップについて	790
	permit 句と deny 句	791
	match 句と set 句の値	791
第 33 章	<b>Firepower Threat Defense のスタティック ルートとデフォルト ルート</b>	<b>793</b>
	スタティック ルートとデフォルト ルートについて	793
	デフォルト ルート	793
	スタティック ルート	793

---

不要なトラフィックを「ブラックホール化」するための null0 インターフェイスへのルート	794
ルートのプライオリティ	794
トランスペアレントファイアウォールモードのルート	794
スタティックルートトラッキング	795
スタティックルートとデフォルトルートのガイドライン	796
スタティックルートの追加	796

## 第 34 章

**Firepower Threat Defense 用の OSPF 799**

Firepower Threat Defense 用の OSPF	799
OSPF について	799
fast hello パケットに対する OSPF のサポート	801
Fast Hello パケットに対する OSPF サポートの前提条件	801
OSPF Hello インターバルと dead 間隔	801
OSPF fast hello パケット	802
OSPF Fast Hello パケットの利点	802
OSPFv2 および OSPFv3 間の実装の差異	802
OSPF のガイドライン	803
OSPFv2 の設定	804
OSPF エリア、範囲、仮想リンクの設定	804
OSPF 再配布の設定	808
OSPF エリア間フィルタリングの設定	809
OSPF のフィルタールールの設定	811
OSPF サマリーアドレスの設定	812
OSPF インターフェイスとネイバーの設定	813
OSPF 詳細プロパティの設定	815
OSPFv3 の設定	818
OSPFv3 エリア、ルート集約、および仮想リンクの設定	818
OSPFv3 再配布の設定	821
OSPFv3 サマリープレフィックスの設定	823
OSPFv3 インターフェイス、認証、およびネイバーの設定	824

OSPFv3 詳細プロパティの設定 827

---

第 35 章

**Firepower Threat Defense の BGP 831**

BGP について 831

ルーティング テーブルの変更 831

BGP を使用する状況 832

BGP パスの選択 833

BGP マルチパス 833

BGP のガイドライン 835

BGP の設定 835

BGP 基本設定 835

BGP 一般設定 838

BGP ネイバーの設定 840

BGP 集約アドレス設定 845

BGPv4 フィルタリング設定 846

BGP ネットワーク設定 847

BGP 再配布設定 847

BGP ルート注入の設定 848

---

第 36 章

**Firepower Threat Defense 用の RIP 851**

RIP について 851

ルーティング アップデート プロセス 852

RIP のルーティング メトリック 852

RIP 安定性機能 852

RIP タイマー 852

RIP のガイドライン 853

RIP の設定 854

---

第 37 章

**Firepower Threat Defense 用のマルチキャスト ルーティング 859**

マルチキャスト ルーティングについて 859

IGMP プロトコル 860



スタブ マルチキャストルーティング	861
PIM マルチキャストルーティング	861
PIM Source Specific Multicast のサポート	861
マルチキャスト双方向 PIM	862
PIM ブートストラップ ルータ (BSR)	862
PIM ブートストラップ ルータ (BSR) の用語	863
マルチキャスト グループの概念	864
マルチキャスト アドレス	864
クラスタリング	864
マルチキャストルーティングのガイドライン	864
IGMP 機能の設定	865
マルチキャスト ルーティングの有効化	865
IGMP プロトコルの設定	866
IGMP アクセスグループの設定	868
IGMP スタティック グループの設定	869
IGMP 参加グループの設定	870
PIM 機能の設定	871
PIM プロトコルの設定	871
PIM ネイバー フィルタの設定	872
PIM 双方向ネイバー フィルタの設定	873
PIM ランデブー ポイントの設定	875
PIM ルート ツリーの設定	876
PIM リクエスト フィルタの設定	877
Firepower Threat Defense デバイスのブートストラップ ルータ設定	878
マルチキャストルートの設定	879
マルチキャスト境界フィルタの設定	880

---

第 X1 部 :	<b>Firepower Threat Defense の VPN</b>	883
----------	---------------------------------------	-----

---

第 38 章	<b>VPN の概要</b>	885
	VPN タイプ	885

VPN の基本	886
インターネット キー エクスチェンジ (IKE)	886
IPsec	888
VPN パケットフロー	889
VPN ライセンス	889
VPN 接続の安全性を確保する方法	889
使用する暗号化アルゴリズムの決定	890
使用するハッシュ アルゴリズムの決定	891
使用する Diffie-Hellman 係数グループの決定	892
VPN トポロジ オプション	892
ポイントツーポイントの VPN トポロジ	893
ハブ アンド スポーク VPN トポロジ	893
フル メッシュ VPN トポロジ	894
暗黙的にサポートされる トポロジ	895

---

**第 39 章**

<b>Firepower Threat Defense VPNの導入</b>	<b>897</b>
Firepower Threat Defense サイト間 VPN について	897
VPN ライセンス	898
Firepower Threat Defense サイト間 VPN ガイドラインと制約事項	899

---

**第 40 章**

<b>Firepower Threat Defense VPN の管理</b>	<b>901</b>
Firepower Threat Defense のサイト間 VPN の管理	901
Firepower Threat Defense サイト間 VPN の設定	902
Firepower Threat Defense VPN エンドポイント オプション	903
Firepower Threat Defense VPN IKE オプション	905
Firepower Threat Defense VPN IPsec オプション	906
Firepower Threat Defense VPN 展開の詳細オプション	908
Firepower Threat Defense VPN のモニタリング	911

---

**第 XII 部 :**

<b>アプライアンス プラットフォームの設定</b>	<b>913</b>
----------------------------	------------

<b>システム設定 (System Configuration)</b>	<b>915</b>
システム設定の概要	916
Firepower Management Center システム設定のナビゲーション	916
システム設定	917
アプライアンス情報	919
システム情報の表示および変更	921
カスタム HTTPS 証明書	921
現在の HTTPS サーバ証明書の表示	923
HTTPS サーバの証明書署名要求の作成	923
HTTPS サーバ証明書のインポート	924
有効な HTTPS クライアント証明書の強制	926
外部データベース アクセスの設定	927
データベースへの外部アクセスの有効化	928
データベース イベント数の制限	929
データベース イベント数の制限の設定	929
データベース イベント数の制限	930
管理インターフェイス	931
管理インターフェイスについて	931
Firepower Management Center 上の管理インターフェイス	932
管理対象デバイス上の管理インターフェイス	932
管理インターフェイスのサポート	933
管理インターフェイス上のネットワーク ルート	935
管理およびイベント トラフィック チャンネルの例	935
管理インターフェイスの設定	936
Firepower Management Center 管理インターフェイスの設定	937
従来型デバイス Web インターフェイスでのデバイス管理インターフェイスの設定	940
CLI でのデバイス管理インターフェイスの設定	943
システムのシャットダウンと再起動	947
システムのシャットダウンと再起動	948
リモートストレージ管理	949

ローカルストレージの設定	950
リモートストレージの NFS の設定	950
リモートストレージの SMB の設定	951
リモートストレージの SSH の設定	953
リモートストレージの管理詳細設定オプション	954
変更調整	954
変更調整の設定	955
変更調整オプション	956
ポリシー変更のコメント	956
ポリシーの変更を追跡するコメントの設定	956
アクセスリスト	957
システムのアクセスリストの設定	958
監査ログ	959
syslog への監査ログメッセージの送信	960
HTTP サーバへの監査ログメッセージの送信	961
カスタム監査ログクライアント証明書	963
現在の監査ログクライアント証明書の表示	964
監査ログクライアントの証明書署名要求の生成	964
監査ログクライアント証明書のインポート	966
有効な監査ログサーバの証明書の強制	967
ダッシュボード設定	968
ダッシュボードのカスタム分析ウィジェットの有効化	969
DNS キャッシュ	969
DNS キャッシュ プロパティの設定	969
電子メールの通知	970
メールリレーホストおよび通知アドレスの設定	971
言語の選択	972
別の言語の指定	972
ログインバナー	973
カスタムログインバナーの追加	973
SNMP ポーリング	974

SNMP ポーリングの設定	975
セキュリティ認定準拠の	976
セキュリティ認定準拠特性	977
セキュリティ認定準拠の推奨事項	978
セキュリティ認定コンプライアンスの有効化	979
時刻および時刻の同期	981
手動での時間指定	981
時刻の手動設定	983
Firepower Management Center からの時間の提供	984
時間の同期	985
セッションタイムアウト	986
セッションタイムアウトの設定	986
脆弱性マッピング	988
サーバの脆弱性のマッピング	988
リモート コンソールのアクセス管理	989
システム上のリモート コンソール設定の構成	989
Lights-Out 管理のユーザ アクセス設定	990
Lights-Out 管理ユーザ アクセスの有効化	991
Serial over LAN 接続の設定	992
IPMItool を使用した Serial Over LAN の設定	993
IPMIutil を使用した Serial Over LAN の設定	993
Lights-Out 管理の概要	994
IPMItool による Lights-Out Management の設定	996
IPMIutil による Lights-Out Management の設定	996
REST API 設定	996
REST API アクセスの有効化	997
VMware Tools と仮想システム	997
VMware 向け Firepower Management Center での VMware ツールの有効化	998
<b>第 42 章</b>	
<b>管理対象デバイス用のプラットフォーム設定ポリシー</b>	<b>999</b>
プラットフォーム設定の概要	999

プラットフォーム設定ポリシーの管理	1000
プラットフォーム設定ポリシーの作成	1001
プラットフォーム設定ポリシーのターゲットデバイスの設定	1002

## 第 43 章

**従来型デバイス用の Firepower プラットフォーム設定 1003**

Firepower プラットフォーム設定の概要	1003
Firepower プラットフォームの設定	1004
アクセスリスト	1005
システムのアクセスリストの設定	1005
監査ログ	1006
監査ログメッセージを Syslog に送信する	1007
監査ログメッセージを HTTP サーバに送信する	1009
カスタム監査ログクライアント証明書	1010
現在の監査ログクライアント証明書の表示	1011
監査ログクライアント証明書の署名要求の生成	1012
監査ログクライアント証明書のインポート	1013
有効な監査ログサーバ証明書の要求	1014
外部認証の設定	1016
外部認証の有効化	1017
言語の選択	1018
別の言語の指定	1018
ログインバナー	1019
カスタムログインバナーの追加	1020
セッションタイムアウト	1021
セッションタイムアウトの設定	1021
SNMP ポーリング	1022
SNMP ポーリングの設定	1023
セキュリティ認定準拠の	1025
セキュリティ認定準拠特性	1025
セキュリティ認定準拠の推奨事項	1027
セキュリティ認定コンプライアンスの有効化	1028

時刻および時刻同期 1029

時刻の同期 1030

---

第 44 章

**Firepower Threat Defense のプラットフォーム設定 1033**

ARP インспекションの設定 1033

バナー設定 1035

フラグメントの処理の設定 1036

HTTP の設定 1037

ICMP アクセス ルールの設定 1039

セキュア シェルの設定 1041

SMTP の設定 1043

SNMP の脅威に対する防御の設定 1043

SNMPv3 ユーザの追加 1045

SNMP ホストの追加 1047

SNMP トラップの設定 1048

Syslog の設定 1050

Syslog について 1050

重大度 1050

syslog メッセージフィルタリング 1051

syslog メッセージクラス 1051

ロギングのガイドライン 1053

Syslog 設定 1054

ロギングの有効化および基本設定の構成 1055

ロギング接続先の有効化 1057

電子メールアドレスへの syslog メッセージの送信 1058

カスタム イベント リストの作成 1059

Syslog メッセージの生成レートの制限 1060

Syslog 設定 1061

Syslog サーバの設定 1063

グローバル タイムアウトの設定 1064

脅威に対する防御のための NTP 時刻同期の設定 1066

---

第 XIII 部 :	ネットワーク アドレス変換 (NAT)	1069
------------	---------------------	------

---

第 45 章	NAT ポリシー管理	1071
	NAT ポリシーの管理	1071
	NAT ポリシーの作成	1072
	NAT ポリシーの設定	1074
	NAT ポリシーの対象の設定	1075
	NAT ポリシーのコピー	1076

---

第 46 章	7000 および 8000 シリーズ デバイス用の NAT	1079
	NAT ポリシーの設定	1079
	NAT ポリシーの設定ガイドライン	1080
	NAT ポリシー内のルール編成	1081
	NAT ルールの編成	1082
	NAT ルールの警告とエラー	1082
	NAT ルール警告の表示と非表示	1083
	NAT ポリシー規則のオプション	1083
	NAT ルールの作成および編集	1085
	NAT ルールのタイプ	1086
	NAT ルールの条件タイプ	1088
	NAT ルールの条件と条件の仕組み	1088
	NAT ルールの条件	1088
	NAT ルールへの条件の追加	1089
	NAT ルールのリテラル条件	1091
	NAT ルールの条件のオブジェクト	1091
	NAT ルール内のゾーン条件	1092
	NAT ルールへのゾーン条件の追加	1093
	ダイナミック NAT ルールの送信元ネットワーク条件	1094
	ネットワーク条件のダイナミック NAT ルールへの追加	1095
	NAT ルールの宛先ネットワーク条件	1096



NAT ルールへの宛先ネットワーク条件の追加	1097
NAT ルールでのポート条件	1098
NAT ルールへのポートの条件の追加	1099
<b>Firepower Threat Defense 用のネットワーク アドレス変換 (NAT)</b>	<b>1101</b>
NAT を使用する理由	1101
NAT の基本	1102
NAT の用語	1102
NAT タイプ	1103
ルーテッドモードとトランスペアレントモードの NAT	1103
ルーテッドモードの NAT	1103
トランスペアレントモードの NAT	1104
自動 NAT および手動 NAT	1106
自動 NAT	1106
手動 NAT	1106
自動 NAT と手動 NAT の比較	1107
NAT ルールの順序	1107
NAT インターフェイス	1109
NAT のルーティング設定	1110
マッピングインターフェイスと同じネットワーク上のアドレス	1110
固有のネットワーク上のアドレス	1110
実際のアドレスと同じアドレス (アイデンティティ NAT)	1111
NAT のガイドライン	1111
NAT のファイアウォールモードのガイドライン	1111
IPv6 NAT のガイドライン	1112
IPv6 NAT の推奨事項	1113
インスペクション対象プロトコルに対する NAT サポート	1113
NAT のその他のガイドライン	1115
脅威に対する防御のための NAT の設定	1117
複数のデバイスの NAT ルールのカスタマイズ	1119
ダイナミック NAT	1122

ダイナミック NAT について	1122
ダイナミック NAT の欠点と利点	1123
ダイナミック自動 NAT の設定	1124
ダイナミック手動 NAT の設定	1125
ダイナミック PAT	1128
ダイナミック PAT について	1128
ダイナミック PAT の欠点と利点	1129
PAT プール オブジェクトのガイドライン	1130
ダイナミック自動 PAT の設定	1131
ダイナミック手動 PAT の設定	1134
スタティック NAT	1138
スタティック NAT について	1138
スタティック自動 NAT の設定	1143
スタティック手動 NAT の設定	1145
アイデンティティ NAT	1149
アイデンティティ自動 NAT の設定	1150
アイデンティティ手動 NAT の設定	1151
Firepower Threat Defense の NAT ルール プロパティ	1155
インターフェイス オブジェクト : NAT のプロパティ	1156
自動 NAT の [変換 (Translation) ] プロパティ	1156
手動 NAT の [一般 (General) ] [変換 (Translation) ] プロパティ	1158
PAT プールの NAT プロパティ	1160
詳細 NAT プロパティ	1161
IPv6 ネットワークの変換	1162
NAT64/46 : IPv6 アドレスの IPv4 への変換	1163
NAT64/46 の例 : 内部 IPv6 ネットワークと外部 IPv4 インターネット	1163
NAT66 : IPv6 アドレスの異なる IPv6 アドレスへの変換	1168
NAT66 の例 : ネットワーク間のスタティック変換	1168
NAT66 の例 : シンプルな IPv6 インターフェイス PAT	1171
NAT のモニタリング	1173
NAT の例	1173

内部 Web サーバへのアクセスの提供（スタティック自動 NAT）	1174
内部ホストのダイナミック自動 NAT および外部 Web サーバのスタティック NAT	1176
複数のマッピングアドレス（スタティック自動 NAT、1 対多）を持つ内部ロードバランサ	1181
FTP、HTTP、および SMTP の単一アドレス（ポート変換を設定したスタティック自動 NAT）	1184
宛先に応じて異なる変換（ダイナミック手動 PAT）	1189
宛先アドレスおよびポートに応じて異なる変換（ダイナミック手動 PAT）	1194
NAT およびサイト間 VPN	1199
NAT を使用した DNS クエリと応答の書き換え	1203
DNS64 応答修正	1205
DNS 応答修正：外部の DNS サーバ	1211
DNS 応答修正：ホスト ネットワーク上の DNS サーバ	1214

---

第 XIV 部：	7000 および 8000 シリーズの高度な導入オプション	1219
----------	-------------------------------	------

---

第 48 章	仮想スイッチのセットアップ	1221
	仮想スイッチ	1221
	スイッチドインターフェイスの設定	1222
	スイッチ型インターフェイスの設定メモ	1222
	物理スイッチドインターフェイスの設定	1223
	論理スイッチドインターフェイスの追加	1225
	論理スイッチドインターフェイスの削除	1226
	仮想スイッチの設定	1227
	仮想スイッチの設定に関する注意事項	1227
	仮想スイッチの追加	1228
	仮想スイッチの詳細設定	1229
	仮想スイッチの詳細設定の設定	1231
	仮想スイッチの削除	1232

---

第 49 章	仮想ルータのセットアップ	1233
	仮想ルータ	1233

ルーテッド インターフェイス	1234
物理ルーテッド インターフェイスの設定	1235
論理ルーテッド インターフェイスの追加	1238
論理ルーテッド インターフェイスの削除	1241
SFRP の設定	1242
仮想ルータ設定	1244
仮想ルータの追加	1245
DHCP リレー	1246
DHCPv4 リレーの設定	1247
DHCPv6 リレーの設定	1247
スタティック ルート	1248
静的ルート テーブルの表示	1249
スタティック ルートの追加	1250
ダイナミック ルーティング	1251
RIP コンフィギュレーション	1251
RIP 設定のインターフェイスの追加	1252
RIP の認証設定	1253
高度な RIP の設定	1254
RIP 設定へのインポート フィルタの追加	1255
RIP 設定へのエクスポート フィルタの追加	1256
OSPF の設定	1257
OSPF ルーティング エリア	1257
OSPF エリア インターフェイス	1259
OSPF エリア インターフェイスの追加	1261
OSPF エリア vlink の追加	1262
OSPF 設定へのインポート フィルタの追加	1264
OSPF 設定へのエクスポート フィルタの追加	1265
仮想ルータのフィルタ	1266
仮想ルータ フィルタの表示	1267
仮想ルータのフィルタの設定	1268
仮想ルータ認証プロファイルの追加	1269

仮想ルータ統計情報の表示 1270

仮想ルータの削除 1271

---

## 第 50 章

### 集約インターフェイスと LACP 1273

集約インターフェイスについて 1273

LAG 設定 1274

スイッチドインターフェイスの集約 1275

ルーテッドインターフェイスの集約 1275

論理集約インターフェイス 1276

ロードバランシングアルゴリズム 1277

リンクセレクションポリシー 1278

リンク集約制御プロトコル (LACP) 1279

LACP 1279

集約スイッチドインターフェイスの追加 1280

集約ルーテッドインターフェイスの追加 1283

論理集約インターフェイスの追加 1287

集約インターフェイス統計情報の表示 1288

集約インターフェイスの削除 1289

---

## 第 51 章

### ハイブリッドインターフェイス 1291

ハイブリッドインターフェイスについて 1291

論理ハイブリッドインターフェイス 1291

論理ハイブリッドインターフェイスの追加 1292

論理ハイブリッドインターフェイスの削除 1295

---

## 第 52 章

### ゲートウェイ VPN 1297

ゲートウェイ VPN の基本 1297

IPsec 1298

IKE 1298

VPN 展開 1299

ポイントツーポイントの VPN 展開 1299

スター VPN 導入	1299
メッシュ VPN 展開	1300
VPN 展開の管理	1301
VPN 展開オプション	1301
ポイントツーポイント VPN 展開オプション	1302
スター VPN の展開オプション	1304
メッシュ VPN 展開オプション	1305
VPN 展開の詳細オプション	1307
VPN 展開の管理	1308
ポイントツーポイント VPN 展開の設定	1309
スター VPN 展開の設定	1310
メッシュ VPN 展開の設定	1311
高度な VPN 展開を設定する方法	1312
VPN 展開の編集	1313
VPN 展開のステータス	1314
VPN ステータスの表示	1314
VPN の統計およびログ	1315
VPN 統計情報およびログの表示	1316
<hr/>	
第 XV 部 :	アクセス制御 1319
<hr/>	
第 53 章	アクセス コントロール ポリシーの開始 1321
アクセス制御の概要	1321
アクセス コントロール ポリシーのコンポーネント	1322
アクセス コントロール ポリシーのデフォルト アクション	1324
アクセス コントロール ポリシーの継承	1327
アクセス コントロール ポリシーの管理	1328
基本的なアクセス コントロール ポリシーの作成	1329
アクセス コントロール ポリシーの編集	1331
アクセス コントロール ポリシーの継承の管理	1333
基本アクセス コントロール ポリシーの選択	1334

基本ポリシーからのアクセス コントロール ポリシー設定の継承	1334
子孫アクセス コントロール ポリシーのロックの設定	1335
ドメインでのアクセス コントロール ポリシーの強制	1336
アクセス コントロール ポリシーのターゲット デバイスの設定	1337
アクセス コントロール ポリシーの詳細設定	1338
アクセス制御への他のポリシーの関連付け	1340

---

**第 54 章**
**アクセス コントロール ルール 1343**

アクセス コントロール ルールの概要	1343
アクセス コントロール ルールの管理	1345
アクセス コントロール ルールのコンポーネント	1346
アクセス コントロール ルールの順序	1348
アクセス制御ルール カテゴリの追加	1349
アクセス コントロール ルールの作成および編集	1350
アクセス コントロール ルールの有効化と無効化	1351
アクセス コントロール ルールの配置	1352
アクセス コントロール ルールのアクション	1353
アクセス コントロール ルールのモニタ アクション	1353
アクセス コントロール ルールの信頼アクション	1354
アクセス コントロール ルールのブロック アクション	1354
アクセス コントロール ルール インタラクティブ ブロック アクション	1355
アクセス コントロール ルールの許可アクション	1355
アクセス コントロール ルールのコメント	1356
アクセス制御ルールへのコメントの追加	1357

---

**第 55 章**
**侵入ポリシーとファイル ポリシーを使用したアクセス制御 1359**

ディープ インスペクションについて	1359
アクセス コントロール トラフィック処理	1360
ファイル インスペクションおよび侵入インスペクションの順序	1362
ファイル制御およびマルウェア保護のためのアクセス コントロール ルールの設定	1364
ファイル制御および AMP を実行するアクセス コントロール ルールの設定	1364

侵入防御のためのアクセス コントロール ルールの設定	1365
アクセス コントロール ルールの設定と侵入ポリシー	1366
侵入防御を実行するアクセス コントロール ルールの設定	1367

## 第 56 章

**HTTP 応答ページとインタラクティブ ブロッキング 1369**

HTTP 応答ページについて	1369
HTTP 応答ページの制限	1370
HTTP 応答ページの選択	1371
HTTP 応答ページでのインタラクティブ ブロッキング	1372
インタラクティブ ブロッキングの設定	1372
ブロックされた Web サイトのユーザ バイパス タイムアウトの設定	1373

## 第 57 章

**セキュリティ インテリジェンス ブラックリスト 1375**

セキュリティ インテリジェンスについて	1375
セキュリティ インテリジェンスの設定	1376
セキュリティ インテリジェンス戦略	1376
セキュリティ インテリジェンスの設定	1378
セキュリティ インテリジェンス オプション	1380

## 第 58 章

**DNS ポリシー 1383**

DNS ポリシーの概要	1383
DNS ポリシーのコンポーネント	1384
基本 DNS ポリシーの作成	1385
DNS ポリシーの編集	1386
DNS ポリシーの管理	1387
DNS ルール	1388
DNS ルールの作成および編集	1389
DNS ルールの管理	1389
DNS ルールの有効化と無効化	1390
DNS ルールの評価順序	1390
DNS ルールのアクション	1391



DNS ルールの条件	1393
DNS およびセキュリティゾーンに基づくトラフィックの制御	1393
DNS およびネットワークに基づくトラフィックの制御	1394
DNS および VLAN に基づくトラフィックの制御	1395
DNS リスト、フィード、またはカテゴリに基づくトラフィックの制御	1396
DNS ポリシーの展開	1397

---

**第 59 章**

<b>プレフィルタ処理とプレフィルタ ポリシー</b>	<b>1399</b>
プレフィルタの概要	1399
モデル制限のプレフィルタ	1400
プレフィルタリングとアクセス コントロール	1400
パススルー トンネルとアクセス制御	1403
プレフィルタ ポリシーについて	1404
プレフィルタリングの設定	1405
トンネルとプレフィルタのルール	1407
トンネルとプレフィルタ ルールのコンポーネント	1408
トンネルゾーンおよびプレフィルタリング	1410
トンネルゾーンの使用	1411
トンネルゾーンの作成	1414

---

**第 60 章**

<b>インテリジェント アプリケーション バイパス</b>	<b>1415</b>
IAB の概要	1415
IAB オプション	1416
IAB の設定	1418
IAB のロギングと分析	1420

---

**第 61 章**

<b>コンテンツ制限を使用したアクセス制御</b>	<b>1425</b>
コンテンツ制限について	1425
アクセス コントロールルールを使用したコンテンツ制限の実施	1427
アクセス制御ルールのセーフサーチ オプション	1429
アクセス制御ルールの YouTube EDU オプション	1429

DNS シンクホールを使用したコンテンツ制限の実施 1430

---

第 XVI 部 : 暗号化トラフィックの処理 1433

---

第 62 章 トラフィック復号の概要 1435

トラフィックの復号の概要 1435

SSL ハンドシェイク処理 1436

ClientHello メッセージ処理 1437

ServerHello とサーバ証明書メッセージの処理 1439

SSL インスペクションの要件 1441

SSL ルール設定の前提条件に関する情報 1441

SSL インスペクションアプライアンス導入シナリオ 1442

パッシブ展開でのトラフィックの復号 1443

パッシブ展開での暗号化トラフィック モニタリング 1444

パッシブ展開での復号されていない暗号化トラフィック 1445

パッシブ展開での暗号化トラフィックの秘密キーによる検査 1446

インライン展開でのトラフィックの復号 1447

インライン展開での暗号化トラフィック モニタリング 1449

インライン展開での復号されていない暗号化トラフィック 1450

インライン展開での暗号化トラフィックのブロック 1451

インライン展開での暗号化トラフィックの秘密キーによる検査 1451

インライン展開での暗号化トラフィックの再署名済み証明書による検査 1453

---

第 63 章 SSL ポリシーの使用を開始するには 1457

SSL ポリシーの概要 1457

SSL ポリシーのデフォルトアクション 1458

復号できないトラフィックのデフォルト処理オプション 1459

SSL ポリシーの管理 1460

基本 SSL ポリシーの作成 1462

復号できないトラフィックのデフォルト処理の設定 1463

SSL ポリシーの編集 1464

## 第 64 章

<b>SSL ルールの使用を開始するには</b>	<b>1467</b>
SSL ルールの概要	1467
SSL ルールのトラフィック処理	1467
暗号化トラフィック インспекションの設定	1469
SSL ルールのコンポーネント	1470
SSL ルールの作成および変更	1472
SSL ルールの順序の評価	1473
ルール カテゴリへの SSL ルールの追加	1473
番号による SSL ルールの配置	1474
SSL ルールの条件	1474
SSL ルールの条件タイプ	1475
SSL ルールのアクション	1477
SSL ルール：モニタ アクション	1477
SSL ルール：復号しないアクション	1478
SSL ルール：ブロッキング アクション	1478
SSL ルール：復号アクション	1479
SSL ルールの復号メカニズムとガイドライン	1479
SSL ルール アクションの設定	1482
復号 - 再署名アクションの設定	1483
復号 - 既知のキー アクションの設定	1483
SSL ルールの管理	1484
SSL ルール検索	1484
SSL ルールの検索	1484
SSL ルールの有効化と無効化	1485
SSL ルールの移動	1486
新しい SSL ルール カテゴリの追加	1486
SSL ルールのトラブルシューティング	1487

## 第 65 章

<b>SSL ルールを使用した復号の調整</b>	<b>1489</b>
SSL ルール条件の概要	1489

ネットワーク ベースの SSL ルールの条件	1490
ネットワーク ゾーン SSL ルールの条件	1490
ネットワーク ゾーンによる暗号化トラフィックの制御	1491
ネットワークまたは地理位置情報 SSL ルールの条件	1492
ネットワークまたは地理位置情報による暗号化トラフィックの制御	1493
VLAN SSL ルールの条件	1494
暗号化された VLAN トラフィックの制御	1495
ポート SSL ルールの条件	1496
ポートによる暗号化トラフィックの制御	1497
ユーザベースの SSL ルールの条件	1498
ユーザ ベースの暗号化トラフィックの制御	1498
レピュテーション ベースの SSL ルール条件	1499
SSL ルールの選択されたアプリケーションとフィルタ	1499
SSL ルールのアプリケーション フィルタ	1500
SSL ルールで使用可能なアプリケーション	1502
アプリケーション ベースの SSL ルール条件の要件	1503
SSL ルールへのアプリケーション条件の追加	1504
暗号化されたアプリケーションの制御に対する制限	1505
暗号化トラフィックでのレピュテーションベースの URL ブロッキング	1506
レピュテーションベースの URL ブロッキングの実行	1506
サーバ証明書ベースの SSL ルール条件	1508
証明書の識別名の SSL ルール条件	1509
証明書の識別名による暗号化トラフィックの制御	1510
証明書の SSL ルール条件	1511
証明書による暗号化トラフィックの制御	1512
証明書ステータスの SSL ルール条件	1513
外部認証局の信頼	1515
証明書ステータスでのトラフィックの照合	1516
暗号スイート SSL ルール条件	1518
暗号スイートによる暗号化トラフィックの制御	1521
暗号化プロトコルバージョンの SSL ルール条件	1522

暗号化プロトコルのバージョンによるトラフィックの制御 1522

第 XVII 部 : 高度なマルウェア防御 (AMP) とファイル制御 1525

第 66 章 ファイルポリシーと AMP for Firepower 1527

ファイルポリシーと AMP for Firepower について 1527

ファイル制御および Cisco AMP の基本 1528

AMP for Firepower 1528

マルウェアの性質 1530

AMP for Firepower を使用しないファイル制御 1532

エンドポイント向け AMP 1532

AMP for Firepower とエンドポイント向け AMP の比較 1533

ファイルポリシー 1535

ファイルポリシーの詳細設定 1536

ファイルポリシーの管理 1538

ファイルポリシーの作成 1539

ファイルポリシーの編集 1541

ファイルルール 1542

ファイルルールのコンポーネント 1543

ファイルルールアクションと評価順序 1544

ファイルポリシーの注意事項と制約事項 1546

ファイルルール設定に関する注意事項と制約事項 1546

ファイル検出に関する注意事項と制約事項 1546

ファイルブロックに関する注意事項と制約事項 1547

ファイルルールの作成 1548

クラウド接続 1549

AMP クラウド接続 1550

AMP for Endpoints クラウド接続の設定 1552

Cisco AMP プライベートクラウド 1553

AMP クラウドおよび AMPv 接続の管理 1556

動的分析接続 1557

デフォルトの動的分析接続の表示	1557
Threat Grid のオンプレミス アプライアンス	1557
オンプレミスの動的分析接続の設定	1558
集合型セキュリティ インテリジェンス通信の設定	1559
集合型セキュリティ インテリジェンスの通信設定オプション	1559
集合型セキュリティ インテリジェンスとの通信の設定	1561

## 第 67 章

## ファイルとマルウェアのインスペクションパフォーマンスとストレージの調整 1563

ファイルおよびマルウェアのインスペクションのパフォーマンスとストレージの調整について	1563
ファイルおよびマルウェアのインスペクション パフォーマンスとストレージのオプション	1564
ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整	1568

## 第 XVIII 部 :

## 侵入検知と防御 1569

## 第 68 章

## ネットワーク分析ポリシーと侵入ポリシーの概要 1571

ネットワーク分析ポリシーと侵入ポリシーの基本	1571
ポリシーが侵入についてトラフィックを検査する仕組み	1572
復号化、正規化、前処理：ネットワーク分析ポリシー	1573
アクセス コントロール ルール：侵入ポリシーの選択	1574
侵入インスペクション：侵入ポリシー、ルール、変数セット	1575
侵入イベントの生成	1577
システム提供およびカスタムのネットワーク分析ポリシーと侵入ポリシー	1578
システム提供のネットワーク分析ポリシーと侵入ポリシー	1579
カスタム ネットワーク分析とカスタム侵入ポリシーの利点	1581
カスタム ネットワーク分析ポリシーの利点	1581
カスタム侵入ポリシーの利点	1582
カスタム ポリシーの制限	1583
ナビゲーション ウィンドウ: ネットワーク分析と侵入ポリシー	1586
競合と変更：ネットワーク分析ポリシーと侵入ポリシー	1587

ネットワーク分析または侵入ポリシーの終了 1589

---

第 69 章

侵入ポリシーおよびネットワーク分析ポリシーのレイヤ 1591

レイヤの基本 1591

レイヤスタック 1591

基本レイヤ 1592

システム提供の基本ポリシー 1593

カスタム基本ポリシー 1593

基本ポリシーに対するルール更新の影響 1594

ベースポリシーの変更 1595

Firepower 推奨レイヤ 1596

レイヤ管理 1597

共有レイヤ 1598

レイヤの管理 1599

レイヤ間のナビゲーション 1600

レイヤでの侵入ルール 1601

レイヤでの侵入ルールの設定 1603

複数のレイヤからのルール設定の削除 1604

カスタム基本ポリシーからのルール変更の受け入れ 1605

レイヤでのプリプロセッサと詳細設定 1606

層のプリプロセッサと詳細の設定 1607

---

第 70 章

侵入ポリシーの使用を開始するには 1609

侵入ポリシーの基本 1609

侵入ポリシーの管理 1611

カスタム侵入ポリシーの作成 1612

カスタム侵入ポリシーの作成 1613

侵入ポリシーの編集 1613

侵入ポリシーの変更 1615

インライン展開でのドロップ動作 1615

インライン展開でのドロップ動作の設定 1616

侵入ポリシーの詳細設定	1616
侵入検知および防御のパフォーマンスの最適化	1618

## 第 71 章

<b>ルールを使用した侵入ポリシーの調整</b>	<b>1619</b>
侵入ルールの調整の基本	1619
侵入ルールのタイプ	1620
侵入ポリシー内の侵入ルールの表示	1621
[侵入ルール (Intrusion Rules) ] ページの列	1621
侵入ルールの詳細	1623
侵入ルール詳細の表示	1623
侵入ルールのしきい値の設定	1624
侵入ルールの抑制の設定	1625
[ルール詳細 (Rule Details) ] ページからの動的ルール状態の設定	1626
侵入ルールの SNMP アラートの設定	1627
侵入ルールへのコメントの追加	1628
侵入ポリシー内の侵入ルール フィルタ	1628
侵入ルール フィルタの注意事項	1629
侵入ポリシールール フィルタ構築のガイドライン	1629
侵入ルール構成フィルタ	1634
侵入ルール コンテンツ フィルタ	1634
侵入ルール カテゴリ	1636
侵入ルールのフィルタ コンポーネント	1636
侵入ルール フィルタの使用	1637
侵入ポリシー内のルール フィルタの設定	1638
侵入ルールの状態	1639
侵入ルールの状態オプション	1639
侵入ルール状態の設定	1640
侵入ポリシーの侵入イベント通知のフィルタ	1641
侵入イベントのしきい値	1641
侵入イベントしきい値の設定	1641
侵入イベントのしきい値の変更と追加	1644



侵入イベントしきい値の表示と削除	1645
侵入ポリシーの抑制の設定	1646
侵入ポリシー抑制タイプ	1646
特定のルール of 侵入イベントの抑制	1647
抑制条件の表示と削除	1648
動的侵入ルール状態	1649
ダイナミックな侵入ルール状態の設定	1650
[ルール (Rule) ] ページからの動的ルール状態の設定	1651
侵入ルールのコメントの追加	1653

---

**第 72 章**

<b>ネットワーク資産に応じた侵入防御の調整</b>	<b>1655</b>
Firepower 推奨ルールについて	1655
Firepower 推奨のデフォルト設定	1656
Firepower 推奨の詳細設定	1657
Firepower の推奨事項の生成と適用	1658

---

**第 73 章**

<b>機密データの検出</b>	<b>1661</b>
機密データ検出の基本	1661
グローバル センシティブ データ検出オプション	1663
個別のセンシティブ データ タイプのオプション	1664
システム提供のセンシティブ データのタイプ	1665
センシティブ データ検出の設定	1666
監視対象のアプリケーション プロトコルおよび機密データ	1668
モニタ対象のアプリケーション プロトコルの選択	1669
特別なケース : FTP トラフィックでのセンシティブ データの検出	1670
カスタム 機密データ タイプ	1671
カスタム機密データ タイプのデータ パターン	1671
カスタム センシティブ データ タイプの設定	1674
カスタムセンシティブ データ タイプの編集	1675

---

**第 74 章**

<b>侵入イベント ロギングのグローバル制限</b>	<b>1677</b>
----------------------------	-------------

グローバル ルールのしきい値の基本	1677
グローバル ルールしきい値オプション	1678
グローバルなしきい値の設定	1681
グローバルしきい値の無効化	1682

## 第 75 章

**侵入ルール エディタ 1685**

侵入ルールの編集について	1685
ルールの詳細	1686
侵入ルール ヘッダー	1687
侵入ルール ヘッダー アクション	1688
侵入ルール ヘッダー プロトコル	1688
侵入ルール ヘッダーの方向	1689
侵入ルール ヘッダーの送信元と宛先の IP アドレス	1689
侵入ルール ヘッダーの送信元および宛先ポート	1693
侵入イベント詳細	1695
カスタム分類の追加	1699
イベント優先順位の定義	1699
イベント参照の定義	1700
カスタム ルールの作成	1701
新規ルールの作成	1702
既存のルールの変更	1703
侵入ルールへのコメントの追加	1704
カスタム ルールの削除	1705
ルールの検索	1706
侵入ルールの検索条件	1707
侵入ルール エディタ ページでのルールのフィルタリング	1708
フィルタリング ガイドライン	1708
キーワードフィルタリング	1709
文字列フィルタリング	1710
キーワードと文字列の組み合わせによるフィルタリング	1711
フィルタリング ルール	1711

侵入ルールのキーワードと引数	1712
content キーワードと protected_content キーワード	1712
基本コンテンツおよび protected_content キーワードの引数	1714
コンテンツ (content) および保護コンテンツ (protected_content) キーワード検索位置	1716
概要 : HTTP content および protected_content キーワードの引数	1719
概要 : content キーワードによる高速パターン マッチ機能	1723
replace キーワード	1727
byte_jump キーワード	1728
byte_test キーワード	1731
byte_extract キーワード	1733
byte_math キーワード	1736
概要 : pcre キーワード	1739
PCRE の構文	1740
PCRE 修飾子のオプション	1742
PCRE のキーワード値の例	1745
metadata キーワード	1747
サービス メタデータ	1749
メタデータ検索のガイドライン	1754
IP ヘッダー値	1755
ICMP ヘッダー値	1758
TCP ヘッダー値とストリーム サイズ	1760
stream_reassembly キーワード	1764
SSL キーワード	1765
appid キーワード	1767
アプリケーション層プロトコル値	1768
RPC キーワード	1768
ASN.1 キーワード	1768
urilen キーワード	1770
DCE/RPC キーワード	1771
SIP キーワード	1775

GTP キーワード	1777
SCADA キーワード	1790
Modbus キーワード	1790
DNP3 キーワード	1791
パケット特性	1794
アクティブ応答のキーワード	1796
resp キーワード	1797
react キーワード	1798
config response コマンド	1799
detection_filter キーワード	1800
tag キーワード	1801
flowbits キーワード	1803
flowbits キーワードのオプション	1803
flowbits キーワードの使用に関するガイドライン	1805
flowbits キーワードの例	1805
http_encode キーワード	1810
http_encode キーワードの構文	1811
http_encode キーワードの例：2つの http_encode キーワードを使用した2つのエンコーディングの検索	1812
概要：file_type および file_group キーワード	1812
file_type キーワードと file_group キーワード	1813
file_data キーワード	1814
pkt_data キーワード	1815
base64_decode キーワードと base64_data キーワード	1815

## 第 76 章

侵入防御パフォーマンスの調整	1819
侵入防御のパフォーマンス チューニングについて	1819
侵入に対するパターン一致の制限	1820
正規表現による侵入ルールのオーバーライドの制限	1821
侵入ルールの正規表現制限のオーバーライド	1822
パケットごとの侵入イベント生成の制限	1823

パケットごとに生成される侵入イベントの制限	1824
パケットおよび侵入ルールの遅延しきい値構成	1825
パケット遅延しきい値構成	1825
パケット遅延しきい値構成の注意事項	1826
パケット遅延しきい値の設定	1827
ルール遅延しきい値構成	1828
ルール遅延しきい値構成の注記	1830
ルール遅延しきい値の設定	1831
侵入パフォーマンス統計情報のロギング設定	1832
侵入パフォーマンス統計情報のロギングの設定	1833

---

第 XIX 部 :           **高度なネットワーク分析と前処理**   1835

---

第 77 章	<b>ネットワーク分析/侵入ポリシーのための高度なアクセス制御の設定</b>	1837
	ネットワーク分析および侵入ポリシーのアクセスコントロールの詳細設定について	1837
	デフォルトの侵入ポリシー	1837
	デフォルトの侵入ポリシーの設定	1839
	ネットワーク分析プロファイルの詳細設定	1840
	デフォルトのネットワーク分析ポリシーの設定	1841
	ネットワーク分析ルール	1842
	ネットワーク分析ルールの設定	1842
	ネットワーク分析ルールの管理	1844

---

第 78 章	<b>ネットワーク分析ポリシーの使用を開始するには</b>	1845
	ネットワーク分析ポリシーの基本	1845
	ネットワーク分析ポリシーの管理	1846
	カスタム ネットワーク分析ポリシーの作成	1847
	カスタム ネットワーク分析ポリシーの作成	1847
	ネットワーク分析ポリシーの管理	1848
	ネットワーク分析ポリシーの設定とキャッシュされた変更	1849
	ネットワーク分析ポリシーの編集	1850

- ネットワーク分析ポリシーでのプリプロセッサの設定 1851
- インライン導入でのプリプロセッサによるトラフィックの変更 1852
- ネットワーク分析ポリシーの注記におけるプリプロセッサの設定 1853

## 第 79 章

## アプリケーション層プリプロセッサ 1855

- アプリケーション層のプリプロセッサの概要 1855
- DCE/RPC プリプロセッサ 1856
  - コネクションレス型およびコネクション型 DCE/RPC トラフィック 1856
  - DCE/RPC ターゲットベース ポリシー 1858
    - RPC over HTTP トランスポート 1858
  - DCE/RPC グローバル オプション 1859
  - DCE/RPC ターゲットベース ポリシー オプション 1861
  - トラフィックに関連する DCE/RPC ルール 1867
  - DCE/RPC プリプロセッサの設定 1867
- DNS プリプロセッサ 1869
  - DNS プリプロセッサ オプション 1871
  - DNS プリプロセッサの設定 1872
- FTP/Telnet デコーダ 1874
  - グローバル FTP および Telnet オプション 1874
  - Telnet オプション 1874
  - サーバレベルの FTP オプション 1875
    - FTP コマンドの検証ステートメント 1878
  - クライアントレベルの FTP オプション 1880
  - FTP/Telnet デコーダの設定 1881
- HTTP Inspect プリプロセッサ 1883
  - グローバル HTTP 正規化オプション 1884
  - サーバレベルの HTTP 正規化オプション 1885
    - サーバレベルの HTTP 正規化エンコード オプション 1895
  - HTTP 検査プリプロセッサの設定 1899
  - その他の HTTP 検査プリプロセッサ ルール 1901
- Sun RPC プリプロセッサ 1902

Sun RPC プリプロセッサのオプション	1902
Sun RPC プリプロセッサの設定	1903
SIP プリプロセッサ	1904
SIP プリプロセッサのオプション	1905
SIP プリプロセッサの設定	1907
その他の SIP プリプロセッサ ルール	1908
GTP プリプロセッサ	1910
GTP プリプロセッサ ルール	1910
GTP プリプロセッサの設定	1911
IMAP プリプロセッサ	1912
IMAP プリプロセッサ オプション	1912
IMAP プリプロセッサの設定	1914
その他の IMAP プリプロセッサ ルール	1915
POP プリプロセッサ	1916
POP プリプロセッサ オプション	1916
POP プリプロセッサの設定	1918
その他の POP プリプロセッサ ルール	1919
SMTP プリプロセッサ	1920
SMTP プリプロセッサのオプション	1920
SMTP デコードの設定	1926
SSH プリプロセッサ	1927
SSH プリプロセッサのオプション	1928
SSH プリプロセッサの設定	1931
SSL プリプロセッサ	1932
SSL 前処理の仕組み	1932
SSL プリプロセッサのオプション	1934
SSL プリプロセッサの設定	1935
SSL プリプロセッサ ルール	1936
第 80 章	SCADA プリプロセッサ 1939
	SCADA プリプロセッサの概要 1939

Modbus プリプロセッサ	1939
Modbus プリプロセッサ ポート オプション	1940
Modbus プリプロセッサの設定	1940
Modbus プリプロセッサ ルール	1941
DNP3 プリプロセッサ	1942
DNP3 プリプロセッサ オプション	1942
DNP3 プリプロセッサの設定	1942
DNP3 プリプロセッサ ルール	1944
<hr/>	
第 81 章	トランスポート層およびネットワーク層プリプロセッサ 1945
トランスポート層およびネットワーク層のプリプロセッサの概要	1945
トランスポート/ネットワーク プリプロセッサの詳細設定	1946
無視される VLAN ヘッダー	1946
侵入廃棄ルールでのアクティブ応答	1946
トランスポート/ネットワーク プリプロセッサの詳細オプション	1947
トランスポート/ネットワーク プリプロセッサの詳細設定の構成	1948
チェックサム検証	1949
チェックサム検証オプション	1950
チェックサムの確認	1950
インライン正規化プリプロセッサ	1951
インライン正規化オプション	1952
インライン正規化の設定	1958
IP 最適化プリプロセッサ	1960
IP フラグメンテーション エクスプロイト	1960
ターゲット ベースの最適化ポリシー	1961
IP 最適化オプション	1961
IP 最適化の設定	1964
パケット デコーダ	1966
パケット デコーダ オプション	1966
パケット復号化の設定	1970
TCP ストリームの前処理	1971



状態に関連する TCP エクスプロイト	1971
ターゲット ベースの TCP ポリシー	1972
TCP ストリームの再構成	1973
TCP ストリームのプリプロセス オプション	1974
TCP ストリームの前処理の設定	1983
UDP ストリームの前処理	1985
UDP ストリームのプリプロセス オプション	1985
UDP ストリームの前処理の設定	1986

---

## 第 82 章

### 特定の脅威の検出 1989

特定の脅威の検出の概要	1989
Back Orifice の検出	1989
Back Orifice 検出プリプロセッサ	1989
Back Orifice の検出	1990
ポートスキャン検出	1991
ポートスキャンタイプ、プロトコル、フィルタリング感度レベル	1991
ポートスキャン イベント生成	1994
ポートスキャン イベント パケット ビュー	1996
ポートスキャン検出の設定	1998
レート ベースの攻撃防御	2000
レート ベースの攻撃防御の例	2001
detection_filter キーワードの例	2002
ダイナミック ルール状態のしきい値構成または抑制の例	2003
ポリシー全体のレート ベース検出としきい値構成または抑制の例	2004
複数のフィルタリング方法によるレート ベース検出の例	2005
レート ベースの攻撃防御オプションと設定	2007
レートベースの攻撃防御、検出フィルタリング、しきい値処理または抑制	2008
レートベース攻撃防止の設定	2009

---

## 第 83 章

### 適応型プロファイル 2013

アダプティブプロファイルについて	2013
------------------	------

アダプティブプロファイルの更新	2014
アダプティブプロファイルの更新および Firepower 推奨ルール	2014
適応型プロファイルのオプション	2015
適応型プロファイルの設定	2016

---

第 XX 部 :           **検出とアイデンティティ**   2019

---

第 84 章	<b>ネットワーク検出とアイデンティティの概要</b>	2021
	ホスト、アプリケーション、ユーザの検出	2021
	ホスト、アプリケーション、およびユーザ検出とアイデンティティ データの使用	2022
	ホストおよびアプリケーション検出の基礎	2023
	オペレーティング システムおよびホスト データのパッシブ検出	2023
	オペレーティング システムおよびホスト データのアクティブ検出	2023
	アプリケーションおよびオペレーティング システムの現在の ID	2024
	現在のユーザ ID	2025
	アプリケーションおよびオペレーティング システムの ID の競合	2026
	Firepower システムの NetFlow データ	2027
	NetFlow データを使用するための要件	2027
	NetFlow データと管理対象デバイス データの違い	2028
	ユーザ アイデンティティについて	2031
	アイデンティティの用語	2031
	アイデンティティ導入	2032
	ユーザ アクティビティ データベース	2033
	ユーザ データベース	2034
	Firepower システムのホストとユーザの制限	2035
	Firepower システムのホスト制限	2035
	Firepower システムのユーザの制限	2036

---

第 85 章           **ホスト ID ソース**   2039

概要：ホストのデータ収集	2039
システムが検出できるホスト オペレーティング システムの判別	2040

ホスト オペレーティング システムの識別	2040
カスタムフィンガープリント	2041
フィンガープリントの管理	2042
フィンガープリントのアクティブおよび非アクティブの設定	2043
アクティブなフィンガープリントの編集	2044
非アクティブなフィンガープリントの編集	2045
クライアント用のカスタム フィンガープリントの作成	2046
サーバ用のカスタム フィンガープリントの作成	2049
ホスト入力データ	2052
サードパーティのデータを使用するための要件	2053
サードパーティ製品のマッピング	2054
サードパーティの製品のマッピング	2054
サードパーティ製品の修正のマッピング	2056
サードパーティの脆弱性のマッピング	2057
カスタム製品マッピング	2058
カスタム製品マッピングの作成	2059
カスタム製品マッピング リストの編集	2060
カスタム製品マッピングのアクティブおよび非アクティブの設定	2061
eStreamer サーバストリーミング	2061
eStreamer イベントタイプの選択	2062
eStreamer クライアント通信の設定	2063
ホスト入力クライアントの設定	2064
Nmap スキャン	2065
Nmap 修復オプション	2066
Nmap スキャンのガイドライン	2076
例：Nmap を使用した不明なオペレーティング システムの解決	2078
例：Nmap を使用した新しいホストへの応答	2080
Nmap スキャンの管理	2081
Nmap スキャン インスタンスの追加	2082
Nmap スキャン インスタンスの編集	2084
Nmap スキャン ターゲットの追加	2085

Nmap スキャン ターゲットの編集	2086
Nmap 修復の作成	2087
Nmap 修復の編集	2090
オンデマンド Nmap スキャンの実行	2091
Nmap スキャンの結果	2092
Nmap スキャン結果の表示	2092
Nmap スキャン結果のフィールド	2094
Nmap スキャン結果のインポート	2095

## 第 86 章

## アプリケーションの検出 2097

概要：アプリケーション検出	2097
アプリケーションディテクタの基本	2098
Web インターフェイスでのアプリケーションプロトコルの識別	2100
クライアント検出からの暗黙的アプリケーションプロトコル検出	2101
ホスト制限と検出イベント ロギング	2102
アプリケーション検出に関する特殊な考慮事項	2102
カスタム アプリケーションディテクタ	2104
カスタム アプリケーションディテクタおよびユーザ定義アプリケーション フィールド	2104
カスタム アプリケーションディテクタの設定	2108
ユーザ定義のアプリケーションの作成	2109
基本ディテクタでの検出パターンの指定	2111
高度なディテクタでの検出条件の指定	2112
カスタム アプリケーションプロトコルディテクタのテスト	2113
ディテクタ詳細の表示またはダウンロード	2114
ディテクタ リストのソート	2115
検出機能リストのフィルタリング	2115
ディテクタ リストのフィルタ グループ	2116
別のディテクタ ページへの移動	2117
ディテクタのアクティブおよび非アクティブの設定	2118
カスタム アプリケーションディテクタの編集	2119

ディテクタの削除 2120

---

第 87 章

**ユーザアイデンティティソース 2121**

ユーザアイデンティティソースについて 2121

ユーザエージェントのアイデンティティソース 2123

ユーザエージェントのガイドライン 2123

ユーザ制御のためのユーザエージェントの設定 2124

ユーザエージェントアイデンティティソースのトラブルシューティング 2125

ISE アイデンティティソース 2126

ISE ガイドライン 2126

ユーザ制御用 ISE の設定 2128

ISE 設定フィールド 2129

ISE アイデンティティソースのトラブルシューティング 2130

ターミナルサービス (TS) エージェントのアイデンティティソース 2131

TS エージェントのガイドライン 2131

TS エージェントのユーザ制御の構成 2132

TS エージェントアイデンティティソースのトラブルシューティング 2132

キャプティブポータルのアイデンティティソース 2133

キャプティブポータルのガイドライン 2133

ユーザ制御のためのキャプティブポータルの設定 2135

キャプティブポータルフィールド 2139

キャプティブポータルからのアプリケーションの除外 2140

キャプティブポータルのアイデンティティソースのトラブルシューティング 2142

トラフィックベース検出のアイデンティティソース 2143

---

第 88 章

**ネットワーク検出ポリシー 2147**

概要：ネットワーク検出ポリシー 2147

ネットワーク検出のカスタマイズ 2148

ネットワーク検出ポリシーの設定 2149

ネットワーク検出ルール 2150

ネットワーク検出ルールの設定 2151

アクションと検出されるアセット	2152
モニタ対象ネットワーク	2153
ポート除外	2156
ネットワーク検出ルールのゾーン	2158
トラフィック ベース検出のアイデンティティ ソース	2159
高度なネットワーク検出オプションの設定	2162
ネットワーク検出の一般設定	2163
ネットワーク検出全般設定	2164
ネットワーク検出アイデンティティ競合の設定	2164
ネットワーク検出アイデンティティ競合の解決の設定	2165
ネットワーク検出の脆弱性の影響の評価オプション	2166
ネットワーク検出の脆弱性影響評価の有効化	2167
侵害の兆候	2167
侵害の兆候ルールの有効化	2168
NetFlow エクスポートのネットワーク検出ポリシーへの追加	2169
ネットワーク検出のデータ ストレージ設定	2170
ネットワーク検出データ ストレージの設定	2172
ネットワーク検出イベント ログिंगの設定	2172
ネットワーク検出 OS およびサーバアイデンティティ ソースの追加	2173
ネットワーク検出戦略のトラブルシューティング	2174

## 第 89 章

レルムとアイデンティティ ポリシー	2177
レルムとアイデンティティ ポリシーについて	2177
レルムについて	2177
レルムおよび信頼できるドメイン	2179
レルムがサポートされているサーバ	2179
サポートされるサーバフィールド名	2181
レルムとユーザのダウンロードのトラブルシューティング	2182
アイデンティティ ポリシーについて	2184
レルムの作成	2185
レルム フィールド	2186

レルム ディレクトリの設定	2189
ユーザとグループのダウンロード	2190
アイデンティティ ポリシーの作成	2192
アイデンティティ ルールの作成	2193
アイデンティティ ルール フィールド	2194
レルムの管理	2197
レルムの比較	2198
アイデンティティ ポリシーの管理	2199
アイデンティティ ルールの管理	2199

---

第 XXI 部 :           **関連とコンプライアンス**   2201

---

第 90 章	<b>コンプライアンス ホワイトリスト</b>	2203
	コンプライアンス ホワイトリストの概要	2203
	コンプライアンス ホワイトリストのターゲット ネットワーク	2205
	コンプライアンス ホワイト リストのホスト プロファイル	2206
	オペレーティング システム固有のホスト プロファイル	2206
	共有ホスト プロファイル	2207
	ホワイト リスト違反のトリガー	2208
	コンプライアンス ホワイト リストの作成	2209
	コンプライアンス ホワイト リストのターゲット ネットワークの設定	2211
	ホワイト リストホスト プロファイルの作成	2213
	アプリケーションプロトコルのホワイトリスト	2214
	クライアントのホワイトリスト	2215
	Web アプリケーションのホワイトリスト	2216
	プロトコルのホワイトリスト	2217
	コンプライアンス ホワイト リストの管理	2218
	コンプライアンス ホワイトリストの編集	2219
	共有ホスト プロファイルの管理	2220

---

第 91 章           **関連ポリシー**   2223

<b>関連ポリシーとルールの概要</b>	<b>2223</b>
<b>関連ポリシーの設定</b>	<b>2225</b>
ルールとホワイトリストに応答を追加する	2226
<b>関連ポリシーの管理</b>	<b>2226</b>
<b>関連ルールの設定</b>	<b>2227</b>
侵入イベント トリガー条件の構文	2230
マルウェア イベント トリガー条件の構文	2232
ディスカバリ イベント トリガー条件の構文	2234
ユーザ アクティビティのイベント トリガー条件の構文	2238
ホスト入力イベント トリガー条件の構文	2239
接続イベント トリガー条件の構文	2240
トラフィック プロファイル変化の構文	2244
<b>関連ホスト プロファイル限定の構文</b>	<b>2247</b>
ユーザ限定の構文	2250
<b>接続トラッカー</b>	<b>2251</b>
接続トラッカーの追加	2252
接続トラッカーの構文	2253
接続トラッカー イベントの構文	2256
外部ホストからの過剰な接続の設定例	2257
BitTorrent の過剰なデータ転送の設定例	2259
スヌーズ期間および非アクティブ期間	2261
<b>関連ルールの作成メカニズム</b>	<b>2262</b>
<b>関連ルールへの条件の追加とリンク設定</b>	<b>2263</b>
<b>関連ルール条件での複数の値の使用</b>	<b>2264</b>
<b>関連ルールの管理</b>	<b>2265</b>
<b>関連応答グループの設定</b>	<b>2266</b>
<b>関連応答グループの管理</b>	<b>2267</b>

<b>トラフィック プロファイル</b>	<b>2269</b>
トラフィック プロファイルの概要	2269
トラフィック プロファイル条件	2271



トラフィック プロファイルの管理	2273
トラフィック プロファイルの設定	2275
トラフィック プロファイル条件の追加	2276
トラフィック プロファイルへのホスト プロファイル認定の追加	2277
トラフィック プロファイル条件の構文	2278
トラフィック プロファイルのホスト プロファイル限定の構文	2279
トラフィック プロファイル条件での複数の値の使用	2282

---

 第 93 章

**修復 2285**

修復の概要	2285
Cisco ISE EPS 修復	2286
ISE EPS 修復の設定	2287
Cisco IOS Null ルート修復	2289
Cisco IOS ルータ用修復の設定	2290
Nmap スキャン修復	2296
セット属性値修復	2296
セット属性修復の設定	2296
修復モジュールの管理	2299
修復インスタンスの管理	2300
1 つの修復モジュールのインスタンスの管理	2301

---

 第 XXII 部 :

**レポートとアラート 2303**


---

 第 94 章

**レポートの操作 2305**

レポートの概要	2305
リスク レポート	2305
リスク レポートの生成、表示および印刷	2306
標準レポートの概要	2307
レポートの設計について	2307
レポート テンプレート	2307
レポート テンプレート フィールド	2308

レポートテンプレートの作成	2310
レポートテンプレートの設定	2315
レポートテンプレートの管理	2330
レポートの生成について	2332
レポートの生成	2332
レポートの生成オプション	2334
レポートの生成時の電子メール配布	2335
将来のレポートのスケジュール	2335
生成されたレポートの操作について	2336
レポートの表示	2336
レポートのダウンロード	2337
リモートでのレポートの保存	2337
リモートストレージへのレポートの移動	2338
レポートの削除	2339

---

**第 95 章**

<b>アラート応答による外部アラート</b>	<b>2341</b>
Firepower Management Center アラート応答	2341
アラート応答のサポート設定	2342
SNMP アラート応答の作成	2342
Syslog アラート応答の作成	2344
Syslog アラート ファシリティ	2345
syslog 重大度レベル	2346
電子メール アラート応答の作成	2347
影響フラグ アラートの設定	2348
検出イベント アラートの設定	2348
AMP for Firepower アラートの設定	2349

---

**第 96 章**

<b>侵入イベントに関する外部アラート</b>	<b>2351</b>
侵入イベントの外部アラートについて	2351
侵入イベントの SNMP アラートの設定	2352
侵入 SNMP アラートのオプション	2352

侵入イベントの Syslog アラートの設定	2354
侵入 syslog アラートのファシリティとプライオリティ	2355
侵入イベントに対する電子メールアラートの設定	2356
侵入電子メールアラートのオプション	2357

---

第 XXIII 部 : イベントとアセットの分析ツール 2359

---

第 97 章 コンテキスト エクスプローラの使用 2361

コンテキスト エクスプローラについて	2361
ダッシュボードと Context Explorer の違い	2362
[時系列のトラフィックおよび侵入イベント数 (Traffic and Intrusion Event Counts Time) ] グラフ	2363
[侵害の兆候 (Indications of Compromise) ] セクション	2364
[兆候別ホスト (Hosts by Indication) ] グラフ	2364
[ホスト別兆候 (Indications by Host) ] グラフ	2364
[ネットワーク情報 (Network Information) ] セクション	2364
[オペレーティング システム (Operating Systems) ] グラフ	2364
[送信元 IP 別トラフィック (Traffic by Source IP) ] グラフ	2365
[送信元ユーザ別トラフィック (Traffic by Source User) ] グラフ	2365
[アクセス コントロールアクション別の接続 (Connections by Access Control Action) ] グラフ	2366
[宛先 IP 別トラフィック (Traffic by Destination IP) ] グラフ	2366
[入力/出力のセキュリティゾーン別トラフィック (Traffic by Ingress/Egress Security Zone) ] グラフ	2366
[アプリケーション情報 (Information) ] セクション	2367
[アプリケーション情報 (Application Information) ] セクションへのフォーカスの移動	2367
[リスク/ビジネスとの関連性とアプリケーション別トラフィック (Traffic by Risk/Business Relevance and Application) ] グラフ	2368
[リスク/ビジネスとの関連度別侵入イベントおよびアプリケーション (Intrusion Events by Risk/Business Relevance and Application) ] グラフ	2369

[リスク/ビジネスとの関連度別ホストおよびアプリケーション (Hosts by Risk/Business Relevance and Application) ] グラフ	2369
アプリケーション詳細リスト	2370
[セキュリティ インテリジェンス (Security Intelligence) ] セクション	2370
[カテゴリ別セキュリティ インテリジェンス トラフィック (Security Intelligence Traffic by Category) ] グラフ	2370
[送信元 IP 別セキュリティ インテリジェンス トラフィック (Security Intelligence Traffic by Source IP) ] グラフ	2371
[宛先 IP 別セキュリティ インテリジェンス トラフィック (Security Intelligence Traffic by Destination IP) ] グラフ	2371
[侵入情報 (Intrusion Information) ] セクション	2371
[影響別侵入イベント (Intrusion Events by Impact) ] グラフ	2372
[上位の攻撃者 (Top Attackers) ] グラフ	2372
[上位のユーザ (Top Users) ] グラフ	2372
[優先度別侵入イベント (Intrusion Events by Priority) ] グラフ	2372
[上位のターゲット (Top Targets) ] グラフ	2372
[入力/出力の上位セキュリティ ゾーン (Top Ingress/Egress Security Zones) ] グラフ	2373
侵入イベント詳細リスト	2373
[ファイル情報 (Files Information) ] セクション	2373
[上位のファイルタイプ (Top File Types) ] グラフ	2374
[上位のファイル名 (Top File Names) ] グラフ	2374
[性質別ファイル (Files by Disposition) ] グラフ	2374
[送信ファイル数上位のホスト (Top Hosts Receiving Files) ] グラフ	2374
[受信ファイル数上位のホスト (Top Hosts Receiving Files) ] グラフ	2375
[上位のマルウェア検出 (Top Malware Detections) ] グラフ	2375
[地理位置情報 (Geolocation Information) ] セクション	2376
[イニシエータ/レスポндаの国別接続 (Connections by Initiator/Responder Country) ] グラフの表示	2376
[送信元/宛先国別侵入イベント (Intrusion Events by Source/Destination Country) ] グラフ	2376
[送信側/受信側の国別ファイル イベント (File Events by Sending/Receiving Country) ] グラフ	2377

[URL 情報 (URL Information) ] セクション	2377
[URL 別トラフィック (Traffic by URL) ] グラフ	2377
[URL カテゴリ別トラフィック (Traffic by URL Category) ] グラフ	2378
[URL レピュテーション別トラフィック (Traffic by URL Reputation) ] グラフ	2378
Context Explorer の更新	2379
Context Explorer の時間範囲の設定	2379
Context Explorer のセクションの最小化および最大化	2380
Context Explorer データのドリルダウン	2381
コンテキスト エクスプローラのフィルタ	2382
データ タイプ フィールド オプション	2383
[フィルタの追加 (Add Filter) ] ウィンドウからのフィルタの作成	2386
コンテキスト メニューからのクイック フィルタの作成	2387
フィルタ処理されたコンテキスト エクスプローラ ビューの保存	2388
フィルタ データの表示	2389
フィルタの削除	2389
<hr/>	
第 98 章	ネットワーク マップの使用 2391
	ネットワーク マップ 2391
	ホストのネットワーク マップ 2392
	ネットワーク デバイスのネットワーク マップ 2393
	モバイル デバイスのネットワーク マップ 2394
	侵害の兆候のネットワーク マップ 2394
	アプリケーションプロトコルのネットワーク マップ 2395
	[脆弱性 (Vulnerabilities) ] のネットワーク マップ 2396
	ホスト属性のネットワーク マップ 2397
	ネットワーク マップの表示 2398
	カスタム ネットワーク トポロジ 2399
	カスタム トポロジの作成 2399
	ネットワーク検出ポリシーからのネットワークのインポート 2400
	手動によるカスタム トポロジへのネットワークの追加 2401
	カスタム トポロジのアクティブおよび非アクティブの設定 2402

カスタム トポロジの編集 2402

---

第 99 章

**インシデント 2405**

インシデント対応について 2405

インシデントの定義 2405

共通のインシデント対応プロセス 2406

Firepower システムのインシデントタイプ 2409

カスタム インシデントタイプの作成 2409

インシデントの作成 2410

インシデントの編集 2411

インシデント レポートの生成 2412

---

第 100 章

**ルックアップの使用 2413**

ルックアップの概要 2413

Whois ルックアップの実行 2413

IP アドレスの地理位置情報の検出 2414

---

第 XXIV 部 :

**ワークフロー (Workflows) 2415**

---

第 101 章

**ワークフロー 2417**

概要 : ワークフロー 2417

定義済みワークフロー 2418

定義済み侵入イベントのワークフロー 2418

定義済みマルウェアのワークフロー 2420

定義済みファイルのワークフロー 2420

定義済みキャプチャ ファイルのワークフロー 2421

定義済み接続データのワークフロー 2421

定義済みセキュリティ インテリジェンスのワークフロー 2423

定義済みホストのワークフロー 2423

定義済み侵害の兆候のワークフロー 2424

定義済みアプリケーション ワークフロー 2424

定義済みアプリケーション詳細ワークフロー	2425
定義済みサーバのワークフロー	2426
定義済みホスト属性のワークフロー	2426
定義済み検出イベントのワークフロー	2426
定義済みユーザ ワークフロー	2427
定義済み脆弱性のワークフロー	2427
定義済みのサードパーティ脆弱性のワークフロー	2427
定義済み関連ワークフロー、ホワイトリスト ワークフロー	2428
定義済みのシステムのワークフロー	2428
カスタム テーブル ワークフロー	2429
ワークフローの使用	2429
ユーザ ロールによるワークフローへのアクセス	2432
ワークフローの選択	2432
ワークフローのページ	2434
ワークフロー ページのナビゲーション ツール	2436
ワークフロー ページのトラバーサル ツール	2436
ファイル トラジェクトリ アイコン	2436
ホスト プロファイルのアイコン	2437
脅威スコア アイコン	2437
ワークフロー ツールバー	2438
ドリルダウン ページの使用	2439
テーブル ビュー ページの使用	2440
位置情報 (GeoLocation)	2440
地理情報の詳細情報	2441
接続イベント グラフ	2442
接続イベント グラフの使用方法	2443
イベント時間の制約	2451
イベントの時間枠のカスタマイズ	2452
イベントのデフォルト時間枠	2456
時間枠の進行	2459
イベント ビューの制約	2460

イベントの制約	2461
複合イベント ビューの制約	2462
複合イベント ビュー制約の使用	2462
ワークフロー間のナビゲーション	2463
ブックマーク	2464
ブックマークの作成	2465
ブックマークの表示	2465

---

**第 102 章****イベントの検索 2467**

イベントの検索	2467
検索の制約	2468
一般的な検索の制約	2468
検索で使用するワイルドカードと記号	2469
検索でのオブジェクトとアプリケーションのフィルタ	2469
検索で指定する時間制約	2470
検索での IP アドレス	2470
検索での管理対象デバイス	2471
検索でのポート	2472
検索のイベント フィールド	2472
検索の実行	2473
検索設定の保存	2474
保存済み検索設定のロード	2475
シェルによるクエリのオーバーライド	2476
シェルベースのクエリ管理の構文	2476
実行時間が長いクエリの停止	2477

---

**第 103 章****カスタム ワークフロー 2479**

カスタム ワークフローの概要	2479
保存済みカスタム ワークフロー	2480
カスタム ワークフローの作成	2481
非接続データに基づくカスタム ワークフローの作成	2482



カスタム接続データ ワークフローの作成	2483
カスタム ワークフローの使用と管理	2485
事前定義されたテーブルに基づいたカスタム ワークフローの表示	2485
カスタム テーブルに基づいたカスタム ワークフローの表示	2486
カスタム ワークフローの編集	2486

---

**第 104 章**
**カスタム テーブル 2489**

カスタム テーブルの概要	2489
定義済みのカスタム テーブル	2489
可能なテーブルの組み合わせ	2490
ユーザ定義のカスタム テーブル	2494
カスタム テーブルの作成	2495
カスタム テーブルの変更	2496
カスタム テーブルの削除	2497
カスタム テーブルに基づいたワークフローの表示	2498
カスタム テーブルの検索	2498

---

**第 XXV 部 :**
**イベントとアセット 2501**


---

**第 105 章**
**接続ロギング 2503**

接続ロギングについて	2503
接続ロギング ストラテジー	2504
設定可能な接続ロギング	2504
自動接続ロギング	2506
接続開始のロギングと終了のロギングの比較	2506
Firepower Management Center と外部ロギング	2508
アクションと接続ロギング	2509
FastPath された接続のロギング	2509
モニタされた監視接続のロギング	2509
信頼されている接続のロギング	2510
ブロックされた接続のロギング	2510

許可された接続のロギング	2512
トンネルルールおよびプレフィルタールールによる接続のロギング	2513
SSLルールによる復号可能接続のロギング	2514
セキュリティインテリジェンスによる接続のロギング	2515
アクセス制御ルールによる接続のロギング	2516
ポリシーのデフォルトアクションによる接続のロギング	2517
長いURLのロギングの制限	2518

## 第 106 章

**接続イベントとセキュリティインテリジェンス イベント 2521**

接続イベントについて	2521
接続イベントとセキュリティインテリジェンス イベントの比較	2521
NetFlow 接続	2522
接続の概要 (グラフ用集約データ)	2522
長時間接続	2523
外部応答側からの統合接続サマリ	2523
接続およびセキュリティインテリジェンス イベント フィールド	2523
接続イベントの理由	2537
接続イベント フィールドの入力の要件	2539
接続イベント フィールドで利用可能な情報	2541
接続およびセキュリティインテリジェンス イベント テーブルの使用	2548
接続で検出されたファイルとマルウェアの表示	2550
接続に関連付けられた侵入イベントの表示	2552
暗号化接続の証明書の詳細	2552
デバイス サマリー ページの表示	2553

## 第 107 章

**侵入イベントの操作 2555**

侵入イベントについて	2555
侵入イベントの表示	2556
侵入イベント フィールド	2557
侵入イベント影響レベル	2567
侵入イベントと関連付けられた接続データの表示	2570

侵入イベントを確認済みとしてマーク	2570
以前に確認された侵入イベントの表示	2571
侵入イベントへの未確認としてマーク	2572
プロプロセッサ イベント	2572
ブリプロセッサのジェネレータ ID	2573
侵入イベントのワークフロー ページ	2576
侵入イベント ワークフローの使用	2577
侵入イベント ドリルダウン ページの制約	2579
侵入イベント テーブル ビューの制約	2580
侵入イベント パケット ビューの使用	2581
イベント情報のフィールド	2583
フレーム情報のフィールド	2591
データリンク層情報フィールド	2592
ネットワーク層情報の表示	2593
トランスポート層情報の表示	2596
パケット バイト情報の表示	2599
侵入イベントのクリップボード	2599
クリップボードのレポートの生成	2599
クリップボードからのイベントの削除	2600
侵入イベントの統計情報の表示	2601
ホスト統計情報	2602
イベントの概要	2602
イベント統計	2603
侵入イベントのパフォーマンス グラフの表示	2604
侵入イベントのパフォーマンス統計情報グラフの種類	2604
侵入イベント グラフの表示	2610

## 第 108 章

## ファイル/マルウェア イベントとネットワーク ファイル トラジェクトリ 2613

ファイル イベント/マルウェア イベントとネットワーク ファイル トラジェクトリについて  
2613

ファイルおよびマルウェア イベント 2614

ファイル イベントおよびマルウェア イベントの種類	2614
ファイル イベント	2614
ネットワーク ベースのマルウェア イベント (AMP for Firepower)	2615
遡及的マルウェア イベント (AMP for Firepower)	2615
エンドポイントベースのマルウェア イベント (AMP for Endpoints)	2616
ファイルおよびマルウェア イベントのワークフローの使用	2616
ファイルおよびマルウェア イベント フィールド	2617
マルウェア イベントのサブタイプ	2626
ファイルおよびマルウェア イベント フィールドで利用可能な情報	2628
ローカル マルウェア分析 (Local Malware Analysis)	2632
ファイル構成	2633
動的分析 (Dynamic Analysis)	2633
自動ダイナミック分析と Spero 分析	2634
手動によるダイナミック分析	2634
動的分析とキャパシティ処理	2635
脅威スコアと動的分析のサマリ レポート	2635
ファイル分析評価	2636
キャプチャ ファイルとファイル ストレージ	2639
マルウェア ストレージ パック	2640
保存されているファイルのダウンロード	2641
キャプチャされたファイル ワークフローの使用	2641
キャプチャされたファイルのフィールド	2642
ネットワーク ファイル トラジェクトリ	2648
最近検出されたマルウェアおよび分析済みトラジェクトリ	2648
ネットワーク ファイル トラジェクトリの詳細ビュー	2648
ネットワーク ファイル トラジェクトリのサマリー情報	2649
ネットワーク ファイル トラジェクトリ マップと関連イベント リスト	2651
ネットワーク ファイル トラジェクトリの使用	2653
第 109 章	
<b>ホスト プロファイルの使用</b>	<b>2655</b>
ホスト プロファイル	2655



ホストプロファイルの脆弱性	2684
脆弱性に対するパッチのダウンロード	2685
個々のホストに対する脆弱性の非アクティブ化	2685
個々の脆弱性の非アクティブ化	2686
ホストプロファイルのスキャン結果	2687
ホストプロファイルからのホストのスキャン	2688

## 第 110 章

<b>ディスカバリ イベントの操作</b>	<b>2689</b>
検出イベントの検出データとアイデンティティ データ	2689
ディスカバリ イベントの統計情報の表示	2690
[統計情報サマリ (Statistics Summary) ]セクション	2691
[イベント分類 (Event Breakdown) ]セクション	2693
[プロトコル分類 (Protocol Breakdown) ]セクション	2693
[アプリケーションプロトコル分類 (Application Protocol Breakdown) ]セクション	2693
[OS 分類 (OS Breakdown) ]セクション	2693
ディスカバリ パフォーマンス グラフの表示	2694
ディスカバリ パフォーマンス グラフ タイプ	2694
ディスカバリおよびアイデンティティ ワークフローの使用	2695
検出イベントおよびホスト入力イベント	2697
ディスカバリ イベント タイプ	2698
ホスト入力イベント タイプ	2703
ディスカバリ イベントとホスト入力イベントの表示	2705
ディスカバリ イベントのフィールド	2706
ホスト データ	2707
ホスト データの表示	2707
ホスト データ フィールド	2708
選択したホストのトラフィック プロファイルの作成	2713
選択したホストに基づいたコンプライアンスのホワイト リストの作成	2714
ホスト属性データ	2714
ホスト属性の表示	2715
ホスト属性データ フィールド	2716

選択したホストのホスト属性の設定	2717
侵害の兆候データ	2717
侵害の兆候データの表示	2719
侵害の兆候データ フィールド	2720
単一ホストにおける侵害の兆候のルール状態の編集	2721
侵害の兆候のタグのソース イベントの表示	2721
侵害の兆候タグの解決	2722
サーバデータ	2722
サーバデータの表示	2723
サーバデータ フィールド	2724
アプリケーションデータとアプリケーション詳細データ	2727
アプリケーションデータの表示	2727
アプリケーションデータ フィールド	2728
アプリケーション詳細データの表示	2730
アプリケーションの詳細データ フィールド	2731
脆弱性データ	2732
脆弱性データのフィールド	2733
脆弱性の非アクティブ化	2735
脆弱性データの表示	2736
脆弱性の詳細の表示	2737
複数の脆弱性の非アクティブ化	2738
サードパーティの脆弱性データ	2738
サードパーティの脆弱性データの表示	2739
サードパーティの脆弱性データのフィールド	2740
ユーザおよびユーザ アクティビティ データ	2741
ユーザ関連フィールド	2741
ユーザ データ (User Data)	2746
ユーザ アクティビティ データ	2749
ユーザ プロファイルとホスト履歴	2752





通信ポートの要件	2787
Firepower システムの機能と運用のためのデフォルト通信ポート	2788

## 付録 B :

## 従来型デバイスのコマンドラインリファレンス 2793

CLI について	2793
CLI モード	2794
CLI アクセス レベル	2794
基本的な CLI コマンド	2795
configure password	2795
終了	2795
exit	2796
ヘルプ	2796
history	2796
ログアウト	2797
? (疑問符)	2797
?? (二重の疑問符)	2798
show コマンド	2798
access-control-config	2798
alarms	2799
arp-tables	2799
audit-log	2800
audit_cert	2800
bypass	2801
High-availability コマンド	2801
config	2801
high-availability ha-statistics	2802
cpu	2802
Database コマンド	2803
processes	2803
slow-query-log	2804
device-settings	2804
disk	2804
disk-manager	2805

dns	2805
expert	2806
fan-status	2806
fastpath-rules	2806
gui	2807
hostname	2807
hosts	2807
hyperthreading	2808
inline-sets	2808
interfaces	2809
ifconfig	2809
lcd	2810
Link-aggregation コマンド	2810
設定 :	2810
統計情報	2811
link-state	2811
log-ips-connection	2811
managers	2812
memory	2812
model	2813
mpls-depth	2813
NAT コマンド	2813
active-dynamic	2814
active-static	2814
allocators	2814
config	2814
dynamic-rules	2815
flows	2815
static-rules	2815
netstat	2816
network	2816
network-modules	2816
network-static-routes	2817
ntp	2817

perfstats	2818
portstats	2818
power-supply-status	2818
process-tree	2819
processes	2819
ルート	2820
routing-table	2820
serial-number	2821
ssl-policy-config	2821
stacking	2821
summary	2822
syslog	2822
時刻	2823
traffic-statistics	2823
user	2824
ユーザ	2825
version	2826
virtual-routers	2826
virtual-switches	2827
vmware-tools	2827
VPN コマンド	2828
config	2828
config by virtual router	2828
status	2828
status by virtual router	2829
counters	2829
counters by virtual router	2829
コンフィギュレーション コマンド	2830
audit_cert コマンド	2830
削除	2830
import	2830
bypass	2831
high-availability	2831

gui	2832
lcd	2832
log-ips-connections	2833
manager コマンド	2833
追加	2833
削除	2834
mpls-depth	2834
network コマンド	2835
dns searchdomains	2835
dns servers	2835
hostname	2835
http-proxy	2836
http-proxy-disable	2836
ipv4 delete	2836
ipv4 dhcp	2837
ipv4 manual	2837
ipv6 delete	2838
ipv6 dhcp	2838
ipv6 manual	2839
ipv6 router	2839
management-interface disable	2840
management-interface disable-event-channel	2840
management-interface disable-management-channel	2840
management-interface enable	2841
management-interface enable-event-channel	2842
management-interface enable-management-channel	2842
management-interface tcpport	2843
management-port	2843
static-routes ipv4 add	2843
static-routes ipv4 delete	2844
static-routes ipv6 add	2844
static-routes ipv6 delete	2844
password	2845
スタッキングの無効化	2845

user コマンド	2846
アクセス	2846
追加	2847
aging	2847
削除	2847
disable	2848
enable	2848
forcereset	2848
maxfailedlogins	2848
password	2849
strengthcheck	2849
unlock	2849
vmware-tools	2850
system コマンド	2851
アクセス制御コマンド	2851
archive	2851
clear-rule-counts	2851
rollback	2851
コンプライアンス コマンド	2852
enable cc	2852
enable ucapl	2852
show	2853
disable-http-user-cert	2853
file コマンド	2854
copy	2854
削除	2854
list	2854
secure-copy	2855
generate-troubleshoot	2855
ldapsearch	2856
lockdown-sensor	2856
nat rollback	2857
reboot	2857

- restart **2857**
- support コマンド **2858**
  - ssl-client-hello-display **2858**
  - ssl-client-hello-enabled **2858**
  - ssl-client-hello-force-reset **2861**
  - ssl-client-hello-reset **2861**
  - ssl-client-hello-tuning **2861**
- shutdown **2863**



# 第 1 章

## Firepower の概要

Cisco Firepower は、専用プラットフォームで展開されるか、ソフトウェアソリューションとして展開される、ネットワークセキュリティおよびトラフィック管理製品の統合スイートです。このシステムは、組織のセキュリティポリシー（ネットワークを保護するためのガイドライン）に準拠する方法でネットワークトラフィックを処理できるように設計されています。

標準的な展開では、ネットワークセグメントにインストールされた複数のトラフィック検知管理対象デバイスが分析対象のトラフィックをモニタし、マネージャにレポートします。

- Firepower Management Center
- Firepower Device Manager
- Adaptive Security Device Manager (ASDM)

マネージャでは、集中管理コンソールのグラフィカルユーザインターフェイスを使用して管理、分析、およびレポートタスクを実行できます。

このガイドでは、*Firepower Management Center* 管理アプライアンスについて説明します。ASDM を介して管理される Firepower Device Manager または ASA with FirePOWER Services については、これらの管理手法のガイドを参照してください。

- *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*
- *ASA with FirePOWER Services Local Management Configuration Guide*
- [管理対象デバイスの概要 \(1 ページ\)](#)
- [Firepower Management Center の概要 \(4 ページ\)](#)
- [Firepower システムのコンポーネント \(6 ページ\)](#)
- [Firepower のオンラインヘルプとドキュメンテーション \(13 ページ\)](#)
- [Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## 管理対象デバイスの概要

ネットワークセグメントにインストールされている管理対象デバイスは、分析のためにトラフィックを監視します。パッシブな展開の場合、管理対象デバイスは、ホスト、オペレーティングシステム、アプリケーション、ユーザ、送信されたファイル（マルウェアを含む）、脆弱

性など、組織の資産に関する詳細情報を収集します。Firepower システムがこの情報を分析用に関連付けることで、ユーザがアクセスする Web サイトと使用するアプリケーションをモニタし、トラフィック パターンを評価して、侵入や他の攻撃の通知を受信できます。

インラインで展開されたシステムは、アクセスコントロールを使用してトラフィックのフローに影響を与えることができ、これによって、ネットワークを出入りしたり通過したりするトラフィックを処理する方法を詳細に指定できます。ネットワークトラフィックについて収集したデータおよびそのデータから収集したすべての情報は、次に基づいてそのトラフィックのフィルタ処理や制御ができます。

- シンプルで容易に決定されるトランスポート層およびネットワーク層の特性（送信元と宛先、ポート、プロトコルなど）
- レピュテーション、リスク、ビジネスとの関連性、使用されたアプリケーション、または訪問した URL などの特性を含む、トラフィックに関する最新のコンテキスト情報
- 組織の Microsoft Active Directory および LDAP ユーザ（ユーザごとに異なるアクセス レベルを付与できます）
- 暗号化されたトラフィックの特性（このトラフィックを復号してさらに分析することもできます）
- 暗号化されていないトラフィックまたは復号化されたトラフィックに、禁止されているファイル、検出されたマルウェア、または侵入イベントが存在するかどうか



(注) システムでトラフィックに影響を与えるには、ルーテッド、スイッチド、またはトランスペアレント インターフェイスあるいはインライン インターフェイス ペアを使用して、関連する設定を管理対象デバイスに展開する必要があります。

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。たとえば、レピュテーションベースのブラックリストはシンプルな送信元と宛先のデータを使用しているため、禁止されているトラフィックを初期の段階でブロックできます。これに対し、侵入およびエクスプロイトの検知とブロックは最終防衛ラインです。

7000 および 8000 シリーズデバイスでネットワーク管理機能を使用すると、スイッチドおよびルーテッド環境での対応、ネットワーク アドレス変換 (NAT) の実行が可能になります。また、設定した仮想ルータ間でセキュアなバーチャルプライベート ネットワーク (VPN) トンネルを構築できます。バイパス インターフェイス、集約インターフェイス、8000 シリーズ 高速パスルール、厳密な TCP の適用を設定することもできます。

## 7000 および 8000 シリーズ 管理対象デバイス

Cisco Firepower 7000 および 8000 シリーズ アプライアンスは、Firepower システム用に作られた物理デバイスです。7000 および 8000 シリーズ デバイスのスループットはさまざまですが、多数の同じ機能を共有します。一般に、8000 シリーズ デバイスは 7000 シリーズ よりも高性能



で、8000 シリーズ 高速パス ルール、リンク集約、およびスタックなどの追加機能もサポートします。

## NGIPSv

NGIPSv (ESXi ホストとしての 64 ビット仮想デバイス) は、VMware vSphere Hypervisor または VMware vCloud Director 環境を使用して展開できます。サポート対象のすべての ESXi バージョンで VMware ツールを有効化できます。

既定では、NGIPSv は e1000 (1 ギガビット/秒) インターフェイスを使用します。また、VMware vSphere クライアントを使用して、既定のセンシングおよび管理インターフェイスを、vmxnet3 (10 ギガビット/秒) インターフェイスで置き換えることもできます。

ライセンスに関係なく、NGIPSv では、システムのハードウェアベースの機能 (冗長性、リソース共有、スイッチング、ルーティングなど) のいずれもサポートされません。

## Cisco ASA with FirePOWER Services

Cisco ASA with FirePOWER Services (または *ASA FirePOWER* モジュール) には、NGIPSv に類似した機能があります。ASA FirePOWER 展開においては、ASA デバイスにより第 1 回線システム ポリシーが提供され、トラフィックが Firepower システムに渡されて、検出とアクセス制御が実行されます。

インストールされ適用されているライセンスに関係なく、ASA FirePOWER は次の Firepower システム機能をサポートしません。

- ASA FirePOWER は、Firepower システムの 7000 および 8000 シリーズハードウェアベースの機能 (デバイス高可用性、スタッキング、スイッチング、ルーティング、VPN、NAT など) をサポートしません。ただし、これらの機能は ASA プラットフォームによって提供され、ASA CLI および ASDM を使用して設定できます。詳細については、ASA のマニュアルを参照してください。
- Firepower Management Center の Web インターフェイスを使用して ASA FirePOWER のインターフェイスを設定することはできません。Firepower Management Center では、ASA FirePOWER が SPAN ポート モードで展開されている場合、ASA インターフェイスを表示しません。
- Firepower Management Center を使用して ASA FirePOWER のシャットダウン、再起動、その他の管理を行うことはできません。

ASA FirePOWER には ASA プラットフォームに固有のソフトウェアとコマンドラインインターフェイス (CLI) があります。ASA 専用のこれらのツールを使用して、システムのインストールおよびプラットフォーム固有のその他の管理タスクを実行します。



- (注) ASA FirePOWER を編集して、マルチ コンテキスト モードからシングル コンテキスト モード (またはその逆) に切り替えると、デバイスはそのインターフェイスの名前をすべて変更します。ASA FirePOWER の更新されたインターフェイス名を使用するように、すべての Firepower System セキュリティ ゾーン、関連ルール、関連する設定を再設定する必要があります。

## Firepower Threat Defense

Firepower Threat Defense アプライアンスは、統合された次世代ファイアウォールと次世代の IPS デバイスを提供します。Firepower ソフトウェアのモデルで使用可能な IPS 機能に加えて、ファイアウォールおよびプラットフォーム機能には、サイト間 VPN、堅牢なルーティング、NAT、クラスタリング (Firepower 9300 の場合)、およびアプリケーションインスペクションとアクセス制御におけるその他の最適化が含まれています。

Firepower Threat Defense ソフトウェアは、次のプラットフォームでサポートされます。

- Firepower 9300
- Firepower 4100 シリーズ
- ASA 5512-X から 5555-X まで
- ASA 5508-X および 5516-X
- ASA 5506-X シリーズ

## Firepower Threat Defense Virtual

Firepower Threat Defense Virtual (64 ビット仮想アプライアンス) は、仮想化環境に対して、統一された次世代ファイアウォールおよび次世代 IPS 機能を提供します。Firepower Threat Defense Virtual は、複数のハイパーバイザー環境で動作するように設計されており、管理作業のオーバーヘッドを削減し、操作効率を向上させます。

Firepower Threat Defense Virtual は、VMware vSphere ハイパーバイザーや KVM (カーネルベースの仮想マシン) ハイパーバイザー環境を使用して展開できます。また Firepower Threat Defense Virtual は、Amazon Web Services (AWS) クラウドプラットフォームによって展開することもできます。

仮想アプライアンスと物理 Firepower Threat Defense アプライアンスについての、包括的なマルチ デバイスの展開と管理のため、Firepower Management Center を使用することができます。

## Firepower Management Center の概要

Firepower Management Center は、Firepower システム展開の一元的な管理コンソールとデータベースリポジトリを提供するフォールトトレラントな専用ネットワークアプライアンスです。また、VMware vSphere と KVM (カーネルベースの仮想マシン) ハイパーバイザー環境を使用し

て、また Amazon Web Services (AWS) クラウドプラットフォームを使用して、64 ビットの仮想 Firepower Management Center を展開することもできます。Firepower Management Center は、さまざまなデバイス管理、イベント保存、ホスト モニタリング、およびユーザ モニタリング機能を備えています。どの Firepower Management Center でも、任意の種類の Firepower システム デバイスを管理することができます。

Firepower Management Center は、ネットワークトラフィック情報とパフォーマンスデータを集約して相互に関連付け、特定のホストに対するイベントの影響を評価します。デバイスから報告される情報を監視することができ、ネットワーク上で発生する活動全体を制御できます。Firepower Management Center は、デバイスのネットワーク管理機能（スイッチング、ルーティング、NAT、VPN など）も制御します。

Firepower Management Center の主な機能は次のとおりです。

- デバイス、ライセンス、およびポリシー管理
- 表、グラフ、図に表示されるイベント情報と状況情報
- 状態とパフォーマンスのモニタリング
- 外部通知およびアラート
- リアルタイムに脅威に対処するための関連付け、侵害の痕跡、および修復機能
- カスタムおよびテンプレート ベースのレポート

## Firepower Management Center の機能

このバージョンを実行している場合、すべての Firepower Management Center には同様の機能がありますが、容量と速度が主な違いとなります。Firepower Management Center のモデルによって、管理できるデバイス数、保存できるイベント数、およびモニタできるホスト数とユーザ数が異なります。

Firepower Management Center Web インターフェイスで利用可能な機能の構成は、管理しているデバイスのライセンスやモデルによって制限されていることがあります。

MC4000 では、シスコのユニファイドコンピューティングシステム (UCS) プラットフォームが Firepower システムに導入されます。MC4000 は、ベースボード管理コントローラ (BMC) 上で UCS Manager や Cisco Integrated Management Controller (CIMC) などのツールを使用するシスコの機能をサポートしないことに注意してください。

### 関連トピック

[デバイス管理](#) (525 ページ)

[データベース イベント数の制限の設定](#) (929 ページ)

# Firepower システムのコンポーネント

以下のトピックでは、組織のセキュリティ、適用可能な使用ポリシー、およびトラフィック管理の戦略に対して有用な Firepower システムの主な機能について説明します。



**ヒント** Firepower システムの多くの機能はアプライアンス モデル、ライセンス、およびユーザ ロールによって異なります。このドキュメントには、それぞれの機能用に Firepower システムのどのライセンスとデバイスが必要か、各手順を完了するための権限を持っているのはどのユーザ ロールかについての情報が含まれています。

## 冗長性およびリソース共有

Firepower システムの冗長性とリソース共有機能を使用すれば、運用継続性を保証し、複数の 7000 および 8000 シリーズ デバイスの処理リソースを統合することができます。

### デバイススタッキング

デバイスのスタッキングでは、1つのスタック構成内で2～4個のデバイスを接続することにより、ネットワーク セグメントで検査されるトラフィックの量を増やすことができます。スタック構成を確立するときに、各スタック構成デバイスのリソースを1つの共有構成に統合します。

### 7000 および 8000 シリーズ デバイスのハイ アベイラビリティ

7000 および 8000 シリーズ デバイス ハイ アベイラビリティを使用すれば、複数の 7000 または 8000 シリーズ デバイスまたはスタック間のネットワーク機能と設定データの冗長性を構築することができます。2つ以上のピア デバイスまたはスタックをハイ アベイラビリティ ペアとして構成すると、ポリシーの適用、システムの更新、および登録について1つの論理システムが生成されます。デバイスのハイ アベイラビリティにより、システムは手動または自動でフェールオーバーを実現することが可能です。

ほとんどの場合、SFRPを使用することによって、ハイ アベイラビリティ ペアを構成することなくレイヤ3の冗長性を実現できます。SFRPでは、指定したIPアドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。ネットワークの冗長性では、2つ以上のデバイスまたはスタックが同じネットワーク接続を提供し、ネットワーク上の他のホストに対する接続性を保証するよう設定することができます。

## 7000 & 8000 シリーズ デバイスのためのネットワーク トラフィック管理

Firepower システムのネットワーク トラフィック管理機能を使用すれば、7000 および 8000 シリーズ デバイスを組織のネットワーク インフラストラクチャの一部として機能させることができます。ユーザは、スイッチド、ルーテッド、または（この両者を組み合わせた）ハイブリッドの環境内で機能するよう 7000 および 8000 シリーズのデバイスを設定し、ネットワーク

アドレス変換 (NAT) を実行することができます。また、安全な仮想プライベートネットワーク (VPN) トンネルを構築することができます。

### スイッチング (Switching)

複数のネットワーク セグメントの間でパケットのスイッチングが可能になるように、レイヤ 2 の展開で Firepower システムを設定することができます。レイヤ 2 の展開では、スタンドアロンのブロードキャストドメインとして動作するよう、7000 および 8000 シリーズ デバイス上でスイッチド インターフェイス および 仮想スイッチを設定します。仮想スイッチは、ホストの MAC アドレスを使用してパケットの送信先を決定します。複数の物理 インターフェイスを単一の論理リンクにグループ化することで、ネットワークの 2 つのエンドポイント間でパケットスイッチングが可能になります。エンドポイントは、2 台の 7000 および 8000 シリーズ デバイス、またはサードパーティ アクセス スイッチに接続している 1 台の管理対象デバイスである場合があります。

### ルーティング

複数のインターフェイス間でトラフィックをルーティングするように、レイヤ 3 の展開で、Firepower システムを設定できます。レイヤ 3 配置では、トラフィックを受信および転送するため、7000 および 8000 シリーズ デバイスでルーテッド インターフェイスと仮想ルータを設定します。システムは宛先 IP アドレスに従ってパケット転送を決定し、パケットをルーティングします。ルータは転送基準に基づいて発信インターフェイスから宛先を取得し、アクセス コントロール ルールは、適用するセキュリティ ポリシーを指定します。

仮想ルータを設定するときに、スタティック (静的) ルートを定義できます。また、Routing Information Protocol (RIP) および Open Shortest Path First (OSPF) のダイナミック ルーティング プロトコルを設定できます。さらに、スタティック ルートと RIP、またはスタティック ルートと OSPF の組み合わせを設定することもできます。ユーザは、設定するそれぞれの仮想ルータに対して DHCP リレーを設定できます。

展開で仮想スイッチと仮想ルータの両方を使用する場合は、それらの 2 つの間でトラフィックをブリッジするように関連付けられているハイブリッド インターフェイスを設定できます。これらのユーティリティはトラフィックを分析し、そのタイプと適切な応答 (ルート、スイッチ、またはそれ以外) を判断します。複数の物理 インターフェイスを単一の論理リンクにグループ化することで、ネットワークの 2 つのエンドポイント間でトラフィックがルーティングされます。エンドポイントは、2 台の 7000 および 8000 シリーズ デバイス、またはサードパーティ ルータに接続している 1 台の管理対象デバイスである場合があります。

### NAT

レイヤ 3 の展開で、7000 および 8000 シリーズ デバイスを使用してネットワーク アドレス変換 (NAT) を設定できます。内部サーバを外部ネットワークに公開することも、内部ホストまたはサーバを外部アプリケーションに接続できるようにすることも可能です。また、IP アドレスのブロックを使用するか、IP アドレスおよびポート変換の制限付きのブロックを使用することにより、外部ネットワークからプライベート ネットワーク アドレスを隠すよう、NAT を設定することもできます。

## VPN

バーチャルプライベートネットワーク（VPN）は、インターネットや他のネットワークなどのパブリックソースを介したエンドポイント間でセキュアなトンネルを確立するネットワーク接続です。7000 および 8000 シリーズ デバイスの仮想ルータ間で安全な VPN トンネルを構築するよう、Firepower システムを設定することができます。

## マルチテナント機能

ドメイン機能では、管理対象デバイス、設定、イベントへのユーザアクセスをセグメント化することによって、Firepower システム展開内にマルチテナンシーを実装できます。

ユーザ ロールによる制限に加えて、現在のドメイン レベルによって設定の変更が制限される場合もあります。システムソフトウェアアップデートなどのほとんどの管理タスクは、グローバルドメインに制限されます。

## 検出とアイデンティティ

Cisco の検出およびアイデンティティ テクノロジーは、ネットワークの全体像を提供するためにホスト、オペレーティングシステム、アプリケーション、ユーザ、ファイル、ネットワーク、位置情報、および脆弱性に関する情報を収集します。

- ネットワーク検出ポリシーは、ネットワーク上のトラフィックを監視し、ホスト、アプリケーション、および権限のないユーザのデータを収集します。
- アイデンティティポリシーは、権限のあるユーザのデータを収集するため、ネットワーク上のユーザを、レムおよび認証方式と関連付けます。

LDAP または AD サーバへの接続を確立し、ユーザデータのダウンロードを実行するため、アイデンティティポリシーと共にレムを構成します。

特定のタイプの検出およびアイデンティティ データを使用すると、ネットワーク アセットの包括的なマップを作成し、フォレンジック分析、動作プロファイリング、アクセス制御を行い、組織が影響を受ける脆弱性およびエクスプロイトに対応して軽減することができます。

また、Firepower Management Center の Web インターフェイスを使用して、収集されたデータを表示および分析することもできます。

## アクセス制御

アクセスコントロールはポリシーベースの機能で、ユーザはこれを使用してネットワークを横断できるトラフィックを指定、検査、および記録できます。アクセス コントロール ポリシーは、システムがネットワーク上のトラフィックを処理する方法を決定します。

最も単純なアクセス コントロール ポリシーでは、デフォルト アクションを使用してすべてのトラフィックを処理するターゲットデバイスを指定します。追加のインスペクションなしですべてのトラフィックをブロックまたは信頼するか、または侵入および検出データがないかトラフィックを検査するようにこのデフォルト アクションを設定できます。

より複雑なアクセスコントロールポリシーは、IP、URL、およびDNSのセキュリティインテリジェンスデータに基づいてトラフィックをブラックリスト登録することができます。さらに、アクセスコントロールルールを使用して、ネットワークトラフィックのロギングおよび処理を細かく制御することができます。これらのルールは単純にすることも複雑にすることもでき、複数の基準を使用してトラフィックを照会および検査します。セキュリティゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求されたURL、およびユーザ別にトラフィックを制御できます。アクセスコントロールの詳細オプションには、復号化、前処理、およびパフォーマンスが含まれます。

各アクセスコントロールルールにはアクションも含まれており、一致するトラフィックをモニタ、信頼、ブロック、または許可するかどうかを決定します。トラフィックを許可するときには、システムが侵入ポリシーまたはファイルポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

## SSL インスペクション

SSLインスペクション（検査）はポリシーベースの機能です。暗号化されたトラフィックを復号化せずに処理したり、暗号化されたトラフィックを復号化して詳細なアクセス制御検査を行ったりすることができます。トラフィックの復号化や詳細な分析を行わずに信頼できない暗号化トラフィックの送信元をブロックすることも、暗号化されたトラフィックを復号化する代わりにアクセス制御を使用して検査することもできます。

暗号化トラフィックをさらに調査するために、システムにアップロードされた公開キー証明書とペア化された秘密キーを使用して、ネットワークを通過する暗号化トラフィックを復号化し、非暗号化の場合と同じ方法で復号化トラフィックをアクセス制御によって検査できます。システムで、復号されたトラフィックのポスト分析をブロックしない場合、トラフィックを再暗号化してから宛先ホストに渡します。システムは、暗号化された接続を処理する際にその詳細をログに記録できます。

## 侵入検知と防御

侵入検知および侵入防御は、トラフィックが宛先に許可される前のシステムの最後の防御ラインです。侵入ポリシーは、アクセスコントロールポリシーによって呼び出される侵入検知および侵入防御の設定の定義済みセットです。侵入ルールおよびその他の設定を使用して、これらのポリシーはセキュリティ違反がないかトラフィックを検査し、インライン展開では、悪意のあるトラフィックをブロックまたは変更できます。

Firepower システムには複数の侵入ポリシーが付属しています。システム付属のポリシーを使用することで、Cisco Talos Security Intelligence and Research Group (Talos) の経験を活用できます。これらのポリシーに対して、Talos は侵入およびプリプロセッサルールの状態（有効または無効）を設定し、他の詳細設定の初期設定も行います。ルールを有効にすると、ルールに一致するトラフィックに対して侵入イベントが生成されます（さらに、必要に応じてトラフィックがブロックされます）。

システムが提供するポリシーが組織のセキュリティのニーズに十分に対応していない場合は、カスタムポリシーを作成することで、環境内のシステムのパフォーマンスを向上させ、ネット

ワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。設定できるカスタムポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

## Cisco Advanced Malware Protection およびファイル制御

マルウェアの影響を特定して軽減しやすくするため、Firepower システムのファイル制御、ネットワーク ファイルトラジェクトリ、および Advanced Malware Protection (AMP) の各コンポーネントによって、ネットワーク トラフィック内のファイル（マルウェア ファイルとアーカイブファイル内にネストされたファイルを含む）の伝送を検出、追跡、キャプチャ、分析、および必要に応じてブロックできます。

### ファイル制御

ファイル制御により、管理対象デバイスは、ユーザが特定のアプリケーションプロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出およびブロックすることができます。ファイル制御は、全体的なアクセスコントロール設定の一部として設定します。アクセス コントロール ルールに関連付けられたファイル ポリシーによって、ルールの条件を満たすネットワーク トラフィックが検査されます。

### AMP for Firepower

AMP for Firepower は、ネットワーク トラフィックにいくつかのファイルタイプのマルウェアが出現するかどうかをシステムが検査できるようにするためのネットワーク ベース AMP ソリューションです。アプライアンスでは、検出されたファイルをさらに分析するためにハードドライブまたは（一部のモデルで）マルウェア ストレージ パックに保存できます。

ローカルマルウェア分析を使用してデバイス上でローカルにファイルを分析し、マルウェアを事前に分類できます。検出されたファイルを手元に保存するかどうかに関わらず、ファイルの SHA-256 ハッシュ値を使用して単純な既知ディスポジションルックアップ用に AMP クラウドにそれを送信することができます。また、脅威のスコアを生成する動的分析を行うためにファイルを AMP Threat Grid クラウドに送信することもできます。このコンテキスト情報を使用して、特定のファイルをブロックまたは許可するようにシステムを設定できます。

AMP for Firepower は、総合的なアクセス コントロール設定の一部として設定することができます。アクセス コントロール ルールに関連付けられているファイル ポリシーは、ルール条件に一致するネットワーク トラフィックを検査します。

### AMP for Endpoint の統合

AMP for Endpoints は、エンタープライズクラスのエンドポイント ベース AMP ソリューションです。ユーザはそれぞれ、AMP クラウドと通信するコンピュータやモバイルデバイスに軽量コネクタをインストールします。次に Firepower Management Center により、スキャン、マルウェア検出、隔離、および侵害の兆候 (IOC) のレコードをインポートし、検出された脅威のトラジェクトリを表示することが可能です。



AMP for Endpoints の展開を構成するには、AMP for Endpoints 管理コンソールを使用します。このコンソールは、マルウェアをすばやく識別し、検疫するのに役立ちます。ユーザはマルウェアを発生時に特定し、それらのトラジェクトリを追跡して影響を把握し、正常にリカバリする方法を学習することができます。AMP for Endpoints を使用すると、カスタム保護の作成、グループ ポリシーに基づく特定のアプリケーションの実行のブロック、カスタム ホワイトリストの作成も可能です。

### ネットワーク ファイル トラジェクトリ

ネットワーク ファイル トラジェクトリ機能を使用すれば、ネットワーク全体のファイルの伝送パスを追跡することができます。システムは SHA-256 ハッシュ値を使用してファイルを追跡するため、ファイルを追跡するには、システムで以下のいずれかの処理を行う必要があります。

- ファイルの SHA-256 ハッシュ値を計算し、その値を使用して AMP クラウドに対するクエリを実行する
- Firepower Management Center と組織の AMP for Endpoints 展開との統合を使用して、ファイルについてエンドポイントベースの脅威および検疫データを受け取る

各ファイルにはトラジェクトリ マップが関連付けられています。このマップには、経時的なファイルの転送を視覚化した情報と、ファイルに関する追加情報が含まれています。

### Cisco AMP プライベート クラウド仮想アプライアンス

AMP for Firepower と AMP for Endpoints のどちらについても、AMP クラウドにシステムから直接接続することが組織のセキュリティポリシーで許可されていない場合は、Cisco AMP プライベート クラウド仮想アプライアンス (AMPv) を構成できます。

AMPv は、AMP クラウドの圧縮されたオンプレミス バージョン、または匿名プロキシとして機能する仮想マシンです。通常は AMP クラウドとの直接接続が必要になるデータやアクション (AMP for Endpoints からのイベント、ファイル性質ルックアップ、レトロスペクティブ イベントなど) が、AMPv とのローカル接続によって処理されるようになります。AMPv では、エンドポイント イベント データは外部接続で共有されません。

(ファイルの性質ルックアップなどのために) AMP クラウドへの接続が必要になったとき、AMPv は、Firepower Management Center と AMP クラウドとの間の匿名化されたプロキシとして機能します。

### Cisco AMP Threat Grid オンプレミス アプライアンス

組織にパブリックの AMP Threat Grid クラウドへのファイルの送信に関してプライバシーまたはセキュリティ上の懸念がある場合、オンプレミスの AMP Threat Grid アプライアンスを展開することができます。このオンプレミス アプライアンスは、パブリック クラウドと同様に適格なファイルをサンドボックス環境で実行し、脅威スコアと動的分析レポートを Firepower システムに返します。ただし、このオンプレミスアプライアンスは、ご使用のネットワークの外部にあるパブリック クラウドや他のすべてのシステムとは通信しません。

## アプリケーション プログラミング インターフェイス

アプリケーションプログラミングインターフェイス (API) を使用してシステムと対話する方法がいくつか用意されています。

### eStreamer

Event Streamer (eStreamer) を使用すると、Firepower Management Center からの数種類のイベントデータを、カスタム開発されたクライアントアプリケーションにストリーム配信できます。クライアントアプリケーションを作成したら、ユーザはそれを Firepower Management Center 上の eStreamer サーバに接続し、eStreamer サービスを開始して、データのやりとりを始めることができます。

eStreamer の統合ではカスタムプログラミングが必要ですが、これによりユーザはアプライアンスの特定のデータを要求することができます。たとえば、ネットワーク管理アプリケーションの1つにネットワークホストデータを表示する場合、Firepower Management Center からホストの重要度または脆弱性のデータを取得し、その情報を表示に追加するためのプログラムを記述することができます。

### 外部データベース アクセス

データベースアクセス機能を使用すれば、JDBC SSL 接続をサポートするサードパーティ製クライアントを使用して、Firepower Management Center 上の複数のデータベーステーブルに対してクエリを実行することができます。

Crystal Reports、Actuate BIRT、JasperSoft iReport などの業界標準のレポート作成ツールを使用してクエリを作成し、送信することができます。また、独自のカスタムアプリケーションを設定して Cisco データをクエリすることもできます。たとえば、侵入およびディスカバリイベントデータについて定期的にレポートしたり、アラートダッシュボードをリフレッシュしたりするサブレットを構築することが可能です。

### ホスト入力

ホスト入力機能では、スクリプトまたはコマンドラインのインポートファイルを使用してサードパーティのソースからデータをインポートすることにより、ディスカバリデータを増やすことができます。

Web インターフェイスにもいくつかのホスト入力機能があります。これらの機能では、オペレーティングシステムまたはアプリケーションプロトコルの識別情報を変更し、脆弱性を有効化または無効化し、ネットワークマップからさまざまな項目（クライアントやサーバポートなど）を削除することができます。

### 修復

システムには API が含まれており、ユーザはこれを使用して修復（修正）を作成することができます。ネットワークの条件が、関連付けられている関連ポリシーまたはコンプライアンスホワイトリストに違反したときに Firepower Management Center が自動的に修復を起動できます。ユーザが攻撃に即時に対処できない場合でも、修正により攻撃の影響を自動的に緩和でき、またシステムが組織のセキュリティポリシーに準拠し続けるようにすることができます。ユーザ

が作成する修復のほかに、Firepower Management Center にはいくつかの事前定義された修復モジュールが付属しています。

## Firepower のオンラインヘルプとドキュメンテーション

オンラインヘルプには、Web インターフェイスからアクセスできます。

- 各ページで状況依存ヘルプのリンクをクリックする。
- [ヘルプ (Help)] > [オンライン (Online)] を選択する。

ドキュメンテーションロードマップを使用して、Firepower に関連する追加ドキュメンテーションを見つけることができます (<http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html>)。

## ドキュメンテーションのライセンスステートメント

項の先頭に記載されているライセンスステートメントは、項で説明される機能を有効にするために Firepower システムの管理対象デバイスに割り当てる必要があるのは従来のライセンスかスマートライセンスかを示します。

ライセンス付きの機能の多くは追加的であるため、ライセンスステートメントでは、各機能で最も必要なライセンスについてのみ記載しています。

ライセンス文の「または」という語は、その項に記載されている機能を有効にするには特定のライセンスを管理対象デバイスに指定する必要があることを示していますが、追加のライセンスで機能を追加できます。たとえば、ファイルポリシー内では、一部のファイルルールアクションではデバイスに保護ライセンスを指定する必要がありますが、他方ではマルウェアライセンスを指定する必要があります。

ライセンスの詳細については、[Firepower の機能ライセンスについて \(137 ページ\)](#) を参照してください。

### 関連トピック

[Firepower の機能ライセンスについて \(137 ページ\)](#)

## ドキュメント内のサポート対象デバイスに関する記述

章または項目の先頭に記載されているサポート対象デバイスに関する記述は、ある機能が特定のデバイス シリーズ、ファミリー、またはモデルでのみサポートされていることを示しています。たとえば、スタッキングは 8000 シリーズのデバイスでのみサポートされています。

このリリースでサポートされているプラットフォームの詳細については、リリースノートを参照してください。

## ドキュメント内のアクセス ステートメント

このドキュメントの各手順の先頭に記載されているアクセスステートメントは、手順の実行に必要な事前定義のユーザロールを示しています。記載されている任意のロールを使用して手順を実行することができます。

カスタムロールを持っているユーザは、事前定義されたロールとは異なる権限セットを持つことができます。事前定義されたロールを使用して手順のアクセス要件が示されている場合は、同様の権限を持つカスタムロールにもアクセス権があります。カスタムロールを持っているユーザは、設定ページにアクセスするために使用するメニューパスが若干異なる場合があります。たとえば、侵入ポリシー権限のみが付与されているカスタムロールを持つユーザは、アクセスコントロールポリシーを使用する標準パスではなく侵入ポリシーを経由してネットワーク分析ポリシーにアクセスします。

ユーザロールの詳細については、[定義済みのユーザロール \(48 ページ\)](#) および [カスタムユーザロール \(50 ページ\)](#) を参照してください。

## Firepower システムの IP アドレス表記法

IPv4 Classless Inter-Domain Routing (CIDR) の表記、および IPv6 と同様のプレフィックス長の表記を使用して、Firepower システムのさまざまな場所でアドレスブロックを定義することができます。

CIDR またはプレフィックス長の表記を使用して IP アドレスのブロックを指定する場合、Firepower システムは、マスクまたはプレフィックス長で指定されたネットワーク IP アドレスの部分のみを使用します。たとえば、10.1.2.3/8 と入力した場合、Firepower システムでは 10.0.0.0/8 が使用されます。

つまり、Cisco では CIDR またはプレフィックス長の表記を使用する場合に、ビット境界上でネットワーク IP アドレスを使用する標準の方法を推奨していますが、Firepower システムではこれは必要ありません。



## 第 1 部

# ユーザアカウント

- [Firepower システムへのログイン \(17 ページ\)](#)
- [ユーザ設定の指定 \(35 ページ\)](#)





## 第 2 章

# Firepower システムへのログイン

以下のトピックでは、Firepower システムにログインする方法を示します。

- [Firepower システムのユーザ アカウント](#) (17 ページ)
- [Firepower システムのユーザ インターフェイス](#) (19 ページ)
- [Web インターフェイスによる Firepower Management Center へのログイン](#) (24 ページ)
- [Web インターフェイスによる管理対象デバイスへのログイン](#) (25 ページ)
- [CAC クレデンシヤルを使用した Firepower Management Center へのログイン](#) (26 ページ)
- [CAC クレデンシヤルを使用した管理対象デバイスへのログイン](#) (27 ページ)
- [従来型デバイスでのコマンドライン インターフェイスへのログイン](#) (28 ページ)
- [Firepower Threat Defense デバイスのコマンドライン インターフェイスへのログイン](#) (29 ページ)
- [Web インターフェイスでの基本システム情報の表示](#) (31 ページ)
- [Firepower Management Center のドメインの切り替え](#) (31 ページ)
- [Firepower システム Web インターフェイスからのログアウト](#) (32 ページ)
- [コンテキスト メニュー](#) (32 ページ)

## Firepower システムのユーザ アカウント

ユーザ名とパスワードを入力して、アプライアンスの Web インターフェイス、シェル、または CLI へのローカルアクセスを取得する必要があります。ユーザがログイン時にアクセスできる機能は、ユーザアカウントに許可されている権限によって制御されます。一部のアプライアンスは、外部 LDAP や RADIUS サーバでユーザ クレデンシヤルを保存する外部認証を使用するように設定できる場合があります。



(注) システムはユーザアカウントに基づいてユーザ アクティビティを監査するため、ユーザが正しいアカウントでシステムにログインしていることが保証されます。



**注意** すべてのアプライアンスで、（外部認証または CLI expert コマンドで取得した）シェルアクセスを持つユーザには、シェルでの `sudoers` 権限がありますが、これはセキュリティリスクを示す場合があります。外部認証を確立する場合は、シェルアクセスが付与されるユーザのリストを適切に制限してください。同様に、CLI アクセス権限を付与する場合は、構成レベルのアクセス権を持つユーザのリストを制限してください。



**注意** Cisco TAC の指示に従って操作する場合を除き、シェルや CLI expert モードを使用して Firepower アプライアンスにアクセスしないよう強くお勧めします。

アプライアンスが異なれば、サポートするユーザアカウントのタイプは異なり、搭載される機能もさまざまです。

### Firepower Management Center

Firepower Management Center では、次のユーザアカウントタイプをサポートします。

- Web インターフェイス アクセス用に事前定義された `admin` アカウント。このアカウントは管理者ロールを保有し、Web インターフェイスから管理できます。
- シェルアクセス用に事前適宜された `admin` アカウント。このアカウントには `sudoers` 権限があります。
- カスタムユーザアカウント。このアカウントは、`admin` ユーザおよび管理者ロールのユーザが作成、管理できます。



**注意** システムセキュリティ上の理由から、シスコは、追加のシェルユーザを Firepower Management Center で確立しないようにすることを推奨します。そのようなリスクを受け入れる場合は、外部認証を使用して、ユーザに Firepower Management Center へのシェルアクセス権を付与できます。

### 7000 & 8000 シリーズ デバイス

7000 & 8000 シリーズ デバイスでは、次のユーザアカウントタイプをサポートします。

- 事前定義された `admin` アカウント。このアカウントはデバイスにアクセスするすべての形態で使用できます。
- カスタムユーザアカウント。このアカウントは、`admin` ユーザおよび管理者ロールのユーザが作成、管理できます。

Firepower システムは、7000 & 8000 シリーズ デバイスにログインしているユーザの外部認証はサポートしています。



### NGIPSv デバイス

NGIPSv デバイスでは次のユーザアカウントタイプがサポートされます。Firepower システムでは、NGIPSv デバイスにログインするユーザ用の外部認証がサポートされません。

- 事前定義された admin アカウント。このアカウントはデバイスにアクセスするすべての形態で使用できます。
- カスタムユーザアカウント。このアカウントは、admin ユーザおよび Configuration アクセス権をもつユーザが作成、管理できます。

### Firepower Threat Defense および Firepower Threat Defense Virtual デバイス

Firepower Threat Defense および Firepower Threat Defense Virtual デバイスでは、次のユーザアカウントタイプをサポートします。

- 事前定義された admin アカウント。このアカウントはデバイスにアクセスするすべての形態で使用できます。
- カスタムユーザアカウント。このアカウントは、admin ユーザおよび管理者ロールのユーザが作成、管理できます。

Firepower システムは、Firepower Threat Defense デバイスにログインしているユーザの外部認証はサポートしていません。

### ASA FirePOWER デバイス

ASA FirePOWER モジュールでは、次のユーザアカウントタイプをサポートします。

- 事前定義された admin アカウント。
- カスタムユーザアカウント。このアカウントは、admin ユーザおよび Configuration アクセス権をもつユーザが作成、管理できます。

Firepower システムは、ASA FirePOWER デバイスにログインしているユーザの外部認証はサポートしていません。ASA CLI および ASDM を介した ASA デバイスへのアクセスについては、『*Cisco ASA Series General Operations CLI Configuration Guide*』および『*Cisco ASA Series General Operations ASDM Configuration Guide*』に記載されています。

## Firepower システムのユーザインターフェイス

Firepower システムでは、グラフィカル ユーザインターフェイス、補助的なコマンドラインインターフェイス (CLI)、Linux シェルのいずれかを使用してアプライアンスにログインできます。(Web インターフェイスのブラウザ要件の詳細については、Firepower システムの該当バージョンのリリース ノートを参照してください)。



(注) Firepower Management Center を使用して複数のデバイスを管理し、それらのデバイスからのデータを関連付けます。単一のデバイスを直接管理するのが適切な場合には、Firepower Device Manager を使用して一部の Firepower Threat Defense デバイスでポリシーやデバイス設定を管理し、Adaptive Security Device Manager (ASDM) を使用して ASA FirePOWER サービス デバイスで同じ機能を管理できます。アプライアンスの管理ツールを選択した後に、別の管理ツールに切り替えると、最新の設定は失われます。7000 & 8000 シリーズデバイスのローカル Web インターフェイスでは、限定的なシステム設定の機能を提供しますが、その機能を使用してポリシーを管理することはできません。それらのデバイスは Firepower Management Center を使用して管理する必要があります。

使用可能なローカル アクセス タイプはアプライアンスのタイプによって異なります。

表 1: アプライアンス別のローカル アクセス

アプライアンス	グラフィカル ユーザインターフェイス	CLI アクセス	Linux シェルへのアクセス
Firepower Management Center	<ul style="list-style-type: none"> <li>• Firepower Web インターフェイス</li> <li>• 事前定義された admin ユーザとカスタム ユーザアカウントでサポートされます</li> <li>• アドミニストレーティブタスク、管理タスク、分析タスクに使用することができます</li> </ul>	none	<ul style="list-style-type: none"> <li>• 事前定義された admin ユーザでサポートされます</li> <li>• シリアルまたはキーボードを使用してアクセス可能であり、接続をモニタできます</li> <li>• Cisco TAC の指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください</li> </ul>

アプライアンス	グラフィカルユーザインターフェイス	CLI アクセス	Linux シェルへのアクセス
7000 & 8000 シリーズ デバイス	<ul style="list-style-type: none"> <li>• Firepower Web インターフェイス</li> <li>• 事前定義された admin ユーザとカスタム ユーザアカウントでサポートされます</li> <li>• 初期設定、基本的な分析、および設定タスクに使用することができます</li> </ul>	<ul style="list-style-type: none"> <li>• 事前定義された admin ユーザとカスタム ユーザアカウントでサポートされます</li> <li>• SSH 接続を使用してアクセスできます</li> <li>• Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます</li> </ul>	<ul style="list-style-type: none"> <li>• 事前定義された admin ユーザとカスタム ユーザアカウントでサポートされます</li> <li>• <b>Configuration</b> アクセス権を持つ CLI ユーザが expert コマンドを使用してアクセスできます</li> <li>• Cisco TAC の指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください</li> </ul>
NGIPSv デバイス	none	<ul style="list-style-type: none"> <li>• 事前定義された admin ユーザとカスタム ユーザアカウントでサポートされます</li> <li>• SSH 接続を使用してアクセスできます</li> <li>• Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます</li> </ul>	<ul style="list-style-type: none"> <li>• 事前定義された admin ユーザとカスタム ユーザアカウントでサポートされます</li> <li>• <b>Configuration</b> アクセス権を持つ CLI ユーザが expert コマンドを使用してアクセスできます</li> <li>• Cisco TAC の指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください</li> </ul>

アプライアンス	グラフィカル ユーザ インターフェイス	CLI アクセス	Linux シェルへのアクセス
<p>Firepower Threat Defense および Firepower Threat Defense Virtual デバイス</p>	<ul style="list-style-type: none"> <li>• Firepower Device Manager、次で動作する Firepower Threat Defense でサポートされます。               <ul style="list-style-type: none"> <li>• ASA 5506-X</li> <li>• ASA 5506H-X</li> <li>• ASA 5506W-X</li> <li>• ASA 5508-X</li> <li>• ASA 5516-X</li> <li>• ASA 5512-X</li> <li>• ASA 5515-X</li> <li>• ASA 5525-X</li> <li>• ASA 5545-X</li> <li>• ASA 5555-X</li> </ul> </li> <li>• 事前定義された <code>admin</code> ユーザでサポートされます</li> <li>• 初期設定、設定、およびシステム モニタリング に使用することができます</li> </ul>	<ul style="list-style-type: none"> <li>• 事前定義された <code>admin</code> ユーザとカスタム ユーザ アカウントでサポートされます</li> <li>• SSH 接続を使用してアクセスできます</li> <li>• Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます</li> </ul>	<ul style="list-style-type: none"> <li>• 事前定義された <code>admin</code> ユーザとカスタム ユーザ アカウントでサポートされます</li> <li>• <b>Configuration</b> アクセス権を持つ CLI ユーザが <code>expert</code> コマンドを使用してアクセスできます</li> <li>• Cisco TAC の指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください</li> </ul>

アプライアンス	グラフィカルユーザインターフェイス	CLI アクセス	Linux シェルへのアクセス
ASA FirePOWER サービス デバイス	<ul style="list-style-type: none"> <li>Adaptive Security Device Manager (ASDM)</li> <li>初回アクセスやカスタムユーザアカウントでサポートされます</li> <li>初期設定、基本的な分析、および設定タスクに使用することができます</li> </ul>	<ul style="list-style-type: none"> <li>事前定義された admin ユーザとカスタムユーザアカウントでサポートされます</li> <li>SSH 接続を使用してアクセスできます</li> <li>設定タスクおよび管理タスクに使用することができます</li> </ul>	none



(注) ASDM を使用した ASA FirePOWER モジュールの管理の詳細については、『Cisco ASA Series General Operations Configuration Guide』参照してください。

## Web インターフェイスに関する考慮事項

- 組織が認証に共通アクセス カード (CAC) を使用している場合は、CAC クレデンシャルを使用してアプライアンスの Web インターフェイスにアクセスすることができます。
- Web セッション時にアプライアンスのホーム ページに初めてアクセスした際に、そのアプライアンスに対する最後のログインセッションに関する情報を表示できます。最後のログインについて、次の情報を表示できます。
  - ログインの曜日、月、日、年
  - ログイン時のアプライアンスのローカル時間 (24 時間表記)
  - アプライアンスにアクセスするために最後に使用されたホストとドメイン名
- デフォルトのホーム ページの上部に表示されるメニューおよびメニュー オプションは、ユーザアカウントの権限に基づきます。ただし、デフォルトホームページのリンクには、ユーザアカウントの権限の範囲に対応するオプションが含まれています。アカウントに付与されている権限とは異なる権限が必要なリンクをクリックすると、システムから警告メッセージが表示され、そのアクティビティがログに記録されます。

- プロセスの中には長時間かかるものがあります。このため、Webブラウザで、スクリプトが応答しなくなっていることを示すメッセージが表示されることがあります。このメッセージが表示された場合は、スクリプトが完了するまでスクリプトの続行を許可してください。

#### 関連トピック

[ホームページの指定](#) (37 ページ)

## セッションのタイムアウト (Session Timeout)

セッションタイムアウトが適用されないように設定しない限り、デフォルトでは、非アクティブな状態が1時間続くと、Firepower システムが自動的にセッションからユーザをログアウトします。

管理者ロールを割り当てられたユーザは、以下の設定を使用して、アプライアンスのセッションタイムアウト間隔を変更できます。

アプライアンス	設定
Firepower Management Center	[システム (System) ] > [設定 (Configuration) ] > [シェル タイムアウト (Shell Timeout) ]
7000 & 8000 シリーズ デバイス	[デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] > [シェル タイムアウト (Shell Timeout) ]

#### 関連トピック

[セッションタイムアウトの設定](#) (986 ページ)

## WebインターフェイスによるFirepowerManagementCenterへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center	任意 (Any)	任意 (Any)

ユーザは単一のアクティブなセッションに制限されます。すでにアクティブセッションがあるユーザアカウントにログインしようとする、もう一方のセッションを終了するか、または別のユーザとしてログインするように求められます。

### 始める前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- [Cisco Firepower Management Center Getting Started Guide for Models 750, 1500, 2000, 3500 and 4000](#) および [ユーザアカウントの作成 \(86 ページ\)](#) の説明に従って、初期セットアップ手順を完了し、ユーザアカウントを作成します。

### 手順

**ステップ 1** ブラウザで `https://hostname/` にアクセスします。ここで、`hostname` は Firepower Management Center のホスト名に対応します。

**ステップ 2** [ユーザ名 (Username) ] および [パスワード (Password) ] フィールドに、ユーザ名とパスワードを入力します。次の注意事項に注意を払ってください。

- ユーザ名は大文字/小文字を区別しません。
- マルチドメイン導入環境では、ユーザアカウントが作成されたドメインをユーザ名の前に付加します。先祖ドメインを前に付加する必要はありません。たとえばユーザアカウントを SubdomainB で作成し、そのドメインの先祖ドメインが DomainA である場合、次の形式でユーザ名を入力します。  
`SubdomainB\username`
- 組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が 1111 で、SecurID トークンが 222222 の場合は、1111222222 と入力します。Firepower システムにログインする前に、SecurID PIN を生成しておく必要があります。

**ステップ 3** [ログイン (Login) ] をクリックします。

### 関連トピック

[セッションのタイムアウト \(Session Timeout\)](#) (24 ページ)

## Web インターフェイスによる管理対象デバイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	7000 & 8000 シリーズ	該当なし	任意 (Any)

ユーザは単一のアクティブなセッションに制限されます。すでにアクティブセッションがあるユーザアカウントにログインしようとする、もう一方のセッションを終了するか、または別のユーザとしてログインするように求められます。

### 始める前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- デバイスに該当する Firepower クイック スタート ガイドおよび [ユーザアカウントの作成 \(86 ページ\)](#) の説明に従って、初期セットアップ手順を完了し、ユーザアカウントを作成します。

### 手順

**ステップ 1** ブラウザで `https://hostname/` にアクセスします。ここで、`hostname` はアクセスする管理対象デバイスのホスト名に対応します。

**ステップ 2** [ユーザ名 (Username)] および [パスワード (Password)] フィールドに、ユーザ名とパスワードを入力します。次の注意事項に注意を払ってください。

- ユーザ名は大文字/小文字を区別しません。
- 組織でログイン時に SecurID<sup>®</sup> トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が 1111 で、SecurID トークンが 222222 の場合は、111122222 と入力します。Firepower システムにログインする前に、SecurID PIN を生成しておく必要があります。

**ステップ 3** [ログイン (Login)] をクリックします。

### 関連トピック

[セッションのタイムアウト \(Session Timeout\)](#) (24 ページ)

## CAC クレデンシアルを使用した Firepower Management Center へのログイン

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center	任意 (Any)	任意 (Any)

ユーザは単一のアクティブなセッションに制限されます。





**注意** ブラウズセッションがアクティブな間は、CAC を削除しないでください。セッション中に CAC を削除または交換すると、Web ブラウザでセッションが終了し、システムにより Web インターフェイスから強制的にログアウトされます。

**始める前に**

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- [Cisco Firepower Management Center Getting Started Guide for Models 750, 1500, 2000, 3500 and 4000](#) および [ユーザアカウントの作成 \(86 ページ\)](#) の説明に従って、初期セットアップ手順を完了し、ユーザアカウントを作成します。
- [CAC 認証の設定 \(100 ページ\)](#) の説明に従って、CAC の認証と認可を設定します。

**手順**

- ステップ 1** 組織の指示に従って CAC を挿入します。
- ステップ 2** ブラウザで `https://hostname/` にアクセスします。ここで、`hostname` は Firepower Management Center のホスト名に対応します。
- ステップ 3** プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられた PIN を入力します。
- ステップ 4** プロンプトが表示されたら、ドロップダウンリストから該当する証明書を選択します。
- ステップ 5** [続行 (Continue) ] をクリックします。

**関連トピック**

- [CAC 認証 \(99 ページ\)](#)
- [セッションのタイムアウト \(Session Timeout\) \(24 ページ\)](#)

# CAC クレデンシャルを使用した管理対象デバイスへのログイン

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	7000 & 8000 シリーズ	該当なし	任意 (Any)

ユーザは単一のアクティブなセッションに制限されます。



**注意** ブラウズセッションがアクティブな間は、CAC を削除しないでください。セッション中に CAC を削除または交換すると、Web ブラウザでセッションが終了し、システムにより Web インターフェイスから強制的にログアウトされます。

#### 始める前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- デバイスに該当する [Firepower クイック スタート ガイド](#) および [ユーザアカウントの作成 \(86 ページ\)](#) の説明に従って、初期セットアップ手順を完了し、ユーザアカウントを作成します。
- [CAC 認証の設定 \(100 ページ\)](#) の説明に従って、CAC の認証と認可を設定します。

#### 手順

- ステップ 1** 組織の指示に従って CAC を挿入します。
- ステップ 2** ブラウザで `https://hostname/` にアクセスします。ここで、`hostname` はアクセスするアプライアンスのホスト名に対応します。
- ステップ 3** プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられた PIN を入力します。
- ステップ 4** プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。
- ステップ 5** [続行 (Continue) ] をクリックします。

#### 関連トピック

[CAC 認証 \(99 ページ\)](#)

[セッションのタイムアウト \(Session Timeout\) \(24 ページ\)](#)

## 従来型デバイスでのコマンドラインインターフェイスへのログイン

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	従来型 (Classic)	該当なし	CLI の基本設定

従来型管理対象デバイス (7000 & 8000 シリーズ、NGIPSv、および ASA FirePOWER) のコマンドライン インターフェイスに直接ログインできます。

### 始める前に

最初のログインにデフォルトの **admin** ユーザを使用して初期設定プロセスを完了します。

- 7000 & 8000 シリーズ デバイスで、[ユーザアカウントの作成 \(86 ページ\)](#) の説明に従って、Web インターフェイスでユーザアカウントを作成します。
- すべてのデバイスで、CLIにログインできる追加のユーザアカウントを **configure user add** コマンドを使用して作成します。

### 手順

- ステップ 1** SSHを使用して、管理インターフェイスのホスト名またはIPアドレスに接続します。または、コンソールポートに接続することもできます。
- ステップ 2** 「log in as:」 コマンドプロンプトに対してユーザ名を入力し、Enter を押します。
- ステップ 3** 「Password:」 プロンプトに対してパスワードを入力し、Enter を押します。
- 組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえばPINが 1111 で、SecurID トークンが 222222 の場合は、1111222222 と入力します。Firepower システムにログインする前に、SecurID PIN を生成しておく必要があります。
- ステップ 4** CLI プロンプトで、コマンドラインアクセスのレベルで許可されている任意のコマンドを使用します。

## Firepower Threat Defense デバイスのコマンドラインインターフェイスへのログイン

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	該当なし	CLI の基本設定

Firepower Threat Defense 管理対象デバイスのコマンドラインインターフェイスに直接ログインできます。

### 始める前に

最初のログインにデフォルトの **admin** ユーザを使用して初期設定プロセスを完了します。**configure user add** コマンドを使用して、CLIにログインできる追加のユーザアカウントを作成します。

## 手順

**ステップ 1** コンソールポートまたは SSH を使用して、Firepower Threat Defense CLI に接続します。

Firepower Threat Defense デバイスの管理インターフェイスに SSH で接続できます。SSH 接続用のインターフェイスを開いている場合、データインターフェイス上のアドレスにも接続できます。データインターフェイスへの SSH アクセスはデフォルトで無効になっています。特定のデータインターフェイスへの SSH 接続を許可する方法については、[セキュアシェルの設定（1041 ページ）](#)を参照してください。

デバイスのコンソールポートに直接接続できます。デバイスに付属のコンソールケーブルを使用し、9600 ボー、8 データビット、パリティなし、1 ストップビット、フロー制御なしに設定されたターミナルエミュレータを用いて PC をコンソールに接続します。コンソールケーブルの詳細については、デバイスのハードウェアガイドを参照してください。

コンソールポートでアクセスする最初の CLI は、デバイスタイプによって異なります。

- ASA シリーズデバイス：コンソールポートの CLI は通常の Firepower Threat Defense CLI です。
- Firepower シリーズデバイス：コンソールポートの CLI は FXOS です。Firepower Threat Defense CLI には、**connect ftd** コマンドを使用してアクセスできます。FXOS CLI はシャールレベルの設定およびトラブルシューティングにのみ使用します。基本設定、モニタリング、および通常のシステムのトラブルシューティングには Firepower Threat Defense CLI を使用します。FXOS コマンドの詳細については、FXOS のマニュアルを参照してください。

**ステップ 2** 管理者ユーザ名とパスワードでログインします。

**ステップ 3** CLI プロンプト (>) で、コマンドラインアクセスレベルで許可されている任意のコマンドを使用します。

**ステップ 4** (オプション) 診断 CLI にアクセスします。

### system support diagnostic-cli

この CLI を使用して、高度なトラブルシューティングを行います。この CLI では、追加の **show** コマンドや、ASA 5506W-X ワイヤレスアクセスポイントの CLI へのアクセスに必要な **session wlan console** コマンドなど、その他のコマンドが利用できます。

この CLI には 2 つのサブモード、ユーザ EXEC モードと特権 EXEC モードがあります。特権 EXEC モードではより多くのコマンドが利用できます。特権 EXEC モードを開始するには、**enable** コマンドを入力し、プロンプトに対してパスワードを入力せずに Enter を押します。

例：

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

通常の CLI に戻るには、**Ctrl+a, d** を入力します。

## Web インターフェイスでの基本システム情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)

[バージョン情報 (About)] ページには、Firepower システムのさまざまなコンポーネントのモデル、シリアル番号、バージョン情報など、アプライアンスに関する情報が示されます。また、シスコの著作権情報も示されます。

### 手順

**ステップ 1** ページ上部のツールバーから [ヘルプ (Help)] をクリックします。

**ステップ 2** [バージョン情報 (About)] を選択します。

## Firepower Management Center のドメインの切り替え

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center	任意 (Any)	任意 (Any)

マルチドメイン導入環境では、ユーザロール権限によって、ユーザがアクセスできるドメインと、そのドメイン内でのユーザの権限が決まります。単一のユーザアカウントを複数のドメインに関連付けて、各ドメインでそのユーザに異なる権限を割り当てることができます。たとえば、あるユーザにグローバルドメインでは読み取り専用権限を割り当て、子孫ドメインでは管理者権限を割り当てることができます。

複数のドメインに関連付けられているユーザは、同じ Web インターフェイスセッション内でドメインを切り替えることができます。

ツールバーのユーザ名の下に、利用可能なドメインのツリーが表示されます。ツリーの表示は次のようになります。

- 先祖ドメインは表示されますが、使用しているユーザアカウントに割り当てられた権限に応じて、先祖ドメインへのアクセスが無効である場合があります。

- 兄弟ドメインや子孫ドメインを含め、使用しているユーザアカウントでアクセスできない他のドメインは非表示になります。

ドメインを切り替えると、以下の項目が表示されます。

- そのドメインのみに関連するデータ。
- そのドメインで割り当てられたユーザ ロールに応じて定められたメニュー オプション。

#### 手順

アクセスするドメインは、ユーザ名の下にあるドロップダウン リストから選択します。

## Firepower システム Web インターフェイスからのログアウト

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)

Firepower システムの Web インターフェイスをアクティブに使用しなくなった場合、シスコでは、少しの間 Web ブラウザから離れるだけでも、ログアウトすることを推奨しています。ログアウトすることで Web セッションを終了し、別のユーザが自分の資格情報を使用してインターフェイスを使用できないようにします。

#### 手順

ユーザ名の下にあるドロップダウンリストから、[ログアウト (Logout)] を選択します。

#### 関連トピック

[セッションのタイムアウト \(Session Timeout\)](#) (24 ページ)

## コンテキスト メニュー

Firepower システム Web インターフェイスの特定のページでは、右クリック (最も一般的) および左クリックでコンテキストメニューを表示できます。コンテキストメニューは、Firepower システム内の他の機能にアクセスするためのショートカットとして使用できます。コンテキス

トメニューの内容はどこでこのメニューにアクセスするか（どのページかだけでなく特定のデータにアクセスしているか）によって異なります。

次に例を示します。

- IPアドレスのホットスポットでは、そのアドレスに関連付けられているホストに関する情報（使用可能な whois とホストプロファイル情報を含む）が表示されます。
- SHA-256 ハッシュ値のホットスポットでは、ファイルの SHA-256 ハッシュ値をクリーンリストまたはカスタム検出リストに追加したり、コピーするためにハッシュ値全体を表示したりできます。

Firepower システム コンテキストメニューをサポートしていないページや場所では、ブラウザの通常のコンテキストメニューが表示されます。

### ポリシー エディタ

多くのポリシーエディタには、各ルールホットスポットが含まれています。新しいルールとカテゴリの挿入、ルールの切り取り、コピー、貼り付け、ルール状態の設定、ルールの編集などを行うことができます。

### 侵入ルール エディタ

侵入ルールエディタには、各侵入ルールホットスポットが含まれています。ルールの編集、ルール状態の設定、しきい値および抑止オプションの設定、ルールのドキュメンテーションの表示などを行うことができます。

### イベント ビューア

イベント ページ（ドリルダウンページとテーブルビュー）には、各イベント、IP アドレス、URL、DNS クエリ、特定のファイルの SHA-256 ハッシュ値のホットスポットが含まれています。ほとんどのイベントタイプでは、表示中に以下の操作を行うことができます。

- Context Explorer で関連情報を表示する。
- 新しいウィンドウでイベント情報をドリルダウンする。
- イベント フィールドに含まれているテキスト（ファイルの SHA-256 ハッシュ値、脆弱性の説明、URL など）が長すぎてイベントビューですべて表示できない場合、テキスト全体を表示する。

接続イベントの表示中は、デフォルトのセキュリティインテリジェンスのホワイトリストとブラックリストに以下の項目を追加できます。

- IP アドレスのホットスポットの場合、IP アドレス。
- URL のホットスポットの場合、URL またはドメイン名。
- DNS クエリのホットスポットの場合、DNS クエリ。

キャプチャ ファイル、ファイル イベント、マルウェア イベントの表示中は、以下の操作を行うことができます。

- クリーン リストまたはカスタム検出リストのファイルを追加または削除する。
- ファイルのコピーをダウンロードする。
- アーカイブ ファイル内のネストされたファイルを表示する。
- ネストされたファイルの親アーカイブ ファイルをダウンロードする。
- ファイルの構成を表示する。
- ローカル マルウェア分析およびダイナミック分析対象のファイルを送信する。

侵入イベントの表示中は、侵入ルールエディタまたは侵入ポリシーで実行できるようなタスクを行うことができます。

- トリガー ルールを編集する。
- ルールの無効化を含め、ルールの状態を設定する。
- しきい値および抑止オプションを設定する。
- ルールのドキュメンテーションを表示する。

#### 侵入イベントの packets ビュー

侵入イベントの packets ビューには、IP アドレスのホットスポットが含まれています。packets ビューでは、左クリックによるコンテキストメニューを使用します。

#### ダッシュボード

多くのダッシュボードウィジェットには、関連する情報を Context Explorer で表示するためのホットスポットが含まれています。ダッシュボードウィジェットには、IP アドレスと SHA-256 ハッシュ値のホットスポットが含まれる場合もあります。

#### Context Explorer

Context Explorer には、図、表、グラフのホットスポットが含まれています。Context Explorer よりも詳細なグラフまたはリストのデータを調べたい場合は、関連するデータのテーブルビューにドリルダウンすることができます。また、関連するホスト、ユーザ、アプリケーション、ファイル、および侵入ルールを表示できます。

Context Explorer でも左クリックのコンテキストメニューを使用します。これには、Context Explorer に特有のフィルタリングおよび他のオプションも含まれています。

#### 関連トピック

[セキュリティインテリジェンスのリストとフィード \(464 ページ\)](#)





## 第 3 章

# ユーザ設定の指定

以下のトピックでは、ユーザ設定を指定する方法について説明します。

- [ユーザ設定の概要 \(35 ページ\)](#)
- [パスワードの変更 \(35 ページ\)](#)
- [失効パスワードの変更 \(36 ページ\)](#)
- [ホームページの指定 \(37 ページ\)](#)
- [イベントビュー設定の設定 \(37 ページ\)](#)
- [デフォルトタイムゾーンの設定 \(43 ページ\)](#)
- [デフォルトのダッシュボードの指定 \(44 ページ\)](#)

## ユーザ設定の概要

ホームページ、アカウントパスワード、タイムゾーン、ダッシュボード、イベントビューの各設定など、単一のユーザアカウントに関連付けられた設定を構成できます。

ユーザロールに応じて、パスワード、イベントビューの設定、タイムゾーンの設定、ホームページの設定など、ユーザアカウントにある特定の設定を指定できます。

マルチドメイン展開では、ユーザ設定は、アカウントでアクセスできるすべてのドメインに適用されます。ホームページ設定とダッシュボード設定を指定した場合、特定のページとダッシュボードウィジェットがドメインから制約を受けることに留意してください。

## パスワードの変更

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)

すべてのユーザアカウントはパスワードで保護されています。パスワードはいつでも変更することができ、ユーザアカウントの設定によっては定期的にパスワードを変更しなければならない場合もあります。

パスワードの強度チェックが有効の場合、パスワードは大文字と小文字が混在する少なくとも8つの英数字で、少なくとも1つの数字が含まれている必要があります。パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。

LDAPまたはRADIUSユーザの場合、Webインターフェイスを介してパスワードを変更することはできません。

#### 手順

- 
- ステップ1** ユーザ名の下にあるドロップダウンリストから、[ユーザプリファレンス (User Preferences)] を選択します。
- ステップ2** [現在のパスワード (Current Password)] を入力して、[変更 (Change)] をクリックします。
- ステップ3** [新しいパスワード (New Password)] および [確認 (Confirm)] フィールドに、新しいパスワードを入力します。
- ステップ4** [変更 (Change)] をクリックします。
- 

## 失効パスワードの変更

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)

ユーザアカウントの設定によっては、パスワードが期限切れになることがあります。パスワードの有効期間は、アカウントが作成されたときに設定され、**変更できない**ことに注意してください。パスワードが期限切れになった場合、[パスワードの有効期限の警告 (Password Expiration Warning)] ページが表示されます。

#### 手順

パスワードの有効期限の警告のページには2つの選択肢があります。

- すぐにパスワードを変更するには、[パスワードの変更 (Change Password)] をクリックします。残りの警告日数がゼロの場合は、パスワードを変更する**必要があります**。

**ヒント** パスワードの強度チェックが有効の場合、パスワードは大文字と小文字が混在する少なくとも8つの英数字で、少なくとも1つの数字が含まれている必要があります。パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。

- 後でパスワードを変更するには、[後で (Skip) ] をクリックします。

## ホームページの指定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	External Database User を除くすべてのユーザ

Web インターフェイス内のページをアプライアンスのホームページに指定できます。デフォルトのホームページは、[サマリーダッシュボード (Summary Dashboard) ] ([概要 (Overview) ] > [ダッシュボード (Dashboards) ]) です (ダッシュボードへのアクセス権がないユーザアカウントを除く)。

マルチドメイン環境では、選択したデフォルトのホームページは、ユーザアカウントがアクセスできるすべてのドメインに適用されます。複数のドメインに頻繁にアクセスするアカウントのホームページを選択する際、特定のページはグローバルドメインに制限されることに注意してください。

### 手順

- ステップ 1** ユーザ名の下にあるドロップダウンリストから、[ユーザ設定 (User Preferences) ] を選択します。
- ステップ 2** [ホームページ (Home Page) ] をクリックします。
- ステップ 3** ホーム ページとして使用するページをドロップダウン リストから選択します。  
ドロップダウン リスト内のオプションは、ユーザ アカウントのアクセス権限に基づいて表示されます。詳細については、[ユーザ アカウントの権限 \(51 ページ\)](#) を参照してください。
- ステップ 4** [Save] をクリックします。

## イベント ビュー設定の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	機能に応じて異なる

[イベントビュー設定 (Event View Settings)] ページを使用して、Firepower Management Center のイベントビューの特性を設定します。イベントビュー設定は、特定のユーザロールでのみ使用可能であることに注意してください。External Database User ロールを持つユーザは、イベントビュー設定のユーザインターフェイスの一部を表示できますが、それらの設定を変更しても意味のある結果は生じません。

#### 手順

- ステップ1 ユーザ名の下にあるドロップダウンリストから、[ユーザ設定 (User Preferences)] を選択します。
- ステップ2 [イベントビュー設定 (Event View Settings)] をクリックします。
- ステップ3 [イベント設定 (Event Preferences)] セクションで、イベントビューの基本特性を設定します。[イベントビュー設定 \(38 ページ\)](#) を参照してください。
- ステップ4 [ファイル設定 (File Preferences)] セクションで、ファイルダウンロードを設定します。[ファイルダウンロード設定 \(40 ページ\)](#) を参照してください。
- ステップ5 [デフォルト時間帯 (Default Time Windows)] セクションで、デフォルトの時間帯を設定します。[デフォルト時間帯 \(41 ページ\)](#) を参照してください。
- ステップ6 [デフォルトワークフロー (Default Workflow)] セクションで、デフォルトワークフローを設定します。[デフォルトワークフロー \(43 ページ\)](#) を参照してください。
- ステップ7 [保存 (Save)] をクリックします。

## イベントビュー設定

[イベントビュー設定 (Event View Settings)] ページの [イベント設定 (Event Preferences)] セクションを使用して、Firepower システムのイベントビューの基本特性を設定します。このセクションはすべてのユーザロールで使用可能ですが、イベントを表示できないユーザには、ほとんどまたはまったく意味がありません。

以下のフィールドが [イベント設定 (Event Preferences)] セクションに示されます。

- [「すべて」の操作を確認 (Confirm "All" Actions)] フィールドは、イベントビューのすべてのイベントに影響を与える操作について、アプライアンスがユーザに確認を要求するかどうかを制御します。

たとえば、この設定が有効である場合、イベントビューで [すべて削除 (Delete All)] をクリックすると、アプライアンスがデータベースからの削除を実行する前に、現在の制約を満たすすべてのイベント (現在のページに表示されていないイベントを含む) を削除することをユーザが確認する必要があります。
- [IP アドレスの解決 (Resolve IP Addresses)] フィールドを使用すると、可能な場合には常に、アプライアンスで IP アドレスの代わりにホスト名がイベントビューに表示されるようになります。

多数のIPアドレスが含まれている場合、このオプションを有効にすると、イベントビューの表示に時間がかかる可能性があることに注意してください。また、この設定を有効にするには、管理インターフェイス設定を使用して、システム設定でDNSサーバを確立する必要があることにも注意してください。

- [パケットビューの展開 (Expand Packet View) ] フィールドでは、侵入イベントのパケットビューをどのように表示するかを設定できます。デフォルトでは、アプライアンスによるパケットビューの表示は折りたたまれた状態になっています。
  - [なし (None) ] : パケットビューの [パケット情報 (Packet Information) ] セクションのサブセクションをすべて折りたたんだ状態にします。
  - [パケットテキスト (Packet Text) ] : [パケットテキスト (Packet Text) ] サブセクションだけを展開します。
  - [パケットバイト (Packet Bytes) ] : [パケットバイト (Packet Bytes) ] サブセクションだけを展開します。
  - [すべて (All) ] : すべてのセクションを展開します。

デフォルト設定に関係なく、パケットビューのセクションを手動で展開することで、キャプチャされたパケットに関する詳細情報を常に表示することができます。

- [1 ページあたりの行数 (Rows Per Page) ] フィールドは、ドリルダウンページとテーブルビューに表示する、ページごとのイベントの行数を制御します。
- [更新間隔 (Refresh Interval) ] フィールドは、イベントビューの更新間隔を分単位で設定します。0を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。
- [統計更新間隔 (Statistics Refresh Interval) ] は、[侵入イベント統計 (Intrusion Event Statistics) ] や [ディスカバリ統計 (Discovery Statistics) ] ページなどのイベントのサマリーページの更新間隔を制御します。0を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。
- [ルール of 非アクティブ化 (Deactivate Rules) ] フィールドは、標準テキストルールによって生成される侵入イベントのパケットビューに、どのリンクを表示させるかを次のように制御します。
  - [すべてのポリシー (All Policies) ] : すべてのローカルで定義されたカスタム侵入ポリシーで標準テキストルールを非アクティブにする単一リンク
  - [現在のポリシー (Current Policy) ] : 現在展開中の侵入ポリシーだけで標準テキストルールを非アクティブにする単一リンク。デフォルトのポリシーのルールは非アクティブにできないことに注意してください。
  - [質問 (Ask) ] : これらの個々のオプションへのリンク

パケットビューでこれらのリンクを表示するには、Administrator または Intrusion Admin のアクセス権があるユーザアカウントが必要です。

## 関連トピック

[管理インターフェイス](#) (931 ページ)

## ファイルダウンロード設定

[ イベントビュー設定 (Event View Settings) ] ページの [ ファイル設定 (File Preferences) ] セクションを使用して、ローカルファイルダウンロードの基本特性を設定します。このセクションは、Administrator、Security Analyst、または Security Analyst (読み取り専用) ユーザロールを持つユーザのみが使用できます。

キャプチャされたファイルのダウンロードをアプライアンスがサポートしていない場合、これらのオプションは無効になることに注意してください。

以下のフィールドが [ ファイル設定 (File Preferences) ] セクションに示されます。

- 「ファイルのダウンロード」アクションを確認する (Confirm 'Download File' Actions) ] チェックボックスは、ファイルをダウンロードするたびに [ ファイルダウンロード (File Download) ] ポップアップウィンドウが表示され、警告が示されて続行するかキャンセルするかを選択するためのプロンプトが出されるようにするかどうかを制御します。



**注意** シスコは、有害な結果が発生することがあるため、マルウェアをダウンロードしないように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先をセキュアにするために必要な予防措置を行っていることを確認します。

ファイルをダウンロードする際には、いつでもこのオプションを無効にできることに注意してください。

- キャプチャされたファイルをダウンロードすると、そのファイルを含むパスワード保護された .zip アーカイブがシステムによって作成されます。[ zip ファイルパスワード (Zip File Password) ] フィールドは、.zip ファイルへのアクセスを制限するためにユーザが使用するパスワードを定義します。このフィールドを空欄にすると、パスワードなしのアーカイブファイルがシステムによって作成されます。
- [ zip ファイルパスワードを表示する (Show Zip File Password) ] チェックボックスによって、[ zip ファイルパスワード (Zip File Password) ] フィールドにプレーンテキストを表示するかまたは不明瞭な文字を表示するかを切り替えます。このフィールドをオフにすると、[ zip ファイルパスワード (Zip File Password) ] には不明瞭な文字が表示されます。

## デフォルト時間枠

時間枠（時間範囲と呼ばれることもある）は、任意のイベントビューでイベントに時間制約を課します。[イベントビュー設定（Event View Settings）] ページの [デフォルト時間枠（Default Time Windows）] セクションを使用して、時間枠のデフォルトの動作を制御します。

このセクションへのユーザ ロール アクセスは以下のとおりです。

- Administrators と Maintenance Users は、セクション全体にアクセスできます。
- Security Analysts と Security Analysts（読み取り専用）は、[監査ログの時間枠（Audit Log Time Window）] 以外のすべてのオプションにアクセスできます。
- アクセス管理者、ディスカバリ管理者、外部データベース ユーザ、侵入管理者、ネットワーク管理者、およびセキュリティ承認者は、[イベントの時間枠（Events Time Window）] オプションにのみアクセスできます。

デフォルトの時間枠設定に関係なく、イベントの分析中にいつでも手動で個別のイベントビューの時間枠を変更できることに注意してください。また、時間枠の設定は、現在のセッションにだけ有効であることにも注意してください。ログアウトしてから再びログインすると、時間枠は、このページで設定したデフォルトにリセットされます。

以下のように、デフォルトの時間枠を設定できる3つのタイプのイベントがあります。

- [イベントの時間枠（Events Time Window）] は、時間で制約できるほとんどイベントのために単一のデフォルトの時間枠を設定します。
- [監査ログの時間枠（Audit Log Time Window）] は、監査ログのためにデフォルトの時間枠を設定します。
- [ヘルス モニタリングの時間枠（Health Monitoring Time Window）] は、ヘルス イベントのためにデフォルトの時間枠を設定します。

時間枠は、ユーザアカウントがアクセスできるイベント タイプにのみ設定できます。すべてのユーザタイプは、イベントの時間枠を設定できます。Administrators、Maintenance Users、および Security Analysts は、ヘルス モニタリングの時間枠を設定できます。Administrators と Maintenance Users は、監査ログの時間枠を設定できます。

すべてのイベントビューが時間で制約できるとは限らないので、時間枠の設定によって、ホスト、ホスト属性、アプリケーション、クライアント、脆弱性、ユーザの ID、ホワイトリスト違反を表示するイベントビューは影響を受けないことに注意してください。

[複数（Multiple）] の時間枠を使用して、上記の各タイプのイベントに1つずつ適用するか、または [単一（Single）] の時間枠を使用して、すべてのイベントに適用することができます。単一の時間枠を使用すると、3つのタイプの時間枠用の設定が非表示になり、新しく [グローバルな時間枠（Global Time Window）] 設定が表示されます。

以下の3つのタイプの時間枠があります。

- 静的は、特定の開始時刻から特定の終了時刻までに生成されたすべてのイベントを表示します

- 拡張は、特定の開始時刻から現在までに生成されたすべてのイベントを表示します。時間の進行と共に時間枠が拡張され、新しいイベントがイベントビューに追加されます
- スライディングは、特定の開始時刻（たとえば1日前）から現在までに生成されたすべてのイベントを表示します。時間の進行と共に時間枠は「スライド」し、設定した範囲内（この例では直前の1日）のイベントだけが表示されます

すべての時間枠の最大時間範囲は、1970年1月1日午前0時（UTC）～2038年1月19日午前3時14分7秒です。

次のオプションは、[時間枠の設定（Time Window Settings）] ドロップダウンリストに表示されます。

- [最後を表示 - スライディング（Show the Last - Sliding）] オプションにより、指定した長さのスライドするデフォルトの時間枠を設定できます。

アプライアンスは、特定の開始時刻（たとえば1時間前）から現在までに生成されたすべてのイベントを表示します。イベントビューの変更と共に、時間枠は「スライド」して、常に最後の1時間内のイベントが表示されます。

- [最後を表示（静的/拡張）（Show the Last - Static/Expanding）]：このオプションで、指定した長さのデフォルトの時間枠を静的または拡張のどちらかに設定できます。

**静的時間枠にするには**、[終了時間を使用（Use End Time）] チェックボックスをオンにします。アプライアンスは、特定の開始時間（1時間前など）から現在までに生成されたすべてのイベントを表示します。イベントビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

**拡張時間枠にするには**、[終了時間を使用（Use End Time）] チェックボックスをオフにします。アプライアンスは、特定の開始時刻（たとえば1時間前）から現在までに生成されたすべてのイベントを表示します。イベントビューを変更すると、時間枠は現在まで拡張されます。

- [本日 - 静的/拡張（Current Day - Static/Expanding）] オプションにより、現在の日付のデフォルトの時間枠を静的または拡張のどちらかに設定できます。現在の日付は、現行セッションのタイムゾーン設定に基づいて午前0時に始まります。

**静的時間枠にするには**、[終了時間を使用（Use End Time）] チェックボックスをオンにします。アプライアンスは、午前0時からユーザがイベントを初めて確認した時刻までに生成されたすべてのイベントを表示します。イベントビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

**拡張時間枠にするには**、[終了時間を使用（Use End Time）] チェックボックスをオフにします。アプライアンスは、午前0時から現在までに生成されたすべてのイベントを表示します。イベントビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に24時間を超えて分析を続けた場合、この時間枠は24時間よりも長くなる可能性があることに注意してください。

- [今週 - 静的/拡張（Current Week - Static/Expanding）] オプションにより、現在の週のデフォルトの時間枠を静的または拡張のどちらかに設定できます。現在の週は、現行セッションのタイムゾーン設定に基づいて直前の日曜日の午前0時に始まります。



静的時間枠にするには、[終了時間を使用 (Use End Time)] チェックボックスをオンにします。アプライアンスは、午前0時からユーザがイベントを初めて確認した時刻までに生成されたすべてのイベントを表示します。イベントビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

拡張時間枠にするには、[終了時間を使用 (Use End Time)] チェックボックスをオフにします。アプライアンスは、日曜日の午前0時から現在までに生成されたすべてのイベントを表示します。イベントビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に1週間を超えて分析を続けた場合、この時間枠は1週間よりも長くなる可能性があります。ご注意ください。

## デフォルトワークフロー

ワークフローは、アナリストがイベントの評価に使用するデータが示された一連のページです。アプライアンスには、各イベントタイプに少なくとも1つの定義済みのワークフローが付属しています。たとえば、セキュリティアナリストの場合、実行する分析のタイプに応じて、それぞれが侵入イベントのデータを別の形式で示している、10の異なる侵入イベントのワークフローから選択できます。

アプライアンスには、イベントタイプごとにデフォルトワークフローが設定されます。たとえば、[優先順位および分類に基づいたイベント (Events by Priority and Classification)] ワークフローが、侵入イベントのデフォルトになります。つまり、侵入イベント (確認済みの侵入イベントを含む) を表示するたびに、アプライアンスは [優先順位および分類に基づいたイベント (Events by Priority and Classification)] ワークフローを表示します。

ただし、イベントタイプごとにデフォルトワークフローは変更できます。設定可能なデフォルトのワークフローは、ユーザロールによって異なります。たとえば、侵入イベントのアナリストがデフォルトのディスカバリ イベントワークフローを設定することはできません。

## デフォルトタイムゾーンの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)

アプライアンスが使用している標準 UTC 時間からイベントの表示に使用するタイムゾーンを変更できます。タイムゾーンを設定すると現在のユーザアカウントにのみ適用され、タイムゾーンをさらに変更するときまで有効になります。



**注意**

タイムゾーン機能は、デフォルトのシステムクロックが UTC 時間に設定されているものと想定しています。ローカルタイムゾーンを使用するようにアプライアンスのシステムクロックを変更した場合は、アプライアンスで正確なローカル時刻が表示されるように、それを変更して UTC 時間に戻す必要があります。

## 手順

- ステップ1** ユーザ名の下にあるドロップダウンリストから、[ユーザ設定 (User Preferences)] を選択します。
- ステップ2** [タイムゾーン設定 (Time Zone Preference)] タブをクリックします。
- ステップ3** 左側のリストボックスで、使用するタイムゾーンを含む大陸または地域を選択します。
- ステップ4** 右側のリストボックスで、使用するタイムゾーンに対応するゾーン (都市名) を選択します。
- ステップ5** [保存 (Save)] をクリックします。

## デフォルトのダッシュボードの指定

スマートライセンス	従来ライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst

[概要 (Overview)] > [ダッシュボード (Dashboards)] を選択すると、デフォルトのダッシュボードが表示されます。変更しない限り、すべてのユーザのデフォルトダッシュボードは、[サマリー (Summary)] ダッシュボードです。

マルチドメイン環境では、選択したデフォルトのダッシュボードは、ユーザアカウントがアクセスできるすべてのドメインに適用されます。複数のドメインに頻繁にアクセスするアカウントのダッシュボードを選択する際、ドメインが特定のダッシュボードウィジェットを制限することに注意してください。

## 手順

- ステップ1** ユーザ名の下にあるドロップダウンリストから、[ユーザ設定 (User Preferences)] を選択します。
- ステップ2** [ダッシュボード設定 (Dashboard Settings)] をクリックします。
- ステップ3** デフォルトとして使用するダッシュボードをドロップダウンリストから選択します。[なし (None)] を選択した場合、[概要 (Overview)] > [ダッシュボード (Dashboards)] を選択するときに、表示するダッシュボードを選択できます。
- ステップ4** [保存 (Save)] をクリックします。

## 関連トピック

[ダッシュボードの表示](#) (274 ページ)



## 第 II 部

# Firepower システムの管理

- [Firepower システム ユーザ管理 \(47 ページ\)](#)
- [Firepower システムのライセンス \(137 ページ\)](#)
- [システム ソフトウェア更新 \(161 ページ\)](#)
- [バックアップと復元 \(197 ページ\)](#)
- [コンフィギュレーションのインポートとエクスポート \(211 ページ\)](#)
- [タスクのスケジューリング \(219 ページ\)](#)
- [Management Center データベースの消去 \(243 ページ\)](#)





## 第 4 章

# Firepower システム ユーザ管理

次のトピックでは、管理アクセス権を持つユーザが Firepower システム内のユーザ アカウントを管理する方法について説明します。

- [ユーザの役割 \(47 ページ\)](#)
- [ユーザ アカウント \(84 ページ\)](#)
- [Firepower システムのユーザ認証 \(94 ページ\)](#)
- [LDAP 認証 \(97 ページ\)](#)
- [RADIUS 認証 \(124 ページ\)](#)
- [シングルサインオン \(SSO\) \(134 ページ\)](#)

## ユーザの役割

Firepower システムでは、ユーザのロールに基づいてユーザ特権を割り当てることができます。たとえば、アナリストに対して Security Analyst や Discovery Admin などの事前定義ロールを付与し、Firepower システムを管理するセキュリティ管理者に対して Administrator ロールを予約することができます。また、組織のニーズに合わせて調整されたアクセス権限を含むカスタムユーザ ロールを作成することもできます。

管理対象デバイスのプラットフォーム設定ポリシーでは、そのデバイスからの外部で認証されたすべてのユーザのデフォルト アクセス ロールを設定します。外部認証ユーザの初回ログイン後に、[ユーザ管理 (User Management)] ページでそのユーザのアクセス権を追加または削除できます。ユーザの権限を変更しない場合、そのユーザにはデフォルトで付与される権限のみが設定されます。内部認証ユーザは手動で作成されるため、内部認証ユーザの作成時にアクセス権を設定します。

LDAP グループを使用したアクセス権の管理を設定した場合、ユーザのアクセス権は LDAP グループのそのメンバーシップに基づきます。属しているグループの中で最も高いレベルのアクセスを持つグループのデフォルトアクセス権が付与されます。ユーザがどのグループにも属していない場合にグループアクセスを設定していた場合、ユーザには、LDAP サーバの認証オブジェクトで設定されているデフォルト ユーザアクセス権が付与されます。グループアクセスを設定すると、それらの設定によってプラットフォーム設定ポリシーのデフォルトアクセス設定がオーバーライドされます。

同様に、RADIUS 認証オブジェクトの特定のユーザ ロールリストにユーザを割り当てると、1 つ以上のロールが相互に矛盾しない限り、割り当てられたすべてのロールがそのユーザに付与されます。2 つの相互に矛盾するロールのリストにユーザが含まれている場合、最も高いレベルのアクセスを持つロールが付与されます。ユーザがどのリストにも属しておらず、認証オブジェクトでデフォルト アクセス ロールを設定している場合、そのユーザにはそのデフォルト アクセス ロールが付与されます。認証オブジェクトでデフォルト アクセスを設定すると、それらの設定によってプラットフォーム設定ポリシーのデフォルトアクセス設定がオーバーライドされます。

マルチドメイン展開では、複数のドメインでユーザ ロールを割り当てることができます。たとえば、ユーザにグローバルドメインでは読み取り専用権限を割り当て、サブドメインでは管理者権限を割り当てることができます。

## 定義済みのユーザ ロール

Firepower System では、組織のニーズを満たすために、アクセス権限セットの範囲を提供する 10 の定義済みのユーザ ロールを含みます。7000 および 8000 シリーズ デバイスは、10 の定義済みユーザ ロールのうちの 3 つ（管理者、メンテナンス ユーザ、セキュリティアナリスト）のみにアクセスする点にご注意ください。

定義済みユーザ ロールは編集できませんが、カスタム ユーザ ロールの基準として、アクセス特権セットを使用できます。また、別のユーザ ロールに対して段階的に増やすように設定できません。

次の表では、利用可能な定義済みのロールを簡単に説明します。

### アクセス管理者 (Access Admin)

[ポリシー (Policies)] メニューでアクセス制御ポリシー機能や関連する機能へのアクセスが可能です。アクセス管理者は、ポリシーを展開できません。

### 管理者 (Administrator)

解析およびレポート機能、ルールおよびポリシーコンフィギュレーション機能、システム管理機能、すべてのメンテナンス機能へのアクセスが可能。管理者は、ポリシーを含むデバイスへの設定変更も展開できます。管理者は、すべてのメニューオプションにアクセスします。侵害された場合には、これらのセッションには高いセキュリティリスクが存在するため、ログインセッションがタイムアウトする可能性があります。

セキュリティ上の理由から、管理者ロールの使用を制限する必要があります。

### 検出管理者 (Discovery Admin)

[ポリシー (Policies)] メニューのネットワーク検出機能、アプリケーション検出機能、相関機能にアクセス可能。検出管理者は、ポリシーを展開できません。

### 外部データベースのユーザ (External Database User)

JDBCSSL 接続に対応しているアプリケーションを用いて、Firepower System データベースに対して読み取り専用のアクセスが可能。Firepower システム アプライアンスの認証を行うサードパーティのアプリケーションについては、システム設定内でデータベースへの

アクセスを有効にする必要があります。Web インターフェイスでは、外部データベースユーザは、[ヘルプ (Help)] メニューのオンラインヘルプ関連のオプションのみにアクセスできます。このロールの機能は、web インターフェイスに搭載されていないため、サポートやパスワードの変更を容易にするためにのみアクセスが可能です。

#### 侵入管理者 (Intrusion Admin)

[ポリシー (Policies)] メニューと [オブジェクト (Objects)] メニューの侵入ポリシー機能、侵入ルール機能、ネットワーク分析ポリシー機能のすべてにアクセスが可能です。侵入管理者は、ポリシーを展開できません。

#### メンテナンス ユーザ (Maintenance User)

監視機能やメンテナンス機能へのアクセスが可能です。メンテナンス ユーザは、[ヘルス (Health)] メニューや [システム (System)] メニューのメンテナンス関連オプションにアクセスできます。

#### ネットワーク管理者 (Network Admin)

[ポリシー (Policies)] メニューのアクセス制御機能、SSL インスペクション機能、DNS ポリシー機能、アイデンティティ ポリシー機能、および [デバイス (Devices)] メニューのデバイス設定機能へのアクセスが可能です。ネットワーク管理者は、デバイスへの設定の変更を展開できます。

#### セキュリティ アナリスト (Security Analyst)

セキュリティ イベント分析機能へのアクセスと [概要 (Overview)] メニュー、[分析 (Analysis)] メニュー、[ヘルス (Health)] メニュー、[システム (System)] メニューのヘルス イベントに対する読み取り専用のアクセスが可能です。

#### セキュリティ アナリスト (読み取り専用) (Security Analyst (Read Only))

[概要 (Overview)] メニュー、[分析 (Analysis)] メニュー、[ヘルス (Health)] メニュー、[システム (System)] メニューのセキュリティ イベント分析機能とヘルス イベント機能への読み取り専用アクセスを提供します。

#### セキュリティ承認者 (Security Approver)

[ポリシー (Policies)] メニューのアクセス制御ポリシーや関連のあるポリシー、ネットワーク検出ポリシーへの制限付きのアクセスが可能です。セキュリティ承認者はこれらのポリシーを表示し、展開できますが、ポリシーを変更することはできません。

外部認証ユーザは、他のロールを割当てられていない場合、LDAP または RADIUS 認証オブジェクトの設定やプラットフォーム設定に基づいて、最低限のアクセス権を有します。追加の権利を外部ユーザに割り当てることはできますが、最低限のアクセス権を削除するまたは変更するには、以下のタスクを実施する必要があります。

- ユーザを認証オブジェクトの1つのリストから別のリストに移動させるか、外部認証サーバのユーザの属性値またはグループ メンバーシップを変更します。
- プラットフォームの設定を更新します。
- ユーザ管理ページを使用して、ユーザアカウントからのアクセスを削除します。

### 関連トピック

[ユーザ アカウントの権限](#) (51 ページ)

## カスタム ユーザ ロール

事前定義ユーザロールの他に、特定の分野に特化したアクセス権限を含むカスタムユーザロールを作成できます。カスタム ユーザ ロールには、メニューベースのアクセス許可およびシステムアクセス許可の任意のセットを割り当てることができます。また、最初から独自に作成したり、事前定義されたユーザロールを基に作成したりできます。事前定義ユーザロールと同様に、カスタム ロールは外部認証ユーザのデフォルト ロールとして使用できます。事前定義ロールとは異なり、カスタム ロールは変更、削除できます。

選択可能なアクセス許可は階層構造になっており、Firepower システムのメニュー レイアウトに基づいています。アクセス許可にサブページが含まれているか、または単純なページアクセスよりも詳細なアクセス許可が含まれている場合、このアクセス許可は拡張可能です。その場合、親のアクセス許可によって、ページ ビュー アクセス、およびそのページの関連機能への詳細な子のアクセス権が付与されます。「管理 (Manage)」という単語が含まれているアクセス許可は、他のユーザが作成する情報を編集および削除できる権限を付与します。



### ヒント

メニュー構造に含まれていないページまたは機能の権限は、親または関連ページにより付与されます。たとえば、侵入ポリシーの変更 (Modify Intrusion Policy) 権限があれば、ネットワーク分析ポリシーの変更もできます。

カスタムユーザロールに制限付き検索を適用できます。これにより、イベントビューアでユーザに対して表示されるデータが制限されます。制限付き検索を設定するには、最初に、プライベートの保存済み検索を作成し、該当するメニューベースのアクセス許可の下で [制限付き検索 (Restricted Search)] ドロップダウンメニューからその検索を選択します。

Firepower Management Center でカスタム ユーザ ロールを設定するときには、すべてのメニューベースのアクセス許可を付与できます。管理対象デバイスでカスタム ユーザ ロールを設定するときには、デバイス機能に関連する一部のアクセス許可だけを使用できます。

[システム許可 (System Permissions)] で選択できるオプションでは、外部データベースに対してクエリを実行したり、対象ユーザロールのアクセス許可にエスケーションしたりすることができるユーザロールを作成できます。

オプションで、新しいカスタム ユーザ ロールを作成する代わりに、別のアプライアンスからカスタム ユーザ ロールをエクスポートし、ご使用のアプライアンスにインポートできます。インポートしたロールは、適用する前に、ニーズに合わせて編集できます。

### 関連トピック

[ユーザ アカウントの権限](#) (51 ページ)

[外部データベース アクセスの設定](#) (927 ページ)



## 例：カスタム ユーザ ロールとアクセス制御

アクセス制御関連機能のカスタム ユーザ ロールを作成して、Firepower システムのユーザのアクセス制御および関連付けられたポリシーの表示、変更権限の有無を指定できます。

次の表に、作成可能なカスタム ロールと例として挙げたロールでそれぞれ与えられるユーザ権限を示します。表にはそれぞれのカスタム ロールに必要な権限が記載されています。この例では、ポリシー承認者 (Policy Approver) はアクセスコントロールポリシーと侵入ポリシーの表示が可能です (変更はできません)。また、ポリシー承認者は設定の変更をデバイスに展開することもできます。

表 2: アクセス制御のカスタム ロールの例

カスタム ロールの権限	例：アクセスコントロール編集者 (Access Control Editor)	例：侵入およびネットワーク分析編集者 (Intrusion & Network Analysis Editor)	例：ポリシー承認者 (Policy Approver)
アクセス制御	Yes	No	Yes
アクセスコントロールポリシー (Access Control Policy)	Yes	No	Yes
アクセス制御ポリシーの変更 (Modify Access Control Policy)	Yes	No	No
侵入ポリシー (Intrusion Policy)	No	Yes	Yes
侵入ポリシーの変更 (Modify Intrusion Policy)	No	Yes	No
設定をデバイスに展開	No	No	Yes

## ユーザ アカウントの権限

ここでは、Firepower システムでの設定可能なユーザ アクセス許可と、それらのアクセス許可にアクセスできる事前定義ユーザロールの一覧を示します。管理対象デバイスでは使用できないアクセス許可があります。Firepower Management Center でのみ使用可能なアクセス許可には、そのようにマークが付いています。

### [概要 (Overview)] メニュー

次の表は、[概要 (Overview)] メニューの各オプションにアクセスするために必要なユーザロール特権と、ユーザロールがオプション内のサブ権限にアクセスできるかどうかを順に示しています。Security Approver、Discovery Admin、Intrusion Admin、Access Admin、Network Admin、

## [概要 (Overview) ]メニュー

および External Database User の各ロールには、[概要 (Overview) ]メニューでのアクセス許可がありません。

表 3: [概要 (Overview) ]メニュー

権限	管理	メンテナンス ユーザ	セキュリティアナリスト	セキュリティアナリスト (RO)
ダッシュボード	Yes	Yes	Yes	Yes
ダッシュボードの管理	Yes	No	No	No
[アプライアンス情報 (Appliance Information) ] ウィジェット	Yes	Yes	Yes	Yes
[アプライアンス ステータス (Appliance Status) ] ウィジェット (Management Center のみ)	Yes	Yes	Yes	Yes
[コリレーション イベント (Correlation Events) ] ウィジェット	Yes	No	Yes	Yes
[現行インターフェイス ステータス (Current Interface Status) ] ウィジェット	Yes	Yes	Yes	Yes
[現行セッション (Current Sessions) ] ウィジェット	Yes	No	No	No
[カスタム分析 (Custom Analysis) ] ウィジェット (Management Center のみ)	Yes	No	Yes	Yes
[ディスク使用率 (Disk Usage) ] ウィジェット	Yes	Yes	Yes	Yes
[インターフェイス トラフィック (Interface Traffic) ] ウィジェット	Yes	Yes	Yes	Yes

権限	管理	メンテナンス ユーザ	セキュリティアナリスト	セキュリティアナリスト (RO)
[侵入イベント (Intrusion Events) ] ウィジェット ( <i>Management Center</i> のみ)	Yes	No	Yes	Yes
[ネットワーク コリレーション (Network Correlation) ] ウィジェット ( <i>Management Center</i> のみ)	Yes	No	Yes	Yes
[製品ライセンス (Product Licensing) ] ウィジェット ( <i>Management Center</i> のみ)	Yes	Yes	No	No
[製品の更新 (Product Updates) ] ウィジェット	Yes	Yes	No	No
[RSS フィード (RSS Feed) ] ウィジェット	Yes	Yes	Yes	Yes
[システムの負荷 (System Load) ] ウィジェット	Yes	Yes	Yes	Yes
[システム時刻 (System Time) ] ウィジェット	Yes	Yes	Yes	Yes
[ホワイトリストイベント (White List Events) ] ウィジェット ( <i>Management Center</i> のみ)	Yes	No	Yes	Yes
[レポート (Reporting) ] ( <i>Management Center</i> のみ)	Yes	No	Yes	Yes

## [概要 (Overview) ]メニュー

権限	管理	メンテナンス ユーザ	セキュリティアナリスト	セキュリティアナリスト (RO)
[レポートの管理テンプレート (Manage Report Templates) ] ( <i>Management Center</i> のみ)	Yes	No	Yes	Yes
要約	Yes	No	Yes	Yes
[侵入イベント統計 (Intrusion Event Statistics) ] ( <i>Management Center</i> のみ)	Yes	No	Yes	Yes
侵入イベントパフォーマンス (Intrusion Event Performance)	Yes	No	No	No
[侵入イベント グラフ (Intrusion Event Graphs) ] ( <i>Management Center</i> のみ)	Yes	No	Yes	Yes
[検出統計情報 (Discovery Statistics) ] ( <i>Management Center</i> のみ)	Yes	No	Yes	Yes
[ディスカバリ パフォーマンス (Discovery Performance) ] ( <i>Management Center</i> のみ)	Yes	No	No	No
[接続の概要 (Connection Summary) ] ( <i>Management Center</i> のみ)	Yes	No	Yes	Yes

## [分析 (Analysis)] メニュー

次の表に、[分析 (Analysis)] メニューの各オプションにアクセスするために必要なユーザーロール特権と、そのユーザーロールがオプション内のサブ権限にアクセスできるかどうかを順に示します。異なる見出しの下に複数回出現する権限は、最初に出現する表にのみ示されています。ただし、サブメニューの見出しを示す場合を除きます。Security Approver、Intrusion Admin、Access Admin、Network Admin、および External Database User の各ロールには、[分析 (Analysis)] メニューに対する権限はありません。[分析 (Analysis)] メニューは Firepower Management Center でのみ使用可能です。

表 4: [分析 (Analysis)] メニュー

メニュー	管理	検出管理者	メンテナンスユーザ	セキュリティアナリスト	セキュリティアナリスト (RO)
コンテキストエクスプローラ (Context Explorer)	Yes	No	No	Yes	Yes
接続イベント	Yes	No	No	Yes	Yes
接続イベントの変更 (Modify Connection Events)	Yes	No	No	Yes	No
接続サマリーイベント (Connection Summary Events)	Yes	No	No	Yes	Yes
接続サマリーイベントの変更 (Modify Connection Summary Events)	Yes	No	No	Yes	No
セキュリティインテリジェンスイベント	Yes	No	No	Yes	Yes
セキュリティインテリジェンスイベントの変更 (Modify Security Intelligence Events)	Yes	No	No	Yes	No
侵入 (Intrusion)	Yes	No	No	Yes	Yes

## [分析 (Analysis) ]メニュー

メニュー	管理	検出管理者	メンテナンスユーザ	セキュリティアナリスト	セキュリティアナリスト (RO)
侵入イベント	Yes	No	No	Yes	Yes
侵入イベントの変更 (Modify Intrusion Events)	Yes	No	No	Yes	No
ローカルルールの表示 (View Local Rules)	Yes	No	No	Yes	Yes
確認済みイベント (Reviewed Events)	Yes	No	No	Yes	Yes
クリップボード (Clipboard)	Yes	No	No	Yes	Yes
[インシデント (Incidents) ]	Yes	No	No	Yes	Yes
インシデントの変更 (Modify Incidents)	Yes	No	No	Yes	No
ファイル (Files)	Yes	No	No	Yes	Yes
マルウェアイベント	Yes	No	No	Yes	Yes
マルウェアイベントの変更 (Modify Malware Events)	Yes	No	No	Yes	No
ファイルイベント	Yes	No	No	Yes	Yes
ファイルイベントの変更 (Modify File Events)	Yes	No	No	Yes	No
キャプチャファイル (Captured Files)	Yes	No	No	Yes	Yes

メニュー	管理	検出管理者	メンテナンスユーザ	セキュリティアナリスト	セキュリティアナリスト (RO)
キャプチャファイル (Captured Files) の編集 (Modify Captured Files)	Yes	No	No	Yes	No
File Trajectory	Yes	No	No	Yes	Yes
ファイルのダウンロード (File Download)	Yes	No	No	Yes	Yes
ダイナミックファイル分析 (Dynamic File Analysis)	Yes	No	No	Yes	No
<b>Hosts</b>	Yes	No	No	Yes	Yes
ネットワークマップ (Network Map)	Yes	No	No	Yes	Yes
Hosts	Yes	No	No	Yes	Yes
ホストの変更 (Modify Hosts)	Yes	No	No	Yes	No
Indications of Compromise	Yes	No	No	Yes	Yes
侵害の兆候の変更 (Modify Indications of Compromise)	Yes	No	No	Yes	No
サーバ	Yes	No	No	Yes	Yes
サーバの変更 (Modify Servers)	Yes	No	No	Yes	No
脆弱性 (Vulnerabilities)	Yes	No	No	Yes	Yes
脆弱性の変更 (Modify Vulnerabilities)	Yes	No	No	Yes	No

メニュー	管理	検出管理者	メンテナンスユーザ	セキュリティアナリスト	セキュリティアナリスト (RO)
ホスト属性 (Host Attributes)	Yes	No	No	Yes	Yes
ホスト属性の変更 (Modify Host Attributes)	Yes	No	No	Yes	No
アプリケーション	Yes	No	No	Yes	Yes
アプリケーション詳細 (Application Details)	Yes	No	No	Yes	Yes
アプリケーションの詳細の変更 (Modify Application Details)	Yes	No	No	Yes	No
ホスト属性の管理 (Host Attribute Management)	Yes	No	No	No	No
検出イベント (Discovery Events)	Yes	No	No	Yes	Yes
検出イベントの変更 (Modify Discovery Events)	Yes	No	No	Yes	No
<b>Users</b>	Yes	Yes	No	Yes	Yes
ユーザアクティビティ (User Activity)	Yes	Yes	No	Yes	Yes
ユーザアクティビティイベントの変更 (Modify User Activity Events)	Yes	Yes	No	Yes	No
Users	Yes	Yes	No	Yes	Yes
ユーザの変更 (Modify Users)	Yes	Yes	No	Yes	No



メニュー	管理	検出管理者	メンテナンスユーザ	セキュリティアナリスト	セキュリティアナリスト (RO)
脆弱性 (Vulnerabilities)	Yes	No	No	Yes	Yes
サードパーティの脆弱性 (Third-party Vulnerabilities)	Yes	No	No	Yes	Yes
サードパーティの脆弱性の変更 (Modify Third-party Vulnerabilities)	Yes	No	No	Yes	No
相関 (Correlation)	Yes	Yes	No	Yes	Yes
相関イベント (Correlation Events)	Yes	Yes	No	Yes	Yes
相関イベントの変更 (Modify Correlation Events)	Yes	Yes	No	Yes	No
ホワイトリストイベント (White List Events)	Yes	Yes	No	Yes	Yes
ホワイトリストイベントの変更 (Modify White List Events)	Yes	Yes	No	Yes	No
ホワイトリスト違反 (White List Violations)	Yes	Yes	No	Yes	Yes
修復ステータス (Remediation Status)	Yes	Yes	No	No	No
修復ステータスの変更 (Modify Remediation Status)	Yes	Yes	No	No	No

## [分析 (Analysis)] メニュー

メニュー	管理	検出管理者	メンテナンスユーザ	セキュリティアナリスト	セキュリティアナリスト (RO)
カスタム (Custom)	Yes	No	No	Yes	Yes
カスタムワークフロー (Custom Workflows)	Yes	No	No	Yes	Yes
カスタムワークフローの管理 (Manage Custom Workflows)	Yes	No	No	Yes	Yes
カスタムテーブル (Custom Tables)	Yes	No	No	Yes	Yes
カスタムテーブルの管理 (Manage Custom Tables)	Yes	No	No	Yes	Yes
検索 (Search)	Yes	No	Yes	Yes	Yes
検索の管理 (Manage Search)	Yes	No	No	No	No
ブックマーク (Bookmarks)	Yes	No	No	Yes	Yes
ブックマークの管理 (Manage Bookmarks)	Yes	No	No	Yes	Yes
アプリケーション統計 (Application Statistics)	Yes	No	No	Yes	Yes
地理位置情報の統計 (Geolocation Statistics)	Yes	No	No	Yes	Yes
ユーザ統計 (User Statistics)	Yes	No	No	Yes	Yes
URL カテゴリ統計 (URL Category Statistics)	Yes	No	No	Yes	Yes

メニュー	管理	検出管理者	メンテナンスユーザ	セキュリティアナリスト	セキュリティアナリスト (RO)
URL レピュテーション統計 (URL Reputation Statistics)	Yes	No	No	Yes	Yes
レコードタイプ別 DNS クエリ (DNS Queries by Record Types)	Yes	No	No	Yes	Yes
SSL 統計 (SSL Statistics)	Yes	No	No	Yes	Yes
アプリケーション別侵入イベント統計 (Intrusion Event Statistics by Application)	Yes	No	No	Yes	Yes
ユーザ別侵入イベント統計 (Intrusion Event Statistics by User)	Yes	No	No	Yes	Yes
セキュリティインテリジェンスカテゴリ統計 (Security Intelligence Category Statistics)	Yes	No	No	Yes	Yes
性質別ファイルストレージ統計 (File Storage Statistics by Disposition)	Yes	No	No	Yes	Yes
タイプ別ファイルストレージ統計 (File Storage Statistics by Type)	Yes	No	No	Yes	Yes
ダイナミックファイル分析統計 (Dynamic File Analysis Statistics)	Yes	No	No	Yes	Yes

## ポリシーメニュー

次の表には、ポリシーメニューのそれぞれのオプションへのアクセスに必要なユーザロールの権限や、ユーザロールがポリシーメニューのサブパーミッションにアクセス可能であることを順番に示します。外部データベースユーザ、メンテナンスユーザ、セキュリティアナリスト、セキュリティアナリスト（読取り専用）ロールには、ポリシーメニューの権限はありません。ポリシーメニューは、Firepower Management Center でのみ利用可能です。

侵入ポリシーおよび「侵入ポリシーの変更」の権限により、ネットワークアナリシスポリシーの作成および変更が可能になる点にご注意ください。

表 5: ポリシーメニュー

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
アクセス制御	Yes	Yes	No	No	Yes	Yes
アクセスコントロールポリシー (Access Control Policy)	Yes	Yes	No	No	Yes	Yes
アクセス制御ポリシーの変更 (Modify Access Control Policy)	Yes	Yes	No	No	Yes	No
管理者ルールの変更 (Modify Administrator Rules)	Yes	Yes	No	No	Yes	No
ルートルールの変更 (Modify Root Rules)	Yes	Yes	No	No	Yes	No
侵入ポリシー (Intrusion Policy)	No	Yes	No	Yes	No	Yes
侵入ポリシーの変更 (Modify Intrusion Policy)	No	Yes	No	Yes	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
マルウェア & ファイル ポリシー (Malware & File Policy)	Yes	Yes	No	No	No	Yes
マルウェア & ファイル ポリシーの変更 (Modify Malware & File Policy)	Yes	Yes	No	No	No	No
DNS ポリシー (DNS Policy)	Yes	Yes	No	No	Yes	Yes
DNS ポリシーの変更 (Modify DNS Policy)	Yes	Yes	No	No	Yes	No
アイデンティティ ポリシー (Identity Policy)	Yes	Yes	No	No	Yes	No
アイデンティティ ポリシーの変更 (Modify Identity Policy)	Yes	Yes	No	No	Yes	No
管理者ルールの変更 (Modify Administrator Rules)	Yes	Yes	No	No	Yes	No
ルート ルールの変更 (Modify Root Rules)	Yes	Yes	No	No	Yes	No
SSL ポリシー (SSL Policy)	Yes	Yes	No	No	Yes	Yes
SSL ポリシーの変更 (Modify SSL Policy)	Yes	Yes	No	No	Yes	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
管理者ルールの変更 (Modify Administrator Rules)	Yes	Yes	No	No	Yes	No
ルート ルールの変更 (Modify Root Rules)	Yes	Yes	No	No	Yes	No
プレフィルタポリシー (Prefilter Policy)	Yes	Yes	No	No	Yes	Yes
プレフィルタポリシーの変更 (Modify Prefilter Policy)	Yes	Yes	No	No	Yes	No
ネットワークディスカバリ (Network Discovery)	No	Yes	Yes	No	No	Yes
カスタムフィンガープリント (Custom Fingerprinting)	No	Yes	Yes	No	No	No
カスタムフィンガープリントの変更 (Modify Custom Fingerprinting)	No	Yes	Yes	No	No	No
カスタムトポロジ (Custom Topology)	No	Yes	Yes	No	No	No
カスタムトポロジの変更 (Modify Custom Topology)	No	Yes	No	No	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
ネットワーク検出の変更 (Modify Network Discovery)	No	Yes	Yes	No	No	No
アプリケーションディテクタ (Application Detectors)	No	Yes	Yes	No	No	No
アプリケーションディテクタの変更 (Modify Application Detectors)	No	Yes	Yes	No	No	No
ユーザサードパーティマッピング (User 3rd Party Mappings)	No	Yes	Yes	No	No	No
ユーザサードパーティマッピングの変更 (Modify User 3rd Party Mappings)	No	Yes	No	No	No	No
カスタム製品のマッピング (Custom Product Mappings)	No	Yes	Yes	No	No	No
カスタム製品マッピングの変更 (Modify Custom Product Mappings)	No	Yes	No	No	No	No
相関 (Correlation)	No	Yes	No	No	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
ポリシーの管理 (Policy Management)	No	Yes	No	No	No	No
ポリシーの管理 の変更 (Modify Policy Management)	No	Yes	Yes	No	No	No
ルールの管理 (Rule Management)	No	Yes	No	No	No	No
ルールの管理の 変更 (Modify Rule Management)	No	Yes	Yes	No	No	No
ホワイトリスト (White List)	No	Yes	No	No	No	No
ホワイトリスト の変更 (Modify White List)	No	Yes	Yes	No	No	No
トラフィック プロファイル (Traffic Profiles)	No	Yes	No	No	No	No
トラフィック プロファイルの 変更 (Modify Traffic Profiles)	No	Yes	Yes	No	No	No
アクション (Actions)	No	Yes	Yes	No	No	Yes
アラート (Alerts)	No	Yes	Yes	No	No	Yes
影響度フラグ アラート (Impact Flag Alerts)	No	Yes	Yes	No	No	No



メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
影響度フラグアラートの変更 (Modify Impact Flag Alerts)	No	Yes	Yes	No	No	No
検出イベントアラート (Discovery Event Alerts)	No	Yes	Yes	No	No	No
検出イベントアラートの変更 (Modify Discovery Event Alerts)	No	Yes	Yes	No	No	No
E メール	No	Yes	No	Yes	No	No
Eメールの変更 (Modify Email)	No	Yes	No	Yes	No	No
アラートの変更 (Modify Alerts)	No	Yes	Yes	No	No	No
スキャナ (Scanners)	No	Yes	Yes	No	No	No
スキャン結果 (Scan Results)	No	Yes	Yes	No	No	No
スキャン結果の変更 (Modify Scan Results)	No	Yes	Yes	No	No	No
スキャナの変更 (Modify Scanners)	No	Yes	Yes	No	No	No
グループ (Groups)	No	Yes	No	No	No	No
グループの変更 (Modify Groups)	No	Yes	Yes	No	No	No

## [デバイス (Devices) ]メニュー

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
モジュール (Modules)	No	Yes	No	No	No	No
モジュールの変更 (Modify Modules)	No	Yes	Yes	No	No	No
インスタンス (Instances)	No	Yes	No	No	No	No
インスタンスの変更 (Modify Instances)	No	Yes	Yes	No	No	No

## [デバイス (Devices) ]メニュー

[Devices (デバイス) ]メニューの表には、[デバイス (Devices) ]メニューの各オプションとそのサブ権限にアクセスするために必要なユーザロール特権を順に示します。検出管理者、外部データベースユーザ、侵入管理者、メンテナンスユーザ、セキュリティアナリスト、セキュリティアナリスト (読取り専用) ロールには、ポリシーメニューの権限はありません。[デバイス (Devices) ]メニューは Firepower Management Center でのみ使用可能です。

表 6:[デバイス (Devices) ]メニュー

メニュー	アクセス管理者	管理者	ネットワーク管理者	セキュリティ承認者
デバイス管理	No	Yes	Yes	Yes
デバイスの変更 (Modify Devices)	No	Yes	Yes	No
<b>NAT</b>	Yes	Yes	Yes	Yes
NAT リスト (NAT List)	Yes	Yes	Yes	Yes
NAT ポリシーの変更 (Modify NAT Policy)	Yes	Yes	Yes	No
<b>VPN</b>	No	Yes	Yes	Yes
VPN の変更 (Modify VPN)	No	Yes	Yes	No
<b>QoS</b>	Yes	Yes	Yes	No
QoS ポリシーの変更 (Modify QoS Policy)	Yes	Yes	Yes	No
デバイス管理	No	Yes	Yes	No

メニュー	アクセス管理者	管理者	ネットワーク管理者	セキュリティ承認者
デバイスの変更 (Modify Devices)	No	Yes	Yes	No

## [オブジェクトマネージャ (Object Manager) ]メニュー

[オブジェクトマネージャ (Object Manager) ]メニューの表には、[オブジェクトマネージャ (Object Manager) ]メニューの各オプションとそのサブ権限にアクセスするために必要なユーザロール特権を順に示します。Discovery Admin、Security Approver、Maintenance User、External Database User、Security Analyst、および Security Analyst (読み取り専用) の各ロールには、[オブジェクトマネージャ (Object Manager) ]メニューでのアクセス許可がありません。[オブジェクトマネージャ (Object Manager) ]メニューは Firepower Management Center でのみ使用可能です。

表 7: [オブジェクトマネージャ (Object Manager) ]メニュー

メニュー	アクセス管理者	管理者	侵入管理者	ネットワーク管理者
[オブジェクトマネージャ (Object Manager) ]	Yes	Yes	No	Yes
[ルールエディタ (Rule Editor) ]	No	Yes	Yes	No
[ルールエディタの変更 (Modify Rule Editor) ]	No	Yes	Yes	No
NAT リスト (NAT List)	Yes	Yes	No	Yes
[オブジェクトマネージャの変更 (Modify Object Manager) ]	No	Yes	No	No

## Cisco AMP

Cisco AMP 権限は、Administrator ユーザロールのみに対して使用可能です。この権限は、Firepower Management Center でのみ使用可能です。

## デバイスへの設定の展開

デバイスに設定を展開する権限は、Administrator、Network Admin、および Security Approver のロールで使用できます。この権限は、Firepower Management Center でのみ使用可能です。

## [システム (System) ]メニュー

次の表は、[システム (System) ]メニューの各オプションにアクセスするために必要なユーザロール特権と、ユーザロールがオプション内のサブ権限にアクセスできるかどうかを順に示します。外部データベースユーザロールには、[システム (System) ]メニューへのアクセス許可が与えられません。

表 8:[システム (System) ]メニュー

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	メンテナンスユーザ	ネットワーク管理者	セキュリティ承認者	セキュリティアナリスト	セキュリティアナリスト (RO)
設定 ( <i>Configuration</i> )	No	Yes	No	No	No	No	No	No	No
ドメイン ( <i>Domains</i> )	No	Yes	No	No	No	No	No	No	No
統合	No	Yes	No	No	No	Yes	Yes	No	No
Cisco CSI	Yes	Yes	No	No	No	Yes	Yes	No	No
アイデンティティレルム ( <i>Identity Realms</i> ) ( <i>Management Center</i> のみ)	Yes	Yes	No	No	No	Yes	Yes	No	No
アイデンティティレルムを変更 ( <i>Modify Identity Realms</i> ) ( <i>Management Center</i> のみ)	Yes	Yes	No	No	No	Yes	No	No	No

メニュー	アクセス 管理者	管理者	検出管理 者	侵入管理 者	メンテナ ンスユー ザ	ネット ワーク管 理者	セキュリ ティ承認 者	セキュリ ティアナ リスト	セキュリ ティアナ リスト (RO)
アイデン ティティ ソース (Identity Sources) ( <i>Management Center</i> の み)	Yes	Yes	No	No	No	Yes	Yes	No	No
アイデン ティティ ソースを 変更 (Modify Identity Sources) ( <i>Management Center</i> の み)	Yes	Yes	No	No	No	Yes	No	No	No
eStreamer	No	Yes	No	No	No	No	No	No	No
ホスト入 力クライ アント (Host Input Client) ( <i>Management Center</i> の み)	No	Yes	No	No	No	No	No	No	No
スマート ソフト ウェアサ テライト (Smart Software Satellite) ( <i>Management Center</i> の み)	Yes	Yes	No	No	No	Yes	Yes	No	No

## [システム (System) ]メニュー

メニュー	アクセス 管理者	管理者	検出管理 者	侵入管理 者	メンテナ ンスユー ザ	ネット ワーク管 理者	セキュリ ティ承認 者	セキュリ ティアナ リスト	セキュリ ティアナ リスト (RO)
スマート ソフト ウェアサ テライト を変更 (Modify Smart Software Satellite) ( <i>Management Center</i> の み)	Yes	Yes	No	No	No	Yes	No	No	No
ユーザ管 理 (User Management)	No	Yes	No	No	No	No	No	No	No
Users	No	Yes	No	No	No	No	No	No	No
ユーザの 役割	No	Yes	No	No	No	No	No	No	No
外部認証 (External Authentication) ( <i>Management Center</i> の み)	No	Yes	Yes	No	No	No	No	No	No
変更点	No	Yes	No	No	No	No	No	No	No
ルール更 新 (Rule Updates) ( <i>Management Center</i> の み)	No	Yes	No	Yes	No	No	No	No	No

メニュー	アクセス 管理者	管理者	検出管理 者	侵入管理 者	メンテナ ンスユー ザ	ネット ワーク管 理者	セキュリ ティ承認 者	セキュリ ティアナ リスト	セキュリ ティアナ リスト (RO)
ルール更 新のイン ポートロ グ (Rule Update Import Log) ( <i>Management Center</i> の み)	No	Yes	No	No	No	No	No	No	No
ライセン ス	No	Yes	No	No	No	No	No	No	No
スマート ライセン ス (Smart Licences)	No	Yes	No	No	No	No	No	No	No
スマート ライセン スの変更 (Modify Smart Licenses)	No	Yes	No	No	No	No	No	No	No
クラシッ クライセ ンス (Classic Licenses)	No	Yes	No	No	No	No	No	No	No
正常性 (Health) ( <i>Management Center</i> の み)	No	Yes	No	No	Yes	No	No	Yes	Yes

## [システム (System) ]メニュー

メニュー	アクセス 管理者	管理者	検出管理 者	侵入管理 者	メンテナ ンスユー ザ	ネット ワーク管 理者	セキュリ ティ承認 者	セキュリ ティアナ リスト	セキュリ ティアナ リスト (RO)
正常性ポ リシー (Health Policy) ( <i>Management Center</i> の み)	No	Yes	No	No	Yes	No	No	Yes	No
正常性ポ リシーを 変更 (Modify Health Policy) ( <i>Management Center</i> の み)	No	Yes	No	No	Yes	No	No	Yes	No
正常性ポ リシーを 適用 (Apply Health Policy) ( <i>Management Center</i> の み)	No	Yes	No	No	Yes	No	No	Yes	No
ヘルスイ ベント (Health Events) ( <i>Management Center</i> の み)	No	Yes	No	No	Yes	No	No	Yes	Yes



メニュー	アクセス 管理者	管理者	検出管理 者	侵入管理 者	メンテナ ンスユー ザ	ネット ワーク管 理者	セキュリ ティ承認 者	セキュリ ティアナ リスト	セキュリ ティアナ リスト (RO)
ヘルスイ ベントを 変更 (Modify Health Events) ( <i>Management Center</i> の み)	No	Yes	No	No	Yes	No	No	Yes	No
モニタリ ング ( <b>Monitoring</b> )	No	Yes	No	No	Yes	Yes	Yes	Yes	No
監査 (Audit)	No	Yes	No	No	Yes	No	No	No	No
監査ログ を変更 (Modify Audit Log)	No	Yes	No	No	Yes	No	No	No	No
Syslog	No	Yes	No	No	Yes	No	No	No	No
統計情報 (Statistics)	No	Yes	No	No	Yes	No	No	No	No
ツール	No	Yes	No	No	Yes	No	No	Yes	No
バック アップ管 理 (Backup Management)	No	Yes	No	No	Yes	No	No	No	No
バック アップを 復元 (Restore Backup)	No	Yes	No	No	Yes	No	No	No	No

## [REST VDI] メニュー

メニュー	アクセス 管理者	管理者	検出管理 者	侵入管理 者	メンテナ ンスユー ザ	ネット ワーク管 理者	セキュリ ティ承認 者	セキュリ ティアナ リスト	セキュリ ティアナ リスト (RO)
スケ ジューリ ング (Scheduling)	No	Yes	No	No	Yes	No	No	No	No
その他の ユーザの スケ ジュール 済みタス クを削除 (Delete Other Users' Scheduled Tasks)	No	Yes	No	No	No	No	No	No	No
インポー ト/エクス ポート (Import/Export)	No	Yes	No	No	No	No	No	No	No
ディスカ バリデー タの消去 (Discovery Data Purge) (Management Center の み)	No	Yes	No	No	No	No	No	Yes	No
whois (Management Center の み)	No	Yes	No	No	Yes	No	No	Yes	Yes

## [REST VDI] メニュー

[REST VDI] メニュー テーブルには、REST VDI メニューのそれぞれのオプションにアクセスするのに必要なユーザロールの特権とその中のサブパーミッションを順番に列挙します。検出

管理者、外部データベース ユーザ、侵入管理者、メンテナンス ユーザ、セキュリティ アナリスト、セキュリティアナリスト (読取り専用) ロールには、ポリシー メニューの権限はありません。[デバイス (Devices) ]メニューは Firepower Management Center でのみ使用可能です。

表 9: REST VDI メニュー

メニュー	アクセス管理者	管理者	ネットワーク管理者	セキュリティ承認者
REST VDI	Yes	Yes	Yes	Yes
REST VDI の変更	Yes	Yes	Yes	No

## [ヘルプ (Help) ]メニュー

[ヘルプ (Help) ]メニューとその権限には、すべてのユーザ ロールがアクセスできます。[ヘルプ (Help) ]メニュー オプションを制限することはできません。

## ユーザ ロールの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

Firepower システムの各ユーザは、ユーザ アクセス ロール (1 つまたは複数) に関連付けられています。これに該当するユーザ ロールには、システムのメニューなどのオプションへのアクセスを決定する権限が割り当てられます。たとえばアナリストは、ネットワークのセキュリティを分析するためにイベント データへのアクセスが必要ですが、Firepower システム自体の管理機能へのアクセスが必要になることはありません。アナリストには Security Analyst のアクセス権を付与し、Firepower システムを管理する 1 人以上のユーザに対して Administrator ロールを予約しておくことができます。

Firepower システムには、さまざまな管理者およびアナリスト用に設計された 10 個の事前定義のユーザ ロールが用意されています。これらの事前定義のユーザ ロールには、事前設定されたアクセス権限のセットが含まれています。

より詳細なアクセス権限を使用して、カスタムのユーザ ロールを作成することもできます。

また、あるユーザ ロールがイベントビューアで表示できるデータを制限するために、そのロールに制限付きの検索を適用することもできます。制限付きアクセスを使用してカスタムロールを作成するには、[権限に基づくメニュー (Menu Based Permissions) ]リストから制限するテーブルを選択し、次に[制限付き検索 (Restrictive Search) ]ドロップダウンリストからプライベート保存検索を選択します。

事前定義のユーザ ロールは削除できませんが、不要になったカスタムロールは削除できます。カスタムロールを完全に削除することなく無効にするには、削除する代わりに非アクティブ化します。自分のユーザ ロール、またはプラットフォーム設定ポリシーでデフォルトユーザ ロールとして設定されているロールは削除できない点に注意してください。

## 手順

ステップ1 [システム (System) ] > [ユーザ (Users) ] を選択します。

ステップ2 [ユーザロール (User Roles) ] タブをクリックします。

ステップ3 ユーザ ロールを管理します。

- アクティブ化：事前定義されたユーザ ロールをアクティブ化または非アクティブ化します。詳細については、[ユーザ ロールのアクティブおよび非アクティブの設定 \(78 ページ\)](#) を参照してください。
- 作成：カスタム ユーザ ロールを作成します。詳細については、[カスタム ユーザ ロールの作成 \(79 ページ\)](#) を参照してください。
- コピー：新しいカスタム ユーザ ロールを作成するために、既存のユーザ ロールをコピーします。詳細については、[ユーザ ロールのコピー \(80 ページ\)](#) を参照してください。
- 編集：カスタム ユーザ ロールを編集します。詳細については、[カスタム ユーザ ロールの編集 \(81 ページ\)](#) を参照してください。
- 削除：削除するカスタム ロールの横にある削除アイコン (🗑️) をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- (注) 削除されたロールが、特定のユーザに割り当てられていた唯一のロールである場合、そのユーザはログインして [ユーザ設定 (User Preferences) ] メニューにアクセスできますが、Firepower システムにはアクセスできなくなります。

## ユーザ ロールのアクティブおよび非アクティブの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

事前定義ユーザロールは削除できませんが、非アクティブにすることができます。ロールを非アクティブにすると、そのロールが割り当てられているすべてのユーザから、そのロールと関連するアクセス許可が削除されます。

マルチドメイン展開では、現在のドメインで作成されたカスタム ユーザ ロールが表示されます。これは編集できます。先祖ドメインで作成されたカスタム ユーザ ロールも表示されますが、これは編集できません。下位のドメインのカスタム ユーザ ロールを表示および編集するには、そのドメインに切り替えます。



**注意** 非アクティブにされたロールが、特定のユーザに割り当てられていた唯一のロールである場合、そのユーザはログインして [User Preferences] メニューにアクセスできますが、Firepower System にはアクセスできません。

### 手順

**ステップ 1** [システム (System)] > [ユーザ (Users)] を選択します。

**ステップ 2** [ユーザロール (User Roles)] タブをクリックします。

**ステップ 3** アクティブまたは非アクティブにするユーザ ロールの横にあるスライダをクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

Lights-Out Management を含むロールが割り当てられているユーザがログインしているときに、このロールを非アクティブにしてから再度アクティブにする場合、またはユーザのログインセッション中にバックアップからユーザまたはユーザ ロールを復元する場合、そのユーザは Web インターフェイスに再度ログインして、IPMIttool コマンドへのアクセスを再度取得する必要があります。

## カスタム ユーザ ロールの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

### 手順

**ステップ 1** [システム (System)] > [ユーザ (Users)] を選択します。

**ステップ 2** [ユーザロール (User Roles)] タブをクリックします。

**ステップ 3** [ユーザロールの作成 (Create User Role)] をクリックします。

**ステップ 4** [名前 (Name)] フィールドに、新しいユーザ ロールの名前を入力します。ユーザ ロール名では、大文字と小文字が区別されます。

**ステップ 5** オプションで、[説明 (Description)] を追加します。

**ステップ 6** 新しいロールのメニューベースのアクセス許可を選択します。

アクセス許可を選択すると、その下位にあるアクセス許可もすべて選択され、複数値を持つアクセス許可では最初の値が使用されます。上位のアクセス許可をクリアすると、下位のアクセ

ス許可もすべてクリアされます。アクセス許可を選択しても、下位のアクセス許可を選択しない場合、アクセス許可がイタリックのテキストで表示されます。

カスタム ロールのベースとして使用する事前定義ユーザ ロールをコピーすると、その事前定義ロールに関連付けられているアクセス許可が事前選択されます。

- ステップ 7** 必要に応じて、[外部データベース アクセス (External Database Access)] チェックボックスをオンまたはオフにして、新規ロールのデータベース アクセス権限を設定します。
- ステップ 8** [エスカレーションに使用するカスタム ユーザ ロールの設定 \(83 ページ\)](#) の説明に従って、必要に応じて Firepower Management Center で、新規ユーザ ロールのエスカレーション アクセス許可を設定します。
- ステップ 9** [保存 (Save)] をクリックします。

## ユーザ ロールのコピー

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

新しいカスタムロールのベースとして使用する既存のロールをコピーできます。これにより、ユーザ ロール エディタで既存のロールの権限が事前に選択されるので、あるロールをモデルとして別のロールを作成できます。

事前定義されたユーザ ロールや先祖ドメインから継承されるカスタム ユーザ ロールなど、既存のロールをコピーできます。

### 手順

- ステップ 1** [システム (System)] > [ユーザ (Users)] を選択します。
- ステップ 2** [ユーザロール (User Roles)] タブをクリックします。
- ステップ 3** コピーするユーザ ロールの横にあるコピー アイコン (📄) をクリックします。
- ステップ 4** 新しい名前を入力します。

システムは、元のユーザ ロールの名前と (copy) サフィックスを組み合わせた新しいユーザ ロールのデフォルト名を作成します。

- ステップ 5** [説明 (Description)] ボックスに新しい説明を入力します。
- 上書きしないことを選択した場合、システムは元のユーザ ロールの説明を保持します。
- ステップ 6** オプションで、元のユーザ ロールから継承されたメニュー ベースの権限を変更します。

アクセス許可を選択すると、その下位にあるアクセス許可もすべて選択され、複数値を持つアクセス許可では最初の値が使用されます。上位のアクセス許可をクリアすると、下位のアクセ

ス許可もすべてクリアされます。アクセス許可を選択しても下位のアクセス許可を選択しない場合、そのアクセス許可はイタリック体のテキストで表示されます。

- ステップ 7** オプションで、[外部データベース アクセス (External Database Access)] チェックボックスをオンまたはオフにすることで、新しいロールのデータベース アクセス権を設定します。
- ステップ 8** オプションで、[エスカレーションに使用するカスタム ユーザ ロールの設定 \(83 ページ\)](#) の説明に従って、新しいユーザ ロールのエスカレーション権を設定します。
- ステップ 9** [保存 (Save)] をクリックします。

## カスタム ユーザ ロールの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

事前定義ユーザ ロールは編集できません。

マルチドメイン展開では、現在のドメインで作成されたカスタム ユーザ ロールが表示されます。これは編集できます。先祖ドメインで作成されたカスタム ユーザ ロールも表示されますが、これは編集できません。下位のドメインのカスタム ユーザ ロールを表示および編集するには、そのドメインに切り替えます。

### 手順

- ステップ 1** [システム (System)] > [ユーザ (Users)] を選択します。
- ステップ 2** [ユーザロール (User Roles)] タブをクリックします。
- ステップ 3** 変更するカスタム ユーザ ロールの横にある編集アイコン (✎) をクリックします。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 4** [名前 (Name)] フィールドと [説明 (Description)] フィールドを変更します。ユーザ ロール名では、大文字と小文字が区別されます。
- ステップ 5** ユーザ ロールのメニューベースのアクセス許可を選択します。
- アクセス許可を選択すると、その下位にあるアクセス許可もすべて選択され、複数値を持つアクセス許可では最初の値が使用されます。上位のアクセス許可をクリアすると、下位のアクセス許可もすべてクリアされます。アクセス許可を選択しても下位のアクセス許可を選択しない場合、そのアクセス許可はイタリック体のテキストで表示されます。
- ステップ 6** 必要に応じて、[外部データベース アクセス (External Database Access)] チェックボックスをオンまたはオフにすることにより、ロールのデータベース アクセス権を設定します。

**ステップ 7** 必要に応じて、[エスカレーションに使用するカスタムユーザ ロールの設定 \(83 ページ\)](#) の説明に従って Firepower Management Center で、ユーザ ロールにエスカレーション アクセス許可を設定します。

**ステップ 8** [保存 (Save) ] をクリックします。

## ユーザ ロールのエスカレーション

カスタム ユーザ ロールにアクセス許可を付与し、パスワードを設定することで、ベース ロールの特権に加え、別のターゲットユーザロールの特権を一時的に取得できます。これにより、あるユーザが不在であるときにそのユーザを別のユーザに容易に置き換えることや、拡張ユーザ特権の使用状況をさらに注意深く追跡することができます。

たとえば、ユーザのベースロールに含まれている特権が非常に限られている場合、そのユーザは管理アクションを実行するために Administrator ロールにエスカレーションする場合があります。この機能は、ユーザが各自のパスワードを使用したり、指定された別のユーザのパスワードを使用したりできるように設定できます。2 番目のオプションでは、該当するすべてのユーザのための 1 つのエスカレーションパスワードを容易に管理できます。

エスカレーションターゲットロールにすることができるユーザ ロールは一度に 1 つだけであることに注意してください。カスタム ユーザ ロールまたは事前定義ユーザ ロールを使用できます。各エスカレーションはログインセッション期間中保持され、監査ログに記録されます。

## エスカレーション ターゲット ロールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

各自のユーザ ロール（事前定義またはカスタム）をシステム全体でのエスカレーション ターゲットロールとして機能するように割り当てることができます。これは、他のロールからのエスカレーション先となるロールです（エスカレーションが可能な場合）。

### 手順

**ステップ 1** [システム (System) ] > [ユーザ (Users) ] を選択します。

**ステップ 2** [ユーザ ロール (User Roles) ] をクリックします。

**ステップ 3** [アクセス許可エスカレーションの設定 (Configure Permission Escalation) ] をクリックします。

**ステップ 4** ドロップダウン リストからユーザ ロールを選択します。

**ステップ 5** [OK] をクリックして変更を保存します。



- (注) エスカレーション ターゲット ロールの変更は即時に反映されます。エスカレーションされたセッションのユーザには、新しいエスカレーションターゲットのアクセス許可が付与されます。

## エスカレーションに使用するカスタム ユーザ ロールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

カスタム ロールのエスカレーション パスワードを設定するときには、部門のニーズを考慮してください。多数のエスカレーションユーザを容易に管理するには、別のユーザを選択し、そのユーザのパスワードをエスカレーション パスワードとして使用することができます。そのユーザのパスワードを変更するか、またはそのユーザを非アクティブにすると、そのパスワードを必要とするすべてのエスカレーションユーザが影響を受けます。このことにより、特に一元管理できる外部認証ユーザを選択した場合に、ユーザ ロール エスカレーションをより効率的に管理できます。

### 手順

- ステップ 1** [カスタム ユーザ ロールの作成 \(79 ページ\)](#) の説明に従って、カスタム ユーザ ロールの設定を開始します。
- ステップ 2** [システム権限 (System Permissions)] で、[このロールをエスカレーションする: (Set this role to escalate to:)] チェックボックスをオンにします。
- 現在のエスカレーション ターゲット ロールは、チェックボックスの横に表示されます。
- ステップ 3** このロールがエスカレーションするとき使用するパスワードを選択します。次の2つの対処法があります。
- このロールが割り当てられているユーザがエスカレーション時に各自のパスワードを使用できるようにするには、[割り当てられているユーザのパスワードで認証 (Authenticate with the assigned user's password)] を選択します。
  - このロールが割り当てられているユーザが、別のユーザのパスワードを使用するには、[指定されたユーザのパスワードで認証 (Authenticate with the specified user's password)] を選択し、そのユーザ名を入力します。

- (注) 別のユーザのパスワードで認証するときには、任意のユーザ名 (非アクティブなユーザまたは存在しないユーザを含む) を入力できます。エスカレーションにパスワードが使用されるユーザを非アクティブにすると、そのパスワードを必要とするロールが割り当てられているユーザのエスカレーションが不可能になります。この機能を使用して、必要に応じてエスカレーション機能をただちに削除できます。

**ステップ 4** [保存 (Save) ] をクリックします。

これで、このロールが割り当てられているユーザはターゲットユーザ ロールにエスカレーションできます。

## ユーザ ロールのエスカレーション

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	任意 (Any)	任意 (Any)

エスカレーション対象のアクセス許可が含まれているカスタム ユーザ ロールが割り当てられているユーザは、いつでもターゲットロールのアクセス許可にエスカレーションできます。エスカレーションはユーザ設定に影響しないことに注意してください。

### 始める前に

- 管理者が、[エスカレーション ターゲット ロールの設定 \(82 ページ\)](#) または [エスカレーションに使用するカスタム ユーザ ロールの設定 \(83 ページ\)](#) に従って、エスカレーション ターゲット ロールまたはカスタム ユーザ ロールをエスカレーション用に設定済みであることを確認してください。

### 手順

**ステップ 1** ユーザ名の下にあるドロップダウンリストから、[アクセス許可のエスカレーション (Escalate Permissions) ] を選択します。

**ステップ 2** 認証パスワードを入力します。

**ステップ 3** [エスカレート (Escalate) ] をクリックします。これで、現行ロールに加え、エスカレーション ターゲット ロールのすべてのアクセス許可が付与されました。

(注) エスカレーションはログインセッションの残り期間にわたって保持されます。ベースロールの特権だけに戻すには、ログアウトしてから新しいセッションを開始する必要があります。

## ユーザ アカウント

Firepower Management Center デバイスまたは Firepower 7000 および 8000 シリーズ デバイス上の管理者アカウント、およびオプションのカスタムのユーザアカウントを使用すれば、ユーザはこれらのデバイスにログインすることができます。内部認証ユーザについては、アカウント

を手動で作成する必要があります。外部認証ユーザについては、アカウントが自動的に作成されます。

Firepower Threat Defense の場合、個別の CLI ユーザを作成できます。これらのユーザは、SSH を通じてデバイスにアクセスして、追加のトラブルシューティングとシステムのモニタリングを行うことができます。ただし、これらのユーザは CLI で作成する必要があり、Firepower Management Center で作成することはできません。

#### 関連トピック

[Firepower システムのユーザ アカウント](#)

[Firepower システムのユーザ インターフェイス](#)

## ユーザ アカウントの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

#### 手順

**ステップ 1** [システム (System)] > [ユーザ (Users)] を選択します。

**ステップ 2** ユーザ アカウントを管理します。

- アクティブ化/非アクティブ化：ユーザの横にあるスライダをクリックすると、非アクティブ化されたユーザの場合は再アクティブ化され、アクティブなユーザアカウントの場合は削除せずに無効化されます。アクティブ化/非アクティブ化できるのは内部で認証されたユーザのみです。
- 作成：新しいユーザアカウントを作成します ([ユーザアカウントの作成 \(86 ページ\)](#) を参照)。
- 編集：既存のユーザアカウントを編集します ([ユーザアカウントの編集 \(87 ページ\)](#) を参照)。
- 削除：ユーザを削除する場合は、削除アイコン (■) をクリックします。admin アカウント以外のユーザアカウントはシステムからいつでも削除できます。admin アカウントは削除できません。

#### 関連トピック

[Lights-Out 管理のユーザ アクセス設定 \(990 ページ\)](#)

[定義済みのユーザ ロール \(48 ページ\)](#)

[カスタム ユーザ ロール \(50 ページ\)](#)

## ユーザ アカウントの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 7000 & 8000 シリーズ	任意 (Any)	Admin

新しいユーザアカウントをセットアップするときに、そのアカウントでアクセスできるシステムの部分を制御できます。ユーザアカウントの作成時に、ユーザアカウントのパスワードの有効期限と強度を設定できます。7000または8000シリーズデバイスのローカルアカウントの場合、ユーザに付与するコマンドラインアクセスのレベルも設定できます。

マルチドメイン型展開では、Admin アクセス権限があるドメインでユーザアカウントを作成できます。また、上位のドメインでアカウントを作成し、それよりも低いアクセス権のみをユーザに割り当てることもできます。たとえば、単一ユーザを2つのドメインの管理者にし、先祖のドメインへのアクセスは拒否することができます。このタイプのユーザアカウントは、アクセス権が割り当てられているサブドメインに切り替えることによるのみ変更することができます。

### 手順

**ステップ 1** [システム (System)] > [ユーザ (Users)] を選択します。

**ステップ 2** [ユーザの作成 (Create User)] をクリックします。

**ステップ 3** [ユーザ名 (User Name)] に入力します。

**ステップ 4** ログイン オプションを変更します ([ユーザ アカウント ログイン オプション \(89 ページ\)](#) を参照)。

**ステップ 5** [パスワード (Password)] と [パスワードの確認 (Confirm Password)] に値を入力します。

入力する値は、以前に設定したパスワード オプションに基づいている必要があります。

**ステップ 6** 7000 または 8000 シリーズ デバイスでユーザ アカウントを作成する場合、[コマンドラインのアクセス レベル \(91 ページ\)](#) の説明に従って、適切なレベルの [コマンドライン インターフェイス アクセス (Command-Line Interface Access)] を割り当てます。

**ステップ 7** 次のようにして、ユーザ ロールを割り当てます。

- ユーザに割り当てるユーザ ロールの横のチェックボックスをオンまたはオフにします。
- マルチドメイン展開では、子孫ドメインを持つドメインにユーザアカウントを追加する場合、ユーザ ロールのチェック ボックスの代わりに表示される [ドメインの追加 (Add Domains)] ボタンをクリックします。[複数のドメインでのユーザ ロールの割り当て \(88 ページ\)](#) の手順に従って進みます。

(注) ユーザロールによって、ユーザのアクセス権が決定します。詳細については、[ユーザロールの管理 \(77 ページ\)](#) を参照してください。

ステップ 8 [Save] をクリックします。

## ユーザ アカウントの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

システムにユーザアカウントを追加したら、アクセス権限、アカウントオプション、パスワードをいつでも変更できます。パスワード管理オプションは、外部ディレクトリサーバに対して認証されるユーザには適用されないことに注意してください。これらの設定は外部サーバで管理します。ただし、外部認証されるアカウントを含め、すべてのアカウントのアクセス権を設定する必要があります。



(注) 外部認証ユーザの場合、LDAP グループ メンバーシップ、RADIUS リスト メンバーシップ、または属性値によってアクセスロールが割り当てられているユーザの Firepower システム ユーザ管理ページでは、最小アクセス権を削除することができません。ただし、追加の権限を割り当てることはできます。外部認証ユーザのアクセス権を変更すると、[ユーザ管理 (User Management)] ページの [認証方式 (Authentication Method)] カラムに、[外部 - ローカルで変更済み (External - Locally Modified)] というステータスが表示されます。

ユーザの認証を外部認証から内部認証に変更した場合は、ユーザの新しいパスワードを指定する必要があります。

### 手順

ステップ 1 [システム (System)] > [ユーザ (Users)] を選択します。

ステップ 2 変更するユーザの横にある編集アイコン (✎) をクリックします。

ステップ 3 [ユーザ アカウントの作成 \(86 ページ\)](#) の説明に従って設定を変更します。

ステップ 4 [保存 (Save)] をクリックします。

## 複数のドメインでのユーザ ロールの割り当て

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

マルチドメイン展開では、先祖や子孫のドメインにユーザ ロールを割り当てることができます。たとえば、グローバルドメインでユーザに読み取り専用権限を割り当てながら、子孫ドメインに管理者権限を割り当てることができます。

### 手順

- 
- ステップ 1** ユーザアカウントエディタで、[ドメインの追加 (Add Domain)] をクリックします。
- ステップ 2** [ドメイン (Domain)] ドロップダウンリストからドメインを選択します。
- ステップ 3** ユーザを割り当てるユーザ ロールをオンにします。
- ステップ 4** [保存 (Save)] をクリックします。
- 

## 内部認証から外部認証へのユーザの変換

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin



- (注) 内部認証から外部認証にユーザを変換するとき、ユーザアカウントに設定されているアクセス許可が保持されます。既存のアクセス許可は、関連する認証オブジェクトグループまたはプラットフォーム設定ポリシーで設定されたデフォルトのユーザ ロールに関連付けられたすべてのアクセス許可より優先されます。
- 

### 始める前に

- 同じユーザ名を持つユーザ レコードが外部認証サーバに存在する必要があります。

### 手順

- 
- ステップ 1** LDAP (CAC を使用する場合または使用しない場合) あるいは RADIUS 認証を有効にします。詳細については、[LDAP 認証 \(97 ページ\)](#) または [RADIUS 認証 \(124 ページ\)](#) を参照してください。

**ステップ 2** 外部サーバに保存されているそのユーザのパスワードを使用してログインするようユーザに指示します。

## ユーザアカウント ログインオプション

次の表に、Firepower システム ユーザのパスワードおよびアカウント アクセスの調整に使用できるオプションの一部について説明します。



- (注)
- パスワード管理オプションは、外部ディレクトリサーバに対して認証されるユーザには適用されません。これらの設定は外部認証サーバで管理します。[外部認証方式を使用する (Use External Authentication Method)] を有効にすると、ディスプレイからパスワード管理オプションが削除されます。
  - アプライアンスでセキュリティ認定コンプライアンスまたは Lights-Out Management (LOM) を有効にすると、異なるパスワード制限が適用されます。セキュリティ認定コンプライアンスの詳細については、[セキュリティ認定準拠の \(976 ページ\)](#) を参照してください。

表 10: ユーザアカウント ログインオプション

オプション	説明
外部認証方式を使用する (Use External Authentication Method)	<p>このユーザの資格情報を外部で認証する場合に、このチェックボックスをオンにします。このオプションを有効にすると、パスワード管理オプションが表示されなくなります。</p> <p>(注)</p> <ul style="list-style-type: none"> <li>外部ディレクトリサーバに対してユーザを認証する場合は、使用するサーバの認証オブジェクトを作成し、認証が有効な状態でプラットフォーム設定ポリシーを適用します。</li> <li>外部認証ユーザの場合、サーバの認証オブジェクトを無効にすると、[ユーザ (Users)] リストの [認証方式 (Authentication Method)] カラムに [外部 (無効) (External (Disabled))] と表示されます。</li> <li>ユーザに対してこのオプションを選択した場合に外部認証サーバが使用できないと、そのユーザは Web インターフェイスにログインできますが、どの機能にもアクセスできません。</li> </ul>

オプション	説明
ログイン失敗の最大許容回数 (Maximum Number of Failed Logins)	各ユーザが、ログイン試行の失敗後に、アカウントがロックされるまでに試行できるログインの最大回数を示す整数を、スペースなしで入力します。デフォルト設定は5回です。ログイン失敗回数を無制限にするには、 <b>0</b> を設定します。
パスワード長の最小値 (Minimum Password Length)	ユーザのパスワードの必須最小長 (文字数) を示す整数を、スペースなしで入力します。デフォルト設定は <b>8</b> です。値 <b>0</b> は、最小長が必須ではないことを示します。 [パスワード強度のチェック (Check Password Strength) ] オプションを有効にして、[パスワード長の最小値 (Minimum Password Length) ] を8文字を超える値に設定すると、いずれか大きい値が適用されます。
パスワードの有効期限の残日数 (Days Until Password Expiration)	ユーザのパスワードの有効期限までの日数を入力します。デフォルト設定は、パスワードが期限切れにならないことを示す <b>0</b> です。このオプションを設定すると、[ユーザ (Users) ] リストの [パスワードのライフタイム (Password Lifetime) ] カラムに、各ユーザのパスワードの残っている日数が表示されます。
パスワードの有効期限の残日数警告 (Days Before Password Expiration Warning)	パスワードが実際に期限切れになる何日前に、ユーザがパスワードを変更する必要があるという警告を表示するかを入力します。デフォルト設定は <b>0</b> 日間です。  (注) 警告日数は、パスワードの残りの有効期間の日数 <b>未</b> 満である必要があります。
ログイン時にパスワードのリセットを強制 (Force Password Reset on Login)	次回ログイン時に、ユーザに強制的に各自のパスワードを変更させるには、このオプションを選択します。
パスワード強度のチェック (Check Password Strength)	強力なパスワードを必須にするには、このオプションを選択します。強力なパスワードとは、8文字以上の英数字からなり、大文字と小文字を使用し、1つ以上の数字と1つ以上の特殊文字を使用するパスワードです。辞書に記載されている単語や、同じ文字を連続して繰り返し使用することはできません。
ブラウザセッションタイムアウトから除外する (Exempt from Browser Session Timeout)	操作が行われなかったことが原因でユーザのログインセッションが終了しないようにするには、このオプションを選択します。管理者ロールが割り当てられているユーザを除外することはできません。



## コマンドラインのアクセス レベル

7000 または 8000 シリーズ デバイスでローカル Web インターフェイスを使用して、コマンドラインインターフェイスアクセスをローカルデバイスのユーザに割り当てることができます。NGIPSv ではコマンドラインアクセスをユーザに割り当てることもできますが、コマンドはコマンドラインインターフェイスから使用することに注意してください。

ユーザが実行できるコマンドは、ユーザに割り当てられているアクセスのレベルによって決まります。[コマンドラインインターフェイス アクセス (Command-Line Interface Access) ] 設定で指定できる値は、次のとおりです。

### なし (None)

ユーザは、コマンドラインでアプライアンスにログインすることはできません。ユーザが資格情報を入力すると、ユーザが開始したセッションがすべて終了します。ユーザ作成時に、アクセス レベルはデフォルトで [なし (None) ] に設定されます。

### 設定 (Configuration)

ユーザは、任意のコマンドライン オプションにアクセスできます。このアクセス レベルをユーザに割り当てるときには注意してください。



**注意** 外部認証ユーザに付与されるコマンドラインアクセスは、デフォルトで [設定 (Configuration) ] レベルのコマンドラインアクセスになり、すべてのコマンドラインユーティリティに対する権限が付与されます。

### 基本

特定の一連のコマンドはユーザが実行できます。それらは、次のとおりです。

表 11: 基本的なコマンドラインコマンド

configure password	interfaces
終了	lcd
exit	link-state
ヘルプ	log-ips-connection
history	managers
ログアウト	memory
?	model
??	mpls-depth
access-control-config	NAT
alarms	network

arp-tables	network-modules
audit-log	ntp
bypass	perfstats
high-availability	portstats
cpu	power-supply-status
データベース	process-tree
device-settings	processes
disk	routing-table
disk-manager	serial-number
dns	stacking
expert	summary
fan-status	時刻
fastpath-rules	traffic-statistics
gui	version
hostname	virtual-routers
hyperthreading	virtual-switches
inline-sets	

## Firepower Threat Defense の CLI ユーザ アカウントの作成

Firepower Threat Defense デバイスで CLI にアクセスするユーザを作成できます。これらのアカウントは管理アプリケーションへのアクセスは許可されず、CLI へのアクセスのみが有効になります。CLI はトラブルシューティングやモニタリング用に役立ちます。

複数のデバイス上にアカウントを一度に作成することはできません。デバイスごとに固有の CLI アカウントのセットがあります。

### 手順

**ステップ 1** config 権限を持つアカウントを使用してデバイスの CLI にログインします。

管理者ユーザアカウントには必要な権限がありますが、config 権限を持っていればどのアカウントでも問題ありません。SSH セッションまたはコンソールポートを使用できます。

特定のデバイスモデルでは、コンソールポートから FXOS CLI に移動します。connect ftd コマンドを使用して Firepower Threat Defense CLI にアクセスします。

**ステップ 2** ユーザ アカウントを作成します。

**configure user add *username* {basic | config}**

次の権限レベルを持つユーザを定義できます。

- **config** : ユーザに設定アクセス権を付与します。すべてのコマンドの管理者権限がユーザに与えられます。
- **basic** : ユーザに基本的なアクセス権を付与します。ユーザはコンフィギュレーション コマンドを入力することはできません。

例 :

次の例では、**config** アクセス権を使用して、**joecool** という名前のユーザアカウントを追加します。パスワードは入力時に非表示となります。

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login          UID   Auth Access  Enabled Reset   Exp Warn  Str Lock Max
admin          1000 Local Config Enabled  No   Never N/A  Dis  No N/A
joecool       1001 Local Config Enabled  No   Never N/A  Dis  No  5
```

(注) **configure password** コマンドを使用して自分のパスワードを変更できることをユーザに伝えます。

**ステップ 3** (オプション) セキュリティ要件を満たすようにアカウントの性質を調整します。

アカウントのデフォルト動作を変更するには、次のコマンドを使用できます。

- **configure user aging *username* max\_days warn\_days**

ユーザパスワードの有効期限を設定します。パスワードの最大有効日数と、有効期限が近づいたことをユーザに通知する警告を期限切れとなる何日前に発行するかを指定します。どちらの値も 1~9999 ですが、警告までの日数は最大日数以内にする必要があります。アカウントを作成した場合、パスワードの有効期限はありません。

- **configure user forcereset *ユーザ名***

次回ログイン時にユーザにパスワードを強制的に変更してもらいます。

- **configure user maxfailedlogins *username* number**

アカウントがロックされる前の連続したログイン失敗の最大回数を 1~9999 までで設定します。アカウントをロック解除するには、**configure user unlock** コマンドを使用します。新しいアカウントのデフォルトは、5 回連続でのログインの失敗です。

- **configure user minpasswlen *username* number**

パスワードの最小長を 1~127 までで設定します。

- **configure user strengthcheck *ユーザ名* {enable | disable}**

パスワードの変更時にユーザに対してパスワード要件を満たすように要求する、パスワードの強度確認を有効または無効にします。ユーザパスワードの有効期限が切れた場合、または **configure user forcereset** コマンドを使用した場合は、ユーザが次にログインしたときにこの要件が自動的に有効になります。

#### ステップ 4 必要に応じてユーザ アカウントを管理します。

ユーザをアカウントからロックアウトしたり、アカウントを削除するか、またはその他の問題を修正したりする必要があります。システムのユーザアカウントを管理するには、次のコマンドを使用します。

- **configure user access** ユーザ名 {basic | config}  
ユーザ アカウントの権限を変更します。
- **configure user delete** ユーザ名  
指定したアカウントを削除します。
- **configure user disable** ユーザ名  
指定したアカウントを削除せずに無効にします。ユーザは、アカウントを有効にするまでログインできません。
- **configure user enable** ユーザ名  
指定したアカウントを有効にします。
- **configure user password** ユーザ名  
指定したユーザのパスワードを変更します。ユーザは通常、**configure password** コマンドを使用して自分のパスワードを変更する必要があります。
- **configure user unlock** ユーザ名  
ログイン試行の最大連続失敗回数の超過が原因でロックされたユーザアカウントをロック解除します。

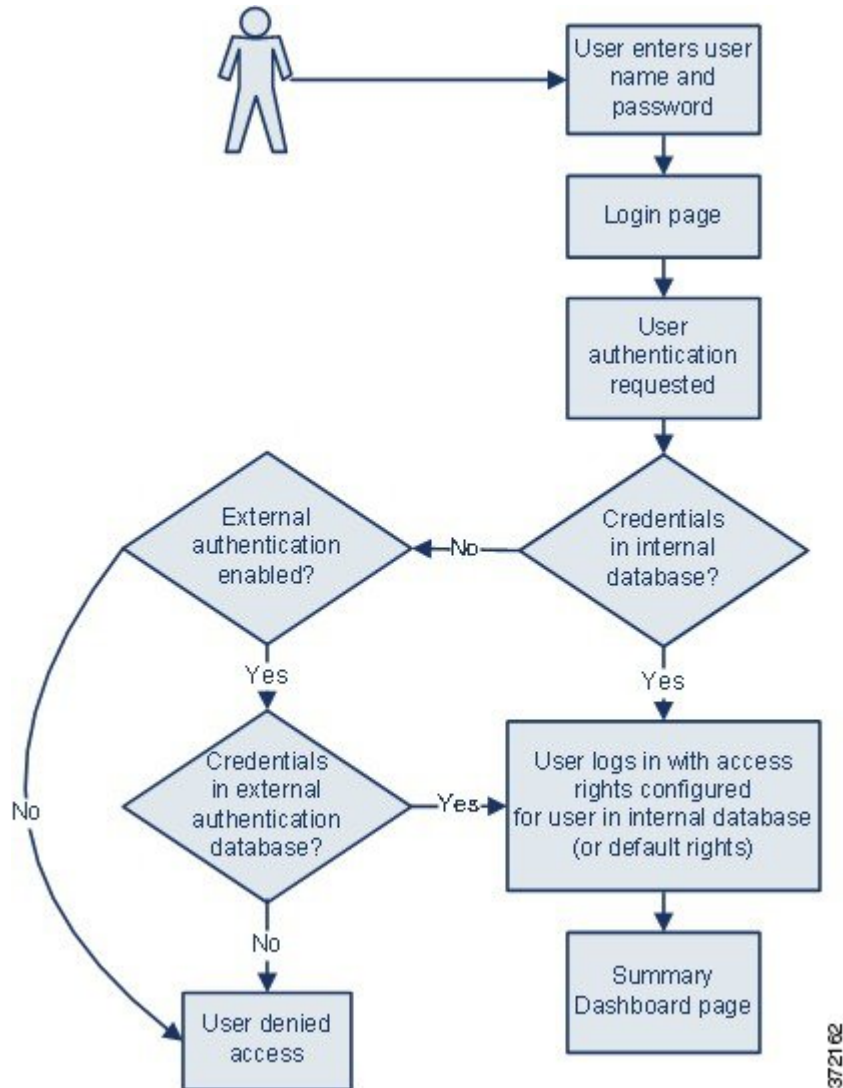
## Firepower システムのユーザ認証

Firepower Management Center または管理対象デバイスでユーザが Web インターフェイスにログインすると、アプリケーションがローカルのユーザリストでユーザ名とパスワードに一致するものを検索します。このプロセスは認証と呼ばれます。

認証には次の 2 種類あります。

- 内部認証：システムはユーザについてローカル データベースのリストを確認します。
- 外部認証：システムはユーザについてローカルデータベースのリストを確認し、そのリストにユーザが存在しない場合は、そのユーザ リストを外部認証サーバに照会します。

認証プロセスは、次のとおりです。



ユーザアカウントを作成する場合は、そのユーザに対して内部認証または外部認証を指定します。

## 内部認証

内部認証では、ユーザクレデンシャルは、内部 Firepower システムのデータベースのレコードに照らして検証されます。これがデフォルトの認証タイプです。

ユーザのアカウントを作成する際に、内部認証のユーザにアクセス権を設定します。



(注) 内部認証ユーザが外部認証に変換された場合、内部認証に戻すことはできません。

## 外部認証 (External Authentication)

外部認証では、Firepower Management Center または管理対象デバイスによって、外部サーバのリポジトリからユーザ クレデンシヤルが取得されます。外部サーバは、Lightweight Directory Access Protocol (LDAP) ディレクトリ サーバまたは Remote Authentication Dial In User Service (RADIUS) 認証サーバにすることができます。

プラットフォーム設定ポリシーおよび個別のユーザアカウントの設定で外部認証を有効にします。アプライアンスに対して使用できる外部認証形式は 1 つだけです。

ユーザがアプライアンスに初めてログインすると、アプライアンスは、ローカルユーザレコードを作成して、これらの外部クレデンシヤルを一連のアクセス許可に関連付けます。ユーザには、次のいずれかに基づいて権限が割り当てられます。

- 属するグループまたはアクセス リスト
- アプライアンスのプラットフォーム設定ポリシーで設定したデフォルトのユーザアクセス ロール

権限がグループまたはリストのメンバーシップによって付与される場合は、権限を変更できません。ただし、デフォルトのユーザ ロールによって割り当てられている場合は、ユーザアカウントで変更でき、この変更でデフォルトの設定がオーバーライドされます。次に例を示します。

- 外部認証ユーザアカウントのデフォルト ロールとして特定のアクセス ロールが設定されている場合、ユーザは外部アカウントクレデンシヤルを使用してアプライアンスにログインでき、この際にシステム管理者による追加の設定は必要ありません。
- アカウントが外部で認証され、デフォルトではアクセス権限が付与されない場合、ユーザはログインできますが、どの機能にもアクセスできません。ユーザ (またはシステム管理者) は、ユーザ機能へ適切なアクセス権を付与する権限を変更することができます。

Firepower システム インターフェイスでは、外部認証ユーザのパスワード管理および外部認証ユーザの非アクティブ化は実行できません。外部認証ユーザの場合、LDAP グループメンバーシップ、RADIUS リスト メンバーシップ、または属性値によってアクセス ロールが割り当てられているユーザの Firepower システム ユーザ管理ページでは、最小アクセス権を削除することができません。外部認証ユーザの [ユーザの編集 (Edit User)] ページでは、外部認証サーバの設定により付与された権限は、[外部変更済み (Externally Modified)] ステータスでマークされます。

ただし、追加の権限を割り当てることはできます。外部認証ユーザのアクセス権を変更すると、[ユーザ管理 (User Management)] ページの [認証方式 (Authentication Method)] カラムに、[外部: ローカルで変更済み (External - Locally Modified)] というステータスが表示されます。

### 関連トピック

[LDAP 認証 \(97 ページ\)](#)

[RADIUS 認証 \(124 ページ\)](#)

## LDAP 認証

LDAP (Lightweight Directory Access Protocol) により、ユーザ クレデンシャルなどのオブジェクトをまとめるためのディレクトリをネットワーク上の一元化されたロケーションにセットアップできます。こうすると、複数のアプリケーションがこれらのクレデンシャルと、クレデンシャルの記述に使用される情報にアクセスできます。ユーザのクレデンシャルを変更する必要がある場合も、常に 1 箇所でクレデンシャルを変更できます。

LDAP 認証オブジェクトは Firepower Management Center 上に作成する必要がありますが、Web インターフェイスを備えた管理対象デバイス (つまり、7000 および 8000 シリーズデバイス) であればどれでも、オブジェクトを有効にするプラットフォーム設定ポリシーをそのデバイスに導入することで、外部認証オブジェクトを使用できます。ポリシーを導入すると、オブジェクトがデバイスにコピーされます。



- (注) 7000 および 8000 シリーズ デバイスで外部認証を有効にする前に、シェルアクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証シェル ユーザまたは CLI ユーザをすべて削除してください。

LDAP 命名標準は、アドレスの指定と、認証オブジェクトのフィルタおよび属性の構文に使用できることに注意してください。詳細については、『Lightweight Directory Access Protocol (v3): Technical Specification』 (RFC 3377) に記載されている RFC を参照してください。この手順ではシンタックスの例が示されています。Microsoft Active Directory Server へ接続するための認証オブジェクトをセットアップするときに、ドメインを含むユーザ名を参照する場合には、Internet RFC 822 (Standard for the Format of ARPA Internet Text Messages) 仕様に記載されているアドレス指定構文を使用できることに注意してください。たとえばユーザオブジェクトを参照する場合は、`JoeSmith@security.example.com` と入力し、Microsoft Active Directory Sever を使用する場合の同等のユーザ識別名 `cn=JoeSmith,ou=security,dc=example,dc=com` は使用しません。



- (注) 現在 Firepower システムでは、Microsoft Active Directory on Windows Server 2008、Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0、OpenLDAP on Linux が稼働する LDAP サーバでの LDAP 外部認証がサポートされています。ただし、Firepower システムでは NGIPSv または ASA FirePOWER デバイスの外部認証はサポートされていません。

## LDAP 認証オブジェクトを作成するために必要な情報

LDAP サーバへの接続を設定する前に、LDAP 認証オブジェクトを作成するのに必要な情報を収集する必要があります。



(注) ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認する必要があります。

基本的な認証オブジェクトを作成するには、少なくとも以下が必要です。

- 接続するサーバのサーバ名または IP アドレス
- 接続するサーバのサーバタイプ
- LDAP ツリーを参照できる十分な権限が付与されているユーザアカウントのユーザ名とパスワード。シスコはこの目的でドメイン管理ユーザのアカウントを使用することを推奨します。
- アプライアンスと LDAP サーバの間にファイアウォールがある場合、発信接続を許可するファイアウォールの項目
- ユーザ名が存在するサーバ ディレクトリのベース識別名 (可能な場合)



**ヒント** サードパーティの LDAP クライアントを使用して、LDAP ツリーを参照し、ベース DN と属性の説明を確認できます。またそのクライアントを使用して、選択したユーザが、選択したベース DN を参照できることを確認することもできます。LDAP 管理者に連絡し、ご使用の LDAP サーバ向けの推奨される認定 LDAP クライアントを確認してください。

詳細な LDAP 認証オブジェクト設定をどのようにカスタマイズするかによって、次の表に示す情報が必要となることがあります。

表 12: 追加の LDAP 設定情報

目的	必要な項目
389 以外のポートを介した接続	ポート番号
暗号化接続を使用した接続	接続の証明書
属性値に基づいてアプライアンスにアクセスできるユーザをフィルタにより絞り込む	フィルタの条件となる属性と値のペア
ユーザ識別名を検査するのではなく、属性を UI アクセス属性として使用する	属性の名前
ユーザ識別名を検査するのではなく、属性をシェル ログイン属性として使用する	属性の名前
属性値に基づいてシェルを介してアプライアンスにアクセスできるユーザをフィルタにより絞り込む	フィルタの条件となる属性と値のペア



目的	必要な項目
特定のユーザ ロールへのグループの関連付け	各グループの識別名、およびグループがスタティック グループの場合はグループ メンバー属性、グループがダイナミック グループの場合はグループ メンバーの URL 属性
認証用および承認用に使用する CAC	CAC。CAC を発行したのと同じ CA によって署名されたサーバ証明書、両方の証明書の証明書チェーン

## CAC 認証

部門で共通アクセス カード (CAC) が使用される場合は、Web インターフェイスにログインするユーザを認証し、グループ メンバーシップまたはデフォルト アクセス権に基づいて特定機能へのアクセスを許可するように、LDAP 認証を設定できます。CAC 認証および認可が設定されている場合、ユーザは、アプライアンスに個別のユーザ名とパスワードを指定せずに直接ログインすることができます。



- (注) CAC 設定プロセスの一部としてユーザ証明書を有効にするには、ブラウザに有効なユーザ証明書 (この場合は CAC を介してユーザのブラウザに渡されるサーバ証明書) が存在している **必要があります**。CAC 認証および認可の設定後に、ネットワーク上のユーザはブラウザセッション期間にわたって CAC 接続を維持する **必要があります**。セッション中に CAC を削除または交換すると、Web ブラウザでセッションが終了し、システムにより Web インターフェイスから強制的にログアウトされます。

システムでは、CAC 認証ユーザは Electronic Data Interchange Personal Identifier (EDIPI) 番号により識別されます。ユーザが CAC クレデンシャルを使用して初めてログインした後で、[ユーザ管理 (User Management)] ページでのこれらのユーザのアクセス権を手動で追加または削除できます。グループ制御アクセスロールを使用してユーザの権限を事前に設定していない場合、ユーザには、プラットフォーム設定ポリシーでデフォルトで付与される権限だけが与えられています。



- ヒント 操作が行われない状態で 24 時間が経過すると、システムによって [ユーザ管理 (User Management)] ページから CAC 認証ユーザを消去されるときに、手動で設定されたアクセス権限が削除されることに注意してください。その後ユーザがログインするたびに、ユーザがページに復元されますが、ユーザのアクセス権限に対する手動での変更はすべて再設定する必要があります。

## CAC 認証の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 および 8000 シリーズ	任意 (Any)	Admin/Network Admin

ネットワークのユーザが各自の CAC クレデンシャルを使用して Firepower Management Center および 7000 および 8000 シリーズ デバイスにログインする前に、適切なアクセス許可を持つユーザが、CAC 認証および認可のマルチステップ設定プロセスを完了しておく必要があります。

### 始める前に

- [LDAP 認証オブジェクトを作成するために必要な情報 \(97 ページ\)](#) の説明に従って情報を収集します。

### 手順

- 
- ステップ 1** 組織の指示に従い CAC を挿入します。
- ステップ 2** ブラウザで `https://hostname/` を開きます (hostname はご使用の Firepower Management Center のホスト名に対応しています)。
- ステップ 3** プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられた PIN を入力します。
- ステップ 4** プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。
- ステップ 5** ログインページで、[ユーザ名 (Username)] フィールドと [パスワード (Password)] フィールドに、管理者権限を持つユーザとしてログインします。ユーザ名では、大文字と小文字が区別されます。
- ヒント** CAC 認証および認可の設定が完了するまで、CAC クレデンシャルを使用したログインはできません。
- ステップ 6** [システム (System)] > [ユーザ (Users)] に移動し、[外部認証 (External Authentication)] タブをクリックします。
- ステップ 7** および [拡張 LDAP 認証オブジェクトの作成 \(104 ページ\)](#) の手順に従い、CAC 認証および認可専用の LDAP 認証オブジェクトを作成します。次の設定を行う必要があります。
- [LDAP 固有パラメータ (LDAP-Specific Parameters)] セクションの詳細設定オプションの [ユーザ名テンプレート (User Name Template)]。
  - [属性マッピング (Attribute Mapping)] セクションの [UI アクセス属性 (UI Access Attribute)]。

- [グループ制御アクセスロール (Group Controlled Access Roles)] セクションの既存の LDAP グループの識別名 (LDAP グループ メンバーシップによってアクセス権を事前に設定する場合)。

**ヒント** 同一認証オブジェクトで CAC 認証とシェルアクセスの両方を設定できないことに注意してください。また、ユーザにシェルアクセスを許可する場合は、個別の認証オブジェクトを作成し、有効にします。

**ステップ 8** [保存 (Save)] をクリックします。

**ステップ 9** [外部認証の有効化 \(1017 ページ\)](#) の説明に従って、外部認証と CAC 認証を有効にします。

**注意** 設定変更を展開するまで変更は有効になりません。

**ステップ 10** [システム (System)] > [設定 (Configuration)] に移動し、[HTTPS 証明書 (HTTPS Certificate)] をクリックします。

**ステップ 11** HTTPS サーバ証明書をインポートし、必要に応じて [HTTPS サーバ証明書のインポート \(924 ページ\)](#) で説明する手順に従います。

(注) 認証および認可に使用する予定の CAC で、HTTPS サーバ証明書とユーザ証明書が同じ認証局 (CA) により発行される必要があります。

**ステップ 12** [HTTPS ユーザ証明書設定 (HTTPS User Certificate Settings)] の [ユーザ証明書を有効にする (Enable User Certificates)] を選択します。詳細については、[有効な HTTPS クライアント証明書の強制 \(926 ページ\)](#) を参照してください。

### 次のタスク

- ユーザが初めてログインした後、手動でユーザのアクセス権を追加または削除できます。権限を変更しない場合、そのユーザにはデフォルトで付与される権限のみが設定されます。詳細については、[ユーザアカウントの編集 \(87 ページ\)](#) を参照してください。

### 関連トピック

[LDAP グループ フィールド \(116 ページ\)](#)

[LDAP 固有フィールド \(110 ページ\)](#)

[CAC クレデンシアルを使用した管理対象デバイスへのログイン \(27 ページ\)](#)

[CAC クレデンシアルを使用した Firepower Management Center へのログイン \(26 ページ\)](#)

## 基本 LDAP 認証オブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

LDAP 認証オブジェクトをセットアップできます。LDAP 認証オブジェクトでは多くの値をカスタマイズします。ただし、特定ディレクトリ内のすべてのユーザを認証するだけの場合は、そのディレクトリのベース DN を使用して基本認証オブジェクトを作成できます。ご使用のサーバタイプでベース DN のデフォルトを設定し、サーバからユーザデータを取得するために使用するアカウントの認証クレデンシャルを指定すれば、認証オブジェクトを簡単に作成できます。このためには、次の手順に従います。



- (注) (たとえば、シェルアクセスを付与するために) 認証オブジェクトを作成するときに、各認証設定を検討してカスタマイズする場合は、高度な手順を使用してオブジェクトを作成します。サーバへの接続の暗号化、ユーザタイムアウトの設定、ユーザ名テンプレートのカスタマイズ、または LDAP グループメンバーシップに基づく Firepower システム ユーザ ロールの割り当てを行う場合にも、この高度な手順を使用してください。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

#### 始める前に

- [LDAP 認証オブジェクトを作成するために必要な情報 \(97 ページ\)](#) の説明に従って情報を収集します。

#### 手順

- ステップ 1** [システム (System)] > [ユーザ (Users)] を選択します。
- ステップ 2** [外部認証 (External Authentication)] タブをクリックします。
- ステップ 3** [外部認証オブジェクトの追加 (Add External Authentication Object)] をクリックします。
- ステップ 4** [認証方式 (Authentication Method)] ドロップダウンリストから [LDAP] を選択します。
- ステップ 5** [LDAP 認証サーバの特定 \(109 ページ\)](#) の説明に従って、[名前 (Name)]、[説明 (Description)]、[サーバタイプ (Server Type)]、[プライマリ サーバ ホスト名/IP アドレス (Primary Server Host Name/IP Address)] を入力します。
- ヒント** [デフォルトの設定 (Set Defaults)] をクリックすると、システムにより、[ユーザ名テンプレート (User Name Template)]、[UI アクセス属性 (UI Access Attribute)]、[シェルアクセス属性 (Shell Access Attribute)]、[グループメンバ属性 (Group Member Attribute)]、[グループメンバ URL 属性 (Group Member URL Attribute)] フィールドにデフォルト値が設定されます。
- ステップ 6** [LDAP 固有パラメータの設定 \(114 ページ\)](#) の説明に従って、[DN の取得 (Fetch DN)] を選択して基本識別名を指定し、オプションで [基本フィルタ (Base Filter)] に入力します。
- ステップ 7** [LDAP 固有パラメータの設定 \(114 ページ\)](#) の説明に従って、[ユーザ名 (UserName)] として識別名を入力し、LDAP サーバを参照するための十分なクレデンシャルを持っているユーザの [パスワード (Password)] を入力します。
- ステップ 8** [パスワードの確認 (Confirm Password)] フィールドに、パスワードを再度入力します。

- ステップ 9 [LDAP 認証接続のテスト \(121 ページ\)](#) の説明に従って、接続をテストします。
- ステップ 10 [保存 (Save)] をクリックします。

## 例

次の図は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの基本設定を示します。この例の LDAP サーバの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 389 が使用されます。

External Authentication Object

Authentication Method: LDAP

CAC:  Use for CAC authentication and authorization

Name \*: Basic Configuration Example

Description:

Server Type: MS Active Directory

Primary Server

Host Name/IP Address \*:  ex. IP or hostname

Port \*: 389

Backup Server (Optional)

Host Name/IP Address:  ex. IP or hostname

Port: 389

LDAP-Specific Parameters

Base DN \*: ou=security,DC=it,DC=example,DC=com ex. dc=sourcefire,dc=com

Base Filter:  ex. (cn=jsmith), (lc=jsmith), (&(cn=jsmith)(!(cn=bsmith)(cn=csmith\*)))

User Name \*: CN=admin,DC=example,DC=com ex. cn=jsmith,dc=sourcefire,dc=com

Password \*:

Confirm Password \*:

Show Advanced Options

372784

この例では、Example 社の情報テクノロジー ドメインで、セキュリティ部門のベース識別名として OU=security,DC=it,DC=example,DC=com を使用した接続を示しています。

The screenshot shows the 'Attribute Mapping' configuration window. It includes the following sections:

- Attribute Mapping:**
  - UI Access Attribute: sAMAccountName
  - Fetch Attrs: [Button]
  - Shell Access Attribute: sAMAccountName
- Group Controlled Access Roles (Optional):** [Dropdown arrow]
- Shell Access Filter:**
  - Same as Base Filter:
  - Shell Access Filter: [Text field]
  - Example: ex. (cn=jsmith), (lcn=jsmith), (&(cn=jsmith)(!(cn=bsmith)(cn=esmith\*)))
- Additional Test Parameters:**
  - User Name: [Text field]
  - Password: [Text field]
- \*Required Field:** [Label]
- Buttons:** Save, Test, Cancel

ただし、このサーバが Microsoft Active Directory Server であるため、ユーザ名の保存に uid 属性ではなく sAMAccountName 属性が使用されます。サーバのタイプとして MS Active Directory を選択し、[デフォルトの設定 (Set Defaults)] をクリックすると、[UI アクセス属性 (UI Access Attribute)] が sAMAccountName に設定されます。その結果、ユーザが Firepower システムへのログインを試行すると、Firepower システムは各オブジェクトの sAMAccountName 属性を検査し、一致するユーザ名を検索します。

また、[シェルアクセス属性 (Shell Access Attribute)] が sAMAccountName の場合、ユーザがアプライアンスでシェルアカウントまたは CLI アカウントにログインすると、ディレクトリ内のすべてのオブジェクトの各 sAMAccountName 属性が検査され、一致が検索されます。

基本フィルタはこのサーバに適用されないため、Firepower システムはベース識別名により示されるディレクトリ内のすべてのオブジェクトの属性を検査することに注意してください。サーバへの接続は、デフォルトの期間（または LDAP サーバで設定されたタイムアウト期間）の経過後にタイムアウトします。

#### 次のタスク

- LDAP 認証を有効にするには、[外部認証の有効化 \(1017 ページ\)](#) の説明に従って、認証オブジェクトを有効にします。
- 取得されるユーザのリストを絞り込む場合の詳細は、[LDAP 認証接続のトラブルシューティング \(122 ページ\)](#) を参照してください。

## 拡張 LDAP 認証オブジェクトの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

基本認証オブジェクトの作成時に、認証サーバに接続できるようにする基本設定を定義します。拡張認証オブジェクトを作成する場合は、基本設定を定義し、サーバからユーザデータを取得するために使用するディレクトリ コンテキストおよび検索条件も選択します。オプションで、シェルアクセス認証を設定できます。

ご使用のサーバタイプのデフォルト設定を使用して LDAP 設定を迅速にセットアップできますが、詳細設定をカスタマイズして、アプライアンスから LDAP サーバに暗号化接続するかどうか、接続のタイムアウト、およびサーバがユーザ情報を検査する属性を制御することもできます。

LDAP 固有のパラメータの場合、LDAP 命名基準とフィルタおよび属性のシンタックスを使用できます。詳細については、『Lightweight Directory Access Protocol (v3): Technical Specification』(RFC 3377) に記載されている RFC を参照してください。この手順ではシンタックスの例が示されています。Microsoft Active Directory Server へ接続するための認証オブジェクトをセットアップするときに、ドメインを含むユーザ名を参照する場合には、Internet RFC 822 (Standard for the Format of ARPA Internet Text Messages) 仕様に記載されているアドレス指定シンタックスを使用することに注意してください。たとえばユーザ オブジェクトを参照する場合は、JoeSmith@security.example.com と入力し、Microsoft Active Directory Server を使用する場合の同等のユーザ識別名 cn=JoeSmith,ou=security, dc=example,dc=com は使用しません。



- (注) CAC 認証に使用する LDAP 認証オブジェクトを設定する場合は、コンピュータに挿入されている CAC を取り外さないでください。ユーザ証明書を有効にした後は、CAC が常に挿入された状態にしておく必要があります。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

#### 始める前に

- [LDAP 認証オブジェクトを作成するために必要な情報 \(97 ページ\)](#) の説明に従って情報を収集します。
- シェルアクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証シェル ユーザをすべて削除します。

#### 手順

- ステップ 1 [システム (System)] > [ユーザ (Users)] を選択します。
- ステップ 2 [外部認証 (External Authentication)] タブをクリックします。
- ステップ 3 [外部認証オブジェクトの追加 (Add External Authentication Object)] をクリックします。
- ステップ 4 [LDAP 認証サーバの特定 \(109 ページ\)](#) の説明に従って、認証サーバを指定します。
- ステップ 5 [LDAP 固有パラメータの設定 \(114 ページ\)](#) の説明に従って、認証設定を行います。
- ステップ 6 オプションで、[グループによるアクセス権の設定 \(117 ページ\)](#) の説明に従って、デフォルトアクセス ロール割り当ての基準として使用する LDAP グループを設定します。

ヒント CAC 認証および認可にこのオブジェクトを使用する予定の場合、Cisco としてはアクセス ロール割り当ての管理のために LDAP グループを設定することを推奨します。

**ステップ 7** オプションで、[LDAP シェルアクセスの設定 \(119 ページ\)](#) の説明に従って、シェルアクセスの認証設定を行います。

**ステップ 8** [LDAP 認証接続のテスト \(121 ページ\)](#) の説明に従って、設定をテストします。

**ステップ 9** [保存 (Save) ] をクリックします。

## 例

次の例は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの詳細設定を示します。この例の LDAP サーバの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 636 が使用されます。

**Authentication Object**

Authentication Method: LDAP

Name \*: Advanced Configuration Example

Description:

Server Type: MS Active Directory [Set Defaults]

**Primary Server**

Host Name/IP Address \*: 10.11.3.4

Port \*: 636

この例では、Example 社の情報テクノロジー ドメインで、セキュリティ部門のベース識別名として OU=security,DC=it,DC=example,DC=com を使用した接続を示しています。ただし、このサーバに基本フィルタ (cn=\*smith) が設定されていることに注意してください。このフィルタは、サーバから取得するユーザを、一般名が smith で終わるユーザに限定します。

**LDAP-Specific Parameters**

Base DN \*: OU=security,DC=it,DC=example,DC=com [Fetch DNs]

Base Filter: (CN=\*smith)

User Name \*: CN=admin,DC=example,DC=com

Password \*:

Confirm Password \*:

Show Advanced Options: ▼

Encryption:  SSL  TLS  None

SSL Certificate Upload Path: C:\certificate.pem [Browse...]

User Name Template: %s

Timeout (Seconds): 60

**Attribute Mapping**

UI Access Attribute \*: sAMAccountName [Fetch Attrs]

Shell Access Attribute \*: sAMAccountName



サーバへの接続が SSL を使用して暗号化され、certificate.pem という名前の証明書が接続に使用されます。また、[タイムアウト (Timeout)] の設定により、60 秒経過後にサーバへの接続がタイムアウトします。

このサーバが Microsoft Active Directory Server であるため、ユーザ名の保存に uid 属性ではなく sAMAccountName 属性が使用されます。設定では、[UI アクセス属性 (UI Access Attribute)] が sAMAccountName であることに注意してください。その結果、ユーザが Firepower システムへのログインを試行すると、Firepower システムは各オブジェクトの sAMAccountName 属性を検査し、一致するユーザ名を検索します。

また、[シェル アクセス属性 (Shell Access Attribute)] が sAMAccountName の場合、ユーザがアプライアンスでシェルアカウントにログインすると、ディレクトリ内のすべてのオブジェクトの各 sAMAccountName 属性が検査され、一致が検索されます。

この例では、グループ設定も行われます。[メンテナンス ユーザ (Maintenance User)] ロールが、member グループ属性を持ち、ベースドメイン名が CN=SFmaintenance,=it,=example,=com であるグループのすべてのメンバーに自動的に割り当てられます。

Group Controlled Access Roles (Optional) ▼

Access Admin	<input type="text"/>
Administrator	<input type="text"/>
External Database User	<input type="text"/>
Intrusion Admin	<input type="text"/>
Maintenance User	<input type="text" value="CN=SFmaintenance,DC=it,DC=example,DC=com"/>
Network Admin	<input type="text"/>
Discovery Admin	<input type="text"/>
Security Approver	<input type="text"/>
Security Analyst	<input type="text"/>
Security Analyst (Read Only)	<input type="text"/>

Default User Role:  (Dropdown menu options: Access Admin, Administrator, External Database User, Intrusion Admin)

Group Member Attribute:

Group Member URL Attribute:

シェルアクセスフィルタは、基本フィルタと同一に設定されます。このため、同じユーザが Web インターフェイスを使用する場合と同様に、シェルまたは CLI を介してアプライアンスにアクセスできます。

### 次のタスク

- LDAP 認証を有効にするには、[外部認証の有効化（1017ページ）](#)で認証オブジェクトを有効化します。

## LDAP 認証サーバのフィールド

### CAC

認証および許可に CAC を使用するには、このチェックボックスをオンにします。

### [名前 (Name) ]

認証サーバの名前。

### 説明

認証サーバの説明。

### サーバタイプ (Server Type)

接続する LDAP サーバのタイプ。タイプを選択する際には、次のオプションから選択できます。

- Microsoft Active Directory Server に接続する場合は、[MS Active Directory] を選択します。
- Sun Java System Directory Server または Oracle Directory Server に接続する場合は、[Oracle Directory] を選択します。
- OpenLDAP サーバに接続する場合は、[OpenLDAP] を選択します。
- 上記のサーバ以外の LDAP サーバに接続し、デフォルト設定をクリアする場合は、[その他 (Other) ] を選択します。



**ヒント** [デフォルトにセット (Set Defaults) ] をクリックすると、[ユーザ名テンプレート (User Name Template) ]、[UI アクセス属性 (UI Access Attribute) ]、[シェル アクセス属性 (Shell Access Attribute) ]、[グループ メンバー属性 (Group Member Attribute) ]、および [グループ メンバー URL 属性 (Group Member URL Attribute) ] フィールドにデフォルト値が入力されます。

#### [プライマリ サーバのホスト名/IP アドレス (Primary Server Host Name/IP Address) ]

認証データを取得するプライマリ サーバの IP アドレスまたはホスト名。



(注) 証明書を使用し、TLSまたはSSL経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要があります。また、暗号化接続では IPv6 アドレスはサポートされていません。

#### [プライマリ サーバのポート (Primary Server Port) ]

プライマリ認証サーバで使用されるポート。

#### [バックアップサーバのホスト名/IP アドレス (Backup Server Host Name/IP Address) ]

認証データを取得するバックアップサーバの IP アドレスまたはホスト名。

#### [バックアップサーバポート (Backup Server Port) ]

バックアップ認証サーバで使用されるポート。

## LDAP 認証サーバの特定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

認証オブジェクトの作成時には、管理対象デバイスまたは Firepower Management Center が認証のために接続する、プライマリおよびバックアップサーバとサーバポートを最初に指定します。



(注) CAC 認証に使用する LDAP 認証オブジェクトを設定する場合は、コンピュータに挿入されている CAC を取り外さないでください。ユーザ証明書を有効にした後は、CAC が常に挿入された状態にしておく必要があります。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

## 手順

- 
- ステップ 1** [システム (System) ] > [ユーザ (Users) ] を選択します。
- ステップ 2** [外部認証 (External Authentication) ] タブをクリックします。
- ステップ 3** [外部認証オブジェクトの追加 (Add External Authentication Object) ] をクリックします。
- ステップ 4** [認証方式 (Authentication Method) ] ドロップダウンリストから [LDAP] を選択します。
- ステップ 5** オプションで、CAC 認証および認可にこの認証オブジェクトを使用する予定の場合は、[CAC] チェックボックスをオンにします。
- (注) CAC 認証および認可を完全に設定するには、[CAC 認証の設定 \(100 ページ\)](#) の手順に従う必要があります。
- ステップ 6** [名前 (Name) ] フィールドと [説明 (Description) ] フィールドに、認証サーバの名前と説明を入力します。
- ステップ 7** ドロップダウンリストから [サーバタイプ (Server Type) ] を選択します。詳細については、[LDAP 認証サーバのフィールド \(108 ページ\)](#) を参照してください。必要に応じて、[デフォルトの設定 (Set Defaults) ] をクリックします。
- ステップ 8** [プライマリ サーバのホスト名または IP アドレス (Primary Server Host Name/IP Address) ] を入力します。
- (注) 証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要があります。また、暗号化接続では IPv6 アドレスはサポートされていません。
- ステップ 9** 必要に応じて、[プライマリ サーバ ポート (Primary Server Port) ] を入力します。
- ステップ 10** 必要に応じて、[バックアップサーバのホスト名または IP アドレス (Backup Server Host Name/IP Address) ] を入力します。
- ステップ 11** 必要に応じて、[バックアップ サーバ ポート (Backup Server Port) ] を入力します。
- 

## 次のタスク

- LDAP 認証オブジェクトの作成を続行します。詳細については、[拡張 LDAP 認証オブジェクトの作成 \(104 ページ\)](#) を参照してください。

## LDAP 固有フィールド

次の表で、各 LDAP 固有パラメータについて説明します。

表 13: LDAP 固有パラメータ

設定	説明	例
ベース DN (Base DN)	<p>アプライアンスがユーザ情報を検索する LDAP サーバのディレクトリのベース識別名を指定します。</p> <p>通常、ベース DN には、企業ドメインおよび部門を示す基本構造があります。</p> <p>プライマリサーバを特定したら、そのサーバから使用可能なベース DN のリストが自動的に取得され、該当するベース DN を選択できることに注意してください。</p>	<p>Example 社のセキュリティ (Security) 部門のベース DN は、 ou=security,dc=example,dc=com となります。</p>
[基本フィルタ (Base Filter) ]	<p>ベース DN でフィルタに設定されている特定の属性と値のペアを含むオブジェクトだけを取得することで、検索を絞り込みます。基本フィルタは、カッコ内に囲まれるフィルタとして使用する属性タイプ、比較演算子、および属性値です。</p>	<p>F で始まる一般名を持つユーザのみをフィルタで検出するには、フィルタ (cn=F*) を使用します。</p>
[ユーザ名 (User Name) ]/[パスワード (Password) ]	<p>ローカル アプライアンスがユーザ オブジェクトにアクセスできるようにします。取得する認証オブジェクトに対する適切な権限を持つユーザのユーザ資格情報を指定します。指定するユーザの識別名は、LDAP サーバのディレクトリ情報ツリーで一意である必要があります。Microsoft Active Directory Server に関連付けられたサーバユーザ名の末尾の文字が \$ であってはなりません。</p>	<p>Example 社のセキュリティ (Security) 部門の admin ユーザのユーザ名は、 cn=admin, ou=security, dc=example,dc=com となります。</p>

設定	説明	例
暗号化 (Encryption)	<p>通信が暗号化されるかどうかと、暗号化方法を示します。暗号化なし、Transport Layer Security (TLS)、または Secure Sockets Layer (SSL) 暗号化を選択できます。TLSまたはSSL経由で接続するときに認証に証明書を使用する場合、証明書の LDAP サーバ名が、指定する<b>ユーザ名</b>と一致している<b>必要がある</b>ことに注意してください。</p> <p>ポートを指定した後で暗号化方式を変更すると、ポートが、選択されているサーバタイプのデフォルト値にリセットされます。</p>	<p>外部認証の設定に 10.10.10.250 を、証明書に computer1.example.com を入力すると、computer1.example.com に IP アドレス 10.10.10.250 がある場合であっても、接続に失敗します。外部認証設定のサーバ名を computer1.example.com に変更すると、接続が正常に行われます。</p>
[SSL 証明書アップロードパス (SSL Certificate Upload Path) ]	ローカルコンピュータで、暗号化に使用する証明書のパスを指定します。	c:/server.crt
[ユーザ名テンプレート (User Name Template) ]	<p>文字列変換文字 (%s) をユーザの [UI アクセス属性 (UI Access Attribute) ] の値にマッピングすることで、ログイン時に入力されるユーザ名の形式を指定します。ユーザ名テンプレートは、認証に使用する識別名の形式です。</p> <p>ユーザがログインページにユーザ名を入力すると、アプライアンスにより文字列変換文字が名前に置き換えられ、その結果生成される識別名がユーザ資格情報の検索に使用されます。</p> <p>CAC 認証および許可にこのオブジェクトを使用するには、[ユーザ名テンプレート (User Name Template) ]に入力する<b>必要があります</b>。</p>	<p>%s@security.example.com,  %s@mail.com,  %s@mil,  %s@smil.mil,</p>

設定	説明	例
Timeout	<p>プライマリ サーバへの接続試行のタイムアウトを設定します。これにより、接続がバックアップサーバにロールオーバーされます。プライマリ認証サーバからの応答がない状態でこのフィールドに示されている秒数（またはLDAPサーバのタイムアウト）が経過すると、アプライアンスはバックアップサーバに対してクエリを実行します。</p> <p>ただしLDAPがプライマリLDAPサーバのポートで実行されており、何らかの理由で要求の処理を拒否する場合は、バックアップサーバへのフェールオーバーは行われません。</p>	<p>プライマリサーバでLDAPが無効な場合、アプライアンスはバックアップサーバに対してクエリを実行します。</p>
[UI アクセス属性 (UI Access Attribute) ]	<p>ローカルアプライアンスに対し、ユーザ識別名の値ではなく、特定の属性の値の照合を行うように指示します。</p> <p>Firepower システム Web インターフェイスの有効なユーザ名が値として設定されている属性であれば、どの属性でも使用できます。いずれかのオブジェクトに一致するユーザ名とパスワードがある場合は、ユーザログイン要求が認証されます。</p> <p>サーバタイプを選択し、デフォルトを設定すると、[UI アクセス属性 (UI Access Attribute) ] に、そのサーバタイプに適した値が取り込まれます。</p> <p>このフィールドを空白のままにすると、ローカルアプライアンスは、LDAPサーバの各ユーザレコードのユーザ識別名値を調べ、ユーザ名に一致しているかどうかを確認します。</p> <p>CAC 認証および許可にこのオブジェクトを使用するには、[ユーザ名テンプレート (User Name Template) ] の値に対応する値を入力する必要があります。</p>	<p>sAMAccountName, userPrincipalName, メール アドレス</p>

## LDAP 固有パラメータの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

LDAP 固有パラメータセクションの設定により、アプライアンスがユーザ名を検索する LDAP ディレクトリの領域が決定され、アプライアンスから LDAP サーバへの接続の詳細が制御されます。

有効なユーザ名は一意のユーザ名であり、アンダースコア ( \_ )、ピリオド ( . )、ハイフン ( - )、英数字を使用できます。

ほとんどの LDAP 固有設定の他に、LDAP 命名基準とフィルタおよび属性の構文を使用できます。詳細については、『Lightweight Directory Access Protocol (v3): Technical Specification』 (RFC 3377) に記載されている RFC を参照してください。この手順ではシンタックスの例が示されています。Microsoft Active Directory Server へ接続するための認証オブジェクトをセットアップするときに、ドメインを含むユーザ名を参照する場合には、Internet RFC 822 (Standard for the Format of ARPA Internet Text Messages) 仕様に記載されているアドレス指定シンタックスを使用することに注意してください。たとえばユーザ オブジェクトを参照する場合は、JoeSmith@security.example.com と入力し、Microsoft Active Directory Server を使用する場合は、同等のユーザ識別名 cn=JoeSmith,ou=security,dc=example,dc=com は使用しません。



- (注) CAC 認証に使用する LDAP 認証オブジェクトを設定する場合は、コンピュータに挿入されている CAC を取り外さないでください。ユーザ証明書を有効にした後では、CAC が常に挿入された状態にしておく必要があります。

### 手順

**ステップ 1** [外部認証オブジェクトの作成 (Create External Authentication Object)] ページの [LDAP 固有パラメータ (LDAP-Specific Parameters)] セクションには、ベース DN を設定する 2 つのオプションがあります。

- [DN の取得 (Fetch DN)] をクリックし、ドロップダウンリストから適切なベース識別名を選択します。
- アクセスする LDAP ディレクトリのベース識別名を [ベース DN (Base DN)] フィールドに入力します。たとえば、Example 社のセキュリティ (Security) 部門の名前を認証するには、ou=security,dc=example,dc=com と入力します。

**ステップ 2** 必要に応じて、[基本フィルタ (Base Filter)] を入力します。

例：

たとえば、ディレクトリ ツリー内のユーザ オブジェクトに physicalDeliveryOfficeName 属性が設定されており、New York 支店のユーザに対しこの属性に値 NewYork が設定されている場合、



New York 支店のユーザだけを取得するには、(physicalDeliveryOfficeName=NewYork) と入力します。

**ステップ 3** LDAP サーバを参照する十分なクレデンシャルがあるユーザの [ユーザ名 (User Name) ] とし  
て識別名と、[パスワード (Password) ] を入力します。

例 :

たとえば、ユーザオブジェクトに uid 属性が含まれている OpenLDAP サーバに接続し、Example 社のセキュリティ (Security) 部門の管理者のオブジェクトの uid に値 NetworkAdmin が設定されている場合は、uid=NetworkAdmin,ou=security,dc=example,dc=com と入力します。

**注意** Microsoft Active Directory Server に接続する場合は、末尾の文字が \$ のサーバユーザ名は指定できません。

**ステップ 4** [パスワードの確認 (Confirm Password) ] フィールドに、パスワードを再度入力します。

**ステップ 5** 基本的な LDAP 固有パラメータの設定後に行う手順には、いくつかの選択肢があります。

- 詳細オプションにアクセスするには、[詳細オプションを表示 (Show Advanced Options) ] の横の矢印をクリックし、次のステップに進みます。
- LDAP グループメンバーシップに基づいてユーザデフォルトロールを設定する場合は、[グループによるアクセス権の設定 \(117 ページ\)](#) に進みます。
- 認証に LDAP グループを使用しない場合は、[LDAP シェルアクセスの設定 \(119 ページ\)](#) に進みます。

**ステップ 6** 必要に応じて、LDAP 接続に [暗号化 (Encryption) ] モードを選択します。

(注) ポートを指定した後で暗号化方式を変更すると、ポートがその方式のデフォルト値にリセットされることに注意してください。[なし (None) ] または [TLS] の場合、ポートはデフォルト値 389 を使用します。SSL 暗号化を選択した場合は、ポートはデフォルト値 636 を使用します。

**ステップ 7** TLS または SSL が暗号化を選択し、認証に証明書を使用する場合は、有効な TLS または SSL 証明書の場所を参照します。

(注) 以前にアップロードした証明書を置き換えるには、新しい証明書をアップロードし、設定をアプライアンスに再展開して、新しい証明書を上書きコピーします。

**ステップ 8** 必要に応じて、[UI アクセス属性 (UI Access Attribute) ] に対応する [ユーザ名テンプレート (User Name Template) ] を指定します。

例 :

たとえば、UI アクセス属性が uid である OpenLDAP サーバに接続し、Example 社のセキュリティ (Security) 部門で働くすべてのユーザを認証するには、[ユーザ名テンプレート (User Name Template) ] フィールドに uid=%s,ou=security,dc=example,dc=com と入力します。Microsoft Active Directory Server の場合は %s@security.example.com と入力します。

(注) 認証および認可に CAC 資格情報を使用するには、[ユーザ名テンプレート (User Name Template) ] フィールドに値を入力する必要があります。

- ステップ 9** オプションで、バックアップ接続にロールオーバーするまでの経過秒数を [タイムアウト (Timeout) ] フィールドに入力します。
- ステップ 10** オプションで、ベース DN および基本フィルタの代わりに属性に基づいてユーザを取得する場合、2つのオプションがあります。
- [属性を取得 (Fetch Attrs) ] をクリックして使用可能な属性のリストを取得し、適切な属性を選択します。
  - [UI アクセス属性 (UI Access Attribute) ] を入力します。たとえば Microsoft Active Directory Server では、Active Directory Server ユーザ オブジェクトに uid 属性がないため、[UI アクセス属性 (UI Access Attribute) ] を使用してユーザを取得することがあります。代わりに [UI アクセス属性 (UI Access Attribute) ] フィールドに userPrincipalName と入力して、userPrincipalName 属性を検索できます。
- (注) 認証および認可に CAC 資格情報を使用するには、[UI アクセス属性 (UI Access Attribute) ] フィールドに値を入力する必要があります。

---

### 次のタスク

- [拡張 LDAP 認証オブジェクトの作成 \(104 ページ\)](#) の説明に従って、引き続き LDAP 認証オブジェクトを作成します。

## LDAP グループ フィールド

参照するグループはすべて LDAP サーバに存在する必要があります。スタティック LDAP グループまたはダイナミック LDAP グループを参照できます。スタティック LDAP グループとは、特定のユーザを指し示すグループオブジェクト属性によってメンバーシップが決定されるグループであり、ダイナミック LDAP グループとは、ユーザ オブジェクト属性に基づいてグループ ユーザを取得する LDAP 検索を作成することでメンバーシップが決定されるグループです。ロールのグループアクセス権は、グループのメンバーであるユーザにのみ影響します。

ユーザが Firepower システムにログインするときに付与されるアクセス権は、LDAP 構成によって異なります。

- LDAP サーバでグループアクセス権が設定されていない場合、新しいユーザがログインすると、Firepower システムはそのユーザを LDAP サーバに対して認証し、プラットフォーム設定ポリシーに設定されているデフォルトの最小アクセスロールに基づいてユーザ権限を付与します。
- グループ設定を設定すると、指定されたグループに属している新しいユーザは、メンバーとなっているグループの最小アクセス設定を継承します。
- 新しいユーザが指定のどのグループにも属していない場合は、認証オブジェクトの [グループ制御アクセス ロール (Group Controlled Access Roles) ] セクションに指定されているデフォルトの最小アクセス ロールが割り当てられます。
- 設定されている複数のグループにユーザが属している場合、ユーザは最も高いアクセスを持つグループのアクセス ロールを最小アクセス ロールとして受け取ります。

Firepower システム ユーザ管理ページでは、LDAP グループ メンバーシップによってアクセス ロールが割り当てられているユーザの最小アクセス権を削除することはできません。ただし、追加の権限を割り当てることはできます。外部認証ユーザのアクセス権を変更すると、[ユーザ管理 (User Management)] ページの [認証方式 (Authentication Method)] カラムに、[外部 - ローカルで変更済み (External - Locally Modified)] というステータスが表示されます。



- (注) ダイナミック グループを使用する場合、LDAP クエリは、LDAP サーバで設定されている通りに使用されます。この理由から、検索構文エラーが原因で無限ループが発生することを防ぐため、Firepower システムでは検索の再帰回数が4回に制限されています。この再帰回数内でユーザのグループ メンバーシップが確立されない場合、[グループ制御アクセス ロール (Group Controlled Access Roles)] セクションで定義されているデフォルト アクセス ロールがユーザに付与されます。

#### [Firepower システムのユーザ権限 (Firepower System User Roles)]

各ユーザ ロールを割り当てる必要があるユーザを含む LDAP グループの識別名。

#### [デフォルトのユーザ ロール (Default User Role)]

指定したグループのいずれにも属していないユーザのデフォルトの最小アクセス。

#### [グループ メンバーの属性 (Group Member Attribute)]

スタティック グループに LDAP 検索文字列を含む LDAP 属性。

#### [グループ メンバーの URL 属性 (Group Member URL Attribute)]

ダイナミック グループのメンバーシップを指定する LDAP 属性。

## グループによるアクセス権の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

LDAP グループのユーザのメンバーシップに基づいてデフォルト アクセス権を設定する場合は、Firepower システムにより使用される各アクセス ロールに、LDAP サーバの既存のグループの識別名を指定できます。これを行うと、LDAP によって検出された、指定のどのグループにも属さないユーザのデフォルト アクセス設定を設定できます。ユーザがログインすると、Firepower システムは LDAP サーバを動的に検査し、ユーザの現在のグループ メンバーシップに基づいてデフォルト アクセス権を割り当てます。

グループ制御アクセス ロールを使用してユーザの権限を事前に設定していない場合、ユーザには、プラットフォーム設定ポリシーでデフォルトで付与される権限だけが与えられています。

CAC 認証および認可にオブジェクトを使用する予定の場合、CAC 認証ユーザへのアクセスロール割り当ての管理のために LDAP グループを設定することを推奨します。



- (注) CAC 認証に使用する LDAP 認証オブジェクトを設定する場合は、コンピュータに挿入されている CAC を取り外さないでください。ユーザ証明書を有効にした後では、CAC が常に挿入された状態にしておく必要があります。

#### 始める前に

- 参照する予定のグループが LDAP サーバに存在することを確認します。

#### 手順

**ステップ 1** [外部認証オブジェクトの作成 (Create External Authentication Object) ] ページで、[グループ制御アクセスロール (Group Controlled Access Roles) ] の横の下矢印をクリックします。

**ステップ 2** 必要に応じて、Firepower システムユーザロールに対応する [DN] フィールドに、これらのロールに割り当てる必要があるユーザを含む LDAP グループの識別名を入力します。

例：

たとえば、Example 社の情報テクノロジー (Information Technology) 部門の名前を認証するには、[管理者 (Administrator) ] フィールドに次のように入力します。

```
cn=itgroup,ou=groups, dc=example,dc=com
```

**ステップ 3** [デフォルト ユーザ ロール (Default User Role) ] を選択します。

**ステップ 4** スタティック グループを使用する場合は、[グループメンバー属性 (Group Member Attribute) ] を入力します。

例：

たとえば、デフォルトの Security Analyst アクセスのために参照するスタティック グループのメンバーシップを示すために member 属性を使用する場合は、member と入力します。

**ステップ 5** ダイナミック グループを使用する場合は、[グループメンバー URL 属性 (Group Member URL Attribute) ] を入力します。

例：

たとえば、デフォルトの Admin アクセスに対して指定したダイナミック グループのメンバーを取得する LDAP 検索が memberURL 属性に含まれている場合は、memberURL と入力します。

#### 次のタスク

- [拡張 LDAP 認証オブジェクトの作成 \(104 ページ\)](#) の説明に従って、引き続き LDAP 認証オブジェクトを作成します。

## LDAP シェルアクセスのフィールド

admin アカウントを除き、シェルアクセスは設定したシェルアクセス属性によって完全に制御されます。設定するシェルアクセス フィルタにより、シェルにログインできる LDAP サーバのユーザが決定します。

ログイン時に各シェルユーザのホームディレクトリが作成されること、および（LDAP 接続を無効にすることで）LDAP シェルアクセスユーザアカウントが無効になっている場合はディレクトリが維持されますが、ユーザシェルは /etc/passwd 内の /bin/false に設定され、シェルが無効になることに注意してください。ユーザが再度有効になると、同じホームディレクトリを使用してシェルがリセットされます。

シェルユーザは、小文字、大文字、または小文字と大文字が混在するユーザ名を使用してログインすることができます。シェルのログイン認証では大文字と小文字が区別されます。

### [シェルアクセス属性 (Shell Access Attribute) ]

ユーザがフィルタリング用に使用するアクセス属性です。シェルアクセスの有効なユーザ名が値として設定されている属性であれば、どの属性でも使用できます。

このフィールドを空白のままにした場合、シェルアクセス認証にはユーザ識別名が使用されません。



**ヒント** サーバタイプを選択し、デフォルトを設定すると、そのサーバタイプに適した属性がこのフィールドに事前に取り込まれます。

### [シェルアクセス フィルタ (Shell Access Filter) ]

シェルアクセス用の管理ユーザのエントリを取得するために使用する属性値です。フィルタは、属性名、比較演算子、および属性値です。

[ベースフィルタと同じ (Same as Base Filter) ] チェックボックスを使用すると、ベース DN で限定されるすべてのユーザが、シェルアクセス権限でも限定される場合に、より効率的に検索できます。通常、ユーザを取得する LDAP クエリは、基本フィルタとシェルアクセスフィルタを組み合わせます。シェルアクセスフィルタが基本フィルタと同一である場合は、同じクエリが 2 回実行されることになり、不必要に時間を消費することになります。[ベースフィルタと同じ (Same as Base Filter) ] オプションを使用すると、この両方の目的でクエリを 1 回だけ実行することができます。

このフィールドを空白のままにすると、シェルアクセスの LDAP 認証が回避されます。

## LDAP シェルアクセスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

LDAP サーバを使用して、管理対象デバイスまたは Firepower Management Center でシェルアクセス用のアカウントを認証できます。シェルアクセスを付与するユーザの項目を取得する検索フィルタを指定します。

同一認証オブジェクトで CAC 認証および認可とシェルアクセスの両方を設定することはできません。代わりに、別の認証オブジェクトを作成し、有効にします。

シェルアクセスの認証オブジェクトは、Firepower Management Center の最初の認証オブジェクトである必要があります。

シスコは、NGIPSv デバイスまたは ASA FirePOWER デバイスの外部認証をサポートしていません。さらに、シェルアクセス認証では IPv6 がサポートされていません。



**注意** すべてのアプライアンスで、（外部認証または CLI expert コマンドで取得した）シェルアクセスを持つユーザには、シェルでの sudoers 権限がありますが、これはセキュリティリスクを示す場合があります。外部認証を確立する場合は、シェルアクセスが付与されるユーザのリストを適切に制限してください。同様に、CLI アクセス権限を付与する場合は、構成レベルのアクセス権を持つユーザのリストを制限してください。Firepower Management Center で追加のシェルユーザを設定しないことをお勧めします。

同一認証オブジェクトで CAC 認証および認可とシェルアクセスの両方を設定することはできません。[CAC] チェックボックスをオンにすると、そのページのシェルアクセス設定のオプションが無効になります。代わりに、別の認証オブジェクトを作成し、有効にします。

#### 始める前に

- シェルアクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証 CLI またはシェルユーザを削除します。

#### 手順

**ステップ 1** [外部認証オブジェクトの作成 (Create External Authentication Object)] ページで、ユーザ識別以外のシェルアクセス属性を使用する場合は、[シェルアクセス属性 (Shell Access Attribute)] に入力します。

#### 例：

たとえば、Microsoft Active Directory Server で sAMAccountName シェルアクセス属性を使用してシェルアクセスユーザを取得するには、[シェルアクセス属性 (Shell Access Attribute)] フィールドに sAMAccountName と入力します。

**ステップ 2** シェルアクセス アカウント フィルタを設定します。次の複数のオプションがあります。

- 属性値に基づいて管理ユーザ項目を取得するには、属性名、比較演算子、およびフィルタとして使用する属性値を、カッコで囲んで [シェルアクセスフィルタ (Shell Access Filter)] フィールドに入力します。たとえば、すべてのネットワーク管理者の manager 属性に属性値 shell が設定されている場合は、基本フィルタ (manager=shell) を設定できます。

- 認証設定の設定時に指定したものと同一フィルタを使用するには、[基本フィルタと同じ (Same as Base Filter)] を選択します。
- シェルアクセスの LDAP 認証を防止するには、このフィールドを空白にします。

### 次のタスク

- [拡張 LDAP 認証オブジェクトの作成 \(104 ページ\)](#) の説明に従って、引き続き LDAP 認証オブジェクトを作成します。

## LDAP 認証接続のテスト

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

LDAP サーバを設定し、認証設定を行ったら、これらの設定をテストするため、認証できる必要があるユーザのユーザ資格情報を指定できます。

[ユーザ名 (User Name)] にテストに使用するユーザの uid 属性の値を入力できます。Microsoft Active Directory Server に接続して uid の代わりに UI アクセス属性を指定する場合は、ユーザ名としてこの属性の値を使用します。ユーザの完全修飾識別名も指定できます。

同じユーザのパスワードを使用します。

テスト出力には、有効なユーザ名と無効なユーザ名が示されます。有効なユーザ名は一意的なユーザ名であり、アンダースコア ( \_ )、ピリオド ( . )、ハイフン ( - )、英数字を使用できます。

Web インターフェイスのページサイズ制限のため、ユーザ数が 1000 を超えているサーバへの接続をテストする場合、返されるユーザの数は 1000 であることに注意してください。



### ヒント

テストユーザの名前とパスワードを誤って入力すると、サーバ設定が正しい場合でもテストが失敗します。最初に、追加のテストパラメータを使用せずにサーバ設定をテストします。正常に完了した場合は、テストする特定ユーザのユーザ名とパスワードを指定します。

### 手順

**ステップ 1** [外部認証オブジェクトの追加 (Add External Authentication Object)] ページで、[ユーザ名 (User Name)] と [パスワード (Password)] を入力します。

例 :

たとえば、Example 社のユーザ JSmith の資格情報を取得できるかどうかをテストするには、「JSmith」および「password」を入力します。

ステップ 2 [テスト (Test)] をクリックします。次の 2 つの対処法があります。

- テストが成功した場合、テストの出力がページ下部に表示されます。[保存 (Save)] をクリックします。
- テストが失敗した場合は、接続のトラブルシューティングの提案事項について、[LDAP 認証接続のトラブルシューティング \(122 ページ\)](#) を参照してください。

---

#### 次のタスク

- LDAP 認証を有効にするには、[外部認証の有効化 \(1017 ページ\)](#) の説明に従って、認証オブジェクトを有効にします。

## LDAP 認証接続のトラブルシューティング

LDAP 認証オブジェクトを作成したが、選択したサーバへの接続が失敗したか、または必要なユーザのリストが取得されなかった場合は、そのオブジェクトの設定を調整できます。

接続のテストで接続が失敗する場合は、設定のトラブルシューティングに関する次の推奨手順を試してください。

- 画面上部とテスト出力に示されるメッセージから、問題の原因となっているオブジェクトの部分を確認します。
- オブジェクトに使用したユーザ名とパスワードが有効であることを確認します。
  - サードパーティの LDAP ブラウザを使用して LDAP サーバに接続し、ベース識別名に示されているディレクトリを参照する権限がユーザにあることを確認します。
  - ユーザ名が、LDAP サーバのディレクトリ情報ツリーで一意であることを確認します。
  - テスト出力に LDAP バインドエラー 49 が示される場合は、ユーザのユーザ バインディングが失敗しています。サードパーティアプリケーションを使用してサーバ認証を試行し、その接続でも同様にバインディングが失敗するかどうかを確認します。
- サーバを正しく指定していることを確認します。
  - サーバの IP アドレスまたはホスト名が正しいことを確認します。
  - ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認します。
  - サーバへのアクセスがファイアウォールによって妨げられないこと、およびオブジェクトで設定されているポートがオープンしていることを確認します。
  - 証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、サーバに使用されているホスト名と一致している必要があります。



- シェル アクセスを認証する場合は、サーバ接続に IPv6 アドレスを使用していないことを確認します。
- サーバタイプのデフォルトを使用している場合は、正しいサーバタイプであることを確認し、[デフォルトを設定 (Set Default)] をもう一度クリックしてデフォルト値をリセットします。
- ベース識別名を入力した場合は、[DN を取得 (Fetch DN)] をクリックし、サーバで使用可能なすべてのベース識別名を取得し、リストから名前を選択します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、それぞれが有効であり正しく入力されていることを確認します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、各設定を削除し、設定なしでオブジェクトをテストしてみます。
- 基本フィルタまたはシェル アクセス フィルタを使用している場合は、フィルタがカッコで囲まれており、有効な比較演算子を使用していることを確認します。
- より制限された基本フィルタをテストするには、特定のユーザだけを取得するため、フィルタにそのユーザのベース識別名を設定します。
- 暗号化接続を使用する場合：
  - 証明書の LDAP サーバの名前が、接続に使用するホスト名と一致していることを確認します。
  - 暗号化されたサーバ接続で IPv6 アドレスを使用していないことを確認します。
- テストユーザを使用する場合、ユーザ名とパスワードが正しく入力されていることを確認します。
- テストユーザを使用する場合、ユーザ資格情報を削除してオブジェクトをテストします。
- 次の構文を使用して、接続するアプライアンスでコマンドラインから LDAP サーバに接続し、使用するクエリをテストします。

```
ldapsearch -x -b 'base_distinguished_name'  
-h LDAPserver_ip_address -p port -v -D  
'user_distinguished_name' -W 'base_filter'
```

たとえば、domainadmin@myrtle.example.com ユーザと基本フィルタ (cn=\*) を使用して myrtle.example.com のセキュリティドメインに接続する場合は、次のステートメントを使用して接続をテストできます。

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'  
-h myrtle.example.com -p 389 -v -D  
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

接続のテストが正常に完了したが、プラットフォーム設定ポリシーの適用後に認証が機能しない場合は、使用する認証とオブジェクトの両方が、アプライアンスに適用されるプラットフォーム設定ポリシーで有効になっていることを確認します。

正常に接続されたが、接続で取得されたユーザリストを調整する必要がある場合は、基本フィルタまたはシェルアクセスフィルタを追加または変更するか、ベース DN をさらに制限するかまたは制限を緩めて使用することができます。

## RADIUS 認証

Remote Authentication Dial In User Service (RADIUS) は、ネットワーク リソースへのユーザアクセスの認証、認可、およびアカウントिंगに使用される認証プロトコルです。RFC 2865 に準拠するすべての RADIUS サーバで、認証オブジェクトを作成できます。

RADIUS サーバで認証されたユーザが初めてログインすると、認証オブジェクトでそのユーザに指定されている権限がユーザに付与されます。どのユーザ ロールにもリストされていないユーザには、認証オブジェクトで選択されているデフォルトアクセス権限が付与されます。認証オブジェクトでデフォルトアクセス権限が選択されていない場合は、プラットフォームの設定ポリシーに設定されているデフォルトアクセス権限が付与されます。設定が認証オブジェクトのユーザリストを介して付与されていない場合は、必要に応じてユーザの権限を変更できます。属性照合を使用して RADIUS サーバで認証されたユーザが初めてログインしようとする時、ユーザアカウントが作成されているためログインが拒否されることに注意してください。ユーザはもう一度ログインする必要があります。



- (注) 7000 または 8000 シリーズ デバイスで外部認証を有効にする前に、シェルアクセスフィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証 CLI ユーザをすべて削除してください。

Firepower システムの RADIUS 実装では、SecurID® トークンの使用がサポートされています。SecurID を使用したサーバによる認証を設定すると、そのサーバに対して認証されているユーザが、SecurID PIN の末尾に SecurID トークンを付加し、Cisco システムへのログイン時にそれをパスワードとして使用します。SecurID が外部のユーザを認証するように適切に設定されている限り、これらのユーザは PIN と SecurID を使用して Firepower Management Center または 7000 または 8000 シリーズ デバイスにログインできるので、追加の設定は不要です。

## RADIUS 認証オブジェクトの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

RADIUS 認証オブジェクトの作成時に、認証サーバに接続できるようにする設定を定義します。また、特定のユーザおよびデフォルトユーザにユーザロールを付与します。RADIUS サーバから、認証予定のユーザのカスタム属性が返される場合は、これらのカスタム属性を定義する必要があります。オプションで、CLI またはシェルアクセス認証も設定できます。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

### 始める前に

- ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認します。

### 手順

- 
- ステップ 1 [システム (System)] > [ユーザ (Users)] を選択します。
  - ステップ 2 [外部認証 (External Authentication)] タブをクリックします。
  - ステップ 3 [外部認証オブジェクトの追加 (Add External Authentication Object)] をクリックします。
  - ステップ 4 [認証方式 (Authentication Method)] ドロップダウン リストから [RADIUS] を選択します。
  - ステップ 5 [RADIUS 接続の設定 \(127 ページ\)](#) の説明に従って、認証サーバを指定します。
  - ステップ 6 [RADIUS ユーザ ロールの設定 \(129 ページ\)](#) の説明に従って、ユーザ ロールを設定します。
  - ステップ 7 オプションで、[RADIUS シェルアクセスの設定 \(131 ページ\)](#) の説明に従ってシェルアクセスを設定します。
  - ステップ 8 オプションで、[カスタム RADIUS 属性の定義 \(132 ページ\)](#) の説明に従ってカスタム属性を定義します。
  - ステップ 9 [RADIUS 認証接続のテスト \(133 ページ\)](#) の説明に従って、設定をテストします。
- 

### 例

#### 例

次の図は、IP アドレスが 10.10.10.98 で FreeRADIUS が稼働しているサーバのサンプル RADIUS ログイン認証オブジェクトを示します。接続ではアクセスのためにポート 1812 が使用されること、および不使用期間が 30 秒を経過するとサーバ接続がタイムアウトになり、バックアップ認証サーバへの接続試行前に、サーバ接続が 3 回再試行されることに注意してください。

次の例は、RADIUS ユーザ ロール設定の重要な特徴を示します。

ユーザ ewharton と gsand には、この認証オブジェクトが有効になっているアプライアンスへの管理アクセスが付与されます。

ユーザ cbronte には、この認証オブジェクトが有効になっているアプライアンスへの [メンテナンス ユーザ (Maintenance User)] アクセスが付与されます。

ユーザ cbronte には、この認証オブジェクトが有効になっているアプライアンスへの [セキュリティ アナリスト (Security Analyst)] アクセスが付与されます。

ユーザ ewharton は、シェル アカウントを使用してアプライアンスにログインできます。

次の図に、この例のロール設定を示します。

**RADIUS-Specific Parameters**

Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	ewharton, gsand
External Database User	
Intrusion Admin	
Maintenance User	cbronte
Network Admin	
Discovery Admin	
Security Approver	
Security Analyst	jausten
Security Analyst (Read Only)	
Default User Role	Access Admin Administrator External Database User Intrusion Admin

**Shell Access Filter**

Administrator Shell Access User List	ewharton
--------------------------------------	----------

371902

属性と値のペアを使用して、特定のユーザロールが付与される必要があるユーザを示すこともできます。使用する属性がカスタム属性の場合、そのカスタム属性を定義する必要があります。

次の図は、前述の例と同じ FreeRADIUS サーバのサンプル RADIUS ログイン認証オブジェクトでのロール設定とカスタム属性の定義を示します。

ただしこの例では、Microsoft リモートアクセスサーバが使用されているため、1人以上のユーザの MS-RAS-Version カスタム属性が返されます。MS-RAS-Version カスタム属性は文字列であることに注意してください。この例では、Microsoft v. 5.00 リモートアクセスサーバ経由で RADIUS にログインするすべてのユーザに対し、[セキュリティアナリスト (読み取り専用) (Security Analyst (Read Only))] ロールが付与される必要があります。このため、属性と値のペア MS-RAS-Version=MSRASV5.00 を [セキュリティアナリスト (読み取り専用) (Security Analyst (Read Only))] フィールドに入力します。

**RADIUS-Specific Parameters**

Timeout (Seconds)

Retries

Access Admin

Administrator

External Database User

Intrusion Admin

Maintenance User

Network Admin

Discovery Admin

Security Approver

Security Analyst

Security Analyst (Read Only)

Default User Role

**Shell Access Filter**

Administrator Shell Access User List

**▼ Define Custom RADIUS Attributes**

Attribute Name	Attribute ID	Attribute Type	
<input type="text"/>	<input type="text"/>	<input type="text" value="string"/>	<input type="button" value="Add"/>
MS-Ras-Version	18	string	<input type="button" value="Delete"/>

371901

### 次のタスク

- RADIUS 認証を有効にするには、[外部認証の有効化 \(1017ページ\)](#) の説明に従って認証オブジェクトを有効にします。

## RADIUS 接続の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

RADIUS 認証オブジェクトの作成時には、ローカルアプライアンス（管理対象デバイスまたは Firepower Management Center）が認証のために接続するプライマリおよびバックアップ サーバとサーバポートを最初に指定します。



- (注) RADIUS が正しく機能するためには、ファイアウォールで認証ポートとアカウントングポート（デフォルトでは 1812 および 1813）を開く必要があります。

バックアップ認証サーバを指定する場合は、プライマリサーバへの接続試行操作のタイムアウトを設定できます。プライマリ認証サーバからの応答がない状態で [タイムアウト (Timeout)] フィールド（または LDAP サーバのタイムアウト）に指定された秒数が経過すると、アプライアンスはプライマリサーバに対してクエリを再実行します。

アプライアンスがプライマリ認証サーバに対してクエリを再実行した後に、プライマリ認証サーバからの応答がない状態で [再試行 (Retries)] フィールドに指定された回数を超え、[タイムアウト (Timeout)] フィールドに指定された秒数が再び経過すると、アプライアンスはバックアップサーバにロールオーバーします。

たとえば、プライマリサーバで RADIUS が無効な場合、アプライアンスはバックアップサーバに対してクエリを実行します。ただし RADIUS がプライマリ RADIUS サーバのポートで実行されており、何らかの理由（誤った設定またはその他の問題など）で要求の処理を拒否する場合は、バックアップサーバへのフェールオーバーは行われません。

#### 手順

- ステップ 1 [システム (System)] > [ユーザ (Users)] を選択します。
- ステップ 2 [外部認証 (External Authentication)] タブをクリックします。
- ステップ 3 [外部の作成 (Create External)] > [認証オブジェクト (Authentication Object)] をクリックします。
- ステップ 4 [認証方式 (Authentication Method)] ドロップダウンリストから [RADIUS] を選択します。
- ステップ 5 認証サーバの名前と説明を入力します。
- ステップ 6 認証データを取得するプライマリ RADIUS サーバの IP アドレスまたはホスト名を [プライマリサーバホスト名/IP アドレス (Primary Server Host Name/IP Address)] フィールドに入力します。

(注) シェル認証では IPv6 アドレスはサポートされていません。プライマリ RADIUS サーバに IPv6 アドレスを使用するときにシェル認証を許可するには、サーバの IPv4 アドレスを使用して認証オブジェクトをセットアップし、Firepower Management Center の最初の認証オブジェクトとしてその IPv4 オブジェクトを使用します。
- ステップ 7 オプションで、[プライマリサーバポート (Primary Server Port)] フィールドでプライマリ RADIUS 認証サーバが使用するポートを変更します。

(注) 認証ポート番号とアカウントングポート番号が連続番号ではない場合は、このフィールドを空白にします。システムは、アプライアンスの /etc/services ファイルの radius データと radacct データから RADIUS ポート番号を判断します。
- ステップ 8 プライマリ RADIUS 認証サーバの RADIUS 秘密キーを入力します。

**ステップ 9** オプションで、認証データを取得するバックアップ RADIUS 認証サーバの IP アドレスまたはホスト名を [バックアップサーバホスト名/IP アドレス (Backup Server Host Name/IP Address)] フィールドに入力します。

**ステップ 10** バックアップサーバを設定する場合は、[バックアップサーバポート (Backup Server Port)]、[RADIUS 秘密キー (RADIUS Secret Key)]、および [タイムアウト (Timeout)] を変更し、[再試行 (Retries)] フィールドに、バックアップ接続にロールオーバーするまでプライマリサーバ接続を試行する回数を入力します。

(注) 認証ポート番号とアカウントングポート番号が連続番号ではない場合は、このフィールドを空白にします。システムは、アプライアンスの /etc/services ファイルの radius データと radacct データから RADIUS ポート番号を判断します。

### 次のタスク

- [RADIUS 認証オブジェクトの作成 \(124 ページ\)](#) の説明に従って、引き続き RADIUS 認証オブジェクトを作成します。

## RADIUS ユーザ ロールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ユーザがログインすると、Firepower システムは RADIUS サーバを検査し、RADIUS 構成に基づいてアクセス権を付与します。

- ユーザに対して特定のアクセス権が設定されておらず、デフォルト アクセス ロールが指定されていない場合、新しいユーザがログインすると、Firepower システムは RADIUS サーバに対してそのユーザを認証してから、プラットフォーム設定ポリシーで設定されているデフォルト アクセス ロールに基づいてユーザ権限を付与します。
- 新しいユーザがどのリストにも指定されておらず、認証オブジェクトの [デフォルト ユーザ ロール (Default User Role)] リストでデフォルト アクセス ロールが指定されている場合、ユーザにはこのデフォルト アクセス ロールが割り当てられます。
- 1 つ以上の特定のロールのリストにユーザを追加すると、割り当てられているすべてのアクセス ロールがそのユーザに付与されます。

また、ユーザ名の代わりに属性と値のペアを使用して、特定のユーザ ロールが付与される必要があるユーザを示すこともできます。たとえば、セキュリティアナリストとする必要があるすべてのユーザの User-Category 属性の値が Analyst である場合、これらのユーザにそのロールを付与するには、[セキュリティアナリストリスト (Security Analyst List)] フィールドに User-Category=Analyst と入力します。

外部認証されるが、特定のロールにリストされないすべてのユーザに、デフォルトのユーザロールを割り当てることができます。[デフォルト ユーザ ロール (Default User Role) ] リストでは、複数のロールを指定できます。

Firepower システムのユーザ管理ページで RADIUS ユーザ リスト メンバーシップが設定されているため、アクセスロールが割り当てられているユーザの最小アクセス権を削除することはできません。ただし、追加の権限を割り当てることはできます。



**注意** ユーザの最小アクセス設定を変更するには、[RADIUS 固有パラメータ (RADIUS Specific Parameters) ] セクションのリスト間でユーザを移動するかまたは RADIUS サーバでユーザの属性を変更する他に、構成を管理対象デバイスに再展開し、ユーザ管理ページで割り当てられているユーザ権限を削除する必要があります。

### 始める前に

- ユーザ ロール メンバーシップの設定に使用する場合は、[カスタム RADIUS 属性の定義 \(132 ページ\)](#) の説明に従ってカスタム属性を定義します。

### 手順

**ステップ 1** [外部認証オブジェクトの作成 (Create External Authentication Object) ] ページで、Firepower システムのユーザロールに対応するフィールドに、各ユーザの名前を入力するか、またはそれらのロールに割り当てる属性と値のペアを指定します。

ユーザ名と属性と値のペアは、カンマで区切ります。

例 :

たとえば、ユーザ jsmith と jdoe に管理者ロールを付与する場合は、[管理者 (Administrator) ] フィールドに jsmith, jdoe と入力します。もう 1 つの例として User-Category の値が Maintenance であるすべてのユーザにメンテナンス ユーザ ロールを付与するには、[メンテナンス ユーザ (Maintenance User) ] フィールドに User-Category=Maintenance と入力します。

**ステップ 2** [デフォルト ユーザ ロール (Default User Role) ] リストから、指定のどのグループにも属していないユーザのデフォルト最小アクセス ロールを選択します。

### 次のタスク

- [RADIUS 認証オブジェクトの作成 \(124 ページ\)](#) の説明に従って、引き続き RADIUS 認証オブジェクトを作成します。



## RADIUS シェルアクセスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

RADIUS サーバを使用して、ローカル アプライアンス（管理対象デバイスまたは Firepower Management Center）で、CLI またはシェルアクセスについてアカウントを認証することもできます。CLI またはシェルアクセスを付与するユーザのユーザ名を指定します。



(注) シェル認証では IPv6 アドレスはサポートされていません。IPv6 アドレスを使用してプライマリ RADIUS サーバを設定し、管理シェルアクセスも設定すると、シェルアクセスの設定は無視されます。プライマリ RADIUS サーバに IPv6 アドレスを使用するときにシェル認証を許可するには、サーバの IPv4 アドレスを使用して別の認証オブジェクトをセットアップし、Firepower Management Center の最初の認証オブジェクトとしてそのオブジェクトを使用します。

Admin アカウント以外は、RADIUS 認証オブジェクトで設定したシェルアクセスリストにより、アプライアンスでの CLI またはシェルアクセスが完全に制御されます。CLI またはシェルユーザは、プラットフォーム設定ポリシーを展開するときに、アプライアンスでローカルユーザとして設定されます。属性照合を使用して RADIUS サーバで認証されたユーザが初めてログインしようとするとき、ユーザアカウントが作成されているためログインが拒否されることに注意してください。ユーザはもう一度ログインする必要があります。

ログイン時に各 CLI またはシェルユーザのホーム ディレクトリが作成されること、および（RADIUS 接続を無効にすることで）RADIUS シェルアクセスユーザアカウントが無効になっている場合はディレクトリが維持されますが、ユーザシェルは /etc/password 内の /bin/false に設定され、シェルが無効になることに注意してください。ユーザが再度有効になると、同じホーム ディレクトリを使用してシェルがリセットされます。

CLI またはシェルユーザは、小文字、大文字、または小文字と大文字が混在するユーザ名を使用してログインできます。CLI またはシェルのログイン認証では大文字と小文字が区別されません。



**注意** すべてのアプライアンスで、（外部認証または CLI expert コマンドで取得した）シェルアクセスを持つユーザには、シェルでの sudoers 権限がありますが、これはセキュリティリスクを示す場合があります。外部認証を確立する場合は、シェルアクセスが付与されるユーザのリストを適切に制限してください。同様に、CLI アクセス権限を付与する場合は、構成レベルのアクセス権を持つユーザのリストを制限してください。Firepower Management Center で追加のシェルユーザを設定しないことをお勧めします。

## 手順

[外部認証オブジェクトの作成 (Create External Authentication Object)] ページで、[管理者シェルアクセス ユーザリスト (Administrator Shell Access User List)] フィールドにユーザ名をカンマで区切って入力します。

(注) シェルアクセス フィルタを指定しないことを選択すると、認証オブジェクトの保存時に、フィルタを空白のままにすることを確認する警告が表示されます。

## 次のタスク

- [RADIUS 認証オブジェクトの作成 \(124 ページ\)](#) の説明に従って、引き続き RADIUS 認証オブジェクトを作成します。

## カスタム RADIUS 属性の定義

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

RADIUS サーバが、`/etc/radiusclient/` 内の `dictionary` ファイルに含まれていない属性の値を返し、これらの属性を使用してユーザにユーザロールを設定する予定の場合は、ログイン認証オブジェクトでこれらの属性を定義する必要があります。RADIUS サーバでユーザプロフィールを調べると、ユーザについて返される属性を見つけることができます。

属性を定義する場合は、英数字からなる属性名を指定します。属性名の中の単語を区切るには、スペースではなくダッシュを使用することに注意してください。また、指定する属性 ID は整数であり、`etc/radiusclient/dictionary` ファイルの既存の属性 ID と競合してはなりません。属性のタイプ (文字列、IP アドレス、整数、または日付) も指定します。

RADIUS 認証オブジェクトの作成時に、そのオブジェクトの新しいディクショナリファイルがアプライアンスの `/var/sf/userauth` ディレクトリに作成されます。認証オブジェクトに追加するカスタム属性はすべて、そのディクショナリ ファイルに追加されます。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

## 手順

**ステップ 1** [外部認証オブジェクトの追加 (Add External Authentication Object)] ページで、矢印をクリックして [カスタム RADIUS 属性の定義 (Define Custom RADIUS Attributes)] セクションを展開します。

**ステップ 2** [属性名 (Attribute Name)] フィールドに属性名を入力します。

**ステップ 3** [属性 ID (Attribute ID)] フィールドに、属性 ID を整数形式で入力します。

**ステップ 4** [属性タイプ (Attribute Type)] ドロップダウン リストから、属性のタイプを選択します。

**ステップ 5** 認証オブジェクトにカスタム属性を追加するには、[追加 (Add)] をクリックします。

ヒント 認証オブジェクトからカスタム属性を削除するには、その属性の横にある [削除 (Delete)] をクリックします。

### 例

シスコルータが接続しているネットワーク上で RADIUS サーバが使用される場合に、Ascend-Assign-IP-Pool 属性を使用して、特定の IP アドレス プールからログインするすべてのユーザに特定のロールを付与するとします。Ascend-Assign-IP-Pool は、ユーザがログインできるアドレス プールを定義する整数属性であり、割り当てられる IP アドレス プールの番号を示す整数が指定されます。

そのカスタム属性を宣言するには、属性名が Ascend-IP-Pool-Definition、属性 ID が 218、属性タイプが integer のカスタム属性を作成します。

次に、Ascend-IP-Pool-Definition 属性値が 2 のすべてのユーザに対し、読み取り専用の Security Analyst 権限を付与するには、Ascend-Assign-IP-Pool=2 を [セキュリティアナリスト (読み取り専用) (Security Analyst (Read Only))] フィールドに入力します。

### 次のタスク

- [RADIUS 認証オブジェクトの作成 \(124 ページ\)](#) の説明に従って、引き続き RADIUS 認証オブジェクトを作成します。

## RADIUS 認証接続のテスト

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

RADIUS 接続、ユーザ ロール、およびカスタム属性を設定したら、これらの設定をテストするため、認証できる必要があるユーザのユーザ資格情報を指定できます。

ユーザ名として、テストするユーザのユーザ名を入力できます。

UI のページサイズ制限のため、ユーザ数が 1000 を超えているサーバへの接続をテストする場合、返されるユーザの数は 1000 であることに注意してください。



**ヒント** テストユーザの名前とパスワードを誤って入力すると、サーバ設定が正しい場合でもテストが失敗します。サーバ設定が正しいことを確認するには、最初に [追加のテストパラメータ (Additional Test Parameters)] フィールドにユーザ情報を入力せずに [テスト (Test)] をクリックします。正常に完了した場合は、テストする特定ユーザのユーザ名とパスワードを指定します。

#### 手順

**ステップ 1** [外部認証オブジェクトの追加 (Add External Authentication Object)] ページの [ユーザ名 (User Name)] フィールドと [パスワード (Password)] フィールドに、RADIUS サーバへのアクセスの検証に資格情報が使用されるユーザのユーザ名とパスワードを入力します。

例 :

たとえば、Example 社の jsmith のユーザ資格情報を取得できるかどうかをテストするには、「jsmith」と入力します。

**ステップ 2** [詳細の表示 (Show Details)] を選択し、[テスト (Test)] をクリックします。

**ステップ 3** テストが成功した場合は [保存 (Save)] をクリックします。

#### 次のタスク

- RADIUS 認証を有効にするには、[外部認証の有効化 \(1017 ページ\)](#) の説明に従って、認証オブジェクトを有効にします。

## シングルサインオン (SSO)

シングルサインオン (SSO) により、Cisco Security Manager (CSM) バージョン 4.7 以上と Firepower Management Center を統合して、ログインの追加認証なしで CSM から Firepower Management Center にアクセスできるようにすることができます。ASA FirePOWER モジュールの管理では、モジュールに展開したポリシーの変更が必要となる場合もあります。CSM で Firepower Management Center を管理して、Web ブラウザで起動するという方法を選択することもできます。

ユーザロールに基づくアクセス権限がある場合、CSM でクロス起動したデバイスの [デバイス管理 (Device Management)] ページの [デバイス (Device)] タブに移動します。それ以外の場合は、[サマリー ダッシュボード (Summary Dashboard)] ページ ([概要 (Overview)] > [ダッシュボード (Dashboards)]) に移動します。ただしダッシュボードにアクセスできないユーザアカウントの場合は、[ようこそ (Welcome)] ページが使用されます。



(注) 組織で認証に CAC が使用されている場合、シングルサインオンでログインすることはできません。

#### 関連トピック

[セキュリティ認定準拠](#)

## SSO の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	ASA FirePOWER	任意 (Any)	Admin

シングルサインオンを設定する前に、CSM から Firepower Management Center への一方向の暗号化認証パスを設定する必要があります。

NAT 環境では、Firepower Management Center と CSM は NAT 境界の同じ側に存在している必要があります。CSM と Firepower Management Center 間の通信を有効にする特定の基準を入力する必要があります。



(注) 組織で認証に CAC が使用されている場合は、シングルサインオンでログインできません。

#### 手順

- ステップ 1** CSM から、接続を識別する SSO 共有暗号キーを生成します。詳細については、CSM のマニュアルを参照してください。
- ステップ 2** Firepower Management Center から、[システム (System)] > [ユーザ (Users)] を選択します。
- ステップ 3** [CSM シングルサインオン (CSM Single Sign-on)] を選択します。
- ステップ 4** CSM ホスト名または IP アドレスとサーバのポートを入力します。
- ステップ 5** CSM から生成した共有キーを入力します。
- ステップ 6** オプションで、Firepower Management Center のプロキシサーバを使用して CSM と通信する場合は、[接続にプロキシを使用 (Use Proxy For Connection)] チェックボックスをオンにします。
- ステップ 7** [送信 (Submit)] をクリックします。
- ステップ 8** [証明書の確認 (Confirm Certificate)] をクリックして証明書を保存します。  
これで CSM から Firepower Management Center にログインできるようになります。追加のログインを実行する必要はありません。





## 第 5 章

# Firepower システムのライセンス

ここでは、Firepower システムのライセンスを適用する方法について説明します。

- [Firepower の機能ライセンスについて](#) (137 ページ)
- [Firepower 機能のサービス サブスクリプション](#) (138 ページ)
- [Firepower システムのスマートライセンス](#) (139 ページ)
- [Firepower システムのクラシック ライセンス](#) (150 ページ)
- [管理対象デバイスへのライセンスの割り当て](#) (159 ページ)

## Firepower の機能ライセンスについて

組織に対して Firepower システムの最適な展開を実現するために、さまざまな機能についてライセンスを取得することができます。Firepower Management Center では、これらの機能ライセンスを管理してデバイスに割り当てることができます。



(注) Firepower Management Center はデバイスの機能ライセンスを管理しますが、Firepower Management Center を使用するための機能ライセンスは必要ありません。

Firepower 機能ライセンスは、デバイスの種類に応じて次のように異なります。

- スマート ライセンスは Firepower Threat Defense および Firepower Threat Defense Virtual デバイスに使用可能です。
- 従来型ライセンスは 7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv デバイスに使用可能です。従来のライセンスを使用するデバイスは、クラシックデバイスと呼ばれることもあります。

1 つの Firepower Management Center で従来のライセンスとスマートライセンスの両方を管理できます。

## Firepower 機能のサービス サブスクリプション

サービスサブスクリプションは、所定の時間内限定で、管理対象デバイス上の特定のFirepower機能を有効にします。サービスサブスクリプションは、1年、3年、または5年単位で購入できます。サブスクリプションの期限が切れると、サブスクリプションの更新が必要であることが通知されます。Firepower Threat Defense デバイスのサブスクリプションの場合、期限が切れても、関連する機能を引き続き使用できます。クラシックデバイスのサブスクリプションの期限が切れた場合、機能のタイプによっては、関連機能を使用できなくなることがあります。

サービスサブスクリプションは、Firepower システムで管理対象デバイスに割り当てるライセンスと、次のように対応しています。

表 14: サブスクリプションおよび対応するスマートライセンス

購入するサブスクリプション	Firepower システム内で割り当てるスマートライセンス
T	脅威 (Threat)
TC	脅威 + URL フィルタリング
TM	脅威 + マルウェア
TMC	脅威 + URL フィルタリング + マルウェア
URL	URL フィルタリング (Threat に追加するか、Threat なしで使用できます)
AMP	マルウェア (Threat に追加するか、Threat なしで使用できます)

スマートライセンスを使用する管理対象デバイスを購入すると、基本ライセンスが自動的に提供されます。このライセンスは無制限であり、システムアップデートを使用可能にします。Firepower Threat Defense デバイスでは、すべてのサービスサブスクリプションがオプションです。

表 15: サブスクリプションおよび対応するクラシックライセンス

購入するサブスクリプション	Firepower システム内で割り当てるクラシックライセンス
TA	制御 + 保護 (別名「脅威 & アプリ」、システム更新に必要)
TAC	制御 + 保護 + URL フィルタリング
TAM	制御 + 保護 + マルウェア
TAMC	制御 + 保護 + URL フィルタリング + マルウェア
URL	URL フィルタリング (TA が既に存在する場合はアドオン)



購入するサブスクリプション	Firepower システム内で割り当てるクラシック ライセンス
AMP	マルウェア (TA が既に存在する場合はアドオン)

クラシック ライセンスを使用する管理対象デバイスを購入すると、制御および保護のライセンスが自動的に提供されます。これらのライセンスは無期限ですが、システムの更新を有効にするには、TA サービス サブスクリプションを購入する必要があります。追加機能のサービス サブスクリプションはオプションです。

## Firepower システムのスマート ライセンス

Firepower Threat Defense デバイスでは Smart Licensing が使用されます。

Cisco Smart Licensing によって、ライセンスを購入し、ライセンスのプールを一元管理することができます。製品認証キー (PAK) ライセンスとは異なり、スマートライセンスは特定のシリアル番号またはライセンスキーに関連付けられません。Smart Licensing を利用すれば、ライセンスの使用状況やニーズをひと目で評価できます。

また、Smart Licensing では、まだ購入していない製品の機能を使用できます。Cisco Smart Software Manager に登録すると、すぐにライセンスの使用を開始できます。また、後でライセンスを購入することもできます。これによって、機能の展開および使用が可能になり、発注書の承認による遅延がなくなります。

## Smart Software Manager

Firepower 機能のスマートライセンスを複数購入する場合は、それらのライセンスを Cisco Smart Software Manager (<http://www.cisco.com/web/ordering/smart-software-manager/index.html>) で管理できます。Smart Software Manager では、組織のマスター アカウントを作成できます。

デフォルトでは、ライセンスはマスターアカウントの下のデフォルトの仮想アカウントに割り当てられます。アカウントの管理者として、たとえば、地域、部門、または子会社ごとに、追加の仮想アカウントを作成できます。複数の仮想アカウントを使用することで、多数のライセンスおよびアプライアンスの管理を行うことができます。

ライセンスとアプライアンスは、バーチャルアカウント別に管理します。バーチャルアカウントに割り当てられているライセンスを使用できるのは、そのバーチャルアカウントのアプライアンスのみです。追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。また、仮想アカウント間でのアプライアンスの譲渡も可能です。

バーチャルアカウントごとに、製品インスタンス登録トークンを作成できます。各 Firepower Management Center を展開するか、または既存の Management Center を登録する場合は、このトークン ID を入力します。既存のトークンの有効期限が切れている場合は、新しいトークンを作成できます。トークンの有効期限が切れても、そのトークンを使用して登録された Management Center には影響しませんが、有効期限が切れたトークンを使用して Management Center を登録することはできません。また、登録済み Management Center は、使用するトークンに基づいてバーチャルアカウントに関連付けられます。

Cisco Smart Software Manager の詳細については、*Cisco Smart Software Manager User Guide* を参照してください。

## ライセンス認証局との定期通信

Firepower Management Center の登録に製品インスタンス登録トークンを使用すると、このアプライアンスがシスコのライセンス認証局に登録されます。ライセンス認証局は、Firepower Management Center とライセンス認証局間の通信用に ID 証明書を発行します。この証明書の有効期間は 1 年ですが、6 か月ごとに更新されます。ID 証明書の期限が切れた場合（通常は、9 か月または 1 年間通信がない状態）、Firepower Management Center は登録解除状態に戻り、ライセンス機能の使用は中断されます。

Firepower Management Center は、定期的にライセンス認証局と通信します。Smart Software Manager で変更を加えた場合は、Firepower Management Center 上で認証を更新すると、その変更がすぐに適用されます。また、スケジュールどおりにアプライアンスが通信するのを待つこともできます。

必要に応じて、スマート ソフトウェア サテライト サーバをライセンス認証局と通信するように設定できます。Firepower Management Center は、Cisco Smart Software Manager を介してライセンス認証局に直接インターネットでアクセスするか、スケジュールした期間でスマートソフトウェア サテライト サーバを介してアクセスする必要があります。通常のライセンスに関する通信は 30 日ごとに行われますが、これには猶予期間があり、アプライアンスはホームをコールすることなく最大で 90 日間は動作します。90 日が経過する前にライセンス認証局と連絡を取る必要があります。

Smart Software Satellite Server の設定についての詳細は、*Smart Software Manager Satellite User Guide* を参照してください。

## スマート ライセンスのステータス

スマートライセンスのステータスでは、次のとおり Firepower Management Center でのライセンス使用の概要を説明します。

### 使用の認証

可能なステータス値は次のとおりです。

- [認証済み (Authorized)] : Firepower Management Center は、アプライアンスのライセンス付与資格を承認するライセンス認証局に正常に連絡して登録されています。
- [コンプライアンス不適合 (Out-of-Compliance)] : ライセンス認証局が Firepower Management Center で使用可能なライセンス権限を識別できませんでした。ライセンスされた機能は動作を継続します。ただし、[認証済み (Authorized)] として表示するには、ステータスの追加の権限付与を購入するか、解放するかのいずれかを行う必要があります。
- [認証期限切れ (Authorization Expired)] : Firepower Management Center は、90 日以上ライセンス認証局と通信していません。ライセンスされた機能は動作を継続します。この状態の場合、アプライアンスは認証要求を再試行します。再試行が成功した場合、ステータス

は [コンプライアンス不適合 (Out-of-Compliance) ] または [認証済み (Authorized) ] のどちらかに設定され、新しい認証期間が開始されます。

### 製品登録

Firepower Management Center がライセンス認証局に連絡し登録された最終日を指定します。

### 割当済みの仮想アカウント

製品インスタンス登録トークンの生成に使用したスマートアカウントの下の仮想アカウントを指定し、Firepower Management Center を登録します。

### 輸出管理機能

Smart Software Manager で Firepower Management Center のエクスポート制御機能を有効にしたかどうかを指定します。このオプションを有効にすると、国家安全保障、外交政策、反テロリズムに関する法律や規制の対象となるソフトウェア機能を導入できます。

Firepower Management Center でエクスポート制御オプションを変更することはできません。このオプションは、Smart Software Manager で Firepower Management Center の製品インスタンス登録トークンを作成するときに設定されます。

## スマート ライセンスの移転

スマート ライセンスを Firepower Management Center に登録すると、バーチャルアカウントでそのライセンスが Management Center に割り当てられます。スマート ライセンスを他の Firepower Management Center に移転する必要がある場合は、現在ライセンスが適用されている Management Center の登録を解除する必要があります。これにより、バーチャルアカウントからスマート ライセンスが削除され、既存のライセンスが解放されるので、そのライセンスを新しい Management Center に登録できるようになります。登録を解除しないと、バーチャルアカウントで使用可能なライセンスの数が足りなくなるので、非準拠通知を受け取ります。

## スマート ライセンスのタイプと制約事項

ここでは、Firepower システムの導入環境で使用可能なスマート ライセンスのタイプについて説明します。Firepower Management Center では、Firepower Threat Defense のデバイスを管理するためスマート ライセンスが必要です。

次の表に、Firepower システムのスマート ライセンスの概要を示します。

表 16: Firepower システムのスマート ライセンス

Firepower システムで割り当てるライセンス	購入するサブスクリプション	時間 (Duration)	付与される機能
基本 (自動的にすべての Firepower Threat Defense デバイスに付属)	なし (デバイスに付属)	永久	ユーザおよびアプリケーション制御 スイッチングとルーティング NAT
脅威 (Threat)	T	期間ベース	侵入検知と防御 ファイル制御 セキュリティインテリジェンス フィルタリング
マルウェア	<ul style="list-style-type: none"> <li>• TM (脅威 (Threat) + マルウェア (Malware) )</li> <li>• TMC (脅威 (Threat) + マルウェア (Malware) + URL)</li> <li>• AMP</li> </ul>	期間ベース	AMP for Firepower (ネットワークベースの高度なマルウェア防御) AMP Threat Grid
URL フィルタリング (URL Filtering)	<ul style="list-style-type: none"> <li>• TC (脅威 (Threat) + URL)</li> <li>• TMC (脅威 (Threat) + マルウェア (Malware) + URL)</li> <li>• URL</li> </ul>	期間ベース	カテゴリとレピュテーションに基づく URL フィルタリング
仮想 Firepower Management Center	なし (ソフトウェアに付属)	永久	Firepower Management Center 仮想アプライアンスでの Firepower Threat Defense デバイスの登録

Firepower システムで割り当てるライセンス	購入するサブスクリプション	時間 (Duration)	付与される機能
輸出管理機能	なし (製品インスタンス登録オプション)	永久	国家安全保障、外交政策、反テロリズムに関する法律や規制の対象となる機能：を参照してください。 <a href="#">スマートライセンスのステータス (140 ページ)</a>

## 基本ライセンス

基本ライセンスでは、次のことができます。

- アクセスコントロールルールにユーザとアプリケーションの条件を追加することで、ユーザとアプリケーションの制御を実装する
- スイッチングおよびルーティング (DHCP リレーおよび NAT を含む) を実行するように Firepower Threat Defense デバイスを設定する
- Firepower Threat Defense デバイスをハイ アベイラビリティ ペアとして設定する
- Firepower 9300 シャーシ内のクラスタとしてセキュリティ モジュールを設定する (シャーシ内クラスタリング)
- Firepower Threat Defense を実行している Firepower 9300 または Firepower 4100 シリーズ デバイスをクラスタとして設定する (シャーシ間クラスタリング)

Firepower Threat Defense デバイスまたは Firepower Threat Defense Virtual を購入すると、自動的に基本ライセンスが付いてきます。すべての追加ライセンス (Threat、Malware、URL Filtering) はオプションです。

基本ライセンスは、登録するすべての Firepower Management Center デバイスの Firepower Threat Defense に追加されます。

## Firepower Threat Defense デバイスのマルウェア ライセンス

Firepower Threat Defense デバイス用のマルウェア ライセンスを使用すると、AMP for Firepower および AMP Threat Grid を使用して Cisco Advanced Malware Protection (AMP) を実行することができます。この機能では、Firepower Threat Defense デバイスを使用して、ネットワーク上で伝送されるファイルのマルウェアを検出してブロックできます。この機能ライセンスをサポートするために、スタンドアロン サブスクリプションとしてマルウェア (AMP) サービス サブスクリプションを購入できます。また、脅威 (TM) や脅威および URL フィルタリング (TMC) サブスクリプションと組み合わせて購入することもできます。



- (注) マルウェアライセンスが有効になっている Firepower Threat Defense 管理対象デバイスは、動的分析を設定していない場合でも、定期的に AMP クラウドへの接続を試行します。このため、デバイスの [インターフェイストラフィック (Interface Traffic)] ダッシュボードウィジェットには、送信済みトラフィックが表示されます。これは正常な動作です。

ファイルポリシーの一部として AMP for Firepower を設定し、その後 1 つ以上のアクセスコントロールルールを関連付けます。ファイルポリシーは、特定のアプリケーションプロトコルを使用して特定のファイルをアップロードまたはダウンロードするユーザを検出できます。AMP for Firepower によって、ローカルマルウェア分析とファイルの事前分類を使用して、これらの制限されたファイルタイプのセットにマルウェアがないかを検査できます。特定のファイルタイプをダウンロードして AMP Threat Grid クラウドにアップロードして、動的 Spero 分析でマルウェアが含まれているかどうかを判別することもできます。これらのファイルでは、ファイルがネットワーク内で経由する詳細なパスを示すネットワークファイルトラジェクトリを表示できます。マルウェアライセンスでは、ファイルリストに特定のファイルを追加し、そのファイルリストをファイルポリシー内で有効にすることもできます。これにより、検出時にこれらのファイルを自動的に許可またはブロックできます。

マルウェアライセンスをすべて無効にすると、システムは AMP への問い合わせを停止し、AMP クラウドから送信される遡及的イベントの確認応答も停止します。既存のアクセスコントロールポリシーに AMP for Firepower 構成が含まれている場合は、それらのポリシーを再展開することができません。マルウェアライセンスが無効にされた後、システムが既存のキャッシュファイルの性質を使用できるのは極めて短時間のみであることに注意してください。この時間枠の経過後、システムは Unavailable という性質をこれらのファイルに割り当てます。

マルウェアライセンスが必要なのは AMP for Firepower および AMP Threat Grid を展開する場合のみであることに注意してください。マルウェアライセンスがなければ、Firepower Management Center は AMP クラウドからエンドポイント向け AMP マルウェア イベントおよび侵害の兆候 (IOC) を受信できます。

## 脅威ライセンス

脅威ライセンスでは、侵入の検出と防御、ファイル制御、およびセキュリティインテリジェンスのフィルタリングを実行することができます。

- 侵入検知および防御により、侵入とエクスプロイトを検出するためネットワークトラフィックを分析できます。またオプションで違反パケットをドロップできます。
- ファイル制御により、特定のアプリケーションプロトコルを介した特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード (送信) またはダウンロード (受信) をブロックできます。マルウェアライセンスが必要な AMP for Firepower を使用すると、制限されたファイルタイプセットを、その処置に基づいて検査およびブロックすることができます。
- セキュリティインテリジェンスフィルタリングにより、トラフィックをアクセス制御ルールによる分析対象にする前に、特定の IP アドレス、URL、および DNS ドメイン名をブラックリストに追加 (その IP アドレスとの間のトラフィックを拒否) できます。ダイナ

ミックフィールドにより、最新の情報に基づいて接続をただちにブラックリストに追加できます。オプションで、セキュリティインテリジェンス フィルタリングに「モニタのみ」設定を使用できます。

脅威ライセンスは、スタンドアロンサブスクリプション (T) として、または URL フィルタリング (TC)、マルウェア (TM)、またはその両方 (TCM) と組み合わせて購入することができます。

管理対象デバイスで脅威ライセンスを無効にすると、Firepower Management Center で、影響を受けたデバイスからの侵入イベントとファイルイベントの確認応答が停止されます。結果として、トリガー条件としてこれらのイベントを使用する関連ルールがトリガーしなくなります。また、Firepower Management Center はシスコ提供またはサードパーティのセキュリティインテリジェンス情報を取得するためにインターネットに接続しなくなります。脅威ライセンスを再度有効にするまでは、既存のポリシーを適用し直すことができません。

## Firepower Threat Defense デバイスの URL フィルタリング ライセンス

URL フィルタリング ライセンスにより、モニタ対象ホストにより要求される URL に基づいて、ネットワーク内を移動できるトラフィックを判別するアクセス制御ルールを作成することができます。この機能ライセンスをサポートするために、スタンドアロンサブスクリプションとして URL フィルタリング (URL) サービスサブスクリプションを購入できます。また、脅威 (TM) や脅威およびマルウェア (TMC) サブスクリプションと組み合わせて購入することもできます。



### ヒント

URL フィルタリング ライセンスがない状態で、許可またはブロックする個別 URL または URL グループを指定できます。これにより、Web トラフィックをカスタムできめ細かく制御できますが、URL カテゴリおよびレピュテーションデータをネットワークトラフィックのフィルタリングに使用することはできません。

URL フィルタリング ライセンスがない状態でも、アクセス制御ルールにカテゴリベースの URL 条件およびレピュテーションベースの URL 条件を追加できますが、Firepower Management Center は URL 情報をダウンロードしません。最初に URL フィルタリングライセンスを Firepower Management Center に追加し、ポリシー適用対象デバイスで有効にするまでは、アクセスコントロールポリシーを適用できません。

管理対象デバイスで URL フィルタリングを無効にすると、URL フィルタリングにアクセスできなくなることがあります。ライセンスが期限切れになるか、ライセンスを無効にすると、URL 条件が含まれているアクセス制御ルールは URL フィルタリングを直ちに停止し、Firepower Management Center は URL データのアップデートをダウンロードできなくなります。既存のアクセスコントロールポリシーに、カテゴリベースまたはレピュテーションベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。

## Firepower Management Center Virtual ライセンス

Firepower Management Center Virtual ライセンスは、機能ライセンスではなく、プラットフォームライセンスです。ご購入いただく仮想ライセンスのバージョンによって、Firepower Management

Center を介して管理可能なデバイスの数が決まります。たとえば、2 台、10 台、または 25 台のデバイスを管理可能なライセンスをご購入いただけます。

## Cisco Smart Software Manager での Firepower Management Center の登録

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	グローバルのみ	Admin

### 始める前に

- まだ作成していない場合は、スマート アカウントを作成します。<https://www.cisco.com/c/en/us/buy/smart-accounts.html>を参照してください。
- Cisco Smart Software Manager によって提供される製品インスタンス登録トークンを取得します。このトークンは、バーチャルアカウントに固有です。
- Firepower Management Center で NTP デーモンが実行されていることを確認します。登録時に、NTP サーバと Cisco Smart Software Manager の間でキー交換が実行されるため、適切な登録には時刻の同期が必要です。

### 手順

- 
- ステップ 1** [システム (System)] > [ライセンス (Licenses)] > [スマート ライセンス (Smart Licenses)] を選択します。
  - ステップ 2** [登録 (Register)] をクリックします。
  - ステップ 3** 製品インスタンス登録トークンがない場合は、[Cisco Smart Software Manager] をクリックして、割り当て済みのバーチャルアカウントからトークンを取得します。
  - ステップ 4** トークンをコピーして、Firepower Management Center の Web インターフェイス内の [製品インスタンス登録トークン (Product Instance Registration Token)] フィールドに貼り付けて、[変更の適用 (Apply Changes)] をクリックします。
- 

### 次のタスク

- Firepower Threat Defense デバイスを登録します。[Firepower Management Center へのデバイスの追加 \(550 ページ\)](#) を参照してください。
- ライセンスを Firepower Threat Defense に割り当てます。[管理対象デバイスへのライセンスの割り当て \(159 ページ\)](#) を参照してください。



## スマートライセンスおよびスマートライセンス ステータスの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	グローバルのみ	Admin

[スマートライセンス (Smart Licenses)] ページで、Firepower Management Center とその管理対象 Firepower Threat Defense デバイスのスマートライセンスを表示します。このページでは、展開におけるライセンスのタイプごとに、そのライセンスを使用している管理対象デバイスの合計数、そのライセンスが準拠されているかどうか、デバイスタイプ、デバイスが配置されているドメインとグループが表示されます。また、Firepower Management Center のスマートライセンス ステータスを表示できます。

[スマートライセンス (Smart Licenses)] ページ以外にも、ライセンスを表示できる方法がいくつかあります。

- [製品ライセンス (Product Licensing)] ダッシュボード ウィジェットはライセンスの概要を示します。
- [デバイス管理 (Device Management)] ページ ([デバイス (Devices)] > [デバイス管理 (Device Management)]) は、各管理対象デバイスに適用されているライセンスをリストします。
- ヘルス ポリシーで使用される際に、スマートライセンス モニタのヘルス モジュールはライセンス ステータスを伝達します。

### 手順

- 
- ステップ 1** [システム (System)] > [ライセンス (Licenses)] > [スマートライセンス (Smart Licenses)] を選択します。
- ステップ 2** 各デバイスのライセンスのステータス、デバイス タイプ、ドメイン、グループを表示するには、目的のライセンス タイプの横にある矢印をクリックします。
- 

## スマートライセンスの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	グローバルのみ	Admin

複数の Firepower Threat Defense デバイスのスマートライセンスを一度に有効または無効にすることができます。一部の例外はありますが、管理対象デバイスでライセンスを無効にすると、そのライセンスに関連付けられている機能は使用できなくなります。

#### 手順

- 
- ステップ 1** [システム (System)] > [ライセンス (Licenses)] > [スマート ライセンス (Smart Licenses)] を選択します。
- ステップ 2** [ライセンスの編集 (Edit Licenses)] をクリックします。
- ステップ 3** [マルウェア (Malware)]、[脅威 (Threat)]、または [URL フィルタリング (URL Filtering)] のいずれかのタブをクリックします。
- ステップ 4** ライセンスを付与するデバイスを選択するには、[追加 (Add)] をクリックします。
- ステップ 5** [適用 (Apply)] をクリックします。
- 

## Cisco Smart Software Manager から Firepower Management Center の登録解除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	グローバルのみ	Admin

Cisco Smart Software Manager から Firepower Management Center の登録を解除すると、バーチャルアカウントから Management Center が削除されます。Firepower Management Center リリースに関連付けられているライセンス権限はすべて、ご使用のバーチャルアカウントに戻ります。登録解除後、Firepower Management Center は適用モードになり、ライセンスが適用される機能に対する更新および変更が許可されなくなります。

#### 手順

- 
- ステップ 1** [システム (System)] > [ライセンス (Licenses)] > [スマート ライセンス (Smart Licenses)] を選択します。
- ステップ 2** 登録解除アイコン (●) をクリックします。
-

## Cisco Smart Software Manager と Firepower Management Center の同期

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	グローバルのみ	Admin

Cisco Smart Software Manager に変更を加えた場合は、すぐに変更が有効になるように Firepower Management Center 上で認証を更新できます。

### 手順

- 
- ステップ 1** [システム (System)] > [ライセンス (Licenses)] > [スマート ライセンス (Smart Licenses)] を選択します。
- ステップ 2** 更新アイコン (🔄) をクリックします。
- 

## Smart Software Satellite Server の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	グローバルのみ	Admin

Cisco Smart Software Manager は、ライセンス認証局と通信してライセンスを管理します。Firepower Management Center はインターネットに接続している場合、Smart Software Manager に直接接続します。また、Smart Software Satellite Server から Smart Software Manager に接続できます。

Smart Software Satellite Server は、ライセンス認証局との定期的な通信を維持し、同期をスケジュールするか、手動でスマート ライセンス認証を Smart Software Manager と同期できます。

Smart Software Satellite Server は、次の場合に使用できます。

- Firepower Management Center がオフラインであるか、接続が制限されているか、接続がない場合。
- Firepower Management Center に固定接続があるが、ネットワークからの単一の接続によってスマート ライセンスを制御する場合。

Smart Software Satellite Server の設定の詳細については、*Smart Software Manager Satellite User Guide*を参照してください。

## 手順

ステップ1 [システム (System)] > [統合 (Integration)] を選択します。

ステップ2 [Smart Software Satellite] タブをクリックします。

ステップ3 次の選択肢があります。

- Firepower Management Center はインターネットにアクセスできる場合は、[Cisco Smart Software Manager に直接接続 (Connect directly to Cisco Smart Software Manager)] を選択します。
- Firepower Management Center がインターネットにアクセスできない場合は、[Cisco Smart Software Satellite Server に接続 (Connect to Cisco Smart Software Satellite Server)] を選択して、サーバの URL を入力し、SSL 証明書を選択します。

ステップ4 [適用 (Apply)] をクリックします。

# Firepower システムのクラシック ライセンス

クラシックライセンスでは、製品認証キー (PAK) をアクティブ化する必要があり、デバイス間で譲渡することはできません。クラシックライセンスは、「従来のライセンス」と呼ばれることもあります。

7000 および 8000 シリーズ デバイス、NGIPSv デバイス、および ASA FirePOWER モジュールはクラシック ライセンスを使用します。

## 製品ライセンス登録ポータル

Firepower 機能のクラシック ライセンスを 1 つ以上購入する場合は、それらのライセンスを Cisco Product License Registration ポータルで管理します。

<http://www.cisco.com/web/go/license>

このポータルの使用方法の詳細については、次を参照してください。

<https://www.cisco.com/web/fw/tools/swift/xui/html/help.html>

## 従来のライセンスのタイプと制約事項

ここでは、Firepower システム展開環境で使用可能な従来のライセンスのタイプについて説明します。デバイスで有効にできるライセンスは、デバイスのモデル、バージョン、および他の有効なライセンスによって異なります。

7000 および 8000 シリーズ デバイス、NGIPSv デバイス、および ASA FirePOWER モジュールの場合、ライセンスはモジュール固有です。ライセンスがデバイスのモデルと完全に一致しない限り、管理対象デバイスでライセンスを有効にすることはできません。たとえば、Firepower

8250 マルウェア ライセンス (FP8250-TAM-LIC=) を使用して 8140 デバイスでマルウェア関連の機能を有効にすることはできません。Firepower 8140 マルウェア ライセンス (FP8140-TAM-LIC=) を購入する必要があります。



(注) NGIPSv または ASA FirePOWER では、制御ライセンスを使用してユーザとアプリケーションの制御を実行できますが、それらのデバイスはスイッチング、ルーティング、スタッキング、または 7000 および 8000 シリーズ デバイスの高可用性をサポートしていません。

Firepower システムでライセンス付き機能にアクセスできなくなる状況がいくつかあります。

- Firepower Management Center から従来のライセンスを削除することができますが、そのようにすると、すべての管理対象デバイスに影響します。
- 特定の管理対象デバイスでライセンス付き機能を無効にすることができます。

いくつかの例外がありますが、期限切れライセンスまたは削除済みライセンスに関連付けられている機能は使用できません。

次の表に、Firepower システムにおける従来のライセンスの概要を示します。

表 17: Firepower システムの従来のライセンス

Firepower システムで割り当てるライセンス	購入するサービスサブスクリプション	プラットフォーム	付与される機能	併せて必要なライセンス	有効期限設定可/不可
任意 (Any)	TA、TAC、TAM、または TAMC	7000 および 8000 シリーズ ASA FirePOWER NGIPSv	ホスト、アプリケーション、ユーザ検出 SSL 暗号化トラフィックと TLS 暗号化トラフィックの復号および検査	none	ライセンスによって異なる
プロテクション (Protection)	TA (デバイスに付属)	7000 および 8000 シリーズ ASA FirePOWER NGIPSv	侵入検知と防御 ファイル制御 セキュリティ インテリジェンスフィルタリング	none	No

Firepower システムで割り当てるライセンス	購入するサービスサブスクリプション	プラットフォーム	付与される機能	併せて必要なライセンス	有効期限設定可/不可
Control	なし（デバイスに付属）	7000 および 8000 シリーズ	ユーザおよびアプリケーション制御  スイッチングとルーティング  7000 および 8000 シリーズ デバイスの高可用性  7000 および 8000 シリーズ ネットワークアドレス変換（NAT）	Protection	No
Control	なし（デバイスに付属）	ASA FirePOWER NGIPSv	ユーザおよびアプリケーション制御	Protection	No
マルウェア (Malware)	TAM、TAMC、または AMP	7000 および 8000 シリーズ  ASA FirePOWER NGIPSv	AMP for Firepower（ネットワークベースの高度なマルウェア防御）	Protection	Yes
URL フィルタリング (URL Filtering)	TAC、TAMC、または URL	7000 および 8000 シリーズ  ASA FirePOWER NGIPSv	カテゴリとレピュテーションに基づく URL フィルタリング	Protection	Yes
VPN	なし（詳細は販売担当者にお問い合わせください）	7000 および 8000 シリーズ	バーチャルプライベートネットワークの展開	Control	Yes

## プロテクションライセンス

プロテクションライセンスでは、侵入検知および防御、ファイル制御、およびセキュリティインテリジェンス フィルタリングを実行できます。

- 侵入検知および防御により、侵入とエクスプロイトを検出するためネットワークトラフィックを分析できます。またオプションで違反パケットをドロップできます。
- ファイル制御により、特定のアプリケーションプロトコルを介した特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード（送信）またはダウンロード（受信）をブロックできます。マルウェアライセンスが必要な *AMP for Firepower* を使用すると、制限されたファイルタイプセットを、その処置に基づいて検査およびブロックすることができます。

- セキュリティインテリジェンスフィルタリングにより、トラフィックをアクセス制御ルールによる分析対象にする前に、特定の IP アドレス、URL、および DNS ドメイン名をブラックリストに追加（その IP アドレスとの間のトラフィックを拒否）できます。ダイナミックフィードにより、最新の情報に基づいて接続をただちにブラックリストに追加できます。オプションで、セキュリティインテリジェンスフィルタリングに「モニタのみ」設定を使用できます。

プロテクションライセンス（制御ライセンスと共に）は、クラシック管理対象デバイスの購入時に自動的に組み込まれます。このライセンスは無期限ですが、システムの更新を有効にするには、TA サブスクリプションも購入する必要があります。

ライセンスがない状態でプロテクション関連の検査を実行するようにアクセス制御ポリシーを設定できますが、プロテクションライセンスを **Firepower Management Center** に追加し、ポリシー展開対象デバイス上でこのライセンスを有効にするまではポリシーを展開できません。

プロテクションライセンスを **Firepower Management Center** から削除するか、または管理対象デバイスでプロテクションを無効にすると、**Firepower Management Center** は対象デバイスからの侵入イベントとファイルイベントを認識しなくなります。結果として、トリガー条件としてこれらのイベントを使用する相関ルールがトリガーしなくなります。また、**Firepower Management Center** はシスコ提供またはサードパーティのセキュリティインテリジェンス情報を取得するためにインターネットに接続しなくなります。プロテクションを再度有効にするまでは、既存のポリシーを再度展開することはできません。

プロテクションライセンスは URL フィルタリング、マルウェア、および制御ライセンスに必要であるため、プロテクションライセンスを削除または無効にすると、URL フィルタリング、マルウェア、または制御ライセンスを削除または無効にすることと同じ効果があります。

## 制御ライセンス

制御ライセンスでは、アクセスコントロールルールにユーザとアプリケーションの条件を追加することで、ユーザとアプリケーションの制御を実装できます。7000 および 8000 シリーズデバイスでは、このライセンスを使用して、スイッチングとルーティング（DHCP リレーおよび NAT を含む）、およびデバイスのハイアベイラビリティペアも構成できます。管理対象デバイスの制御ライセンスを有効にするには、保護ライセンスも有効にする必要があります。制御ライセンスは（保護ライセンスとともに）、従来の管理対象デバイスの購入時に自動的に付属します。このライセンスは無期限ですが、システムの更新を有効にするには、TA サブスクリプションも購入する必要があります。

従来の管理対象デバイスの制御ライセンスを有効にしない場合は、アクセスコントロールポリシーのルールにユーザおよびアプリケーションの条件を追加できますが、デバイスにポリシーを展開することはできません。7000 または 8000 シリーズデバイスの制御ライセンスを明確に有効にしないと、次の操作も行えません。

- スイッチド、ルーテッド、またはハイブリッドインターフェイスの作成
- NAT エントリの作成
- 仮想ルータの DHCP リレーの設定
- デバイスへのスイッチまたはルーティングが含まれているデバイス設定の展開

- デバイス間のハイ アベイラビリティの確立



(注) 制御ライセンスがなくても仮想スイッチおよびルータを作成できますが、データを取り込むスイッチドインターフェイスおよびルーテッドインターフェイスがない状態ではこれらのスイッチとルータは有用ではありません。

制御ライセンスを Firepower Management Center から削除するか、または個別のデバイスで制御を無効にしても、対象デバイスでのスイッチングとルーティングの実行が行われなくなったり、デバイスのハイ アベイラビリティ ペアが解除されたりすることは**ありません**。既存の設定の編集や削除を続けることはできますが、影響を受けるデバイスに対する変更を展開することはできません。新しいスイッチドインターフェイス、ルーテッドインターフェイス、またはハイブリッドインターフェイスを追加することも、新しい NAT エントリの追加、DHCP リレーの設定、7000 または 8000 シリーズ デバイスのハイ アベイラビリティの確立もできません。既存のアクセス コントロール ポリシーに、ユーザ条件またはアプリケーション条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。

## 従来のデバイスの URL フィルタリング ライセンス

URL フィルタリングにより、モニタ対象ホストにより要求される URL に基づいて、ネットワーク内を移動できるトラフィックを判別するアクセス制御ルールを作成することができます。URL フィルタリング ライセンスを有効にする場合は、保護ライセンスも有効にする必要があります。従来のデバイスの URL フィルタリング ライセンスは、脅威 & アプリ (TAC) または脅威 & アプリおよびマルウェア (TAMC) サブスクリプションと組み合わせてサービス サブスクリプションとして購入できます。また、脅威 & アプリ (TA) が既に有効になっているシステムの場合は、アドオン サブスクリプションとして購入できます。



**ヒント** URL フィルタリング ライセンスがない状態で、許可またはブロックする個別 URL または URL グループを指定できます。これにより、Web トラフィックをカスタムできめ細かく制御できますが、URL カテゴリおよびレピュテーション データをネットワーク トラフィックのフィルタリングに使用することはできません。

URL フィルタリング ライセンスがない状態でも、アクセス制御ルールにカテゴリ ベースの URL 条件およびレピュテーションベースの URL 条件を追加できますが、Firepower Management Center は URL 情報をダウンロードしません。最初に URL フィルタリング ライセンスを Firepower Management Center に追加し、ポリシー適用対象デバイスで有効にするまでは、アクセス コントロール ポリシーを適用できません。

Firepower Management Center からライセンスを削除するか、または管理対象デバイスで URL フィルタリングを無効にすると、URL フィルタリングにアクセスできなくなることがあります。また、URL フィルタリング ライセンスの有効期限が切れることもあります。ライセンスが期限切れになるか、ライセンスを削除または無効化すると、URL 条件が含まれているアクセス制御ルールは URL フィルタリングを直ちに停止し、Firepower Management Center は URL データのアップデートをダウンロードできなくなります。既存のアクセス コントロール ポリシー



に、カテゴリ ベースまたはレピュテーションベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。

## 従来のデバイスのマルウェア ライセンス

マルウェア ライセンスを使用すると、AMP for Firepower および AMP Threat Grid を使用して Cisco Advanced Malware Protection (AMP) を実行することができます。管理対象デバイスを使用して、ネットワーク上で伝送されるファイルのマルウェアを検出してブロックできます。マルウェア ライセンスを有効にするには、保護も有効にする必要があります。マルウェア ライセンスは、脅威 & アプリ (TAM) と組み合わせたサブスクリプションまたは脅威 & アプリおよび URL フィルタリング (TAMC) サブスクリプションとして購入できます。また、脅威 & アプリ (TA) が既に有効になっているシステムの場合は、アドオン サブスクリプションとして購入できます。



- (注) マルウェア ライセンスが有効になっている 7000 および 8000 シリーズ 管理対象デバイスは、動的分析を設定していない場合でも、定期的に AMP クラウドへの接続を試行します。このため、デバイスの [インターフェイストラフィック (Interface Traffic) ] ダッシュボードウィジェットには、送信済みトラフィックが表示されます。これは正常な動作です。

ファイル ポリシーの一部として AMP for Firepower を設定し、その後 1 つ以上のアクセス コントロールルールを関連付けます。ファイル ポリシーは、特定のアプリケーションプロトコルを使用して特定のファイルをアップロードまたはダウンロードするユーザを検出できます。AMP for Firepower によって、ローカル マルウェア分析とファイルの事前分類を使用して、これらの制限されたファイルタイプのセットにマルウェアがないかを検査できます。特定のファイルタイプをダウンロードして AMP Threat Grid クラウドにアップロードして、動的 Spero 分析でマルウェアが含まれているかどうかを判別することもできます。これらのファイルでは、ファイルがネットワーク内で経由する詳細なパスを示すネットワーク ファイルトラジェクトリを表示できます。マルウェアライセンスでは、ファイルリストに特定のファイルを追加し、そのファイルリストをファイル ポリシー内で有効にすることもできます。これにより、検出時にこれらのファイルを自動的に許可またはブロックできます。

AMP for Firepower 構成を含むアクセス コントロール ポリシーを展開する前に、マルウェア ライセンスを追加してから、そのポリシー展開対象デバイスで有効にする必要があります。デバイスでライセンスを後で無効にする場合、既存のアクセス コントロール ポリシーをそれらのデバイスに再度展開することはできません。

マルウェア ライセンスをすべて削除するか、それらがすべて期限切れになると、システムは AMP への問い合わせを停止し、AMP クラウドから送信される遡及的イベントの確認応答も停止します。既存のアクセス コントロール ポリシーに AMP for Firepower 構成が含まれている場合は、それらのポリシーを再展開することができません。マルウェアライセンスが失効したか削除された後、システムが既存のキャッシュファイルの性質を使用できるのは極めて短時間のみであることに注意してください。この時間枠の経過後、システムは Unavailable という性質をこれらのファイルに割り当てます。

マルウェア ライセンスが必要なのは AMP for Firepower および AMP Threat Grid を展開する場合のみです。マルウェア ライセンスがなければ、Firepower Management Center は AMP クラウド

ドからエンドポイント向け AMP マルウェア イベントおよび侵害の兆候 (IOC) を受信できます。

#### 関連トピック

[ファイル制御および Cisco AMP の基本](#) (1528 ページ)

## VPN ライセンス

VPNを使用すると、インターネットやその他のネットワークなどの公共ソースを経由してエンドポイント間にセキュア トンネルを確立できます。7000 および 8000 シリーズ デバイスの仮想ルータ間で安全な VPN トンネルを構築するよう、Firepower システムを設定することができます。VPNを有効にするには、保護および制御のライセンスも有効にする必要があります。VPN ライセンスを購入するには、販売担当者までお問い合わせください。

VPN ライセンスがないと、7000 および 8000 シリーズ デバイスで VPN 導入環境を設定できません。導入環境の作成はできますが、データを取り込むための 1 つ以上の VPN 対応スイッチド インターフェイスおよびルーテッド インターフェイスがない状態では、導入環境は有用ではありません。

VPN ライセンスを Firepower Management Center から削除するか、または個別のデバイスで VPN を無効にすると、対象デバイスは現在の VPN 導入環境をブレイクしません。既存の導入環境を編集または削除できますが、対象デバイスに変更を適用することはできません。

## デバイス スタックおよびハイ アベイラビリティ ペアのクラシック ライセンス

スタックや 7000 または 8000 シリーズ デバイス ハイ アベイラビリティ ペアを構成するデバイスは、それぞれが同等のライセンスを持っている必要があります。デバイスのスタック構成後に、スタック全体のライセンスを変更できます。ただし、7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアでは有効なライセンスを変更することはできません。

## 従来型ライセンスの表示

スマート ライセンス	従来型ライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	従来型 (Classic)	グローバルのみ	Admin

[Classic ライセンス (Classic Licenses)] ページを使用して、Firepower Management Center に追加した Classic ライセンスを表示します。展開環境内の管理対象デバイスのタイプごとに、所有しているライセンスの総数と、使用中のライセンスの割合がこのページにリストされます。

[ライセンス (Licenses)] ページには、各ライセンスの詳細も表示されます。モデルごとに、各タイプの所有ライセンス数、各タイプのライセンスでライセンス付与できる管理対象デバイスの数が表示されます。有効期限のあるライセンスの場合、このページに有効期限が表示されます。

次のように、ライセンスおよびライセンス制限を表示できます。

- [製品ライセンス (Product Licensing) ] ダッシュボード ウィジェットはライセンスの概要を示します。
- [デバイス管理 (Device Management) ] ページ ([デバイス (Devices) ] > [デバイス管理 (Device Management) ]) は、各管理対象デバイスに適用されているライセンスをリストします。
- ヘルス ポリシーで使用される際に、Classic ライセンス モニタのヘルス モジュールはライセンス ステータスを伝達します。

#### 手順

[システム (System) ] > [ライセンス (Licenses) ] > [クラシック ライセンス (Classic Licenses) ] を選択します。

## ライセンス キーの特定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	従来型 (Classic)	グローバルのみ	Admin

ライセンス キーによって、Firepower Management Center はシスコ ライセンス 登録ポータルで一意に識別されます。これは、Firepower Management Center の製品コード (66) と MAC アドレスで構成されます (たとえば、66:00:00:77:FF:CC:88) 。

シスコ ライセンス 登録ポータルでは、ライセンス キーを使用して、Firepower Management Center にライセンスを追加する際に必要になるライセンス テキストを取得する必要があります。

#### 手順

- ステップ 1** [システム (System) ] > [ライセンス (Licenses) ] > [クラシック ライセンス (Classic Licenses) ] を選択します。
- ステップ 2** [新規ライセンスの追加 (Add New License) ] をクリックします。
- ステップ 3** [機能ライセンスの追加 (Add Feature License) ] ダイアログの上部にある [ライセンス キー (License Key) ] フィールドの値をメモします。

## 次のタスク

- ライセンスを Firepower Management Center に追加します。 [Firepower Management Center への従来型ライセンスの追加 \(158 ページ\)](#) を参照してください。

## Firepower Management Center への従来型ライセンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	従来型 (Classic)	グローバルのみ	Admin



- (注) バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを（それらが使用されている場所をメモした上で）削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。



- ヒント サポート サイトにログインした後で、[ライセンス (Licenses)] タブでライセンスを要求することもできます。

## 始める前に

- まだ作成していない場合は、スマート アカウントを作成します。 <https://www.cisco.com/c/en/us/buy/smart-accounts.html> を参照してください。
- ライセンス購入時に Cisco が提供したソフトウェア権利証明書にある製品アクティベーションキー (PAK) をお手元にご用意ください。レガシーの、以前のシスコのライセンスの場合は、サポートに問い合わせてください。
- Firepower Management Center のライセンス キーの種類を確認します。 [ライセンス キーの特定 \(157 ページ\)](#) を参照してください。

## 手順

- ステップ 1** [システム (System)] > [ライセンス (Licenses)] > [クラシック ライセンス (Classic Licenses)] を選択します。
- ステップ 2** [新規ライセンスの追加 (Add New License)] をクリックします。
- ステップ 3** 必要に応じ、続いて以下を行います。
- ライセンステキストをすでに取得している場合は、ステップ 8 にスキップしてください。

- ライセンスのテキストを取得する必要がある場合は、次の手順を実行します。

- ステップ 4** [ライセンス取得 (Get License)] をクリックして、Cisco ライセンス登録ポータルを開きます。
- (注) ご使用のコンピュータからインターネットにアクセスできない場合は、アクセスできるコンピュータから <http://cisco.com/go/license> を探します。
- ステップ 5** ライセンス登録ポータルで、PAK からライセンスを生成します。詳細については、<https://www.cisco.com/web/fw/tools/swift/xui/html/help.html> を参照してください。
- この手順には、購入時に入手した PAK と、Firepower Management Center のライセンスキーが必要です。
- ステップ 6** ライセンス登録ポータルの表示から、ないしはライセンス登録ポータルより送られてくるメールからライセンス テキストをコピーします。
- ステップ 7** Firepower Management Center の web インターフェイスの [機能ライセンスの追加 (Add Feature License)] ページに戻ります。
- ステップ 8** [ライセンス (License)] フィールドにライセンス テキストを貼り付けます。
- ステップ 9** [ライセンスの検証 (Verify License)] をクリックします。
- ライセンスが無効となる場合は、ライセンス テキストが正しくコピーされているか確認します。
- ステップ 10** [ライセンスの提出 (Submit License)] をクリックします。

#### 次のタスク

- 管理対象デバイスにライセンスを割り当てます。[管理対象デバイスへのライセンスの割り当て \(159 ページ\)](#) を参照してください。管理対象デバイスのライセンス取得済み機能を使用するには、これらのデバイスにライセンスを割り当てる必要があります。

## 管理対象デバイスへのライセンスの割り当て

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Network Admin

一部の例外はありますが、管理対象デバイスでライセンスを無効にすると、そのライセンスに関連づけられている機能は使用できなくなります。

## 手順

---

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2** ライセンスを割り当てまたは無効にするデバイスの横にある編集アイコン (✎) をクリックします。
- マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** [デバイス (Device) ] タブをクリックします。
- ステップ 4** [ライセンス (License) ] セクションの横にある編集アイコン (✎) をクリックします。
- ステップ 5** 適切なチェックボックスをオンまたはオフにして、デバイスのライセンスを割り当て、または無効にします。
- ステップ 6** [保存 (Save) ] をクリックします。
- 

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。



## 第 6 章

# システム ソフトウェア更新

ここでは、Firepower システム ソフトウェアを更新する方法について説明します。

- システム ソフトウェア アップデートの概要 (161 ページ)
- Firepower システムのソフトウェア アップデート (164 ページ)
- Firepower システムのソフトウェア アップデートのアンインストール (174 ページ)
- 脆弱性データベースの更新 (177 ページ)
- 侵入ルールの更新 (179 ページ)
- 地理位置情報データベースの更新 (192 ページ)

## システム ソフトウェア アップデートの概要

Cisco は、以下を含む各種のアップデートを電子的に配信します。

- システム ソフトウェア自体に対するメジャーおよびマイナー アップデート
- 侵入ルールの更新
- 地理位置情報データベース (GeoDB) の更新
- 脆弱性データベース (VDB) の更新

ほとんどのタイプの更新では、ダウンロードとインストールをスケジュールすることができません。



### 注意

この章では、Firepower システムの更新に関する全般的な情報について説明します。Firepower システムのいずれかの部分 (VDB、GeoDB、侵入ルールなど) を更新する前に、更新に付随しているリリース ノートまたはアドバイザリ テキストを読んでおく**必要があります**。リリース ノートでは、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストールおよびアンインストールの手順など重要なデータが提供されます。



- (注) 更新には、Firepower Management Center から管理対象デバイスへの大量のデータ転送が必要になる場合があります。開始する前に、管理ネットワークに、転送を正常に実行するために十分な帯域幅があることを確認してください。 <https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212043-Guidelines-for-Downloading-Data-from-the.html> で、トラブルシューティングのテクニカル ノートを参照してください。

表 18: Firepower システム アップデートのタイプ

更新のタイプ	説明	スケジュールを行うか	アンインストールをするか	タブ	ドメイン
Firepower システムに対するパッチ	パッチには、限定された範囲の修正が含まれています（また通常は、6.0.0.1 のようにバージョン番号の4桁目に変更されます）。	Yes	Yes	製品の更新	グローバルのみ
Firepower システムの機能の更新	機能の更新はパッチよりも包括的であり、通常は新しい機能が含まれています（また通常は、6.0.1 のようにバージョン番号の3桁目に変更されます）。	Yes	Yes	製品の更新	グローバルのみ
Firepower システムに対するメジャーな更新 (メジャーおよびマイナーバージョンのリリース)	メジャーな更新はアップグレードと呼ばれることもあります。この更新には新しい機能が含まれており、製品に対する大規模な変更が含まれることがあります（通常は、6.1 または 6.2 のようにバージョン番号の最初の桁または2桁目に変更されます）。メジャーな更新では、Cisco エンドユーザ ライセンス契約 (EULA) の再承認が必要な場合があります。	No	No	製品の更新	グローバルのみ



更新のタイプ	説明	スケジュールを 行うか	アンインストール をするか	タブ	ドメイン
脆弱性データ ベース (VDB)	VDB の更新は、オペレーティング システム、アプリケーション、クライアントによって検出された脆弱性、および Firepower システムによって報告された脆弱性に影響を与えます。	Yes	No	製品の更新	グローバルのみ
侵入ルール	侵入ルールの更新には、新規および更新された侵入ルールとプリプロセッサ ルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が含まれています。ルールの更新では、ルールが削除されたり、新しいルール カテゴリとデフォルトの変数が提供されたり、デフォルトの変数値が変更されたりすることもあります。	Yes	No	ルールの更新	<ul style="list-style-type: none"> <li>侵入ルールの更新：グローバルのみ</li> <li>ローカルルールのインポート：任意</li> </ul>
位置情報データ ベース (GeoDB)	GeoDB の更新には、物理的な場所や接続タイプなど、検出されたルート可能な IP アドレスにシステムが関連付けることができるものに関する更新情報が含まれています。位置情報データは、アクセスコントロール ルールとして使用できます。位置情報の詳細を表示するには、GeoDB をインストールする必要があります。	Yes	No	地理位置情報の更新	グローバルのみ

ただし、Firepower システムに対するパッチや他のマイナーな更新はアンインストールできませんが、VDB、GeoDB、侵入ルールに対するメジャーな更新をアンインストールしたり、前のバージョンに戻したりすることはできません。自分のアプライアンスを、Firepower システムの新しいメジャーバージョンに更新した場合、古いバージョンに戻す必要がある場合は、サポートに連絡してください。

リリース ノートまたはアドバイザリ テキストに特に記載されていない限り、アプライアンスを更新しても設定は変更されず、アプライアンスの設定はそのまま保持されます。

# Firepower システムのソフトウェア アップデート

Firepower システムの展開を更新するには、いくつかの基本的な手順があります。最初にリリースノート参照し、必要な更新前のタスクをすべて完了することで更新の準備を整えておく必要があります。その後更新を開始することができます。まず Firepower Management Center を更新し、次にこれが管理するデバイスを更新します。更新が完了し、更新が正常に終了したことを確認するまで、更新の進捗状況を監視する必要があります。最後に、更新後の必要な手順を完了させます。

## Firepower システムのソフトウェア アップデートの準備

更新を開始する前に、リリース ノートをよく読んで理解する必要があります。リリース ノートはサポート サイトからダウンロードすることができます。リリース ノートには、サポートされているプラットフォーム、新しい機能、既知および解決済みの問題、製品の互換性について記載されています。また、リリースノートには前提条件、警告、および特別なインストールおよびアンインストールの手順についての重要な情報が含まれています。

### Firepower システムのバージョンの要件

アプライアンス（ソフトウェアベースのデバイスを含む）が、Firepower システムの正しいバージョンを実行していることを確認する必要があります。リリースノートには必要なバージョンが示されています。古いバージョンを実行している場合は、サポートサイトから更新を取得することができます。

### オペレーティング システム要件

ソフトウェアベースのデバイスをインストールしたコンピュータが、オペレーティング システムの正しいバージョンを実行していることを確認します。リリースノートには必要なバージョンが示されています。NGIPSv デバイスでサポートされるオペレーティング システムの詳細については、『*Firepower System Virtual Installation Guide*』を参照してください。

### 時間とディスク スペース要件

十分な空きディスク領域があることを確認し、更新のために十分な時間を確保しておく必要があります。管理対象デバイスを更新する場合は、Firepower Management Center 上に追加のディスク領域が必要になります。リリースノートには、ディスク領域と時間の要件が示されています。

### 設定とイベント バックアップのガイドライン

更新を開始する前に、アプライアンスに残っているバックアップを外部の場所にコピーしてから、アプライアンス上のバックアップを削除することを強く推奨します。また、現在のイベント データと設定 データを外部の場所にバックアップする必要があります。Firepower Management Center は、以前の更新でローカルに保存されたバックアップを消去します。イベント データは更新プロセスの一部としてバックアップされません。

Firepower Management Center を使用して、そのイベント データと設定データ、および管理しているデバイスのイベント データと設定データをバックアップできます。

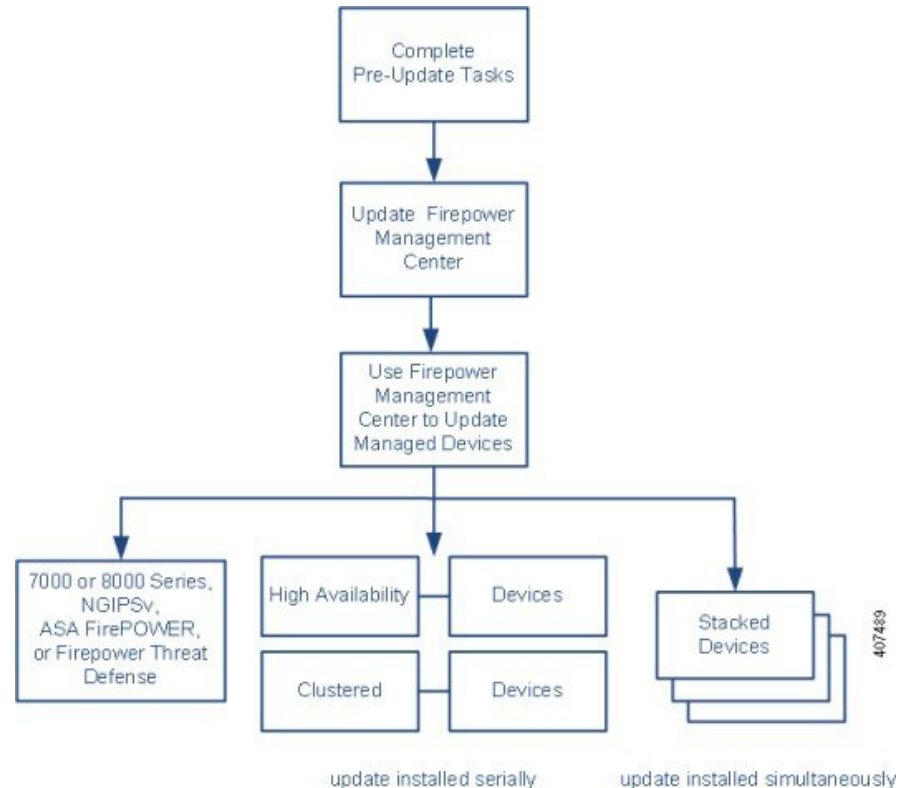
### 更新を実行するタイミング



**注意** 更新プロセスはトラフィックの調査、トラフィック フロー、およびリンク ステートに影響を与えることがあること、および更新を行っている間は Data Correlator が無効になっていることにより、保守を行っている間、または中断が展開に及ぼす影響が最も少ない時間に更新を行うことをお勧めします。

## Firepower システムのソフトウェア アップデート プロセス

次のフローチャートは、Firepower システムの更新プロセスを示しています。



### 更新の順序

使用している Firepower Management Center を更新してから、それらが管理するデバイスを更新する必要があります。

## Firepower Management Centerを使用した更新の実行

Firepower Management Center の Web インターフェイスを使用して、アプライアンス自体とその管理対象デバイスを更新します。



**ヒント** パッチおよび機能の更新では、自動更新機能を利用することができます。

管理対象デバイスの更新は、2段階のプロセスです。まず、サポートサイトから更新をダウンロードして、管理元の Firepower Management Center にアップロードします (<http://www.cisco.com/cisco/web/support/index.html>)。

次に、ソフトウェアをインストールします。



**注意** トラフィックのインスペクション、トラフィック フロー、およびリンク ステートは、デバイスがどのように設定および展開されているか、更新がどのコンポーネントに影響を及ぼすか、更新によってデバイスがリブートされるかどうかによって、更新中に影響を受けることがあります。特定の更新に対してネットワークトラフィックがいつ、どのように影響を受けるかについての具体的な情報は、対象の更新のリリース ノートを参照してください。

## ハイアベイラビリティ ペアの 7000 および 8000 シリーズ デバイスの更新

ハイアベイラビリティ ペアの 7000 または 8000 シリーズ デバイスまたはデバイス スタック上で更新をインストールすると、システムは、複数のデバイスまたはスタック上で同時に更新を実行します。更新を開始すると、システムは最初にスタンバイ デバイスまたはスタックに更新を適用し、必要なプロセスが再開され、デバイスまたはスタックがトラフィックを再処理するまでメンテナンスモードになります。システムは、アクティブなデバイスまたはスタックに更新を適用し、同じプロセスを行います。

ハイアベイラビリティ ペアのスタック内のデバイスを更新するには、ハイアベイラビリティ ペアのすべてのメンバー上で同時に、管理している Firepower Management Center から更新を実行する必要があります。デバイスから直接更新を実行することはできません。

## スタック内の 8000 シリーズ デバイスの更新

スタック構成のデバイスで更新をインストールする場合、システムは更新を同時に実行します。各デバイスは、更新が完了すると通常の動作を再開します。次の点に注意してください。

- すべてのセカンダリ デバイスの更新が完了する前にプライマリ デバイスの更新が完了すると、すべてのデバイスで更新が完了するまでスタックは限定的な、バージョンが混在している状態で動作します。
- すべてのセカンダリ デバイスの更新が完了した後でプライマリ デバイスの更新が完了した場合は、プライマリ デバイスで更新が完了したときに、スタックは通常の動作を再開します。

## トラフィック フローとインスペクション

管理対象デバイスから更新をインストールまたはアンインストールすると、次の機能に影響を及ぼすことがあります。

- トラフィック インスペクション (アプリケーションおよびユーザの認識と制御、URL フィルタリング、セキュリティインテリジェンスフィルタリング、侵入/ファイル/マルウェアのインスペクションと制御、接続のロギングなど)
- トラフィック フロー (スイッチング、ルーティング、NAT、VPN、関連機能など)
- リンク ステート

Data Correlator は、システムの更新中は動作しません。更新が完了すると再開します。

ネットワーク トラフィックの中断の方法と期間は、更新が影響を及ぼす Firepower システムのコンポーネント、デバイスがどのように設定および展開されているか、更新によりデバイスがリポートされるかどうか、によって異なります。特定の更新に対してネットワーク トラフィックがいつ、どのように影響を受けるかについての情報は、リリース ノートを参照してください。



### ヒント

ハイ アベイラビリティ ペア内の 7000 または 8000 シリーズ デバイスを更新する場合、システムは、トラフィックの中断を回避するために、一度に 1 つずつ更新を実行します。

## 更新中の Web インターフェイスの使用

更新のタイプに関係なく、更新中のアプライアンスの Web インターフェイスを使用して、更新のモニタ以外のタスクを実行しないでください。

メジャーな更新中にユーザがアプライアンスを使用しないようにし、メジャーな更新の進捗をユーザが簡単にモニタできるようにするために、アプライアンスの Web インターフェイスが合理化されています。メッセージセンターでマイナーな更新の進捗をモニタできます。マイナーな更新中に Web インターフェイスを使用することは禁止されていませんが、シスコでは推奨していません。



### ヒント

管理対象デバイスの更新をモニタするには、Firepower Management Center でメッセージセンターを使用します。

マイナーな更新であっても、更新プロセス中は、更新しているアプライアンスの Web インターフェイスは使用できないか、またはアプライアンスでユーザがログアウトされることがあります。これは想定されている動作です。これが発生した場合は、再度ログインして、メッセージセンター (マイナー更新の場合) または [更新ステータス (Update Status)] ページ (メジャー更新の場合) を表示します。まだ更新が実行中の場合は、更新が完了するまで Web インターフェイスを使用しないでください。更新中は、管理対象デバイスが 2 回リポートされることがありますが、これは予想される動作です。



**注意** (Web インターフェイスに更新が失敗したことが示されている、メッセージセンターまたは [更新ステータス (Update Status)] ページに進捗が表示されないなど) 更新で問題が発生した場合には、更新を再開しないでください。代わりに、サポートに連絡してください。

#### 更新後

リリースノートに記載されている更新後のタスクをすべて完了し、展開が正常に実行されていることを確認する**必要があります**。



**注意** Firepower Management Center の更新後、およびその管理対象デバイスの更新後に**再度**、設定を展開する必要があります。

また、次の作業を実行する必要があります。

- 更新が正常に終了したことを確認する
- 展開のすべてのアプライアンスが正常に通信していることを確認する
- 必要に応じて侵入ルール、VDB、および GeoDB を更新する
- リリース ノートの情報に基づいて、必要な設定変更を行う
- リリース ノートに記載されている、更新後の追加タスクを実行する

## Firepower システム ソフトウェア アップデートに関する注意事項

更新のタイプ、および Firepower Management Center がインターネットへアクセスできるかどうかによって、Firepower Management Center の Firepower システム ソフトウェアを次のいずれかの方法で更新できます。

- Firepower Management Center がインターネットにアクセスできる場合は、サポートサイトから直接アップデートを取得します。このオプションは、メジャーな更新ではサポートされていません。
- サポートサイトからアップデートを手動でダウンロードして、Firepower Management Center へアップロードします。Firepower Management Center がインターネットへアクセスできない場合、またはメジャーな更新を実行している場合は、この方法を選択します。



(注) 上記のいずれかの方法を使用して、アップデートを取得します。電子メールで更新ファイルを転送すると、破損する可能性があります。

[製品アップデート (Product Updates)] ページ ([システム (System)] > [更新 (Updates)]) には、それぞれの更新のバージョン、およびその更新が生成された日時が表示されます。また、更新の一環としてレポートが必要かどうかも示されます。

サポートから取得した更新をアプライアンスへアップロードすると、更新がページに示されます。パッチ機能および機能の更新のアンインストーラも表示されます。Firepower Management Center で、ページに VDB 更新を表示できます。

メジャーな更新の場合は、Firepower Management Center を更新すると、以前の更新のアンインストーラが削除されます。

## Firepower Management Center でのソフトウェアの更新

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin

### 始める前に

- Firepower Management Center で実行時間が長いタスクの実行を許可します。
- Firepower Management Center に更新をアップロードします。詳細については、[Firepower システムのソフトウェア更新のダウンロード \(170 ページ\)](#) と [Firepower Management Center にソフトウェア更新をアップロードする \(171 ページ\)](#) を参照してください。

### 手順

- 
- ステップ 1** リリース ノートを読んで、更新前の必要なタスクを完了させます。
- ステップ 2** 展開内でデバイスが正常に通信していること、およびヘルスマニタによって問題が報告されていないことを確認します。
- ステップ 3** [システム (System)] > [更新 (Updates)] を選択します。
- ステップ 4** アップロードした更新の横にあるインストールアイコンをクリックします。
- ステップ 5** Firepower Management Center を選択し、[インストール (Install)] をクリックします。プロンプトが表示されたら、更新をインストールすることを確認して Firepower Management Center をリブートします。
- ステップ 6** オプションで、更新ステータスをモニタします。
- マイナー更新については、[タスクメッセージの表示 \(330 ページ\)](#) を参照してください。
  - メジャー更新については、[主要な Firepower システム ソフトウェア更新のモニタリング \(173 ページ\)](#) を参照してください。

**注意** 更新のタイプに関係なく、更新が完了するまで、更新の監視以外のタスクを実行するために Web インターフェイスを使用しないでください。必要な場合は、Firepower Management Center を再起動します。

更新で問題が発生した場合（更新に失敗したことがメッセージセンターに示されている場合、またはメッセージに進捗が表示されない場合など）、更新を再開しないでください。代わりに、サポートに連絡してください。

- ステップ 7** 更新が完了したら、必要に応じて Firepower Management Center にログインします。
- ステップ 8** メジャー更新の後に最初にログインするユーザの場合、エンドユーザライセンス契約（EULA）を確認して同意し、続行します。
- ステップ 9** ブラウザのキャッシュを消去し、ブラウザを強制的にリロードします。そうしない場合、ユーザインターフェイスが予期しない動作を示すことがあります。
- ステップ 10** システム情報を表示するには、[ヘルプ（Help）]>[バージョン情報（About）]を選択します。
- ステップ 11** システム情報ページで、ソフトウェアバージョンが正しくリストされていることを確認し、Firepower Management Center のルールを更新および VDB のバージョンをメモします。これらの情報が後で必要になります。
- ステップ 12** すべての管理対象デバイスが、Firepower Management Center と正常に通信していることを確認します。

#### 次のタスク

- 新しい侵入ルールの更新があれば、それをインポートします（[侵入ルールの更新（179ページ）](#)を参照）。
- Firepower Management Center 上の VDB より新しい VDB があれば、サポートサイトからインストールします（[脆弱性データベースの更新（177ページ）](#)を参照）。
- 管理対象デバイスのシステム ソフトウェアを更新します（を参照）。
- 設定変更を展開します。[設定変更の導入（350ページ）](#)を参照してください。

## Firepower システムのソフトウェア更新のダウンロード

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin

メジャーアップデートを除くすべてのアップデートについて、Firepower Management Center にソフトウェアアップデートをダウンロードできます。ダウンロードするには、Firepower Management Center がインターネットにアクセスできる必要があります。



## 始める前に

- Firepower Management Center にインターネットアクセス権があることを確認してください（[セキュリティ、インターネットアクセス、および通信ポート（2785 ページ）](#) を参照）。

## 手順

- 
- ステップ 1** [システム (System)] > [更新 (Updates)] を選択します。
- ステップ 2** [アップデートのダウンロード (Download Updates)] をクリックして、Cisco サポート サイト (<http://www.cisco.com/cisco/web/support/index.html>) の最新の更新を確認します。
- ステップ 3** 更新をインストールします。詳細については、[Firepower Management Center でのソフトウェアの更新（169 ページ）](#) と [脆弱性データベースの更新（178 ページ）](#) を参照してください。
- 

## Firepower Management Center にソフトウェア更新をアップロードする

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin

次の場合に、Firepower Management Center に更新をアップロードする必要があります。

- メジャー更新を実行している。
- Firepower Management Center にインターネットへのアクセスがない。
- 管理対象デバイスを更新している。

## 手順

- 
- ステップ 1** シスコのサポート サイト (<http://www.cisco.com/cisco/web/support/index.html>) から更新を手動でダウンロードします。
- ステップ 2** [システム (System)] > [更新 (Updates)] を選択します。
- ステップ 3** [更新のアップロード (Upload Update)] をクリックします。
- ステップ 4** 更新を参照し、[アップロード (Upload)] をクリックします。
- 

## 次のタスク

- 更新をインストールします。詳細については、[Firepower Management Center でのソフトウェアの更新（169 ページ）](#) と [脆弱性データベースの更新（178 ページ）](#) を参照してください。

## 管理対象デバイスでのソフトウェア更新

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin

この手順のすべてのステップは、注記がない限り、Firepower Management Center で実行されます。

### 始める前に

- デバイスを管理する Firepower Management Center で Firepower System ソフトウェアを更新します。詳細については、[Firepower システム ソフトウェア アップデートに関する注意事項 \(168 ページ\)](#) を参照してください。
- Firepower Management Center に更新をアップロードします。詳細については、[Firepower Management Center にソフトウェア更新をアップロードする \(171 ページ\)](#) を参照してください。

### 手順

- 
- ステップ 1** リリースノートを読んで、更新前に必要なタスクを完了させます ([Firepower システム ソフトウェア アップデートに関する注意事項 \(168 ページ\)](#) および [Firepower システムのソフトウェア アップデートの準備 \(164 ページ\)](#) を参照)。
- ステップ 2** 展開内でアプライアンスが正常に通信していること、およびヘルスマニタによって問題が報告されていないことを確認します。
- ステップ 3** [システム (System)] > [更新 (Updates)] を選択します。
- ステップ 4** インストール中の更新の横にあるインストールアイコンをクリックします。
- ステップ 5** 更新をインストールするデバイスを選択し、[インストール (Install)] をクリックします。

同じ更新が使用される場合、複数のデバイスを一度に更新することができます。プロンプトが表示されたら、更新をインストールすることを確認してデバイスを再起動します。

ファイルのサイズによっては、すべてのデバイスで更新をインストールするのに時間がかかることがあります。更新中に、管理対象デバイスが2回再起動されることがありますが、これは正常な動作です。

- ステップ 6** オプションで、更新ステータスをモニタします。
- マイナー更新については、[タスクメッセージの表示 \(330 ページ\)](#) を参照してください。
  - メジャー更新については、[主要な Firepower システム ソフトウェア更新のモニタリング \(173 ページ\)](#) を参照してください。

**注意** 更新のタイプに関係なく、更新が完了するまで、更新の監視以外のタスクを実行するために Web インターフェイスを使用しないでください。必要な場合は、管理対象デバイスを再起動します。

更新で問題が発生した場合（更新に失敗したことがメッセージセンターに示されている場合、またはメッセージに進捗が表示されない場合など）、更新を再開しないでください。代わりに、サポートに連絡してください。

**ステップ 7** ブラウザのキャッシュを消去し、ブラウザを強制的にリロードします。そうしない場合、ユーザ インターフェイスが予期しない動作を示すことがあります。

**ステップ 8** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択して、更新したデバイスに正しいバージョンがリストされていることを確認します。

**ステップ 9** 更新したデバイスが、Firepower Management Center と正常に通信していることを確認します。

### 次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。
- オプションで、7000 または 8000 シリーズ デバイスへのメジャー更新の後でデバイスのローカル Web インターフェイスにログインします。メジャー更新の後に最初にログインするユーザには、エンドユーザライセンス契約 (EULA) が表示されることがあります。EULA を確認して承認し、処理を続行します。Web インターフェイスではなくコマンドライン インターフェイスを介して最初にログインした場合も EULA が表示されるので、必ず承認してください。

## 主要な Firepower システム ソフトウェア更新のモニタリング

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	グローバルだけ	Admin

この手順は、アプライアンスのローカル Web インターフェイスを使用して実行する必要があります。

### 手順

**ステップ 1** アプライアンスが必要な更新前チェックを完了するまで、メジャー ソフトウェア アップデートの進行を Message Center でモニタします。  
この時点で、自分も含めてすべてのユーザは、システムによって Web インターフェイスからログアウトされます。管理者またはメンテナンスユーザ以外は、更新が完了するまでログインし直すことはできません。

**ステップ2** 管理者の場合は、Web インターフェイスにログインし直します。簡略化された更新ページが表示されます。

**ステップ3** 更新ログを表示するには、[現在のスクリプトのログを表示する (show log for current script) ] をクリックします。ログをもう一度非表示にするには、[現在のスクリプトのログを非表示する (hide log for current script) ] をクリックします。

**注意** 更新で問題が生じた場合は（簡略化された更新ページを手動更新しても長時間にわたって進捗が表示されない場合など）、更新を再開しないでください。代わりに、サポートに連絡してください。

---

### 次のタスク

- 何らかの理由で更新に失敗した場合は、このページにエラーメッセージが表示され、失敗した日時、更新が失敗したときに実行していたスクリプト、およびサポートへの連絡方法が表示されます。更新は再開しないでください。
- 更新が正常に完了すると、ページに成功メッセージが表示され、アプライアンスがリブートされます。アプライアンスのリブートが完了したら、ページを更新してログインし、更新後の必要な手順を完了します。

## Firepower システムのソフトウェア アップデートのアンインストール

パッチまたは機能の更新を適用すると、更新プロセスによってアンインストーラが作成されます。これにより、Web インターフェイスを使用してアプライアンスから更新を削除することができます。

更新をアンインストールした場合、結果として保持されるバージョンは、アプライアンスの更新パスに応じて異なります。たとえば、アプライアンスをバージョン 6.0 からバージョン 6.0.0.2 へ直接更新した場合のシナリオについて考えてみます。バージョン 6.0.0.2 のパッチをアンインストールすると、バージョン 6.0.0.1 の更新をインストールしたことがなくても、バージョン 6.0.0.1 を実行するアプライアンスが結果として生成されます。更新をアンインストールしたときに結果として生成される Firepower ソフトウェアのバージョンの詳細については、リリースノートを参照してください。



---

**注意** メジャーな更新では、Web インターフェイスからのアンインストールはサポートされていません。アプライアンスを Firepower システムの新しいメジャーバージョンに更新して、古いバージョンに戻す必要がある場合は、サポートに連絡してください。

---

### アンインストールの順序

更新は、インストールと逆の順序でアンインストールします。つまり、最初に管理対象デバイスから更新をアンインストールしてから、Firepower Management Center からアンインストールします。

### ローカル Web インターフェイスを使用した更新のアンインストール

更新をアンインストールするにはローカル Web インターフェイスを使用する必要があります。Firepower Management Center を使用して、管理対象デバイスから更新をアンインストールすることはできません。ローカル Web インターフェイスを持たないデバイス（NGIPSv デバイスなど）からパッチをアンインストールする場合の詳細については、リリースノートを参照してください。

### ハイ アベイラビリティ ペアからの 7000 および 8000 シリーズ デバイスのアンインストール

ハイ アベイラビリティ ペアの 7000 または 8000 シリーズ デバイスは、同じバージョンの Firepower システムを実行する必要があります。アンインストールプロセスは自動フェールオーバーをトリガーしますが、不一致のハイ アベイラビリティ ペアの 7000 または 8000 シリーズ デバイスは、設定情報を共有せず、同期の一部として更新をインストールまたはアンインストールすることもあります。冗長デバイスから更新をアンインストールする必要がある場合は、即時および連続的にアンインストールを実行するように計画します。

アンインストールによって、これらのデバイスが、ハイ アベイラビリティ へのスタックの設定がサポートされないバージョンに戻される場合は、ハイ アベイラビリティ ペアとして設定されたスタックの 7000 または 8000 シリーズ デバイスから更新をアンインストールできません。

運用の継続性を保証するために、ハイ アベイラビリティ ペアのデバイスから一度に 1 つずつ更新をアンインストールします。まず、セカンダリデバイスから更新をアンインストールします。アンインストールプロセスが完了するまで待ってから、すぐにプライマリ デバイスから更新をアンインストールします。



#### 注意

ハイ アベイラビリティ ペアのデバイスでのアンインストール プロセスが失敗した場合は、アンインストールを再開したり、ピアの設定を変更したりしないでください。代わりに、サポートに連絡してください。

### スタック構成のデバイスからの更新のアンインストール

スタック内のすべてのデバイスが、同じバージョンの Firepower システムを実行する必要があります。スタック構成のデバイスのいずれかから更新をアンインストールすると、そのスタックではデバイスが限定的な、バージョンが混在する状態になります。

展開への影響を最小にするために、スタック構成のデバイスから更新を同時にアンインストールします。スタック内のすべてのデバイスで更新が完了すると、スタックは通常の動作を再開します。

アンインストールによって、これらのデバイスが、ハイアベイラビリティへのスタックの設定がサポートされないバージョンに戻される場合は、ハイアベイラビリティペアとして設定されたスタックの7000または8000シリーズデバイスから更新をアンインストールできません。

### トラフィックフローとインスペクション

管理対象デバイスから更新をアンインストールすると、トラフィックのインスペクション、トラフィックフロー、およびリンクステートに影響を及ぼすことがあります。特定の更新に対してネットワークトラフィックがいつ、どのように影響を受けるかについての情報は、リリースノートを参照してください。

### アンインストール後

更新をアンインストールした後で、展開が正しく機能していることを確認するために、いくつかの手順を実行する必要があります。これらはアンインストールが成功したこと、および展開のすべてのアプライアンスが正常に通信していることを確認することが含まれます。それぞれの更新に特定の情報については、リリースノートを参照してください。

## Firepower システムのソフトウェア更新のアンインストール

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin

この手順は、Firepower Management Center と 7000 & 8000 シリーズデバイスで実行できます。

### 始める前に

- アプライアンスを Firepower System の新しいメジャーバージョンに更新した後に、古いバージョンに戻す必要が生じた場合は、サポートに連絡してください。メジャー更新では、Web インターフェイスからのアンインストールはサポートされていません。

### 手順

**ステップ 1** [システム (System)] > [更新 (Updates)] を選択します。

**ステップ 2** 削除する更新のアンインストーラの隣にあるインストールアイコンをクリックします。プロンプトが表示されたら、更新をアンインストールすることを確認して、アプライアンスをリブートします。

- Firepower Management Center で、[アップデートをインストール (Install Update)] ページが表示されます。Firepower Management Center を選択し、[インストール (Install)] をクリックします。
- 管理対象デバイスには、操作のページがありません。

**注意** アンインストールが完了するまで、更新の監視以外のタスクを実行するために Web インターフェイスを使用しないでください。必要に応じて、アプライアンスをリブートします。

- ステップ 3** 必要に応じて、タスクのステータスをモニタします ([タスク メッセージの表示 \(330 ページ\)](#) を参照)。
- ステップ 4** アンインストールが完了したら、必要に応じてアプライアンスにログインします。
- ステップ 5** ブラウザのキャッシュを消去し、ブラウザを強制的にリロードします。そうしない場合、ユーザ インターフェイスが予期しない動作を示すことがあります。
- ステップ 6** [ヘルプ (Help)] > [バージョン情報 (About)] を選択し、ソフトウェアのバージョンが正しく示されていることを確認します。

#### 次のタスク

- パッチをアンインストールしたアプライアンスが正常に管理対象デバイスと通信していること (Firepower Management Center の場合)、または管理元の Firepower Management Center と通信していること (管理対象デバイスの場合) を確認します。
- アンインストールが成功したこと、および展開環境のすべてのアプライアンスが正常に通信していることを確認します。それぞれの更新に特定の情報については、リリースノート を参照してください。

## 脆弱性データベースの更新

シスコの脆弱性データベース (VDB) は、オペレーティング システム、クライアント、およびアプリケーションのフィンガープリントだけでなく、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。Firepower システムはフィンガープリントと脆弱性を関連付けて、特定のホストがネットワークの侵害のリスクを増大させているかどうかを判断するのをサポートします。Cisco Talos Security Intelligence and Research Group (Talos) では、VDB の定期的な更新を配布しています。

VDB を更新するには、Firepower Management Center で [製品の更新 (Product Updates)] ページを使用します。サポートから取得した VDB 更新をアプライアンスへアップロードすると、このページに、アップロードした更新と Firepower システムの更新およびそのアンインストールの更新が表示されます。



- (注) 手動でまたは [アップデートのダウンロード (Download Updates)] をクリックして、サポート サイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、破損する可能性があります。

脆弱性のマッピングを更新するのにかかる時間は、ネットワークマップ内のホストの数によって異なります。システムのダウンタイムの影響を最小にするために、システムの使用率が低い時間帯に更新をスケジュールすることをお勧めします。一般的に、更新の実行にかかるおおよその時間（分）を判断するには、ネットワーク上のホストの数を 1000 で割ります。

VDB を更新した後、更新されたアプリケーションディテクタとオペレーティングシステムフィンガープリントを有効にするために、設定を展開する必要があります。



**注意** 脆弱性データベース（VDB）アップデートをインストールした後、初めて VDB アップデートをインストールするか、またはアクセスコントロールポリシーを展開すると、すぐに Snort プロセスが再起動され、トラフィックインスペクションが一時的に中断されることがあります。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作（356 ページ）](#)を参照してください。

自動更新機能を利用して VDB 更新をスケジュールすることができます。

## 脆弱性データベースの更新

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin

この手順は、Firepower Management Center でしか実行できません。

### 始める前に

- Firepower Management Center に更新をアップロードします。詳細については、[Firepower システムのソフトウェア更新のダウンロード（170 ページ）](#)と [Firepower Management Center にソフトウェア更新をアップロードする（171 ページ）](#)を参照してください。



**注意** 脆弱性データベース（VDB）更新をインストールした時点、または VDB 更新をインストールした後に初めてアクセスコントロールポリシーを展開した時点で、すぐに Snort プロセスが再起動してトラフィックインスペクションが一時的に中断されることがあります。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作（356 ページ）](#)を参照してください。



## 手順

- ステップ 1 更新用の VDB 更新アドバイザリ テキストを読みます。このアドバイザリ テキストには、更新で作成された VDB に対する変更、および製品の互換性情報が含まれています。
- ステップ 2 [システム (System)] > [更新 (Updates)] を選択します。
- ステップ 3 [製品の更新 (Product Updates)] タブで、VDB 更新の横にあるインストールアイコンをクリックします。
- ステップ 4 Firepower Management Center エントリの横にあるチェックボックスをオンにします。
- ステップ 5 [Install (インストール)] をクリックします。ネットワークマップ内のホストの数によっては、更新のインストールに時間がかかることがあります。
- ステップ 6 必要に応じて、タスクのステータスをモニタします ([タスク メッセージの表示 \(330 ページ\)](#) を参照)。  
  
**注意** 更新が完了するまで、マップされた脆弱性に関連するタスクを実行するために Web インターフェイスを使用しないでください。更新で問題が発生した場合には (たとえば、メッセージセンターに進捗が表示されない、更新が失敗したことが示されているなど)、更新を再開しないでください。代わりに、サポートに連絡してください。
- ステップ 7 更新が終了したら、[ヘルプ (Help)] > [バージョン情報 (About)] を選択して、VDB のビルド番号が、インストールした更新と一致していることを確認します。

## 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。
- オプションで、VDB 更新をスケジュールします ([脆弱性データベースの更新の自動化 \(235 ページ\)](#) を参照)。

## 関連トピック

[Snort® の再起動シナリオ \(354 ページ\)](#)

# 侵入ルールの更新

新しい脆弱性が明らかになるのに伴い、Cisco Talos Security Intelligence and Research Group (Talos) は侵入ルールの更新をリリースします。これらの更新を Firepower Management Center にインポートして、変更後の設定を管理対象デバイスに導入することで、侵入ルールの更新を実装できます。それらの更新は、侵入ルール、プリプロセッサルール、およびルールを使用するポリシーに影響を及ぼします。

侵入ルール更新は更新を累積されていくものなので、常に最新の更新をインポートすることをお勧めします。現在インストールされているルールのバージョン以前の侵入ルールの更新をインポートすることはできません。

侵入ルールの更新では、次のものを提供します。

- **新規または変更されたルールおよびルールステータス**：ルール更新は、新規および更新された侵入ルールとプリプロセッサルールを提供します。新規ルールの場合は、システム付属の各侵入ポリシーでルールステータスが異なることがあります。たとえば、新規ルールが、**Security over Connectivity** 侵入ポリシーでは有効になっており、**Connectivity over Security** 侵入ポリシーでは無効になっていることがあります。ルールの更新では、既存のルールのデフォルトの状態が変更されたり、既存のルールが完全に削除されることもあります。
- **新しいルール カテゴリ**：ルール更新には、常に追加される新しいルール カテゴリが含まれている場合があります。
- **変更されたプリプロセッサおよび詳細設定**：ルール更新によって、システム付属侵入ポリシーの詳細設定、およびシステム付属ネットワーク分析ポリシーのプリプロセッサ設定が変更されることがあります。また、アクセス コントロール ポリシーの高度な前処理およびパフォーマンスのオプションのデフォルト値も変更される場合があります。
- **新規および変更された変数**：ルール更新によって、既存のデフォルト変数のデフォルト値が変更されることがありますが、ユーザによる変更は上書きされません。新しい変数が常に追加されます。

マルチドメイン展開では、ローカル侵入ルールを任意のドメインにインポートできますが、グローバルドメイン内の Talos からでなければ、侵入ルールの更新をインポートすることはできません。

#### 侵入ルールの更新によってポリシーが変更されるタイミングについて

侵入ルールの更新は、システムが提供するネットワーク分析ポリシーとカスタムネットワーク分析ポリシーの両方だけでなく、すべてのアクセス コントロール ポリシーにも影響する場合があります。

- **システム提供**：システムが提供するネットワーク解析および侵入ポリシーへの変更は、その他のアクセスコントロールの詳細設定と同様に、更新後にポリシーを再適用すると自動的に有効になります。
- **カスタム**：すべてのカスタムネットワーク分析ポリシーと侵入ポリシーは、システム付属ポリシーをそのベースとして、またはポリシーチェーンの根本的ベースとして使用しているので、ルール更新によってカスタムネットワーク分析ポリシーと侵入ポリシーが影響を受けることがあります。ただし、ルール更新によるこれらの自動的な変更は回避することができます。これにより、ルール更新のインポートとは関係ないスケジュールで、システムによって提供される基本ポリシーを手動で更新できます。ユーザによる選択（カスタムポリシーごとに実装）とは関係なく、システム付属ポリシーに対する更新によって、カスタマイズ済みの設定が上書きされることは**ありません**。

ルール更新をインポートすると、ネットワーク分析ポリシーと侵入ポリシーのキャッシュされていた変更がすべて廃棄されるので注意してください。便宜のために、[ルール更新 (Rule Updates)] ページには、キャッシュされている変更があるポリシー、および変更を行ったユーザが表示されます。

## 侵入ルールの更新の展開

侵入ルールの更新によって行われた変更を有効にするには、設定を再導入する必要があります。侵入ルールの更新をインポートする際に、影響を受けるデバイスに自動的に再導入するようシステムを設定できます。この手法が特に役立つのは、侵入ルールの更新によるシステム提供の基本侵入ポリシーの変更を許可する場合です。



### 注意

ルール更新をインポートするときには、設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。ルール更新のダウンロードおよびインストールプロセスがセキュリティ ポリシーに従っていることを確認してください。また、侵入ルールの更新のサイズは大きいことがあるため、ルールのインポートはネットワークの使用量が少ないときに行うようにしてください。

## 侵入ルールの更新の繰り返し

[ルールの更新 (Rule Updates)] ページを使用して、ルール更新を日次、週次、または月次ベースでインポートすることができます。

侵入ルールの更新のインポートに適用されるサブタスクは、ダウンロード、インストール、ベースポリシーの更新、設定の展開の順で実行されます。1つのサブタスクが完了すると、次のサブタスクが開始されます。

スケジュールされた時間になると、システムはルールの更新をインストールして、前のステップで指定したように変更後の設定を展開します。インポートの前、またはインポート中にログオフすることも、Web インターフェイスを使用して他のタスクを実行することもできます。インポート中に [ルールの更新ログ (Rule Update Log)] にアクセスすると、赤色のステータスアイコン (❗) が表示され、[ルールの更新ログ (Rule Update Log)] 詳細ビューに表示されるメッセージを確認できます。ルール更新のサイズと内容によっては、ステータスメッセージが表示されるまでに数分かかることがあります。

## ローカル侵入ルールのインポート

ローカル侵入ルールは、ASCII または UTF-8 エンコーディングによるプレーン テキスト ファイルとしてローカルマシンからインポートするカスタム標準テキストルールです。Snort ユーザマニュアル (<http://www.snort.org> で入手可能) の指示に従って、ローカルルールを作成することができます。

マルチドメイン展開では、任意のドメインにローカル侵入ルールをインポートできます。現在のドメインと親ドメインにインポートされたローカル侵入ルールを表示できます。

## 侵入ルールのワンタイム手動更新

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin

Firepower Management Center にインターネットアクセスがない場合、新しい侵入ルールの更新を手動でインポートします。

### 手順

- ステップ 1** シスコのサポートサイト (<http://www.cisco.com/cisco/web/support/index.html>) から更新を手動でダウンロードします。
- ステップ 2** [システム (System)] > [更新 (Updates)] を選択し、[ルールの更新 (Rule Updates)] タブをクリックします。
- ステップ 3** 削除されるフォルダに作成またはインポートしたすべてのユーザ定義ルールを移動する場合、ツールバーで [すべてのローカルルールの削除 (Delete All Local Rules)] をクリックして [OK] をクリックする必要があります。
- ステップ 4** [アップロードおよびインストールするルールの更新またはテキストルールファイル (Rule Update or text rule file to upload and install)] を選択し、[参照 (Browse)] をクリックして、ルールアップデートファイルを選択します。
- ステップ 5** 更新が完了した後に、ポリシーを管理対象デバイスに自動的に再展開する場合、[ルールの更新のインポートが完了した後にすべてのポリシーを再適用する (Reapply all policies after the rule update import completes)] をオンにします。
- ステップ 6** [インポート (Import)] をクリックします。ルールの更新がインストールされ、[ルールアップデートログ (Rule Update Log)] 詳細ビューが表示されます。

(注) ルール更新のインストール中にエラーメッセージが表示された場合は、サポートに連絡してください。

## 侵入ルールのワンタイム自動更新

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin

新しい侵入ルールの更新を自動的にインポートするには、サポートサイトに接続するためのインターネットアクセスがアプライアンスで必要になります。

## 始める前に

- Firepower Management Center にインターネットアクセス権があることを確認してください（[セキュリティ、インターネットアクセス、および通信ポート（2785 ページ）](#) を参照）。

## 手順

- 
- ステップ 1** [システム (System)] > [更新 (Updates)] を選択します。
- ステップ 2** [ルールの更新 (Rule Updates)] タブをクリックします。
- ステップ 3** 削除されるフォルダに作成またはインポートしたすべてのユーザ定義ルールを移動する場合、ツールバーで [すべてのローカルルールの削除 (Delete All Local Rules)] をクリックして [OK] をクリックします。
- ステップ 4** [サポートサイトから新しいルールの更新をダウンロードする (Download new Rule Update from the Support Site)] を選択します。
- ステップ 5** 更新が完了した後に、変更した設定を管理対象デバイスに自動的に再展開する場合、[ルールの更新のインポートが完了した後にすべてのポリシーを再適用する (Reapply all policies after the rule update import completes)] チェックボックスをオンにします。
- ステップ 6** [インポート (Import)] をクリックします。  
ルールの更新がインストールされ、[ルールアップデートログ (Rule Update Log)] 詳細ビューが表示されます。

**注意** ルール更新のインストール中にエラーメッセージが表示された場合は、サポートに連絡してください。

---

## 定期的な侵入ルール更新の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin

## 手順

- 
- ステップ 1** [システム (System)] > [更新 (Updates)] を選択します。
- ステップ 2** [ルールの更新 (Rule Updates)] タブをクリックします。
- ステップ 3** 作成した、または削除されたフォルダにインポートしたすべてのユーザ定義ルールを移動するには、ツールバーで [すべてのローカルルールの削除 (Delete All Local Rules)] をクリックし、[OK] をクリックします。

**ステップ 4** [ルールアップデートの再帰的なインポートを有効にする (Enable Recurring Rule Update Imports) ] チェックボックスをオンにします。

[ルールアップデートの再帰的なインポート (Recurring Rule Update Imports) ] セクションの見出しの下に、インポート ステータスに関するメッセージが表示されます。

**ステップ 5** [インポート頻度 (Import Frequency) ] フィールドで、次を指定します。

- 更新の頻度 ([日次 (Daily) ]、[週次 (Weekly) ]、または [月次 (Monthly) ]) 。
- 更新が必要な曜日または日付。
- 更新を開始する時刻。

**ステップ 6** 更新の完了後、変更された設定を管理対象デバイスに自動的に再展開するには、[ルール更新の完了後、更新されたポリシーを管理対象デバイスに展開する (Deploy updated policies to targeted devices after rule update completes) ] チェックボックスをオンにします。

**ステップ 7** [保存 (Save) ] をクリックします。

**注意** 侵入ルール更新のインストール中にエラーメッセージが表示された場合は、サポートに連絡してください。

[ルールアップデートの再帰的なインポート (Recurring Rule Update Imports) ] セクションの見出しの下のステータスメッセージが変わり、ルールの更新がまだ実行されていないことが示されます。

## ローカル侵入ルール ファイル インポート

ローカルルール ファイルをインポートする際には次のガイドラインに従います。

- ルールのインポータには、すべてのカスタム ルールが ASCII または UTF-8 でエンコードされるプレーン テキスト ファイルにインポートされることが必要です。
- テキストファイル名には英数字とスペースを使用できますが、下線 ( \_ )、ピリオド ( . )、ダッシュ ( - ) 以外の特殊記号は使用できません。
- システムは、単一のポンド文字 ( # ) で始まるローカルルールをインポートしますが、これらには削除のフラグが立てられます。
- 単一のポンド文字 ( # ) で始まるローカルルールはインポートされますが、2つのポンド文字 ( ## ) で始まるローカルルールはインポートされません。
- ルールにはエスケープ文字を含めることはできません。
- ローカルルールをインポートするときにはジェネレータ ID (GID) を指定する必要はありません。指定する場合は、標準テキストルールに GID 1 のみを指定します。
- ルールを初めてインポートするときには、SnortID (SID) またはリビジョン番号を指定しないでください。これにより、削除されたルールを含むその他のルールの SID の競合を回避できます。システムはルールに対して、1000000 以上の次に使用できるカスタムルール SID、およびリビジョン番号の 1 を自動的に割り当てます。

SID を持つルールをインポートする必要がある場合、SID は 1,000,000 ～ 9,999,999 の間の一意の数字でなければなりません。

マルチドメイン展開では、SID が Firepower Management Center 上のすべてのドメインによって使用される共有プールからインポートされたルールに割り当てられます。複数の管理者がローカルルールを同時にインポートしている場合、個々のドメイン内の SID が連続していないように見える場合があります。それは、数字が別のドメインにシーケンスに割り込んで指定されたためです。

- 以前にインポートしたローカルルールの更新バージョンをインポートするとき、または削除したローカルルールを元に戻すときは、システムによって指定された SID および現在のリビジョン番号より大きいリビジョン番号を含める**必要があります**。ルールを編集して、現在のルールまたは削除されたルールのリビジョン番号を判別できます。



(注) ローカルルールを削除すると、システムは自動的にリビジョン番号を増やします。これは、ローカルルールを元に戻すための方法です。削除されたすべてのローカルルールは、ローカルルールカテゴリから、削除されたルールカテゴリへ移動されます。

- ルールに次のいずれかが含まれていると、インポートに失敗します。
  - 2147483647 より大きい SID。
  - 64 文字よりも長い送信元ポートまたは宛先ポートのリスト。
- 非推奨の `threshold` キーワードと侵入イベントしきい値機能を組み合わせて使用しているローカルルールをインポートして、侵入ポリシーで有効にすると、ポリシーの検証に失敗します。
- インポートされたすべてのローカルルールは、ローカルルールカテゴリに自動的に保存されます。
- システムによって、インポートしたローカルルールは常に無効なルール状態に設定されます。ローカルルールを侵入ポリシーで使用できるようにするには、ローカルルールの状態を手動で設定する必要があります。

## ローカル侵入ルール ファイルのインポート

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

次の説明に従ってインポートした進入ルールは、ローカルルールカテゴリに保存されます。

## 手順

- 
- ステップ 1** [システム (System)] > [更新 (Updates)] を選択します。
- ステップ 2** [ルールの更新 (Rule Updates)] タブをクリックします。
- ステップ 3** [ルールの更新またはアップロードおよびインストールするテキスト ルール ファイル (Rule Update or text rule file to upload and install)] を選択して、ルール ファイルにナビゲートするために [参照 (Browse)] をクリックします。
- ステップ 4** [インポート (Import)] をクリックします。
- 

## 次のタスク

- 侵入ポリシーで、適切なルールが有効になっていることを確認してください。
- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## ルールの更新ログ

Firepower Management Center は、ユーザがインポートする各ルール更新およびローカルルールファイルごとに 1 つのレコードを生成します。

各レコードにはタイムスタンプ、ファイルをインポートしたユーザの名前、およびインポートが正常に終了したか失敗したかを示すステータスアイコンが含まれています。ユーザは、インポートしたすべてのルール更新とローカルルールファイルのリストを管理したり、リストからレコードを削除したり、インポートしたすべてのルールとルール更新コンポーネントに関する詳細レコードにアクセスすることができます。

[ルールアップデートのインポート ログ (Rule Update Import Log)] 詳細ビューには、ルール更新またはローカルルールファイルにインポートされた各オブジェクトの詳細レコードが表示されます。表示されるレコードのうち、自分のニーズに合う情報のみを含むカスタムワークフローまたはレポートを作成することもできます。

## 侵入ルール更新のログ テーブル

表 19: 侵入ルール更新のログ フィールド

フィールド	説明
要約	インポート ファイルの名前。インポートが失敗した場合は、ファイル名の下に、失敗した理由の簡単な説明が表示されます。
時刻 (Time)	インポートが開始された日時。
ユーザ ID (User ID)	インポートをトリガーとして使用したユーザ名。



フィールド	説明
ステータス (Status)	<p>インポートの状態を表します</p> <ul style="list-style-type: none"> <li>• 正常終了 (🟢)</li> <li>• 失敗、または実行中 (🔴)</li> </ul> <p>インポート中には [ルールアップデートログ (Rule Update Log)] ページで、正常終了しなかった、または完了していないことを示す赤いステータス アイコンが表示され、インポートが正常終了した場合のみこれが緑色のアイコンに変わります。</p>



**ヒント** 侵入ルール更新のインポートの進行中に示される、インポートの詳細を表示することができます。

## 侵入ルールの更新ログの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

**ステップ 1** [システム (System)] > [更新 (Updates)] を選択します。


**ヒント** 侵入ルール エディタ ページ ([オブジェクト (Objects)] > [侵入ルール (Intrusion Rules)]) の [インポート ページ (Import Rules)] をクリックすることもできます。

**ステップ 2** [ルールの更新 (Rule Updates)] タブをクリックします。

**ステップ 3** [ルールアップデートログ (Rule Update Log)] をクリックします。

**ステップ 4** 次の 2 つの対処法があります。

- 詳細の表示：ルールの更新またはローカルルールファイルにインポートされる各オブジェクトの詳細を表示するには、表示するファイルの横にある表示アイコン (🔍) をクリックします (侵入ルールの更新インポート ログの詳細の表示 (191 ページ) を参照)。

- 削除：インポート ログからインポート ファイル レコード（ファイルに含まれるすべてのオブジェクトに関する詳細レコードを含む）を削除するには、インポート ファイル名の横にある削除アイコン（）をクリックします。

（注） ログからファイルを削除しても、インポート ファイルにインポートされているオブジェクトはいずれも削除されませんが、インポート ログ レコードのみは削除されます。

---

## ルールアップデートのインポート ログの詳細ビュー



---

**ヒント** 1つのインポート ファイルのレコードのみが表示されている [ルールアップデートのインポート ログ (Rule Update Import Log) ] 詳細ビューからツールバーの [検索 (Search) ] をクリックして検索を開始した場合でも、[ルールアップデートのインポート ログ (Rule Update Import Log) ] データベースの全体が検索されます。検索の対象とするすべてのオブジェクトが含まれるように、時間制限が設定されていることを確認します。

---

表 20: [ルール アップデートのインポート ログ (Rule Update Import Log) ] 詳細ビューのフィールド

フィールド	説明
操作 (Action)	<p>オブジェクト タイプについて、次のいずれかが発生していることを示します。</p> <ul style="list-style-type: none"> <li>• [新規 (new) ] (ルールで、このアプライアンスにルールが最初に格納された場合)</li> <li>• [変更済み (changed) ] (ルール更新コンポーネントまたはルール用。ルール更新コンポーネントが変更された場合、またはルールのリビジョン番号が大きく、GID と SID が同じ場合)</li> <li>• [競合 (collision) ] (ルール更新コンポーネントまたはルール用。アプライアンス上の既存のコンポーネントまたはルールとリビジョンが競合しているため、インポートがスキップされた場合)</li> <li>• [削除済み (deleted) ] (ルール用。ルール更新からルールが削除された場合)</li> <li>• [有効 (enabled) ] (ルール更新の編集で、プリプロセッサ、ルール、または他の機能が、システムで提供されるデフォルト ポリシーで有効になっていた場合)</li> <li>• [無効 (disabled) ] (ルールで、システム提供のデフォルト ポリシーでルールが無効になっていた場合)</li> <li>• [ドロップ (drop) ] (ルールで、システムで提供されるデフォルト ポリシーで、ルールが [ドロップおよびイベントの生成 (Drop and Generate Events) ] に設定されていた場合)</li> <li>• [エラー (error) ] (ルール更新またはローカル ルール ファイル用。インポートに失敗した場合)</li> <li>• [適用 (apply) ] (インポートに対して [ルール更新のインポート完了後にすべてのポリシーを再適用する (Reapply all policies after the rule update import completes) ] オプションが有効だった場合)</li> </ul>
デフォルト アクション (Default Action)	<p>ルールの更新によって定義されたデフォルトのアクション。インポートされたオブジェクトのタイプが [ルール (rule) ] の場合、デフォルトのアクションは [通過 (Pass) ]、[アラート (Alert) ]、または [ドロップ (Drop) ] になります。インポートされた他のすべてのオブジェクト タイプには、デフォルトのアクションはありません。</p>

フィールド	説明
詳細 (Details)	コンポーネントまたはルールに対する一意の文字列。ルールの場合、変更されたルールの <b>GID</b> 、 <b>SID</b> 、および旧バージョン番号は、 <code>previously (GID:SID:Rev)</code> と表示されます。変更されていないルールについては、このフィールドは空白です。
ドメイン (Domain)	侵入ポリシーで更新されたルールを使用できるドメイン。子孫ドメインの侵入ポリシーもルールを使用できます。このフィールドは、マルチドメイン展開の場合にのみ存在します。
GID	ルールのジェネレータ ID。たとえば、1 (標準テキストルール) または 3 (共有オブジェクトルール)。
[名前 (Name) ]	インポートされたオブジェクトの名前。ルールの場合はルールの [メッセージ (Message) ] フィールドに対応した名前、ルール更新コンポーネントの場合はコンポーネント名です。
ポリシー	インポートされたルールの場合、このフィールドには [すべて (All) ] が表示されます。これは、インポートされたルールがデフォルトのすべての侵入ポリシーに含まれていたことを意味します。インポートされた他のタイプのオブジェクトについては、このフィールドは空白です。
Rev	ルールのリビジョン番号。
ルール アップデート (Rule Update)	ルール更新のファイル名。
SID	ルールの <b>SID</b> 。
時刻 (Time)	インポートが開始された日時。

フィールド	説明
タイプ (Type)	<p>インポートされたオブジェクトのタイプで、有効な値は次のいずれかです。</p> <ul style="list-style-type: none"> <li>• [ルール更新コンポーネント (rule update component) ] (ルールパックやポリシーパックなどのインポートされたコンポーネント)</li> <li>• [ルール (rule) ] (ルール用。新しいルールまたは更新されたルール。バージョン 5.0.1 では、廃止された update 値の代わりにこの値が使用されます)。</li> <li>• [ポリシー適用 (policy apply) ] (インポートに対して [ルール更新のインポート完了後にすべてのポリシーを再適用する (Reapply all policies after the rule update import completes) ] オプションが有効だった場合)</li> </ul>
メンバー数 (Count)	<p>各レコードのカウント (1)。テーブルが制限されており、[ルールアップデートログ (Rule Update Log) ] 詳細ビューがデフォルトでルール更新レコードに制限されている場合は、テーブルビューに [メンバー数 (Count) ] フィールドが表示されます。このフィールドは検索できません。</p>

#### 関連トピック

[侵入ルールの更新インポート ログの詳細の表示 \(191 ページ\)](#)

## 侵入ルールの更新インポート ログの詳細の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

#### 手順

- ステップ 1** [システム (System) ] > [更新 (Updates) ] を選択します。
- ステップ 2** [ルールの更新 (Rule Updates) ] タブをクリックします。
- ステップ 3** [ルールアップデートログ (Rule Update Log) ] をクリックします。
- ステップ 4** 表示する詳細レコードが含まれているファイルの隣にある表示アイコン (🔍) をクリックします。
- ステップ 5** 次のいずれかの処理を実行できます。

- ブックマーク：現在のページをブックマークするには、[このページをブックマーク (Bookmark This Page)] をクリックします。
- 検索の編集：現在の単一制約が事前入力されている検索ページを開くには、検索制約の横にある [検索の編集 (Edit Search)] または [検索の保存 (Save Search)] を選択します。
- ブックマークの管理：ブックマークの管理ページに移動するには、[レポート デザイナ (Report Designer)] をクリックします。
- レポート：現在のビューのデータに基づいてレポートを生成するには、[レポート デザイナ (Report Designer)] をクリックします。
- 検索：ルールの更新インポート ログ データベース全体でルールの更新インポート レコードを検索するには、[検索 (Search)] をクリックします。
- ソート：現在のワークフローページでレコードをソートしたり制約したりするには、詳細について [ドリルダウン ページの使用 \(2439 ページ\)](#) を参照してください。
- ワークフローの切り替え：別のワークフローを一時的に使用するには、[(ワークフローの切り替え) (switch workflows)] をクリックします。

## 地理位置情報データベースの更新

シスコ地理位置情報データベース (GeoDB) は、ルーティング可能な IP アドレスと関連付けられた地理的データ (国、都市、座標など) および接続関連のデータ (インターネットサービス プロバイダー、ドメイン名、接続タイプなど) のデータベースです。検出された IP アドレスと一致する GeoDB 情報が検出された場合は、その IP アドレスに関連付けられている位置情報を表示できます。国や大陸以外の位置情報の詳細を表示するには、システムに GeoDB をインストールする必要があります。シスコでは、GeoDB の定期的な更新を提供しています。

GeoDB を更新するには、Firepower Management Center で [位置情報の更新 (Geolocation Updates)] ページ ([システム (System)] > [更新 (Updates)] > [位置情報の更新 (Geolocation Updates)]) を使用します。サポートまたは自身のアプライアンスから取得した GeoDB の更新をアップロードすると、それらがこのページに表示されます。



- (注) [位置情報の更新 (Geolocation Updates)] ページで [位置情報の更新をサポートサイトからダウンロードおよびインストールする (Download and install geolocation update from the Support Site)] をクリックするか、または手動でサポート サイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、破損する可能性があります。

GeoDB の更新にかかる時間はアプライアンスによって異なります。インストールには通常、30 ~ 40 分かかります。GeoDB の更新によって他のシステム機能 (進行中の位置情報収集など) が中断されることはありませんが、更新が完了するまでシステム リソースが消費されます。更新を計画する場合には、この点について考慮してください。

GeoDB を更新すると、GeoDB の以前のバージョンが上書きされ、すぐに有効になります。GeoDB を更新すると、Firepower Management Center により、管理対象デバイス上の関連データが自動的に更新されます。GeoDB の更新が展開全体で有効になるまでに数分かかることがあります。更新後に再度展開する必要はありません。

## 手動による GeoDB の更新（インターネット接続）

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin

新しい GeoDB 更新プログラムは、アプライアンスがインターネットにアクセスできる場合のみ、サポートサイトに接続することで自動的にインポートできます。

### 手順

- ステップ 1 [システム (System)] > [更新 (Updates)] を選択します。
- ステップ 2 [位置情報の更新 (Geolocation Updates)] タブをクリックします。
- ステップ 3 [サポートサイトから地理位置情報の更新をダウンロードしてインストールする (Download and install geolocation update from the Support Site)] を選択します。
- ステップ 4 [インポート (Import)] をクリックします。  
システムは [地理位置情報の更新 (Geolocation Update)] タスクをキューに入れます。このタスクは、最新の更新について、シスコ サポート サイト (<http://www.cisco.com/cisco/web/support/index.html>) で確認します。
- ステップ 5 必要に応じて、タスクのステータスをモニタします。[タスク メッセージの表示 \(330 ページ\)](#) を参照してください。
- ステップ 6 更新が終了したら、[地理位置情報の更新 (Geolocation Updates)] ページに戻るか、[ヘルプ (Help)] > [バージョン情報 (About)] を選択して、GeoDB のビルド番号がインストールした更新と一致していることを確認します。

## 地理位置情報データベース (GeoDB) の手動更新：インターネット接続なし

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin

Firepower Management Center がインターネットにアクセスできない場合は、シスコサポートサイトからネットワーク上のローカルマシンに GeoDB の更新をダウンロードして、その更新を手動で Firepower Management Center にアップロードできます。

#### 手順

- ステップ 1 シスコ サポート サイト (<http://www.cisco.com/cisco/web/support/index.html>) から、手動で更新をダウンロードします。
- ステップ 2 [システム (System)] > [更新 (Updates)] を選択します。
- ステップ 3 [位置情報の更新 (Geolocation Updates)] タブをクリックします。
- ステップ 4 [地理位置情報の更新のアップロードとインストール (Upload and install geolocation update)] を選択します。
- ステップ 5 ダウンロードした更新を参照して、[アップロード (Upload)] をクリックします。
- ステップ 6 [インポート (Import)] をクリックします。
- ステップ 7 必要に応じて、タスクのステータスをモニタします。[タスクメッセージの表示 \(330 ページ\)](#) を参照してください。
- ステップ 8 更新が終了したら、[地理位置情報の更新 (Geolocation Updates)] ページに戻るか、[ヘルプ (Help)] > [バージョン情報 (About)] を選択して、GeoDB のビルド番号がインストールした更新と一致していることを確認します。

## GeoDB 更新のスケジューリング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin

地理位置情報データベース (GeoDB) の定期更新を自動化できます。GeoDB の定期更新は 7 日ごとに 1 度 (週 1 回) 実行されます。週ごとに更新が繰り返される時刻を設定できます。

#### 手順

- ステップ 1 [システム (System)] > [更新 (Updates)] を選択します。
- ステップ 2 [位置情報の更新 (Geolocation Updates)] タブをクリックします。
- ステップ 3 [位置情報の定期更新 (Recurring Geolocation Updates)] の下で、[週ごとの定期更新を有効にする (Enable Recurring Weekly Updates)] チェックボックスをオンにします。
- ステップ 4 [更新の開始時刻 (Update Start Time)] フィールドで、週ごとに GeoDB 更新を行う曜日と時刻を指定します。



ステップ 5 [保存 (Save) ] をクリックします。

---





## 第 7 章

# バックアップと復元

次のトピックでは、Firepower システムでバックアップおよび復元機能を使用する方法について説明します。

- [バックアップと復元の概要 \(197 ページ\)](#)
- [バックアップと復元に関する制限事項 \(197 ページ\)](#)
- [バックアップ ファイル \(199 ページ\)](#)
- [Firepower Management Center のバックアップ \(200 ページ\)](#)
- [管理対象デバイスのローカルでのバックアップ \(201 ページ\)](#)
- [Firepower Management Center からの管理対象デバイスのバックアップ \(203 ページ\)](#)
- [バックアップ プロファイルの作成 \(204 ページ\)](#)
- [ローカル ホストからのバックアップのアップロード \(205 ページ\)](#)
- [\[バックアップ管理 \(Backup Management\) \] ページ \(206 ページ\)](#)
- [バックアップ ファイルからのアプライアンスの復元 \(207 ページ\)](#)

## バックアップと復元の概要

災害から回復する能力は、システム保守計画の重要な部分を占めます。

Firepower Management Center または 7000/8000 シリーズ デバイスでデータをバックアップしたり復元したりすることができます。

## バックアップと復元に関する制限事項

アプライアンスまたはローカルコンピュータにバックアップファイルを保存できます。Firepower Management Center を使用してバックアップを実行する場合は、リモートストレージを使用できます。



(注) バックアップデータの収集中に、データの相関付けが一時的に停止してバックアップ関連の設定を変更できなくなることがあります。

バックアップと復元に関する次の制限事項に注意してください。

- 代替アプライアンスにバックアップを復元できるのは、2 台のアプライアンスが同じモデルであり、同じバージョンの Firepower システム ソフトウェアを実行している場合のみです。
- バックアップには、キャプチャされたファイル データは含まれません。
- NGIPSv、Firepower Threat Defense物理または仮想管理対象デバイス、あるいは ASA FirePOWER モジュールのバックアップファイルを作成または復元することはできません。イベントデータをバックアップするには、管理元の Firepower Management Center のバックアップを実行します。
- アプライアンス間で設定をコピーするためにバックアップおよび復元プロセスを使用しないでください。バックアップファイルは、アプライアンスを一意に識別する情報を含んでおり、共有することはできません。
- Firepower Management Center を復元した後、最新の侵入ルールの更新を適用する必要があります。
- PKI オブジェクトに関連付けられている秘密キーは、アプライアンスに保存されるたびに、ランダムに生成されたキーで暗号化されます。PKI オブジェクトに関連付けられている秘密キーを含むバックアップを実行すると、秘密キーは復号されてから、暗号化されていないバックアップ ファイルに含められます。バックアップ ファイルは安全な場所に保存してください。
- PKI オブジェクトに関連付けられている秘密キーを含むバックアップを復元すると、その秘密キーはランダムに生成されたキーで暗号化されてからアプライアンスに保存されます。
- クリーン リストとカスタム検出リストのいずれかを有効にしてファイル ポリシーを含むバックアップを復元すると、復元されるファイルのリストとあらゆる既存のファイルリストがマージされます。
- バックアップを実行してから、確認済みの侵入イベントを削除し、そのバックアップを使用して復元すると、削除された侵入イベントは復元されますが、それらの確認済みステータスは復元されません。それらの復元された侵入イベントは、[確認済みイベント (Reviewed Events)] ではなく [侵入イベント (Intrusion Events)] に表示されます。
- 侵入イベントのデータを含むバックアップを、そのデータがすでに含まれているアプライアンスに復元すると、重複したイベントが作成されることとなります。そのようなことが起こらないようにするため、侵入イベントのバックアップは、以前の侵入イベントデータが含まれていないアプライアンスにのみ復元してください。
- セキュリティ ゾーンまたはインターフェイス グループとのインターフェイス アソシエーションが設定されている場合、それらのアソシエーションはバックアップされません。それらは、復元後に再設定する必要があります。
- Firepower Management Center では、バックアップ機能と復元機能はグローバル ドメインのみで使用できます。サブドメインの範囲内では、バックアップと復元の代わりにエクスポート機能とインポート機能を使用することができます。

## 関連トピック

[リモートストレージ管理](#) (949 ページ)[コンフィギュレーションのインポート/エクスポートについて](#) (211 ページ)[侵入イベントを確認済みとしてマーク](#) (2570 ページ)[インターフェイスオブジェクト：インターフェイスグループとセキュリティゾーン](#) (437 ページ)

## バックアップ ファイル

実行するバックアップのタイプに応じて、さまざまなデータがバックアップされます。キャプチャされたファイルデータはバックアップされませんことに注意してください。次の表を使用して、どのようなタイプのバックアップを実行するかを決定します。

表 21: それぞれのバックアップタイプで保存されるデータ

バックアップタイプ	構成データが含まれるか	イベントデータが含まれるか	統合ファイルが含まれるか
Firepower Management Center	○	○	[いいえ (No) ]
7000 & 8000 シリーズ (デバイス自体から実行)	[はい (Yes) ]	[いいえ (No) ]	[いいえ (No) ]
7000 & 8000 シリーズ (管理元の Firepower Management Center から実行)	[はい (Yes) ]	[いいえ (No) ]	○



(注) NGIPSv デバイス、Firepower Threat Defense 物理または仮想管理対象デバイス、あるいは ASA FirePOWER モジュールについては、バックアップ ファイルを作成または復元することはできません。イベント データをバックアップするには、管理元の Firepower Management Center のバックアップを実行します。

イベント データに加えて、アプライアンスの復元に必要なすべてのコンフィギュレーション ファイルを含むバックアップファイルを定期的に保存する必要があります。設定の変更をテストする際にもシステムをバックアップして、必要に応じて保存されている設定に戻すことができます。バックアップ ファイルを、アプライアンスに保存するか、ローカル コンピュータに保存するかを選択できます。

あるいは、バックアップ ファイルが 4GB を超える場合は、SCP 経由でリモート ホストにコピーします。4 GB を超えるファイルのアップロードは Web ブラウザでサポートされていないため、バックアップ ファイルがそのように大きい場合には、ローカル コンピュータからバック

クアッブをアップロードすることはできません。Firepower Management Center では、バックアップ ファイルをリモート ロケーションに保存できます。

#### 関連トピック

[リモートストレージ管理](#) (949 ページ)

## Firepower Management Center のバックアップ

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin/Maint

#### 始める前に

- アプライアンスに十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の90%以上を使用すると、バックアップは失敗することがあります。必要に応じて、古いバックアップファイルを削除するか、古いバックアップファイルをアプライアンスの外部に転送するか、リモートストレージを使用してください。[リモートストレージ管理](#) (949 ページ) を参照してください。

#### 手順

**ステップ 1** [システム (System)] > [ツール (Tools)] > [バックアップ/復元 (Backup/Restore)] を選択します。

**ステップ 2** [Firepower 管理バックアップ (Firepower Management Backup)] をクリックします。

**ステップ 3** [名前 (Name)] を入力します。

**ステップ 4** その他以下の2つの対処法があります。

- 設定をアーカイブするには、[設定をバックアップ (Back Up Configuration)] を選択します。マルチドメイン展開では、このオプションを無効にできません。
- イベントデータベース全体をアーカイブするには、[イベントをバックアップ (Back Up Events)] を選択します。

**ステップ 5** バックアップの完了時に通知を受けるためには、[電子メール (Email)] チェックボックスを選択して、用意されているテキストボックスに電子メールアドレスを入力します。

(注) 電子メール通知を受信するには、[メールリレーホストおよび通知アドレスの設定](#) (971 ページ) で説明されているように、リレーホストを設定する必要があります。

**ステップ 6** セキュアなコピー (scp) を使用してバックアップアーカイブを異なるマシンにコピーするには、[完了時にコピー (Copy when complete)] チェックボックスを選択してから、用意されているテキストボックスに以下の情報を入力します。

- [ホスト (Host) ] フィールドに、バックアップのコピー先となるマシンのホスト名または IP アドレス
- [パス (Path) ] フィールドに、バックアップのコピー先となるディレクトリへのパス
- [ユーザ (User) ] フィールドに、リモート マシンへのログインに使用するユーザ名
- [パスワード (Password) ] フィールドに、そのユーザ名のパスワード。パスワードの代わりに SSH 公開キーを使用してリモート マシンにアクセスする場合は、そのマシンの指定ユーザの `authorized_keys` ファイルに、[SSH 公開キー (SSH Public Key) ] フィールドの内容をコピーします。

**ヒント** このオプションをオフにする場合、バックアップ中に使用された一時ファイルがシステムによってリモートサーバに保存されます。このオプションをオンにする場合は、一時ファイルはリモートサーバに保存されません。Cisco は、システム障害が発生した場合にアプライアンスを復元できるように、バックアップをリモート ロケーションに定期的に保存することを推奨します。

**ステップ 7** 次の選択肢があります。

- バックアップ ファイルをアプライアンスに保存するには、[バックアップ開始 (Start Backup) ] をクリックします。バックアップ ファイルは `/var/sf/backup` ディレクトリに保存されます。
- この設定を後で使用できるバックアップ プロファイルとして保存するには、[新規として保存 (Save As New) ] をクリックします。

#### 次のタスク

- バックアップファイルに PKI オブジェクトデータが含まれる場合は、バックアップ内に暗号化されていない秘密キーが含まれています。このため、バックアップはセキュアな場所に保存してください。

## 管理対象デバイスのローカルでのバックアップ

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	該当なし	Admin/Maint

アプライアンスのローカル Web インターフェイスを使用して、次の手順を実行する必要があります。

## 始める前に

- アプライアンスに十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の90%以上を使用すると、バックアップは失敗することがあります。必要に応じて、古いバックアップファイルを削除するか、古いバックアップファイルをアプライアンスの外部に転送してください。

## 手順

**ステップ 1** [システム (System)] > [ツール (Tools)] > [バックアップ/復元 (Backup/Restore)] を選択します。

**ステップ 2** [デバイス バックアップ (Device Backup)] をクリックします。

**ステップ 3** [名前 (Name)] フィールドに、バックアップ ファイルの名前を入力します。

**ステップ 4** バックアップの完了時に通知を受けるためには、[電子メール (Email)] チェックボックスを選択して、用意されているテキスト ボックスに電子メールアドレスを入力します。

(注) 電子メール通知を受信するには、[メール リレー ホストおよび通知アドレスの設定 \(971 ページ\)](#) で説明されているように、リレー ホストを設定する必要があります。

**ステップ 5** セキュアなコピー (scp) を使用してバックアップ アーカイブを異なるマシンにコピーするには、[完了時にコピー (Copy when complete)] チェックボックスを選択してから、用意されているテキストボックスに以下の情報を入力します。

- [ホスト (Host)] フィールドに、バックアップのコピー先となるマシンのホスト名または IP アドレス。
- [パス (Path)] フィールドに、バックアップのコピー先となるディレクトリへのパス。
- [ユーザ (User)] フィールドに、リモート マシンへのログインに使用するユーザ名。
- [パスワード (Password)] フィールドに、そのユーザ名のパスワード。パスワードの代わりに SSH 公開キーを使用してリモート マシンにアクセスする場合は、そのマシンの指定ユーザの `authorized_keys` ファイルに、[SSH 公開キー (SSH Public Key)] フィールドの内容をコピーします。

**ヒント** このオプションをオフにする場合、バックアップ中に使用された一時ファイルがシステムによってリモートサーバに保存されます。このオプションをオンにする場合は、一時ファイルはリモートサーバに保存されません。Cisco は、システム障害が発生した場合にアプライアンスを復元できるように、バックアップをリモート ロケーションに定期的に保存することを推奨します。

**ステップ 6** 次の選択肢があります。

- バックアップ ファイルをアプライアンスに保存するには、[バックアップ開始 (Start Backup)] をクリックします。バックアップ ファイルは `/var/sf/backup` ディレクトリに保存されます。



- この設定を後で使用できるバックアップ プロファイルとして保存するには、[新規として保存 (Save As New)] をクリックします。

### 次のタスク

- バックアップファイルに PKI オブジェクトデータが含まれる場合は、バックアップ内に暗号化されていない秘密キーが含まれています。このため、バックアップはセキュアな場所に保存してください。

## Firepower Management Center からの管理対象デバイスのバックアップ

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

### 始める前に

- アプライアンスに十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の 90% 以上を使用すると、バックアップは失敗することがあります。必要に応じて、古いバックアップファイルを削除するか、古いバックアップファイルをアプライアンスの外部に転送するか、リモートストレージを使用してください。[リモートストレージ管理 \(949 ページ\)](#) を参照してください。

### 手順

- ステップ 1** [システム (System)] > [ツール (Tools)] > [バックアップ/復元 (Backup/Restore)] を選択します。
- ステップ 2** [管理対象デバイスのバックアップ (Managed Device Backup)] をクリックします。
- ステップ 3** [管理対象デバイス (Managed Devices)] フィールドで、1 つ以上の管理対象デバイスを選択します。
- ステップ 4** 設定データと共に統合ファイルも含めるには、[すべての統合ファイルを含める (Include All Unified Files)] チェックボックスを選択します。統合ファイルは、管理対象デバイスがまだ Firepower Management Center へ送っていない、分析と保管のためのイベントデータのバイナリファイルです。
- ステップ 5** Firepower Management Center にバックアップファイルのコピーを保存するには、[管理センターで取得する (Retrieve to Management Center)] チェックボックスを選択します。各デバイスの

バックアップファイルをそのデバイス自体のみに保存するには、このチェックボックスをオフにしておいてください。

(注) [管理センターで取得する (Retrieve to Management Center)] を選択したのに Firepower Management Center がリモートストレージにバックアップするよう設定されている場合は、デバイスのバックアップファイルはリモートに設定されている場所に保存されます。

**ステップ 6** [バックアップ開始 (Start Backup)] をクリックします。バックアップファイルは `/var/sf/backup` ディレクトリに保存されます。

#### 次のタスク

- バックアップファイルに PKI オブジェクトデータが含まれる場合は、バックアップ内に暗号化されていない秘密キーが含まれています。このため、バックアップはセキュアな場所に保存してください。

## バックアッププロファイルの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

この手順は、デバイスの Web ユーザ インターフェイスを使用して実行する必要があります。

さまざまな種類のバックアップに使用する設定値を含むバックアッププロファイルを作成できます。後にアプライアンスのファイルをバックアップするときに、これらのプロファイルの 1 つを選択できます。



**ヒント** 新規ファイル名を使用して Firepower Management Center のバックアップファイルを作成する場合、システムにより自動的に、その名前がバックアッププロファイルが作成されます。

#### 手順

- ステップ 1** [システム (System)] > [ツール (Tools)] > [バックアップ/復元 (Backup/Restore)] を選択します。
- ステップ 2** [バックアッププロファイル (Backup Profiles)] タブをクリックします。
- ステップ 3** [プロファイルの作成 (Create Profile)] をクリックします。
- ステップ 4** バックアッププロファイルの名前を入力します。

- ステップ 5** バックアップ プロファイルを設定します。 [Firepower Management Center のバックアップ \(200 ページ\)](#) を参照してください。
- ステップ 6** バックアップ プロファイルを保存するには、[新規として保存 (Save As New) ] をクリックします。

## ローカル ホストからのバックアップのアップロード

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

ローカル ホストからアプライアンスにバックアップ ファイルをアップロードできます。この手順は、デバイスの Web インターフェイスを使用して実行する必要があります。

バックアップ ファイルに PKI オブジェクトが含まれている場合、アップロード時に、システムはランダム生成されたキーを使用して、内部 CA および内部証明書オブジェクトに関連付けられた秘密キーを再暗号化します。

### 始める前に

- [\[バックアップ管理 \(Backup Management\) \] ページ \(206 ページ\)](#) の説明に従って、ダウンロード機能を使用し、バックアップ ファイルをローカル ホストにダウンロードします。
- SCP を介してローカル ホストからリモート ホストに 4GB より大きいバックアップをコピーし、そこから Firepower Management Center に取り出します (Web ブラウザではその大きさのファイルのアップロードがサポートされていないため)。詳細については、[リモートストレージ管理 \(949 ページ\)](#) を参照してください。

### 手順

- ステップ 1** [システム (System) ] > [ツール (Tools) ] > [バックアップ/復元 (Backup/Restore) ] を選択します。
- ステップ 2** [バックアップのアップロード (Upload Backup) ] をクリックします。
- ステップ 3** [参照 (Browse) ] をクリックし、アップロードするバックアップファイルまで移動して選択します。
- ステップ 4** [バックアップのアップロード (Upload Backup) ] をクリックします。
- ステップ 5** [バックアップ管理 (Backup Management) ] をクリックして、[バックアップ管理 (Backup Management) ] ページに戻ります。

## 次のタスク

- アプライアンスによってファイルの整合性が確認された後、[バックアップ管理 (Backup Management) ] ページを更新し、詳細なファイル システム情報を表示します。

## [バックアップ管理 (Backup Management) ] ページ

バックアップ ファイルに PKI オブジェクトが含まれている場合は、アップロード時に、内部 CA および内部証明書オブジェクトに関連付けられている秘密キーが、ランダムに生成されたキーで再暗号化されます。

ローカル ストレージを使用する場合、バックアップ ファイルは /var/sf/backup に保存されて、/var パーティションで使用されているディスク領域量と共に [バックアップ管理 (Backup Management) ] ページの下部にリストされます。Firepower Management Center で、[バックアップ管理 (Backup Management) ] ページの上部にある [リモートストレージ (Remote Storage) ] を選択して、リモートストレージ オプションを設定します。その後、リモートストレージを有効にするには [バックアップ管理 (Backup Management) ] ページの [バックアップ用にリモートストレージを有効にする (Enable Remote Storage for Backups) ] チェック ボックスをオンにします。リモートストレージを使用している場合は、プロトコル、バックアップ システム、およびバックアップ ディレクトリがページの下部に表示されます。

次の表では、[バックアップ管理 (Backup Management) ] ページの各列とアイコンについて説明します。

表 22: バックアップ管理 (Backup Management)

機能	説明
システム情報 (System Information)	元のアプライアンスの名前、タイプ、バージョン。バックアップを復元できるのは、同一のアプライアンス タイプとバージョンに対してだけであることに注意してください。
作成日	バックアップ ファイルが作成された日時
ファイル名 (File Name)	バックアップ ファイルのフルネーム
VDBバージョン (VDB Version)	バックアップ時にアプライアンスで実行されている脆弱性データベース (VDB) のビルド。
参照先	バックアップ ファイルの場所
サイズ (MB) (Size (MB))	バックアップファイルのサイズ (メガバイト)
イベント? (Events?)	[はい (Yes) ] は、バックアップにイベント データが含まれていることを示します

機能	説明
表示 (View)	バックアップファイルの名前をクリックすると、圧縮されたバックアップファイルに含まれるファイルのリストが表示されます。
復元 (Restore)	バックアップファイルを選択した状態でクリックすると、そのバックアップファイルがアプライアンスに復元されます。VDBバージョンがバックアップファイルのVDBのバージョンと一致しない場合、このオプションは無効になります。
ダウンロード (Download)	バックアップファイルが選択された状態でクリックすると、そのバックアップファイルがローカルコンピュータに保存されます。
削除 (Delete)	バックアップファイルが選択された状態でクリックすると、そのバックアップファイルが削除されます。
[移動 (Move) ] をクリックします	Firepower Management Center で、以前に作成したローカルバックアップが選択された状態でクリックすると、そのバックアップが指定のリモートバックアップロケーションに送信されます。

## バックアップファイルからのアプライアンスの復元

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

[バックアップ管理 (Backup Management) ] ページを使用して、バックアップファイルからアプライアンスを復元できます。この手順は、デバイスの Web インターフェイスを使用して実行する必要があります。

**注意**

- この操作により、すべてのコンフィギュレーションファイルが上書きされ、管理対象デバイスでは、すべてのイベントデータが上書きされます。
- 仮想 Firepower Management Center で作成されたバックアップを物理 Firepower Management Center に復元しないでください。これはシステムリソースに負荷をかける可能性があります。



- (注) バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを（それらが使用されている場所をメモした上で）削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。

**始める前に**

- バックアップファイル内の VDB のバージョンが、アプライアンスの現在の VDB のバージョンと一致していることを確認します。詳細については、[ダッシュボードの表示 \(274 ページ\)](#) を参照してください。
- バックアップの完了後にアプライアンスに追加したライセンスは、リストア時の競合を避けるために、バックアップの復元前に削除します。詳細については、[Firepower の機能ライセンスについて \(137 ページ\)](#) を参照してください。
- バックアップに保管されているものと同じ侵入イベントデータがアプライアンスに存在しないことを確認します。これは、そのような状況下でバックアップを復元すると、重複するイベントが作成されるためです。詳細については、[侵入イベントについて \(2555 ページ\)](#) を参照してください。

**手順**

- ステップ 1** [システム (System)] > [ツール (Tools)] > [バックアップ/復元 (Backup/Restore)] を選択します。
- ステップ 2** バックアップファイルをクリックして、そのコンテンツを表示します。詳細には、ファイルの所有者、ファイルの権限、ファイルサイズ、および日付が含まれています。
- ステップ 3** [システム (System)] > [ツール (Tools)] > [バックアップ/復元 (Backup/Restore)] を選択して、[バックアップ管理 (Backup Management)] ページに戻ります。
- ステップ 4** 復元するバックアップファイルを選択します。
- ステップ 5** [復元 (Restore)] をクリックします。

(注) バックアップの VDB バージョンがアプライアンスに現在インストールされている VDB のバージョンと一致しない場合、[復元 (Restore)] ボタンはグレー表示されません。

**ステップ 6** ファイルを復元するには、次のいずれかまたは両方のオプションを選択します。

• **設定データの復元 (Restore Configuration Data)**

(注) 管理対象デバイスの設定をバックアップファイルから復元すると、デバイスの管理用の Firepower Management Center から行われたデバイス設定の変更も復元されます。バックアップファイルを復元することで、バックアップファイルの作成後に行った変更は上書きされます。

• **イベントデータの復元 (Restore Event Data)**

**ステップ 7** [復元 (Restore)] をクリックします。

**ステップ 8** アプライアンスを再起動します。

---

### 次のタスク

- 最新のシスコルールアップデートをインポートします。[侵入ルールのワンタイム手動更新 \(182 ページ\)](#) を参照してください。インポートの一環としてポリシーを再展開する場合、設定の変更を展開する必要はありません (後述)。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。
- バックアップの復元前に、アプライアンスから削除したライセンスを追加して再設定します。
- 復元時にアプライアンスがライセンスの競合を示した場合は、サポートまでお問い合わせください。







## 第 8 章

# コンフィギュレーションのインポートとエクスポート

次のトピックでは、インポート/エクスポート機能を使用する方法について説明します。

- [コンフィギュレーションのインポート/エクスポートについて \(211 ページ\)](#)
- [設定のエクスポート \(214 ページ\)](#)
- [設定のインポート \(214 ページ\)](#)

## コンフィギュレーションのインポート/エクスポートについて

インポート/エクスポート機能を使用して、アプライアンス間で構成をコピーできます。インポート/エクスポートはバックアップツールではありませんが、展開に新しいアプライアンスを追加するプロセスを簡素化できます。

単一の設定をエクスポートすることや、(同じタイプまたは異なるタイプの) 一連の設定を単一操作でエクスポートすることができます。後に別のアプライアンスにパッケージをインポートするとき、パッケージ内のどの設定をインポートするかを選択できます。

エクスポートされたパッケージには、その構成のリビジョン情報が含まれ、これにより、別のアプライアンスにその構成をインポートできるかどうかが決まります。アプライアンスに互換性があるものの、パッケージに重複構成が含まれていると、解決オプションが示されます。



- (注) インポート側とエクスポート側のアプライアンスは、同じバージョンの Firepower システムを実行している必要があります。アクセスコントロールとそのサブポリシー (侵入ポリシーを含む) の場合、侵入ルールの更新バージョンも一致している必要があります。バージョンが一致しない場合、インポートは失敗します。インポート/エクスポート機能を使用して侵入ルールを更新することはできません。代わりに、最新バージョンのルール更新をダウンロードして適用します。

## インポート/エクスポートをサポートする構成

インポート/エクスポートは、次の構成でサポートされます。

- アクセス コントロール ポリシーとそれが呼び出すポリシー：プレフィルタ、ネットワーク分析、侵入、SSL、ファイル
- 侵入ポリシー（アクセス コントロールとは無関係に）
- NAT ポリシー（Firepower Threat Defense のみ）
- プラットフォーム設定
- 正常性ポリシー
- アラート応答
- アプリケーションディテクタ（ユーザ定義および Cisco Professional サービスによって提供されるディテクタ）
- ダッシュボード
- カスタム テーブル
- カスタム ワークフロー
- 保存済み検索
- カスタム ユーザ ロール
- レポート テンプレート
- サードパーティ製品および脆弱性マッピング

## 設定のインポート/エクスポートに関する特別な考慮事項

構成をエクスポートすると、他の必要な構成もエクスポートされます。たとえば、アクセスコントロールポリシーをエクスポートすると、そのポリシーが呼び出すサブポリシー、使用しているオブジェクトとオブジェクトグループ、先祖ポリシー（マルチドメイン展開の場合）などもエクスポートされます。別の例として、外部認証が有効になっているプラットフォーム設定ポリシーをエクスポートした場合は、認証オブジェクトもエクスポートされます。ただし、いくつかの例外があります。

- システム提供のデータベースとフィールド：URL フィルタリング カテゴリとレピュテーションデータ、シスコインテリジェンス フィールドデータ、または地理位置情報データベース（GeoDB）はエクスポートされません。展開内のすべてのアプライアンスがシスコから最新情報を取得していることを確認してください。
- グローバルなセキュリティインテリジェンスのリスト：エクスポートされた構成に関連するグローバルなセキュリティインテリジェンスのブラックリストとホワイトリストがエクスポートされます（マルチドメイン展開では、これは現在のドメインに関係なく実行されます。子孫ドメインのリストはエクスポートされません）。インポートプロセスはこれら

のブラックリストとホワイトリストをユーザ作成リストに変換してから、インポートされた構成でそれらの新しいリストを使用します。これにより、インポートされたリストが既存のグローバルなブラックリストおよびホワイトリストと競合することはありません。インポートされた構成でインポート側の Firepower Management Center のグローバルリストを使用するには、これらを手動で追加します。

- 侵入ポリシー共有層：エクスポートプロセスにより、侵入ポリシー共有レイヤが切断されます。以前の共有レイヤはパッケージに含まれ、インポートされた侵入ポリシーには共有レイヤは含まれません。
- 侵入ポリシーのデフォルト変数セット：エクスポートパッケージには、カスタム変数とシステム提供の変数を含むデフォルト変数セットがユーザ定義値とともに含まれています。インポートプロセスでは、インポートされた値でインポート側の Firepower Management Center のデフォルト変数セットを更新します。ただし、インポートプロセスはエクスポートパッケージに存在しないカスタム変数を削除しません。また、エクスポートパッケージに設定されていない値については、インポート側の Firepower Management Center のユーザ定義値を元に戻しません。したがって、インポート側の Firepower Management Center で設定されているデフォルト変数が異なる場合は、インポートされた侵入ポリシーの動作が予想とは異なる可能性があります。
- カスタム ユーザ オブジェクト：Firepower Management Center でカスタム ユーザ グループまたはオブジェクトを作成済みで、そのようなカスタム ユーザ オブジェクトがアクセスコントロールポリシーのいずれかのルールに含まれている場合、エクスポート ファイル (.sfo) にはそのユーザオブジェクト情報が格納されません。このため、そうしたポリシーをインポートする際、これらのカスタム ユーザ オブジェクトへの参照が削除され、宛先 Firepower Management Center にはインポートされません。不明なユーザグループが原因で検出の問題が発生するのを避けるには、カスタマイズされたユーザオブジェクトを新しい Firepower Management Center に手動で追加し、インポート後にアクセスコントロールポリシーを再設定します。

オブジェクトおよびオブジェクト グループをインポートする場合：

- インポートプロセスは、オブジェクトとグループを新規としてインポートします。既存のオブジェクトおよびグループを置き換えることはできません。
- インポートしたオブジェクトの名前がインポートする Firepower Management Center 上の既存のオブジェクトと一致する場合、システムはそれらの名前を一意にするため、インポートされたオブジェクトとグループの名前に自動生成した番号を付加します。
- インポートした設定で使用されているセキュリティゾーンとインターフェイスグループを、インポート側の Firepower Management Center で管理されているタイプが一致するゾーンとグループにマッピングする必要があります。
- 秘密キーを含むPKIオブジェクトを使用する構成をエクスポートすると、エクスポートの前に秘密キーが復号されます。インポート時に、キーはランダムに生成されたキーで暗号化されます。


## 設定のエクスポート

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

エクスポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、エクスポートプロセスに数分かかる場合があります。



### ヒント

Firepower システムの多くのリストページには、リスト項目の横にエクスポートアイコン  があります。このアイコンがある場合は、それを使用することにより、その後のエクスポート操作を簡単に代行させることができます。

### 始める前に

- インポートおよびエクスポートするアプライアンスが同じバージョンの Firepower システムを実行していることを確認します。アクセス制御とそのサブポリシー（侵入ポリシーを含む）の場合は、侵入ルールの更新バージョンも一致する必要があります。

### 手順

**ステップ 1** [システム (System)] > [ツール (Tools)] > [インポート/エクスポート (Import/Export)] を選択します。

折りたたむ  アイコンか、展開する  アイコンをクリックし、使用可能な設定のリストを折りたたんだり、展開したりします。

**ステップ 2** エクスポートする構成をチェックして [エクスポート (Export)] をクリックします。

**ステップ 3** Web ブラウザのプロンプトに従って、エクスポートされたパッケージをコンピュータに保存します。

## 設定のインポート

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

インポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、インポートプロセスに数分かかる場合があります。

### 始める前に

- インポートおよびエクスポートするアプライアンスが同じバージョンの Firepower システムを実行していることを確認します。アクセス制御とそのサブポリシー（侵入ポリシーを含む）の場合は、侵入ルールの更新バージョンも一致する必要があります。

### 手順

- 
- ステップ 1** インポートするアプライアンスで、[システム (System)] > [ツール (Tools)] > [インポート/エクスポート (Import/Export)] を選択します。
- ステップ 2** [パッケージのアップロード (Upload Package)] をクリックします。
- ステップ 3** エクスポートしたパッケージへのパスを入力するか、そのパッケージの場所を参照して [アップロード (Upload)] をクリックします。
- ステップ 4** バージョンが一致していないなどの問題がない場合は、インポートする設定を選択して、[インポート (Import)] をクリックします。  
競合の解決やインターフェイスオブジェクトのマッピングを実行する必要がない場合は、インポートが完了して、成功メッセージが表示されます。この手順の残りは省略してください。
- ステップ 5** プロンプトが表示されたら、[アクセス制御インポートの解決 (AccessControl Import Resolution)] [インポートの競合解決 (Import Conflict Resolution)] ページで、インポートする Firepower Management Center で管理されているインターフェイスタイプと一致するゾーンおよびグループに、インポートした設定で使用されているインターフェイスオブジェクトをマップします。  
  
インターフェイスオブジェクトタイプ（セキュリティゾーンまたはインターフェイスグループ）およびインターフェイスタイプ（パッシブ、インライン、ルーテッドなど）が送信元と宛先で一致している必要があります。詳細については、[インターフェイスオブジェクト：インターフェイスグループとセキュリティゾーン（437 ページ）](#) を参照してください。  
  
インポートする設定が存在しないセキュリティゾーンまたはインターフェイスグループを参照する場合は、その設定を既存のインターフェイスオブジェクトにマップするか、新しいインターフェイスオブジェクトを作成します。
- ステップ 6** [インポート (Import)] をクリックします。
- ステップ 7** プロンプトが表示されたら、[インポートの解決 (Import Resolution)] ページで、各設定を展開して適切なオプションを選択します。詳細については、[インポート競合の解決（216 ページ）](#) を参照してください。
- ステップ 8** [インポート (Import)] をクリックします。
-

## 次のタスク

- 必要に応じて、インポートした設定の概要を示すレポートを表示します。[タスクメッセージの表示 \(330 ページ\)](#) を参照してください。

## インポート競合の解決

構成をインポートしようすると、同じ名前とタイプの構成がアプライアンスにすでに存在するかどうかシステムによって確認されます。マルチドメイン展開では、構成が現在のドメイン、またはその先祖あるいは子孫ドメインのいずれかで定義されている構成の複製であるかどうか確認されます。（子孫ドメインの構成は表示できませんが、重複する名前の構成が子孫ドメインに存在する場合は、システムにより競合が通知されます）。インポートに重複構成が含まれている場合、次の中から展開に適切な解決オプションが表示されます。

- **既存のものを維持する (Keep existing)**

その構成はインポートされません。

- **既存のものを置換する (Replace existing)**

インポート用に選択した構成で現在の構成が上書きされます。

- **最新バージョンを残す (Keep newest)**

選択した構成は、タイムスタンプがアプライアンスの現在の構成のタイムスタンプより新しい場合にのみインポートされます。

- **新たにインポート (Import as new)**

選択した重複する構成はインポートされ、システム生成の番号が適用されて一意の構成になります。（インポートプロセスが完了する前にこの名前を変更できます）。アプライアンスの元の構成は変更されません。

表示される解決オプションは、展開でドメインを使用するかどうか、およびインポートされた構成が現在のドメインで定義されている構成の複製であるか、または現在のドメインの先祖あるいは子孫で定義された構成であるかどうかによって異なります。次の表に、どの場合に解決オプションが表示されるか表示されないかを示します。

解決オプション	Firepower Management Center		管理対象デバイス
	現在のドメインの複製	子孫または先祖ドメインの複製	
既存のものを維持する (Keep existing)	○	○	○
既存のものを置換する (Replace existing)	[はい (Yes) ]	[いいえ (No) ]	○

解決オプション	Firepower Management Center		管理対象デバイス
	現在のドメインの複製	子孫または先祖ドメインの複製	
最新バージョンを残す (Keep newest)	[はい (Yes) ]	[いいえ (No) ]	○
新たにインポート (Import as new)	○	○	○

クリーンまたはカスタム定義ファイルリストを使用するファイルポリシーとともにアクセスコントロールポリシーをインポートし、ファイルリストに重複する名前競合が示されている場合、上記の表に示すように競合解決オプションが表示されますが、ポリシーおよびファイルリストに対して実行されるアクションは、次に表に示すように異なります。

解決オプション	システムアクション	
	アクセスコントロールポリシーと関連ファイルポリシーが新たにインポートされ、ファイルリストは統合される	既存のアクセスコントロールポリシーと関連ファイルポリシーおよびファイルリストは変更されない
既存のものを維持する (Keep existing)	なし	○
既存のものを置換する (Replace existing)	[はい (Yes) ]	[いいえ (No) ]
新たにインポート (Import as new)	[はい (Yes) ]	[いいえ (No) ]
最新バージョンを残す (Keep newest)。インポートされるアクセスコントロールポリシーが最新	[はい (Yes) ]	[いいえ (No) ]
最新バージョンを残す (Keep newest)。既存のアクセスコントロールポリシーが最新	なし	○

アプライアンスにインポートされた構成を修正し、後で同じアプライアンスにその構成を再インポートする場合は、保持する構成のバージョンを選択する必要があります。







## 第 9 章

# タスクのスケジューリング

ここでは、タスクをスケジューリングする方法について説明します。

- [タスクのスケジューリングの概要 \(219 ページ\)](#)
- [定期タスクの設定 \(219 ページ\)](#)
- [スケジューリング済みタスクの確認 \(239 ページ\)](#)

## タスクのスケジューリングの概要

さまざまな種類の管理タスクを、指定した回数（1 度または繰り返し）実行するようにスケジューリングを設定できます。



- (注) タスクによっては低帯域幅のネットワークに非常に負荷をかけることがあります（ソフトウェアの自動更新が含まれるタスクや、管理対象デバイスに更新をプッシュする必要があるタスクなど）。ネットワーク使用率が低い時間帯にこのようなタスクを実行するよう、スケジューリングしてください。

## 定期タスクの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	タスクに応じて異なる	タスクに応じて異なる	Admin/Maint

定期タスクの頻度を設定する際には、すべてのタイプのタスクで同じ手順に従います。

Web インターフェイスのほとんどのページに表示される時間はローカル時刻であり、ローカル設定で指定したタイムゾーンに従ってそれが決定されます。さらに、Firepower Management Center は、該当する場合にはローカル時刻の表示を夏時間 (DST) に合わせて自動的に調整します。ただし、DST から標準時への移行日および元に戻る移行日をまたがる定期タスクは、移

行を考慮して調整されません。つまり、標準時の午前 2:00 にタスク スケジュールを作成すると、DST 期間中は午前 3:00 に実行されます。同様に、DST の午前 2:00 にタスク スケジュールを作成すると、標準時には午前 1:00 に実行されます。

## 手順

- ステップ 1 [システム (System)] > [ツール (Tools)] > [スケジューリング (Scheduling)] を選択します。
- ステップ 2 [タスクの追加 (Add Task)] をクリックします。
- ステップ 3 [ジョブタイプ (Job Type)] ドロップダウンリストから、スケジュールするタスクのタイプを選択します。
- ステップ 4 [実行するタスクのスケジュール (Schedule task to run)] オプションの横にある [定期 (Recurring)] オプション ボタンをクリックします。
- ステップ 5 [開始日付 (Start On)] フィールドに、定期タスクを開始する日付を指定します。
- ステップ 6 [繰り返し設定 (Repeat Every)] フィールドに、タスクを繰り返す頻度を指定します。  
数値を入力するか、上矢印 (▲) および下矢印 (▼) アイコンをクリックして、間隔を指定できます。たとえば、2 日おきにタスクを実行するには、2 を入力して [日 (Days)] オプション ボタンをクリックします。
- ステップ 7 [実行時刻 (Run At)] フィールドで、定期タスクを開始する時刻を指定します。
- ステップ 8 週または月単位で実行するタスクの場合は、[繰り返す (オン) (Repeat On)] フィールドでタスクを実行する日付を選択します。
- ステップ 9 作成するタスクのタイプについて残りのオプションを選択します。
  - [バックアップ (Backup)] : [Firepower Management Center のバックアップの自動化 \(221 ページ\)](#) の説明に従って、バックアップ ジョブをスケジュールします。
  - [CRL のダウンロード (Download CRL)] : [証明書失効リストのダウンロードの設定 \(223 ページ\)](#) の説明に従って、証明書失効リストのダウンロードをスケジュールします。
  - [ポリシーの展開 (Deploy Policies)] : [ポリシー展開の自動化 \(224 ページ\)](#) の説明に従って、ポリシーの展開をスケジュールします。
  - [Nmap スキャン (Nmap Scan)] : [Nmap スキャンのスケジュール \(226 ページ\)](#) の説明に従って、Nmap スキャンをスケジュールします。
  - [レポート (Report)] : 次の説明に従って、レポート生成をスケジュールします。 [レポートの生成の自動化 \(227 ページ\)](#)
  - [Firepower 推奨ルール (Firepower Recommended Rules)] : 次の説明に従って、Firepower 推奨ルールの自動更新をスケジュールします。 [Firepower の推奨ルールの自動化 \(229 ページ\)](#)
  - [最新の更新のダウンロード (Download Latest Update)] : [ソフトウェアダウンロードの自動化 \(232 ページ\)](#) または [VDB 更新のダウンロードの自動化 \(236 ページ\)](#) の説明に従って、ソフトウェアまたは VDB の更新のダウンロードをスケジュールします。

- [最新の更新のインストール (Install Latest Update) ] : [ソフトウェアインストールの自動化 \(234 ページ\)](#) または次の説明に従って、Firepower Management Center または管理対象デバイスでのソフトウェアまたは VDB の更新のインストールをスケジュールします。 [VDB 更新のインストールの自動化 \(237 ページ\)](#)
- [最新の更新のプッシュ (Push Latest Update) ] : [ソフトウェアプッシュの自動化 \(233 ページ\)](#) の説明に従って、管理対象デバイスへのソフトウェア更新のプッシュをスケジュールします。
- [URL フィルタリングデータベースの更新 (Update URL Filtering Database) ] : 次の説明に従って、URL フィルタリングデータの自動更新をスケジュールします。 [URL フィルタリング更新の自動化 \(238 ページ\)](#)

## バックアップタスクの自動化

スケジューラを使用して、Firepower Management Center や物理管理対象デバイスのバックアップを自動化することができます。

物理管理対象デバイスの設定データのスケジュールバックアップを実行するには、デバイス自体の Web インターフェイスを使用します。

Firepower Management Center で設定データとイベントデータまたは設定データのみのスケジュールバックアップを実行するには、Firepower Management Center Web インターフェイスを使用します。タスクのスケジュール時に選択するバックアッププロファイルによってデータのバックアップのタイプが決まります。

管理対象デバイスのバックアップを管理元の Firepower Management Center からスケジュールすることはできませんが、管理対象デバイスの一部のモデルについてはオンデマンドバックアップを Firepower Management Center から実行することができます。

### 関連トピック

[バックアップと復元の概要 \(197 ページ\)](#)

## Firepower Management Center のバックアップの自動化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin/Maint

### 始める前に

- バックアッププロファイルを作成します。 [バックアッププロファイルの作成 \(204 ページ\)](#) を参照してください。

## 手順

- ステップ 1** [システム (System)] > [ツール (Tools)] > [スケジューリング (Scheduling)] を選択します。
- ステップ 2** [タスクの追加 (Add Task)] をクリックします。
- ステップ 3** [ジョブタイプ (Job Type)] リストから、[バックアップ (Backup)] を選択します。
- ステップ 4** バックアップをスケジュールする頻度として、ワンタイム タスクを示す [1 回 (Once)] または定期タスクを示す [定期 (Recurring)] を指定します。
- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
  - 定期タスクの詳細については、[定期タスクの設定 \(219 ページ\)](#) を参照してください。
- ステップ 5** [ジョブ名 (Job Name)] フィールドに名前を入力します。
- ステップ 6** [バックアッププロファイル (Backup Profile)] リストから、適切なバックアッププロファイルを選択します。
- ステップ 7** 必要に応じて、[コメント (Comment)] を追加します。
- [コメント (Comment)] フィールドはスケジュール予定表ページの [タスクの詳細 (Task Details)] セクションに表示されます。コメントは手短にします。
- ステップ 8** タスクのステータス メッセージをメールで送信するには、[ステータスの送信先 (Email Status To:)] フィールドにメールアドレス (またはコンマで区切った複数のメールアドレス) を入力します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。
- ステップ 9** [保存 (Save)] をクリックします。

## 関連トピック

[メールリレーホストおよび通知アドレスの設定 \(971 ページ\)](#)

## 管理対象デバイスのバックアップの自動化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	該当なし	Admin/Maint

7000 または 8000 シリーズ デバイスのローカル Web インターフェイスを使用して、次の手順を実行する必要があります。

## 始める前に

バックアッププロファイルを作成します。参照先 [バックアッププロファイルの作成 \(204 ページ\)](#)

## 手順

- ステップ 1** [システム (System)] > [ツール (Tools)] > [スケジューリング (Scheduling)] を選択します。
- ステップ 2** [タスクの追加 (Add Task)] をクリックします。
- ステップ 3** [ジョブ タイプ (Job Type)] リストから、[バックアップ (Backup)] を選択します。
- ステップ 4** バックアップをスケジュールする頻度として、ワンタイム タスクを示す [1 回 (Once)] または定期タスクを示す [定期 (Recurring)] を指定します。
- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
  - 定期タスクの詳細については、[定期タスクの設定 \(219 ページ\)](#) を参照してください。
- ステップ 5** [ジョブ名 (Job Name)] フィールドに名前を入力します。
- ステップ 6** [バックアップ プロファイル (Backup Profile)] リストから、適切なバックアップ プロファイルを選択します。
- ステップ 7** 必要に応じて、[コメント (Comment)] を追加します。
- [コメント (Comment)] フィールドはスケジュール予定表ページの [タスクの詳細 (Task Details)] セクションに表示されます。コメントは手短にします。
- ステップ 8** タスクのステータス メッセージをメールで送信するには、[ステータスの送信先 (Email Status To:)] フィールドにメールアドレス (またはコンマで区切った複数のメールアドレス) を入力します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。
- ステップ 9** [保存 (Save)] をクリックします。

## 関連トピック

[メール リレー ホストおよび通知アドレスの設定 \(971 ページ\)](#)

## 証明書失効リストのダウンロードの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	デバイスに応じて異なる	Admin/Maint

Firepower Management Center または 7000 または 8000 シリーズ デバイスのローカル Web インターフェイスを使用して、この手順を実行する必要があります。マルチドメイン展開では、このタスクは Firepower Management Center のグローバル ドメインでのみサポートされます。

アプライアンスのユーザ証明書または監査ログ証明書を有効にするアプライアンスのローカル設定で証明書失効リスト (CRL) のダウンロードを有効にすると、CRL のダウンロードタスクが自動的に作成されます。スケジューラを使用してタスクを編集し、更新の頻度を設定できます。

### 始める前に

- ユーザ証明書または監査ログ証明書を有効にして設定し、1つ以上のCRLのダウンロードURLを設定します。詳細については、[有効なHTTPSクライアント証明書の強制 \(926ページ\)](#) と [有効な監査ログサーバの証明書の強制 \(967ページ\)](#) を参照してください。

### 手順

- 
- ステップ 1** [システム (System)] > [ツール (Tools)] > [スケジューリング (Scheduling)] を選択します。
- ステップ 2** [タスクの追加 (Add Task)] をクリックします。
- ステップ 3** [ジョブタイプ (Job Type)] リストから、[CRLのダウンロード (Download CRL)] を選択します。
- ステップ 4** CRLダウンロードをスケジュールする頻度として、ワンタイムタスクを示す [1回 (Once)] または定期タスクを示す [定期 (Recurring)] を指定します。
- ワンタイムタスクの場合、ドロップダウンリストを使用して開始日時を指定します。
  - 定期タスクの詳細については、[定期タスクの設定 \(219ページ\)](#) を参照してください。
- ステップ 5** [ジョブ名 (Job Name)] フィールドに名前を入力します。
- ステップ 6** タスクについてコメントするには、[コメント (Comment)] フィールドにコメントを入力します。
- [コメント (Comment)] フィールドはスケジュール予定表ページの [タスクの詳細 (Task Details)] セクションに表示されます。コメントは手短にします。
- ステップ 7** タスクのステータスメッセージを電子メールで送信する場合は、[ステータスの宛先電子メール: (Email Status To:)] フィールドに電子メールアドレス (またはカンマで区切った複数の電子メールアドレス) を入力します。ステータスメッセージを送信するには、Firepower Management Centerで有効な電子メール中継サーバが設定されている必要があります。
- ステップ 8** [保存 (Save)] をクリックします。

### 関連トピック

[メールリレーホストおよび通知アドレスの設定 \(971ページ\)](#)

## ポリシー展開の自動化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint

Management Center の設定を変更した後は、影響を受けるデバイスへ変更を展開する必要があります。

マルチドメイン展開では、現在のドメインに限ってポリシーの展開をスケジュールできます。

## 手順

**ステップ 1** [システム (System) ]>[ツール (Tools) ]>[スケジューリング (Scheduling) ] を選択します。

**ステップ 2** [タスクの追加 (Add Task) ] をクリックします。

**ステップ 3** [ジョブタイプ (Job Type) ] リストから、[ポリシーの展開 (Deploy Policies) ] を選択します。

**ステップ 4** タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回 (Once) ] または定期タスクを示す [定期 (Recurring) ] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、[定期タスクの設定 \(219 ページ\)](#) を参照してください。

**ステップ 5** [ジョブ名 (Job Name) ] フィールドに名前を入力します。

**ステップ 6** [デバイス (Device) ] フィールドで、ポリシーを展開するデバイスを選択します。

**ステップ 7** タスクについてコメントを付加するには、[コメント (Comment) ] フィールドにコメントを入力します。

[コメント (Comment) ] フィールドはスケジュール予定表ページの [タスクの詳細 (Task Details) ] セクションに表示されます。コメントは手短にします。

**ステップ 8** タスクのステータス メッセージをメールで送信するには、[ステータスの送信先 (Email Status To:) ] フィールドにメールアドレス (またはコンマで区切った複数のメールアドレス) を入力します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

**ステップ 9** [保存 (Save) ] をクリックします。

## 関連トピック

[メールリレー ホストおよび通知アドレスの設定 \(971 ページ\)](#)

[失効ポリシー \(363 ページ\)](#)

# Nmap スキャンの自動化

ネットワーク上のターゲットに対する定期的な Nmap スキャンをスケジュールできます。スキャンを自動化すると、Nmap スキャンによって以前に提供された情報を更新できます。Firepower システムは Nmap から提供されるデータを更新できないため、このデータを最新に保つには定期的に再スキャンする必要があります。また、ネットワーク上のホストに識別不能なアプリケーションやサーバがあるかどうか自動的に検査するよう、スキャンをスケジュールすることもできます。

さらに、Discovery Administrator が修正用に Nmap スキャンを使用する場合があることにも注意してください。たとえば、ホストでオペレーティング システム競合が発生したために、Nmap

スキャンがトリガーされることがあります。スキャンが実行されると、そのホストでのオペレーティングシステムの更新済み情報が取得され、こうして競合が解決されます。

以前にNmap スキャン機能を使用していない場合は、スケジュールスキャンを定義する前に、Nmap スキャンを設定します。

### 関連トピック

[Nmap スキャン](#) (2065 ページ)

## Nmap スキャンのスケジュール

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint

システムで検出されたホストのオペレーティングシステム、アプリケーション、またはサーバがNmap スキャンの結果で置き換えられると、システムは、Nmap によって置換されたホストに関する情報を更新しなくなります。Nmap によって提供されるサービスやオペレーティングシステムのデータは、もう1度Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、Nmap 提供のオペレーティングシステム、アプリケーション、またはサーバを最新の状態に保つために、定期的なスキャンスケジュールをセットアップしてください。ネットワークマップからホストが削除されて再び追加されると、Nmap スキャン結果はすべて破棄され、システムはホストに関するすべてのオペレーティングシステムとサービスのデータのモニタリングを再開します。

マルチドメイン展開では、次のようになります。

- スキャンのスケジュールは、現在のドメインに対してのみ可能です。
- 選択する修正およびNmap ターゲットは、現在のドメインまたは先祖ドメインに存在している必要があります。
- 非リーフドメインでのNmap スキャンの実行を選択すると、そのドメインの各子孫に含まれる同じターゲットをスキャンすることになります。

### 手順

- ステップ 1** [システム (System)] > [ツール (Tools)] > [スケジューリング (Scheduling)] を選択します。
- ステップ 2** [タスクの追加 (Add Task)] をクリックします。
- ステップ 3** [ジョブタイプ (Job Type)] リストから、[Nmap スキャン (Nmap Scan)] を選択します。
- ステップ 4** タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回 (Once)] または定期タスクを示す [定期 (Recurring)] を指定します。
  - ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
  - 定期タスクの詳細については、[定期タスクの設定 \(219 ページ\)](#) を参照してください。



- ステップ 5** [ジョブ名 (Job Name) ] フィールドに名前を入力します。
- ステップ 6** [Nmap 修復 (Nmap Remediation) ] フィールドで、Nmap 修復を選択します。
- ステップ 7** [Nmap ターゲット (Nmap Target) ] フィールドで、スキャン ターゲットを選択します。
- ステップ 8** [ドメイン (Domain) ] フィールドで、増補するネットワーク マップを持つドメインを選択します。
- ステップ 9** タスクにコメントを付ける場合は、[コメント (Comment) ] フィールドにコメントを入力します。
- ヒント** [コメント (Comment) ] フィールドはスケジュール予定表ページの [タスクの詳細 (Task Details) ] セクションに表示されます。コメントは手短かにします。
- ステップ 10** タスクのステータス メッセージをメールで送信するには、[ステータスの送信先 (Email Status To:) ] フィールドにメールアドレス (またはコンマで区切った複数のメールアドレス) を入力します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。
- ステップ 11** [保存 (Save) ] をクリックします。

#### 関連トピック

[メール リレー ホストおよび通知アドレスの設定 \(971 ページ\)](#)

## レポートの生成の自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint

一定期間ごとにレポートを実行するよう自動化できます。

マルチドメイン展開では、現在のドメインに限ってレポートをスケジュールできます。

#### 始める前に

- リスク レポート以外のレポートの場合：レポート テンプレートを作成します。詳細については、[レポート テンプレート \(2307 ページ\)](#) を参照してください。
- スケジューラを使用してメール レポートを配布するには、メール リレーのホストを設定し、レポートの受信者およびメッセージ情報を指定します。[メール リレー ホストおよび通知アドレスの設定 \(971 ページ\)](#) と、(リスク レポート以外のレポートの場合) [レポートの生成時の電子メール配布 \(2335 ページ\)](#) または (リスク レポートの場合) [リスク レポートの生成、表示および印刷 \(2306 ページ\)](#) を参照してください。
- (オプション) スケジュール設定されたレポートのファイル名、出力フォーマット、時間枠、またはメール配布の設定を設定または変更します。[スケジュールされたレポート生成設定の指定 \(228 ページ\)](#) を参照してください。

## 手順

- 
- ステップ 1** [システム (System) ]>[ツール (Tools) ]>[スケジューリング (Scheduling) ]を選択します。
- ステップ 2** [タスクの追加 (Add Task) ]をクリックします。
- ステップ 3** [ジョブタイプ (Job Type) ]リストから、[レポート (Report) ]を選択します。
- ステップ 4** タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回 (Once) ]または定期タスクを示す [定期 (Recurring) ]を指定します。
- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
  - 定期タスクの詳細については、[定期タスクの設定 \(219 ページ\)](#) を参照してください。
- ステップ 5** [ジョブ名 (Job Name) ]フィールドに名前を入力します。
- ステップ 6** [レポートテンプレート (Report Template) ]フィールドで、リスクレポート、またはレポートテンプレートを選択します。
- ステップ 7** タスクについてコメントを付加するには、[コメント (Comment) ]フィールドにコメントを入力します。
- [コメント (Comment) ]フィールドはスケジュール予定表ページの[タスクの詳細 (Task Details) ]セクションに表示されます。コメントは手短にします。
- ステップ 8** タスクのステータス メッセージをメールで送信するには、[ステータスの送信先 (Email Status To:)]フィールドにメールアドレス (またはコンマで区切った複数のメールアドレス) を入力します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。
- (注) このオプションを設定しても、レポートは配布されません。
- ステップ 9** レポートのデータがない場合 (たとえばレポート期間中に特定のタイプのイベントが発生しなかった場合) にレポート電子メール添付ファイルを受信しないようにするには、[空のレポートも添付 (If report is empty, still attach to email) ]チェックボックスを選択します。
- ステップ 10** [保存 (Save) ]をクリックします。
- 

## スケジュールされたレポート生成設定の指定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

スケジュールされたレポートのファイル名、出力形式、時間枠、電子メール配布の設定を指定または変更するには、次の手順に従います。

## 手順

**ステップ 1** [概要 (Overview)] > [レポート (Reporting)] > [レポート テンプレート (Report Templates)] の順に選択します。

**ステップ 2** 変更するレポート テンプレートの [編集 (Edit)] をクリックします。

**ステップ 3** [生成 (Generate)] をクリックします。

(注) 今すぐレポートを生成せずにレポート生成の設定を変更する場合は、テンプレート設定ページで [生成 (Generate)] をクリックする必要があります。レポートを生成しない限り、テンプレート リスト ビューで [生成 (Generate)] をクリックしても変更は保存されません。

**ステップ 4** 設定を変更します。

**ステップ 5** レポートを生成せずに新しい設定を保存するには、[キャンセル (Cancel)] をクリックします。

新しい設定を保存してレポートを生成するには、[生成 (Generate)] をクリックし、この手順の残りのステップをスキップします。

**ステップ 6** [保存 (Save)] をクリックします。

**ステップ 7** 保存を求めるプロンプトが出されたら、まだ変更していない場合でも [OK] をクリックします。

## Firepower の推奨ルールの自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Maint

カスタム侵入ポリシーで保存済みの最新の設定を使用し、ネットワークのディスカバリ データに基づいてルール状態の推奨を自動的に生成することができます。



(注) 変更が未保存のまま、侵入ポリシーに関するスケジュール済み推奨がシステムによって自動生成される場合、自動生成された推奨をポリシーに反映させるには、そのポリシー内の変更を破棄してポリシーをコミットする必要があります。

タスクを実行すると、推奨ルール状態が自動的に生成され、ポリシーの設定に基づいて侵入ルールの状態が変更されます。変更されたルール状態は、侵入ポリシーを次回に展開するとき有効になります。

マルチドメイン展開では、現在のドメインレベルの侵入ポリシーに関する推奨を自動化できません。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、先祖ドメインの侵入ポリシーでこの機能を有効にすると、システムはすべての

子孫のリーフ ドメインからのデータを使用して、推奨事項を生成します。これにより、侵入ルールをすべてのリーフ ドメインに存在しない可能性があるアセットに調整することができ、パフォーマンスに影響を与えることができます。

### 始める前に

- 以下で説明されている、侵入ポリシーでの Firepower 推奨ルールを設定します。 [Firepower の推奨事項の生成と適用 \(1658 ページ\)](#)
- タスクのステータス メッセージをメールで送るには、有効なメール リレー サーバを設定します。

### 手順

- 
- ステップ 1** [システム (System)] > [ツール (Tools)] > [スケジューリング (Scheduling)] を選択します。
  - ステップ 2** [タスクの追加 (Add Task)] をクリックします。
  - ステップ 3** [ジョブ タイプ (Job Type)] リストから、[Firepower 推奨ルール (Firepower Recommended Rules)] を選択します。
  - ステップ 4** タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回 (Once)] または定期タスクを示す [定期 (Recurring)] を指定します。
    - ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
    - 定期タスクの詳細については、[定期タスクの設定 \(219 ページ\)](#) を参照してください。
  - ステップ 5** [ジョブ名 (Job Name)] フィールドに名前を入力します。
  - ステップ 6** [ポリシー (Policies)] の横で、推奨を生成する 1 つ以上の侵入ポリシーを選択します。[すべてのポリシー (All Policies)] チェックボックスをオンにして、すべての侵入ポリシーを選択します。
  - ステップ 7** (任意) [コメント (Comments)] フィールドにコメントを入力します。

コメントは手短かにします。コメントはスケジュール予定表ページの [タスクの詳細 (Task Details)] セクションに表示されます。
  - ステップ 8** (任意) タスクのステータスメッセージをメールで送信するには、[ステータスの送信先 (Email Status To:)] フィールドにメールアドレス (またはコンマで区切った複数のメールアドレス) を入力します。
  - ステップ 9** [保存 (Save)] をクリックします。

### 関連トピック

- [競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)
- [Firepower 推奨ルールについて \(1655 ページ\)](#)
- [メール リレー ホストおよび通知アドレスの設定 \(971 ページ\)](#)

## ソフトウェア更新の自動化

ほとんどのパッチや機能リリースは、自動的にダウンロードして Firepower システムに適用することができます。

ソフトウェア更新をインストールするためにどんなタスクをスケジュールする必要があるかは、Management Center を更新する場合と、Management Center を使用して管理対象デバイスを更新する場合とで異なります。



(注) シスコでは、Management Center を使用して管理対象デバイスを更新することを強くお勧めしています。

- Management Center を更新するには、Install Latest Update タスクを使用してソフトウェアインストールをスケジュールします。
- Management Center を使用して管理対象デバイスのソフトウェア更新を自動化するには、次の 2 つのタスクをスケジュールする必要があります。
  - Push Latest Update タスクを使用して、管理対象デバイスに更新をプッシュ（コピー）します。
  - Install Latest Update タスクを使用して、管理対象デバイスに更新をインストールします。

管理対象デバイスに更新をスケジュールする場合、push and install タスクが連続して発生するようにスケジュールします。更新をインストールする前に、最初にデバイスに更新をプッシュする必要があります。デバイス グループでのソフトウェア更新を自動化するには、グループ内のすべてのデバイスを選択する必要があります。タスク間に、プロセスが完了するのに十分な時間があるようにします。タスクとタスクの間に 30 分以上の間隔をあけてスケジュールしてください。更新をインストールするようにタスクをスケジュールしても、Management Center からデバイスへの更新のコピーが終了していないと、インストールタスクは正しく実行されません。ただし、スケジュール済みインストールタスクが毎日繰り返される場合は、翌日の実行時に、すでにプッシュされた更新がインストールされます。



(注) 手動で更新をアップロードしてインストールする必要がある状況が 2 つあります。まず、Firepower システムへのメジャーアップデート（主要な更新）をスケジュールすることはできません。次に、サポートサイトにアクセスできない Management Center の更新や、そのアプライアンスからのプッシュをスケジュールすることはできません。Management Center がインターネットに直接接続しない場合、管理インターフェイスの設定を使用して、サポートサイトから更新をダウンロードできるようプロキシをセットアップする必要があります。

デバイス グループに更新プログラムをインストールするようにスケジュールされたタスクによって、デバイス グループ内の各デバイスにプッシュされた更新プログラムが同時にインス

トールされることに注意してください。デバイスグループ内の各デバイスについてスケジュールされたタスクが完了するだけの十分な時間を確保してください。

このプロセスをより確実に制御するには、更新がリリースされたことがわかった後、[1 回 (Once)] オプションを使用してオフピーク時間帯に更新をダウンロードしインストールできます。

#### 関連トピック

[管理インターフェイス](#) (931 ページ)

[システム ソフトウェア アップデートの概要](#) (161 ページ)

## ソフトウェア ダウンロードの自動化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin/Maint

Cisco から最新のソフトウェア更新を自動的にダウンロードするスケジュール済みタスクを作成することができます。このタスクを使用すると、手動でインストールする予定の更新のダウンロードをスケジュールできます。

#### 手順

- ステップ 1** [システム (System)] > [ツール (Tools)] > [スケジューリング (Scheduling)] を選択します。
- ステップ 2** [タスクの追加 (Add Task)] をクリックします。
- ステップ 3** [ジョブタイプ (Job Type)] リストから、[最新の更新のダウンロード (Download Latest Update)] を選択します。
- ステップ 4** タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回 (Once)] または定期タスクを示す [定期 (Recurring)] を指定します。
  - ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
  - 定期タスクの詳細については、[定期タスクの設定](#) (219 ページ) を参照してください。
- ステップ 5** [ジョブ名 (Job Name)] フィールドに名前を入力します。
- ステップ 6** [アップデート項目 (Update Items)] の横の [ソフトウェア (Software)] チェックボックスをオンにします。
- ステップ 7** タスクについてコメントを付加するには、[コメント (Comment)] フィールドにコメントを入力します。

[コメント (Comment)] フィールドはスケジュール予定表ページの [タスクの詳細 (Task Details)] セクションに表示されます。コメントは手短にします。
- ステップ 8** タスクのステータス メッセージをメールで送信するには、[ステータスの送信先 (Email Status To:)] フィールドにメールアドレス (またはコンマで区切った複数のメールアドレス) を入力

します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

**ステップ 9** [保存 (Save) ] をクリックします。

#### 関連トピック

[メールリレー ホストおよび通知アドレスの設定 \(971 ページ\)](#)

## ソフトウェア プッシュの自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin/Maint

管理対象デバイスでのソフトウェア更新のインストールを自動化するには、インストールの前に、更新をデバイスにプッシュする必要があります。

ソフトウェア更新を管理対象デバイスにプッシュするタスクを作成する際には、更新がデバイスに確実にコピーされるよう、プッシュ タスクとスケジュール済みインストール タスクの間に十分な時間を確保してください。

#### 手順

**ステップ 1** [システム (System) ] > [ツール (Tools) ] > [スケジューリング (Scheduling) ] を選択します。

**ステップ 2** [タスクの追加 (Add Task) ] をクリックします。

**ステップ 3** [ジョブタイプ (Job Type) ] リストから、[最新の更新をプッシュ (Push Latest Update) ] を選択します。

**ステップ 4** タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回 (Once) ] または定期タスクを示す [定期 (Recurring) ] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、[定期タスクの設定 \(219 ページ\)](#) を参照してください。

**ステップ 5** [ジョブ名 (Job Name) ] フィールドに名前を入力します。

**ステップ 6** [デバイス (Device) ] ドロップダウン リストから、更新するデバイスを選択します。

**ステップ 7** タスクについてコメントを付加するには、[コメント (Comment) ] フィールドにコメントを入力します。

[コメント (Comment) ] フィールドはスケジュール予定表ページの [タスクの詳細 (Task Details) ] セクションに表示されます。コメントは手短にします。

**ステップ 8** タスクのステータス メッセージをメールで送信するには、[ステータスの送信先 (Email Status To: ) ] フィールドにメールアドレス (またはコンマで区切った複数のメールアドレス) を入力

します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

**ステップ 9** [保存 (Save) ] をクリックします。

#### 関連トピック

[メールリレー ホストおよび通知アドレスの設定](#) (971 ページ)

## ソフトウェア インストールの自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin/Maint

管理対象デバイスへ更新をプッシュするタスクと、その更新をインストールするタスクの間に十分な時間を確保する必要があります。



**注意** インストールする更新によっては、ソフトウェアのインストール後にアプライアンスがリブートする場合があります。

#### 手順

- ステップ 1** [システム (System) ] > [ツール (Tools) ] > [スケジューリング (Scheduling) ] を選択します。
- ステップ 2** [タスクの追加 (Add Task) ] をクリックします。
- ステップ 3** [ジョブタイプ (Job Type) ] リストから、[最新の更新のインストール (Install Latest Update) ] を選択します。
- ステップ 4** タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回 (Once) ] または定期タスクを示す [定期 (Recurring) ] を指定します。
- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
  - 定期タスクの詳細については、[定期タスクの設定](#) (219 ページ) を参照してください。
- ステップ 5** [ジョブ名 (Job Name) ] フィールドに名前を入力します。
- ステップ 6** [デバイス (Device) ] ドロップダウンリストから、更新をインストールするアプライアンス (Firepower Management Centerを含む) を選択します。
- ステップ 7** [アップデート項目 (Update Items) ] の横の [ソフトウェア (Software) ] チェックボックスをオンにします。
- ステップ 8** タスクについてコメントを付加するには、[コメント (Comment) ] フィールドにコメントを入力します。

[コメント (Comment) ] フィールドはスケジュール予定表ページの [タスクの詳細 (Task Details) ] セクションに表示されます。コメントは手短にします。



- ステップ 9** タスクのステータス メッセージをメールで送信するには、[ステータスの送信先 (Email Status To:)] フィールドにメールアドレス (またはコンマで区切った複数のメールアドレス) を入力します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。
- ステップ 10** [保存 (Save)] をクリックします。

#### 関連トピック

[メール リレー ホストおよび通知アドレスの設定 \(971 ページ\)](#)

## 脆弱性データベースの更新の自動化

Cisco では脆弱性データベース (VDB) 更新を使用して、Firepower システムで認識されるネットワークアセット、トラフィック、および脆弱性のリストを拡張しています。スケジュール機能を使用して VDB を更新できるため、常に最新の情報を使ってネットワーク上のホストを評価することができます。

VDB 更新を自動化する場合、次に示す 2 つの別個の手順を自動化する必要があります。

- VDB 更新のダウンロード。
- VDB 更新のインストール。



**注意** 脆弱性データベース (VDB) アップデートをインストールした後、初めて VDB アップデートをインストールするか、またはアクセスコントロールポリシーを展開すると、すぐに Snort プロセスが再起動され、トラフィックインスペクションが一時的に中断されることがあります。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

プロセスを完了させるには、タスクとタスクの間に十分な時間を確保してください。たとえば、更新のインストールタスクをスケジュールした場合、更新がまだ完全にダウンロードされていないと、インストールタスクは正しく実行されません。ただし、スケジュール済みインストールタスクが毎日繰り返される場合は、翌日のタスク実行時に、ダウンロード済みの VDB 更新がインストールされます。

(注)

- サポートサイトにアクセスできないアプライアンスの更新をスケジュールすることはできません。Management Center がインターネットに直接接続されていない場合、管理インターフェイスの設定を使用して、プロキシが更新をサポートサイトからダウンロードできるようにプロキシをセットアップする必要があります。
- このプロセスをより確実に制御するには、更新がリリースされたことがわかった後、[1 回 (Once)] オプションを使用してオフピーク時間帯に VDB 更新をダウンロードしてインストールできます。

- マルチドメイン展開では、VDB 更新をスケジュールできるのはグローバルドメインについてのみです。変更は、ポリシーを再度展開したときに有効になります。

#### 関連トピック

[管理インターフェイス](#) (931 ページ)

## VDB 更新のダウンロードの自動化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin/Maint

#### 手順

- ステップ 1** [システム (System)] > [ツール (Tools)] > [スケジューリング (Scheduling)] を選択します。
- ステップ 2** [タスクの追加 (Add Task)] をクリックします。
- ステップ 3** [ジョブタイプ (Job Type)] リストから、[最新の更新のダウンロード (Download Latest Update)] を選択します。
- ステップ 4** タスクをスケジュールする頻度として、ワンタイムタスクを示す [1 回 (Once)] または定期タスクを示す [定期 (Recurring)] を指定します。
  - ワンタイムタスクの場合、ドロップダウンリストを使用して開始日時を指定します。
  - 定期タスクの詳細については、[定期タスクの設定](#) (219 ページ) を参照してください。
- ステップ 5** [ジョブ名 (Job Name)] フィールドに名前を入力します。
- ステップ 6** [アップデート項目 (Update Items)] の横の [脆弱性データベース (Vulnerability Database)] チェックボックスをオンにします。
- ステップ 7** タスクについてコメントを付加するには、[コメント (Comment)] フィールドにコメントを入力します。  
[コメント (Comment)] フィールドはスケジュール予定表ページの [タスクの詳細 (Task Details)] セクションに表示されます。コメントは手短にします。
- ステップ 8** タスクのステータスメッセージをメールで送信するには、[ステータスの送信先 (Email Status To:)] フィールドにメールアドレス (またはコンマで区切った複数のメールアドレス) を入力します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。
- ステップ 9** [保存 (Save)] をクリックします。

#### 関連トピック

[メールリレーホストおよび通知アドレスの設定](#) (971 ページ)

## VDB 更新のインストールの自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin/Maint

VDB 更新をダウンロードするタスクと、その更新をインストールするタスクの間に十分な時間を確保してください。



### 注意

脆弱性データベース (VDB) 更新をインストールした時点、または VDB 更新をインストールした後に初めてアクセスコントロールポリシーを展開した時点で、すぐに Snort プロセスが再起動してトラフィックインスペクションが一時的に中断されることがあります。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### 手順

- ステップ 1 [システム (System) ] > [ツール (Tools) ] > [スケジューリング (Scheduling) ] を選択します。
- ステップ 2 [タスクの追加 (Add Task) ] をクリックします。
- ステップ 3 [ジョブタイプ (Job Type) ] リストから、[最新の更新のインストール (Install Latest Update) ] を選択します。
- ステップ 4 タスクをスケジュールする頻度として、ワンタイムタスクを示す [1 回 (Once) ] または定期タスクを示す [定期 (Recurring) ] を指定します。
  - ワンタイムタスクの場合、ドロップダウンリストを使用して開始日時を指定します。
  - 定期タスクの詳細については、[定期タスクの設定 \(219 ページ\)](#) を参照してください。
- ステップ 5 [ジョブ名 (Job Name) ] フィールドに名前を入力します。
- ステップ 6 [デバイス (Device) ] ドロップダウンリストから Management Center を選択します。
- ステップ 7 [アップデート項目 (Update Items) ] の横の [脆弱性データベース (Vulnerability Database) ] チェックボックスをオンにします。
- ステップ 8 タスクについてコメントを付加するには、[コメント (Comment) ] フィールドにコメントを入力します。
 

ヒント コメントフィールドはページの [タスクの表示 (View Tasks) ] セクションに表示されるので、ある程度短くしてください。
- ステップ 9 タスクのステータスメッセージをメールで送信するには、[ステータスの送信先 (Email Status To:) ] フィールドにメールアドレス (またはコンマで区切った複数のメールアドレス) を入力

します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

**ステップ 10** [保存 (Save) ] をクリックします。

#### 関連トピック

[メールリレー ホストおよび通知アドレスの設定](#) (971 ページ)

## URL フィルタリング更新の自動化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
URL フィルタリング (URL Filtering)	URL フィルタリング (URL Filtering)	任意 (Any)	グローバルだけ	Admin/Maint

スケジューラを使用して、Cisco Collective Security Intelligence (CSI) からの URL フィルタリングデータの更新を自動化できます。

また、URL フィルタリングを有効にする際に、自動更新を有効にできることに注意してください。その場合、URL フィルタリングデータの更新を確認するために Management Center は必ず 30 分ごとに CSI と通信します。



(注) URL フィルタリングを有効にしたときに自動更新を有効にした場合は、URL フィルタリングデータを更新するスケジュール済みタスクを作成しないでください。URL フィルタリングの更新を厳密に制御する場合のみタスクをスケジュールします。

通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL フィルタリングデータのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

#### 始める前に

- Firepower Management Center にインターネットアクセス権があることを確認してください ([セキュリティ、インターネットアクセス、および通信ポート \(2785 ページ\)](#) を参照)。
- URL フィルタリングをイネーブルにします。詳細については、[集合型セキュリティインテリジェンスとの通信の設定 \(1561 ページ\)](#) を参照してください。

#### 手順

**ステップ 1** [システム (System) ] > [ツール (Tools) ] > [スケジューリング (Scheduling) ] を選択します。

**ステップ 2** [タスクの追加 (Add Task) ] をクリックします。

- ステップ 3** [ジョブ タイプ (Job Type)] リストから、[URL フィルタリング データベースの更新 (Update URL Filtering Database)] を選択します。
- ステップ 4** 更新をスケジュールする頻度として、ワнтаイム更新を示す [1 回 (Once)] または定期更新を示す [定期 (Recurring)] を指定します。
- ワнтаイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
  - 定期タスクの詳細については、[定期タスクの設定 \(219 ページ\)](#) を参照してください。
- ステップ 5** [ジョブ名 (Job Name)] フィールドに名前を入力します。
- ステップ 6** タスクについてコメントを付加するには、[コメント (Comment)] フィールドにコメントを入力します。
- [コメント (Comment)] フィールドはスケジュール予定表ページの [タスクの詳細 (Task Details)] セクションに表示されます。コメントは手短にします。
- ステップ 7** タスクのステータス メッセージをメールで送信するには、[ステータスの送信先 (Email Status To:)] フィールドにメールアドレス (またはコンマで区切った複数のメールアドレス) を入力します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。
- ステップ 8** [保存 (Save)] をクリックします。

#### 関連トピック

[メール リレー ホストおよび通知アドレスの設定 \(971 ページ\)](#)

## スケジュール済みタスクの確認

スケジュール済みタスクを追加した後、それらのタスクを表示したり、状態を評価したりできます。ページの [表示オプション (View Options)] セクションで、カレンダーやスケジュール済みタスク リストを使用してスケジュール済みタスクを表示できます。

カレンダー表示オプションを使用すると、どの日にどのスケジュール済みタスクが行われるかを表示できます。

タスク リストには、タスクとその状態のリストが表示されます。タスク リストは、カレンダーを開いたときにカレンダーの下に表示されます。また、カレンダーで 1 つの日付またはタスクを選択して表示することもできます。

以前に作成したスケジュール済みタスクを編集できます。この機能は、パラメータが正しいことを確認するために、スケジュール済みタスクを 1 度テストする場合に特に役立ちます。タスクが正常に完了したら、後で定期タスクに変更できます。

[スケジュール表示 (Schedule View)] ページから 2 種類の削除操作を実行できます。まだ実行されていない特定のワнтаイムタスク、または定期タスクのすべてのインスタンスを削除できます。定期タスクの 1 つのインスタンスを削除すると、そのタスクのすべてのインスタンスが削除されます。1 度だけ実行するようスケジュールされているタスクを削除すると、そのタスクだけが削除されます。

## タスク一覧の詳細

表 23: タスク一覧のカラム

カラム (Column)	説明
[名前 (Name) ]	スケジュール済みタスクの名前と、関連付けられているコメントを表示します。
タイプ (Type)	スケジュール済みタスクのタイプを表示します。
開始時刻 (Start Time)	スケジュールされている開始日時を表示します。
頻度 (Frequency)	タスクの実行頻度を表示します。
前回の実行時間 (Last Run Time)	実際の開始日時を表示します。 定期タスクの場合、これは最新の実行に適用されます。
最終実行ステータス (Last Run Status)	スケジュール済みタスクの現在の状態を次のように示します。 <ul style="list-style-type: none"> <li>• チェックマークアイコン (✓) は、タスクが正常に実行されたことを示します。</li> <li>• 疑問符アイコン (?) は、タスクの状態が不明であることを示します。</li> <li>• 感嘆符アイコン (!) は、タスクが失敗したことを示します。</li> </ul> 定期タスクの場合、これは最新の実行に適用されます。
次の実行時間 (Next Run Time)	定期タスクの次の実行時間を表示します。 ワンタイムタスクの場合に「該当なし (N/A)」と表示します。
作成者 (Creator)	スケジュール済みタスクを作成したユーザーの名前を表示します。
編集 (Edit)	スケジュール済みタスクを編集します。
削除 (Delete)	スケジュール済みタスクを削除します。

## カレンダーのスケジュール済みタスクの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint

マルチドメイン展開では、現在のドメインのスケジュール済みタスクのみを表示できます。

### 手順

**ステップ 1** [システム (System)] > [ツール (Tools)] > [スケジューリング (Scheduling)] を選択します。

**ステップ 2** カレンダー ビューを使用して、次のタスクを実行できます。

- 二重左矢印アイコン (⏪) をクリックすると、1 年戻ります。
- 単一の左矢印アイコン (⏩) をクリックすると、1 ヶ月戻ります。
- 単一の右矢印アイコン (⏴) をクリックすると、1 ヶ月進みます。
- 二重右矢印アイコン (⏴) をクリックすると、1 年進みます。
- [今日 (Today)] をクリックすると、現在の年月に戻ります。
- [タスクの追加 (Add Task)] をクリックすると、新しいタスクをスケジュールできます。
- 1 つの日付をクリックすると、カレンダーの下にあるタスク リスト表に、特定の日付のスケジュール済みタスクがすべて表示されます。
- ある日付の特定のタスクをクリックすると、カレンダーの下にあるタスク リスト表にそのタスクが表示されます。

## スケジュール済みタスクの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint

マルチドメイン展開では、現在のドメインのスケジュール済みタスクのみを編集できます。

### 手順

**ステップ 1** [システム (System)] > [ツール (Tools)] > [スケジューリング (Scheduling)] を選択します。

**ステップ 2** カレンダーで、編集するタスク、またはタスクが表示されている日付をクリックします。

**ステップ 3** [タスクの詳細 (Task Details)] テーブルで、編集するタスクの横にある編集アイコン (✎) をクリックします。

**ステップ 4** タスクを編集します。

**ステップ 5** [保存 (Save)] をクリックします。

## スケジュール済みタスクの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint

マルチドメイン導入では、現在のドメインのスケジュール済みタスクのみを削除できます。

### 手順

**ステップ 1** [システム (System)] > [ツール (Tools)] > [スケジューリング (Scheduling)] を選択します。

**ステップ 2** カレンダーで、削除するタスクをクリックします。繰り返しタスクの場合は、タスクのインスタンスをクリックします。

**ステップ 3** [タスク詳細 (Task Details)] テーブルで、削除アイコン (🗑️) をクリックし、選択内容を確認します。





## 第 10 章

# Management Center データベースの消去

以下のトピックでは、Management Center から検出データを消去する方法を示します。

- [Management Center データベースからのデータの消去](#) (243 ページ)

## Management Center データベースからのデータの消去

スマートライセンス	従来のライセンス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	グローバルだけ	Admin/Security Analyst

データベース消去ページを使用すると、検出、アイデンティティ、接続、およびセキュリティインテリジェンスのデータ ファイルを Management Center データベースから消去できます。データベースを消去すると、該当するプロセスが再起動される点に注意してください。



**注意** データベースを消去すると、Firepower Management Center から指定したデータが削除されます。削除されたデータは復元できません。

### 手順

**ステップ 1** [システム (System)] > [ツール (Tools)] > [データの削除 (Data Purge)] を選択します。

**ステップ 2** [ネットワーク検出 (Network Discovery)] で、次のいずれかまたはすべてを実行します。

- [ネットワーク検出イベント (Network Discovery Events)] チェックボックスをオンにして、データベースからすべてのネットワーク検出イベントを削除します。
- [ホスト (Hosts)] チェックボックスをオンにして、データベースからすべてのホストと侵害の兆候フラグを削除します。
- [ユーザ アクティビティ (User Activity)] チェックボックスをオンにして、データベースからすべてのユーザ アクティビティ イベントを削除します。

- [ユーザアイデンティティ (User Identities) ] チェックボックスをオンにして、データベースからすべてのユーザ ログインとユーザ履歴データを削除します。

**ステップ 3** [接続 (Connections) ] で、次のいずれかまたはすべてを実行します。

- [接続イベント (Connection Events) ] チェックボックスをオンにして、データベースからすべての接続データを削除します。
- [接続の概要イベント (Connection Summary Events) ] チェックボックスをオンにして、データベースからすべての接続の概要データを削除します。
- [セキュリティ インテリジェンス イベント (Security Intelligence Events) ] チェックボックスをオンにして、データベースからすべてのセキュリティ インテリジェンス データを削除します。

(注) [接続イベント (Connection Events) ] チェックボックスをオンにしても、セキュリティ インテリジェンス イベントは削除されません。セキュリティ インテリジェンス データとの接続は、セキュリティ インテリジェンス イベント ビューアに引き続き表示されます。同様に、[セキュリティ インテリジェンス イベント (Security Intelligence Events) ] チェックボックスをオンにしても、セキュリティ インテリジェンス データに関連する接続イベントは削除されません。

**ステップ 4** [選択したイベントの消去 (Purge Selected Events) ] をクリックします。項目が消去され、該当するプロセスが再起動されます。

---



## 第 III 部

# システム モニタリングとトラブルシューティング

- [ダッシュボード \(247 ページ\)](#)
- [ヘルス モニタリング \(275 ページ\)](#)
- [システムのモニタリング \(309 ページ\)](#)
- [システムのトラブルシューティング \(323 ページ\)](#)





## 第 11 章

# ダッシュボード

次のトピックでは、Firepower システムでダッシュボードを使用する方法について説明します。

- [ダッシュボードについて \(247 ページ\)](#)
- [Firepower システムのダッシュボードウィジェット \(248 ページ\)](#)
- [ダッシュボードの管理 \(265 ページ\)](#)

## ダッシュボードについて

Firepower システム ダッシュボードは、システムによって収集および生成されたイベントに関するデータを含む、現在のシステムのステータスを概要的なビューとして提供します。またダッシュボードを使用して、展開のアプライアンスのステータスと全体の正常性に関する情報を表示することもできます。ダッシュボードが提供する情報はシステムのライセンス方法、設定方法、展開方法によって異なる点に注意してください。



**ヒント** ダッシュボードは網羅的なデータを提供する複雑で高度にカスタマイズ可能なモニタリング機能です。モニタ対象のネットワークについての広範、簡潔でカラフルな画像を得るには、Context Explorer を使ってください。ダッシュボードは、Firepower Management Center および 7000 & 8000 シリーズ デバイスで使用できます。

ダッシュボードはウィジェットの表示にタブを使用します。ウィジェットは小さな自己完結型のコンポーネントで、システムのさまざまな側面を理解するうえで役に立ちます。たとえば、定義済みの [アプライアンス情報 (Appliance Information)] ウィジェットは、アプライアンスの名前、モデル、および Firepower システム ソフトウェアの現在実行中のバージョンを通知します。システムはダッシュボードの時間範囲によってウィジェットを制約します。この時間範囲は、最短で 1 時間前から、最長では 1 年前からの期間を反映するように変更できます。

システムには、いくつかの事前定義されたダッシュボードウィジェットが付属していて、使用および変更できます。ユーザロールにダッシュボードへのアクセス権が付与されている (管理者、メンテナンス ユーザ、セキュリティ アナリスト (読み取り専用)、およびダッシュボードの権限付きのカスタム ロール) 場合、デフォルトでホームページは事前定義されたサマリダッシュボードになっています。ただし、ダッシュボード以外を含む別のデフォルト ホーム

ページを設定できます。デフォルトのダッシュボードを変更することもできます。ダッシュボードへのアクセス権がないユーザロールの場合、デフォルトのホームページはロールに関連するページです。たとえば、Discovery Admin ロールの場合はネットワーク検出ページが表示されます。

また、事前定義済みのダッシュボードをカスタムダッシュボードのベースとして使用することもできます。これは共有することもプライベートとして制限することもできます。管理者アクセス権がない場合、他のユーザが作成したプライベートダッシュボードは表示も変更もできません。



- (注) イベントのドリルダウンページとテーブルビューには、[ダッシュボード (Dashboard)] ツールバーのリンクが含まれているものがあります。このリンクをクリックして、関連する事前定義されたダッシュボードを表示することができます。事前定義されたダッシュボードまたはタブを削除すると、関連付けられているツールバーのリンクが機能しなくなります。

マルチドメイン展開では、先祖ドメインのダッシュボードを表示することはできません。ただし、高位レベルのダッシュボードをコピーした新規のダッシュボードを作成することはできます。

## Firepower システムのダッシュボードウィジェット

ダッシュボードには1つ以上のタブがあり、それぞれのタブには、3列のレイアウトで1つ以上のウィジェットを表示できます。Firepower システムには、事前定義された多数のダッシュボードウィジェットが付属しています。それぞれのウィジェットは、Firepower システムのさまざまな側面を理解するうえで役に立ちます。ウィジェットは、次の3つのカテゴリに分類されます。

- [分析およびレポート (Analysis & Reporting)] ウィジェットは、Firepower システムで収集および生成されたイベントに関するデータを表示します。
- [その他 (Miscellaneous)] ウィジェットは、イベントデータもオペレーションデータも表示しません。現時点では、このカテゴリのウィジェットのみが RSS フィードを表示します。
- [オペレーション (Operations)] ウィジェットは、Firepower システムのステータスおよび全体の正常性に関する情報を表示します。

表示されるダッシュボードウィジェットは、次の項目に応じて異なります。

- 使用しているアプライアンスのタイプ
- ユーザロール
- 現在のドメイン (マルチドメイン展開内)

また、各ダッシュボードには、動作を決定する一連のプリファレンスがあります。

ユーザは、ウィジェットを最小化および最大化する、タブに対してウィジェットを追加および削除する、タブ上でウィジェットを再配置する、といったことができます。



- (注) 所定の時間範囲でのイベントカウントを表示するウィジェットでは、イベントビューアで利用できる詳細なデータのイベント数が、イベントの総数に反映されないことがあります。これは、ディスク領域の使用率を管理するために、古いイベントの詳細がシステムによってプルーニングされることがあるために発生します。イベント詳細のプルーニングを最小限にするために、対象の展開にとって最も重要なイベントだけを記録するようにイベントロギングを調整できます。

## ウィジェットの使用可能性

表示できるダッシュボードウィジェットは、使用中のアプライアンスのタイプ、使用するユーザロール、および（マルチドメイン展開での）現在のドメインによって異なります。

マルチドメイン展開で、予期したウィジェットが表示されない場合、グローバルドメインに切り替えます。[Firepower Management Center のドメインの切り替え \(31 ページ\)](#) を参照してください。

次の点に注意してください。

- 無効なウィジェットとは、ユーザが誤ったタイプのアプライアンスを使用しているために表示できないウィジェットのことで、
- 不正なウィジェットとは、ユーザアカウントに必要な権限がないために表示できないウィジェットのことで、

たとえば、[アプライアンスの状態 (Appliance Status)] ウィジェットを使用できるのは、Management Center で、管理者 (Administrator)、メンテナンス ユーザ (Maintenance User)、セキュリティアナリスト (Security Analyst)、またはセキュリティアナリスト (読み取り専用) (Security Analyst (Read Only)) のアカウント権限を持つユーザだけです。

不正なウィジェットまたは無効なウィジェットはダッシュボードに追加できませんが、インポートしたダッシュボードに不正なウィジェットまたは無効なウィジェットが含まれていることがあります。たとえば、インポートしたダッシュボードが次の場合に、このようなウィジェットが含まれている可能性があります。

- 各種アクセス権限を持つユーザによって作成された場合、または
- 先祖ドメインに属している場合。

使用できないウィジェットは無効になり、それらのウィジェットを表示できない理由を示すエラーメッセージが表示されます。

これらのウィジェットがタイムアウトした場合、またはそれ以外で問題が発生した場合には、個々のウィジェットでもエラーメッセージが表示されます。



- (注) 不正なウィジェットと無効なウィジェット、および表示するデータがないウィジェットは、削除または最小化できます。共有されているダッシュボード上でウィジェットを変更すると、アプライアンスのすべてのユーザのウィジェットも変更されることに注意してください。

## ユーザ ロール別のダッシュボード ウィジェットの可用性

次の表に、各ウィジェットを表示するために必要なユーザ アカウントの権限を示します。Administrator、Maintenance User、Security Analyst、または Security Analyst（読み取り専用）のアクセス権を持つユーザ アカウントのみがダッシュボードを使用できます。

カスタム ロールを持つユーザは、自身のユーザ ロールの許可によって、ウィジェットのいずれかの組み合わせにアクセスできる場合もあれば、どのウィジェットにもアクセスできない場合もあります。

表 24: ユーザ ロールとダッシュボード ウィジェットの可用性

ウィジェット	管理者 (Administrator)	メンテナンス ユーザ	セキュリティ ア ナリスト	セキュリティ ア ナリスト (RO)
アプライアンス情 報 (Appliance Information)	Yes	Yes	Yes	Yes
アプライアンス ステータス (Appliance Status)	Yes	Yes	Yes	No
相関イベント (Correlation Events)	Yes	No	Yes	Yes
現在のインター フェイス ステ ータス (Current Interface Status)	Yes	Yes	Yes	Yes
現在のセッション (Current Sessions)	Yes	No	No	No
カスタム分析 (Custom Analysis)	Yes	No	Yes	Yes



ウィジェット	管理者 (Administrator)	メンテナンス ユーザ	セキュリティ ア ナリスト	セキュリティ ア ナリスト (RO)
ディスク使用量	Yes	Yes	Yes	Yes
インターフェイス トラフィック (Interface Traffic)	Yes	Yes	Yes	Yes
侵入イベント	Yes	No	Yes	Yes
ネットワーク コ ンプライアンス (Network Compliance)	Yes	No	Yes	Yes
製品ライセンスの 認証 (Product Licensing)	Yes	Yes	No	No
製品アップデート (Product Updates)	Yes	Yes	No	No
RSS フィード (RSS Feed)	Yes	Yes	Yes	Yes
システム ロード (System Load)	Yes	Yes	Yes	Yes
システム タイム (System Time)	Yes	Yes	Yes	Yes
ホワイトリスト イベント (White List Events)	Yes	No	Yes	Yes

## 定義済みダッシュボードウィジェット

Firepower システムには、いくつかの定義済みウィジェットが付属しています。これらのウィジェットをダッシュボード上で使用することで、現在のシステムステータスを一目で確認できます。ウィジェットのビューには、以下の情報が表示されます。

- システムが収集および生成したイベントに関するデータ
- 使用している導入のライセンスのステータスと全体的なヘルスに関する情報



(注) 表示できるダッシュボード ウィジェットは、使用しているアプライアンスのタイプとユーザーロール、およびマルチドメイン展開の場合は現在のドメインによって異なります。

## [アプライアンス情報 (Appliance Information) ] ウィジェット

[アプライアンス情報 (Appliance Information) ] ウィジェットは、アプライアンスのスナップショットを提供します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス (Status) ] タブにデフォルトで表示されます。このウィジェットは以下の情報を提供します。

- アプライアンスの名前、IPv4 アドレス、IPv6 アドレス、およびモデル
- ダッシュボードでアプライアンスにインストールされている、Firepower システム ソフトウェア、オペレーティング システム、Snort、ルール アップデート、ルール パック、モジュール パック、脆弱性データベース (VDB) 、および地理情報のアップデートのバージョン (仮想 Firepower Management Center は除く)
- 管理対象アプライアンスの場合は、管理アプライアンスとの通信リンクの名前とステータス

単純なビューまたは高度なビューを表示するようにウィジェットのプリファレンスを変更することで、ウィジェットで表示する情報量を調整できます。プリファレンスでは、ウィジェットをアップデートする頻度を調整することもできます。

## [アプライアンス ステータス (Appliance Status) ] ウィジェット

[アプライアンス ステータス (Appliance Status) ] ウィジェットは、アプライアンスの正常性、およびそのアプライアンスが管理しているアプライアンスの正常性を示します。Firepower Management Center は、管理対象のデバイスに対して自動的に正常性ポリシーを適用しないため、ユーザーは正常性ポリシーをデバイスへ手動で適用する必要があります。このようにしないと、デバイスのステータスは Disabled として示されます。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス (Status) ] タブにデフォルトで表示されます。

ウィジェットの設定を変更して、アプライアンスのステータスを円グラフまたは表で表示するように設定できます。

プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

円グラフの一部、またはアプライアンス ステータス表のいずれかの数字をクリックすると、[ヘルス モニタ (Health Monitor) ] ページが表示され、対象のアプライアンス、およびそのアプライアンスが管理しているすべてのアプライアンスのコンパイル済みの正常性ステータスを参照することができます。

## [関連イベント (Correlation Events) ] ウィジェット

[関連イベント (Correlation Events) ] ウィジェットは、ダッシュボードの時間範囲における 1 秒あたりの関連イベントの平均数を、優先度ごとに示します。このウィジェットは、詳細ダッシュボードの [関連 (Correlation) ] タブにデフォルトで表示されます。

ウィジェットを設定して、線形 (増分) や対数 (10 の倍数) のスケールを選択するだけでなく、ウィジェットの設定を変更してさまざまな優先度の関連イベントを表示することができます。

優先度を持たないイベントも含めて、特定の優先度のイベントに対して別のグラフを表示するには、1 つ以上の [優先順位 (Priorities) ] チェックボックスをオンにします。優先度に関係なくすべての関連イベントに対して追加のグラフを表示するには、[すべて表示 (Show All) ] を選択します。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

グラフをクリックして特定の優先度の関連イベントを表示することも、[すべて (All) ] グラフをクリックしてすべての関連イベントを表示することもできます。いずれの場合も、イベントはダッシュボードの時間範囲に制限されます。ダッシュボードを介して関連イベントにアクセスすると、そのアプライアンスに対するイベント (またはグローバル) の期間が変わります。

## [現在のインターフェイス ステータス (Current Interface Status) ] ウィジェット

[現在のインターフェイス ステータス (Current Interface Status) ] ウィジェットは、有効になっているか未使用のアプライアンスのすべてのインターフェイスのステータスを示します。

Firepower Management Center では、管理 (eth0、eth1 など) インターフェイスを表示できません。管理対象デバイスでは、センシング (s1p1 など) インターフェイスのみを表示するか、または管理インターフェイスとセンシング インターフェイスの両方を選択できます。インターフェイスは、タイプ (管理、インライン、パッシブ、スイッチド、ルーテッド、スタック、未使用) 別にグループ化されます。

ウィジェットは、各インターフェイスに対して次の情報を提供します。


- インターフェイスの名前
- インターフェイスのリンク状態
- インターフェイスのリンク モード (100Mb 全二重、または 10Mb 半二重など)
- インターフェイスのタイプ (銅線または光ファイバ)
- インターフェイスで受け取ったデータ量 (Rx) および送信したデータ量 (Tx)

リンク状態を表すボールの色は、次のように現在のステータスを示します。



- 緑色：リンクがフルスピードでアップ状態になっています
- 黄色：リンクはアップ状態ですがフルスピードではありません
- 赤色：リンクはアップ状態ではありません
- 灰色：リンクは管理上無効になっています
- 青色：リンク ステータス情報は使用できません (たとえば ASA)

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。

## [現在のセッション (Current Sessions) ] ウィジェット

[現在のセッション (Current Sessions) ] ウィジェットは、アプライアンスに現在ログインしているユーザ、セッションが生じたマシンに関連付けられている IP アドレス、各ユーザがアプライアンス上のページにアクセスした最後の (アプライアンスのローカル時間に基づいた) 時間を示します。自分を表すユーザ (現在ウィジェットを表示しているユーザ) には、ユーザアイコン (  ) のマークが付けられ、太字で示されます。ログオフするか非アクティブになってから1時間以内に、セッションはこのウィジェットのデータからブルーニングされます。このウィジェットは、詳細ダッシュボードおよびサマリダッシュボードの[ステータス (Status) ] タブにデフォルトで表示されます。

[現在のセッション (Current Sessions) ] ウィジェットでは、次のことができます。

- いずれかのユーザ名をクリックして、[ユーザ管理 (User Management) ] ページでユーザアカウントを管理します。
- ホストアイコン (  )、または IP アドレスの隣の侵害されたホストアイコン (  ) をクリックして、関連付けられているマシンのホストプロファイルを表示します。
- いずれかの IP アドレスまたはアクセス時間をクリックして、その IP アドレスおよびその IP アドレスに関連付けられているユーザが Web インターフェイスにログオンした時間によって制約される監査ログを表示します。

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。

## [カスタム分析 (Custom Analysis) ] ウィジェット

[カスタム分析 (Custom Analysis) ] ウィジェットは高度にカスタマイズ可能なウィジェットで、これを使用すると、Firepower システムで収集および生成されたイベントの詳細情報を表示できます。

このウィジェットには複数のプリセットが用意されており、導入に関する情報にすばやくアクセスできます。事前定義済みのダッシュボードから、これらのプリセットを幅広く使用できます。これらのプリセットを使用することも、カスタム設定を作成することもできます。カスタム構成では少なくとも、関心のあるデータ (表とフィールド) とそのデータの集計方法を指定します。イベントの相対的な発生数を表示するのか (棒グラフ)、一定期間のイベント数を表示するのか (折れ線グラフ) など、その他の表示関連の設定を適用することもできます。

このウィジェットは、ローカル時間に基づいて、最後にアップデートされた時間を表示します。ウィジェットのアップデートは、ダッシュボードの時間範囲に基づいた頻度で実行されます。たとえば、ダッシュボードの時間範囲を1時間に設定すると、ウィジェットは5分ごとにアップデートされます。また、ダッシュボードの時間範囲を1年に設定すると、ウィジェットは1週間ごとにアップデートされます。ダッシュボードが次にアップデートされるタイミングを設定するには、ウィジェットの左下にある [最終更新日 (Last updated) ] の通知にポインタを移動します。



- (注) [カスタム分析 (Custom Analysis) ]ウィジェットに赤い影が付いている場合は、そのウィジェットの使用がシステムのパフォーマンスに悪影響を及ぼしています。ウィジェットが長時間赤い状態のままになっている場合は、そのウィジェットを削除してください。また、システム構成 ([システム (System) ]>[設定 (Configuration) ]>[ダッシュボード (Dashboard) ]) のダッシュボード設定で、すべての [カスタム分析 (Custom Analysis) ]ウィジェットを無効にすることもできます。

### イベントの相対的な発生数の表示 (棒グラフ)

[カスタム分析 (Custom Analysis) ]ウィジェットの棒グラフでは、ウィジェットの背景の色付きバーが、各イベントの相対的な発生数を示します。バーは右から順にお読みください。

矢印のアイコン (▼) は、表示のソート順を示して、制御しています。下向きのアイコンは降順を表し、上向きのアイコンは昇順を表します。ソート順を変更するには、アイコンをクリックします。

最新の結果以降何らかの変更点があることを示すために、ウィジェットでは、各イベントの横に次の3つのアイコンのうちの1つを表示します。

- 新しいイベントアイコン (🟢) は、イベントが、最新の結果以降のものであることを示します。
- 上向き矢印のアイコン (↑) は、ウィジェットが最後にアップデートされた後で、イベントがこの場所に上がってきたことを示します。イベントが何段階上がってきたかを表す数字が、アイコンの横に示されます。
- 下向き矢印のアイコン (↓) は、ウィジェットが最後にアップデートされた後で、イベントがこの場所に下がってきたことを示します。イベントが何段階下がってきたかを表す数字が、アイコンの横に示されます。

### 一定期間のイベントの表示 (折れ線グラフ)

一定期間のイベントまたは収集されたその他のデータに関する情報が必要な場合は、対象の展開で、一定期間に発生した侵入イベントの合計数を表示するような線グラフを表示するように [カスタム分析 (Custom Analysis) ]ウィジェットを設定することができます。

### [カスタム分析 (Custom Analysis) ]ウィジェットの制限

[カスタム分析 (Custom Analysis) ]ウィジェットは、表示するように設定されたデータを表示する権限がないことを示すことがあります。たとえば、メンテナンスユーザには検出イベントを表示する権限がありません。また、このウィジェットは、ライセンスされていない機能に関連する情報を表示しません。ただし、そのユーザ (およびダッシュボードを共有している他のユーザ) は、ウィジェットの設定を変更して、自分が表示できるデータを表示することも、ウィジェットを削除することもできます。これを防ぐには、ダッシュボードをプライベート (非公開) で保存します。

ユーザ データを表示した場合は、権限のあるユーザのみが表示されます。

URL カテゴリ情報を表示した場合、分類されていない URL は表示されません。

[カウント (Count) ]で集約した侵入イベントを表示した場合、この数には、侵入イベントについてレビューされたイベントが含まれています。イベント数をイベントビューアで表示する場合は、レビューされたイベントは含まれません。



- (注) マルチドメイン展開では、システムは、各リーフ ドメインに個別のネットワーク マップを作成します。その結果、リーフ ドメインには、ネットワーク内で一意である IP アドレスを含めることができますが、別のリーフ ドメイン内の IP アドレスと同じにすることができます。先祖ドメインで [カスタム分析 (Custom Analysis) ]ウィジェットを表示すると、繰り返し使用される IP アドレスの複数のインスタンスを表示できます。一見すると、エントリが重複しているように見えることがあります。ただし、各 IP アドレスのホストプロファイル情報までドリルダウンすると、それらが異なるリーフ ドメインに属していることがわかります。

#### 例：カスタム構成

最近の侵入イベントのリストを表示するように [カスタム分析 (Custom Analysis) ]ウィジェットを設定するには、[侵入イベント (Intrusion Events) ]テーブルのデータを表示するようにウィジェットを設定します。[分類 (Classification) ]フィールドを選択し、このデータを [カウント (Count) ]で集約すると、各タイプのイベントがいくつ生成されたかが通知されます。

一方、[一意のイベント (Unique Events) ]で集約すると、各タイプで一意の侵入イベントがいくつ発生したかが通知されます (たとえばネットワークの Trojan、企業ポリシーの潜在的な違反、行われたサービス妨害攻撃の検出個数など)。

ウィジェットをさらに制約するには、保存されている検索 (アプライアンスに付属している事前定義の検索、またはユーザが作成したカスタム検索のいずれか) を使用します。たとえば、最初の例 ([分類 (Classification) ]フィールドを使用して [カウント (Count) ]で集約する) を、[ドロップされたイベント (Dropped Events) ]の検索を使用して制約すると、各タイプの侵入イベントがいくつドロップされたかが通知されます。

#### 関連トピック

[ダッシュボードの時刻設定の変更 \(272 ページ\)](#)

### [カスタム分析 (Custom Analysis) ]ウィジェットのプリファレンス

次の表に、[カスタム分析 (Custom Analysis) ]ウィジェットで設定できるプリファレンスについて示します。

さまざまなプリファレンスは、ウィジェットを設定する方法に応じて表示されます。たとえば、イベントの相対頻度 (棒グラフ) を表示する場合と、時系列のグラフ (線グラフ) を表示する場合とでは、ウィジェットの設定時に異なるプリファレンスセットが表示されます。フィ

ルタなど、一部のプリファレンスは、表示するデータが存在する特定のテーブルを選択する場合にのみ表示されます。

表 25: [カスタム分析 (Custom Analysis)] ウィジェットのプリファレンス

設定	詳細 (Details)
役職 (Title)	ウィジェットのタイトルを指定しない場合、システムは、設定済みのイベントタイプをタイトルとして使用します。
プリセット (Preset)	[カスタム分析 (Custom Analysis)] のプリセットによって、展開に関する情報に簡単にアクセスできます。事前定義済みのダッシュボードから、これらのプリセットを幅広く使用できます。これらのプリセットを使用することも、カスタム設定を作成することもできます。
テーブル (Table) (必須)	ウィジェットが表示するデータを含むイベントまたはアセットのテーブル。
フィールド (Field) (必須)	表示するイベントタイプの特定のフィールド。時系列でデータ (線グラフ) を表示するには、[時間 (Time)] を選択します。イベントの相対頻度 (棒グラフ) を表示するには、もう一方のオプションを選択します。
集約 (Aggregate) (必須)	集約方法は、表示するデータをウィジェットがどのようにグループ化するかを設定します。ほとんどのイベントタイプのデフォルト オプションは [カウント (Count)] です。
フィルタ	[アプリケーション統計 (Application Statistics)] および [アプリケーション別の侵入イベント統計 (Intrusion Event Statistics by Application)] テーブルのデータを制約するには、アプリケーションフィルタを使用できます。

## Custom Analysis ウィジェットから関連付けられているイベントを表示する

設定	詳細 (Details)
検索 (Search)	<p>保存した検索を使用して、ウィジェットが表示するデータを制約することができます。検索を指定する必要はありませんが、プリセットの中には事前定義された検索が使用されるものがあります。</p> <p>ユーザがアクセスできる検索は、プライベートで保存した検索だけです。共有ダッシュボード上にウィジェットを設定し、プライベートの検索を使用してイベントを制約すると、ウィジェットは、他のユーザがログインしたときにその検索を使用しないようにリセットされます。ウィジェットのビューにも影響します。これを防ぐには、ダッシュボードをプライベート（非公開）で保存します。</p> <p>接続イベントに基づいて [カスタム分析 (Custom Analysis) ] ダッシュボード ウィジェットを制約できるのは、接続サマリーを制限しているフィールドだけです。保存した無効な検索はグレー表示されます。</p> <p>保存されている検索を使用して [カスタム分析 (Custom Analysis) ] ウィジェットを制約し、その後で検索を編集すると、次にアップデートされるまでウィジェットには変更が反映されません。</p>
表示 (Show)	最も高い ([最上位 (Top) ]) または最も低い ([最下位 (Bottom) ]) 頻度で発生するイベントを表示するかどうかを選択します。
結果 (Results)	表示する結果の行数を選択します。
Mover の表示 (Show Movers)	最新の結果以降の変更を示すアイコンを表示するかどうかを選択します。
タイムゾーン	結果の表示に使用するタイムゾーンを選択します。
カラー (Color)	ウィジェットの棒グラフのバーの色を変更できます。

## 関連トピック

[ウィジェットの設定](#) (268 ページ)

## Custom Analysis ウィジェットから関連付けられているイベントを表示する

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Maint



Custom Analysis ウィジェットから、ウィジェットに表示されるイベントに関する詳細情報を提供するイベント ビュー (ワークフロー) を起動することができます。イベントは、ダッシュボードの時間範囲によって制限されて、そのイベントタイプのデフォルトのワークフローで表示されます。設定した時間枠の数やイベントタイプに応じて、Firepower Management Center の時間枠が適宜変更されます。

次に例を示します。

- 複数の期間が設定されている場合に、Custom Analysis ウィジェットからヘルス イベントにアクセスすると、デフォルトのヘルス イベント ワークフローにイベントが表示され、ヘルス モニタリング期間はダッシュボードの時間範囲に変更されます。
- 1つの時間枠を設定して Custom Analysis ウィジェットから任意のタイプのイベントにアクセスすると、イベントはそのイベントタイプのデフォルトワークフローに表示され、グローバル期間がダッシュボードの時間範囲に変更されます。

## 手順

次の選択肢があります。

- Custom Analysis ウィジェットの右下にあるすべて表示のアイコン (🔍) をクリックして、ウィジェットの設定で制約して、すべての関連イベントを表示することができます。
- 関連するイベントの発生数 (棒グラフ) を表示するように設定された Custom Analysis ウィジェットで、任意のイベントをクリックして、ウィジェットの設定、およびそのイベントで制約して、関連イベントを表示します。

## [ディスク使用量 (Disk Usage) ]ウィジェット

[ディスク使用量 (Disk Usage) ]ウィジェットは、ディスク使用率のカテゴリに基づいて、ハードドライブで使用される領域のパーセンテージを表示します。また、アプライアンスのハードドライブの各パーティションで使用される領域のパーセンテージおよび容量も示します。[ディスク使用量 (Disk Usage) ]ウィジェットがデバイスにインストールされている場合、または Firepower Management Center が、マルウェアストレージパックが含まれているデバイスを管理している場合、[ディスク使用量 (Disk Usage) ]ウィジェットはマルウェアストレージパックについて同じ情報を表示します。このウィジェットは、デフォルトダッシュボードおよびサマリ ダッシュボードの [ステータス (Status) ] タブにデフォルトで表示されます。

[カテゴリ別 (By Category) ]スタックバーは、各ディスク使用率のカテゴリを、使用可能な合計ディスク領域に対する使用量の割合として表示します。次の表で、使用可能なカテゴリについて説明します。

表 26: ディスク使用率のカテゴリ

ディスク使用率のカテゴリ	説明
イベント	システムで記録されたすべてのイベント
ファイル (Files)	システムに格納されたすべてのファイル
バックアップ	すべてのバックアップ ファイル
変更点	ルールのアップデートやシステムのアップデートなど、アップデートに関連するすべてのファイル
その他	システムのトラブルシューティング ファイルおよびその他のファイル
未使用	アプライアンス上の残りの空き領域

[カテゴリ別 (By Category) ] スタック バーのディスク使用率カテゴリにポインタを合わせると、使用可能なディスク領域のうち、そのカテゴリで使用された領域の割合、ディスク上の実際のストレージ領域、およびそのカテゴリで使用可能なディスク領域の合計を表示することができます。マルウェアストレージパックがインストールされている場合、[ファイル (Files) ] カテゴリで使用できるディスク領域の合計は、マルウェアストレージパックで使用できるディスク領域になることに注意してください。

マルウェア ストレージパックがインストールされている場合は、ウィジェットのプリファレンスを変更して、[カテゴリ別 (By Category) ] スタック バーのみを表示したり、スタック バーと `admin (/)`、`/Volume`、および `/boot` パーティションの使用率、および `/var/storage` パーティションを表示したりするようにウィジェットを設定できます。

ウィジェットのプリファレンスは、ウィジェットのアップデート頻度、およびダッシュボードの時間範囲で現在のディスク使用率または収集したディスク使用率の統計のいずれかを表示することも制御します。

## [インターフェイストラフィック (Interface Traffic) ]ウィジェット

[インターフェイストラフィック (Interface Traffic) ]ウィジェットには、アプライアンスのインターフェイスで送受信された受信 (Rx) トラフィックと送信 (Tx) トラフィックの割合が示されます。7000 & 8000 シリーズ デバイスの場合、ウィジェットにはセンシング インターフェイスに関する情報も表示されます。このウィジェットは、事前定義されたダッシュボードにデフォルトでは表示されません。

アウトバウンド (送信) トラフィックには、フロー制御パケットが含まれます。そのため、7000 & 8000 シリーズ デバイス上のパッシブ センシング インターフェイスには、送信トラフィックが表示されることがあり、これは想定されている動作です。マルウェアライセンスが有効になっているデバイスは、動的分析を設定していない場合でも、定期的に AMP クラウドへの接続を試行します。そのため、これらのデバイスには送信トラフィックが表示されます。これもまた想定されている動作です。

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。7000 & 8000 シリーズ デバイスでは、設定によって、使用されていないインターフェイスのトラフィック レートをウィジェットに表示するかどうかを制御します (デフォルトでは、ウィジェットにはアクティブなインターフェイスのトラフィック レートのみが表示されます)。

## [侵入イベント (Intrusion Events) ]ウィジェット

[侵入イベント (Intrusion Events) ]ウィジェットは、ダッシュボードの時間範囲で発生した侵入イベントを、優先度ごとに表示します。これには、ドロップされたパケットおよびさまざまな影響を含む、侵入イベントの統計が含まれています。このウィジェットは、サマリダッシュボードの [侵入イベント (Intrusion Events) ]タブにデフォルトで表示されます。

ウィジェットの設定では、次のことができます。

- [イベントフラグ (Event Flags) ]には、パケットが欠落したイベント、パケットが欠落した可能性のあるイベント、または特定の影響を示すグラフが個別に表示されます。影響やルールの状態に関係なくすべての侵入イベントに対して追加のグラフを表示するには、[すべて (All) ]を選択します。
- [表示 (Show) ]では、[1 秒あたりの平均イベント数 (Average Events Per Second) ]または [イベントの合計数 (Total Events) ]を選択できます。
- [縦方向スケール (Vertical Scale) ]では、[線形 (Linear) ] (増分) または [対数 (Logarithmic) ] (10 の倍数) のスケールを選択できます。
- ウィジェットの更新頻度。

ウィジェットでは次のことができます。

- ドロップされたパケット、ドロップされた可能性のあるパケット、または特定の影響に対応するグラフをクリックして、そのタイプの侵入イベントを表示します。
- ドロップされたイベントに対応するグラフをクリックして、ドロップされたイベントを表示します。
- ドロップされたと考えられるイベントに対応するグラフをクリックして、ドロップされたと考えられるイベントを表示します。
- [すべて (All) ] グラフをクリックして、すべての侵入イベントを表示します。

結果のイベントビューは、ダッシュボードの時間範囲に制約されます。ダッシュボードを介して侵入イベントにアクセスすると、そのアプライアンスに対するイベント (またはグローバル) の期間が変わります。侵入ルールの状態または侵入ポリシーのインラインドロップ動作に関係なく、パッシブな配置のパケットはドロップされないことに注意してください。

## [ネットワーク コンプライアンス (Network Compliance) ]ウィジェット

[ネットワーク コンプライアンス (Network Compliance) ]ウィジェットは、ユーザが設定したホワイトリストに対するホストのコンプライアンスを要約します。デフォルトではこのウィジェットに、アクティブな関連ポリシーにおけるすべてのコンプライアンス ホワイトリスト

## [製品ライセンス (Product Licensing) ] ウィジェット

に対して準拠しているホスト、準拠していないホスト、および評価されなかったホストの数を示す円グラフが表示されます。このウィジェットは、詳細ダッシュボードの[**相関 (Correlation)**] タブにデフォルトで表示されます。

ウィジェットの設定を変更して、すべてのホワイト リスト、または特定のホワイト リストのいずれかについてネットワーク コンプライアンスを表示するようにウィジェットを設定できます。

すべてのホワイトリストに対してネットワーク コンプライアンスを表示するよう選択すると、あるホストが、アクティブな相関ポリシーのいずれのホワイト リストにも準拠していない場合、ウィジェットはそのホストが非準拠であるとみなします。

また、このウィジェットの設定を使用すると、ネットワーク コンプライアンスの表示で次の3つのスタイルのうちどれを使用するかを指定することができます。

[**ネットワーク コンプライアンス (Network Compliance)**] スタイル (デフォルト) は、準拠しているホスト、準拠していないホスト、および評価されなかったホストの数を示す円グラフを表示します。ホストの違反の件数を表示するには、円グラフをクリックします。このようにすると、少なくとも1つのホワイト リストに違反しているホストが表示されます。

[**一定期間のネットワーク コンプライアンス (%) (Network Compliance over Time (%))**] スタイルは、ダッシュボードの時間範囲において準拠しているホスト、準拠していないホスト、およびまだ評価されていないホストの相対的な割合を示す積み重ね面積グラフを表示します。

[**一定期間のネットワーク コンプライアンス (Network Compliance over Time)**] スタイルは、ダッシュボードの時間範囲において準拠しているホスト、準拠していないホスト、およびまだ評価されていないホストの数を示す線グラフを表示します。

ウィジェットをアップデートする頻度は、設定で調整します。まだ評価されていないイベントを非表示にするには、[**未評価を表示 (Show Not Evaluated)**] ボックスをオンにします。

## [製品ライセンス (Product Licensing) ] ウィジェット

[製品ライセンス (Product Licensing) ] ウィジェットは、Firepower Management Center に現在インストールされているデバイスおよび機能のライセンスを示します。また、ライセンス契約されているアイテムの数、許可される残りのライセンス契約アイテム数も示します。これは、事前定義されたどのダッシュボードにおいてもデフォルトでは表示されません。

このウィジェットの上部のセクションには、一時的なライセンスも含めて、Firepower Management Center にインストールされているすべてのデバイスおよび機能のライセンスが表示されますが、[**期限の切れたライセンス (Expiring Licenses)**] セクションには、一時的なライセンスおよび期限の切れたライセンスのみが表示されます。

ウィジェットの背景のバーは、使用中のライセンスのそれぞれのタイプの割合を示しています。このバーは右から左へ読みます。期限の切れたライセンスには、取り消し線が付けられています。

ウィジェットのプリファレンスを変更して、現在ライセンス契約されている機能を表示するか、またはライセンス契約が可能なすべての機能を表示するようにウィジェットを設定することができます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

任意のライセンスタイプをクリックすると、ローカル設定の[ライセンス (License)] ページに移動して、機能ライセンスを追加または削除することができます。

## 【製品更新 (Product Updates)】ウィジェット

【製品更新 (Product Updates)】ウィジェットは、アプライアンスに現在インストールされているソフトウェアの概要、およびダウンロード済みだがまだインストールしていない更新プログラムの情報を提供します。このウィジェットは、詳細ダッシュボードおよびサマリダッシュボードの[ステータス (Status)] タブにデフォルトで表示されます。

このウィジェットは、スケジュールされたタスクを使用して最新バージョンを判別するため、更新プログラムをダウンロード、プッシュ、またはインストールするようにスケジュールされたタスクを構成するまで、Unknown と表示されます。

ウィジェットのプリファレンスを変更して、最新のバージョンを非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されません。

このウィジェットには、ソフトウェアを更新できるページへのリンクもあります。次の操作を実行できます。

- 現在のバージョンをクリックして、アプライアンスを手動で更新します。
- 最新バージョンをクリックして、更新プログラムをダウンロードするタスクをスケジュールします。

## 【RSS フィード (RSS Feed)】ウィジェット

【RSS フィード (RSS Feed)】ウィジェットは、ダッシュボードに RSS フィードを追加します。デフォルトでは、ウィジェットはシスコのセキュリティニュースのフィードを示します。このウィジェットは、詳細ダッシュボードおよびサマリダッシュボードの[ステータス (Status)] タブにデフォルトで表示されます。

また、企業ニュース、Snort.org ブログ、または Cisco 脅威調査ブログの事前設定済みのフィードを表示するようウィジェットを設定することができます。ウィジェットの設定で URL を指定して、他の RSS フィードに対するカスタム接続を作成することもできます。

フィードは 24 時間ごとに更新されます (ただしユーザはフィードを手動で更新できます)。また、ウィジェットはアプライアンスのローカル時間に基づいて、フィードが最後に更新された時間を表示します。アプライアンスは、(事前設定された 2 つのフィードについて) Web サイトに対するアクセス権を持っている、または設定したいいずれかのカスタムフィードに対するアクセス権を持っている必要があります。

ウィジェットを設定する場合には、フィードからいくつのストーリーをウィジェットに表示するか、およびヘッドラインとともにストーリーの説明を表示するかどうかを選択することができます。ただしすべての RSS フィードで説明が使用できるわけではないことに注意してください。

【RSS フィード (RSS Feed)】ウィジェットでは、次のことができます。

- フィード内のストーリーのいずれかをクリックして、ストーリーを表示します

- [さらに表示 (more) ] リンクをクリックして、フィードの Web サイトへ移動します
- 更新アイコン (🔄) をクリックして、フィードを手動で更新します

## [システム負荷 (System Load) ] ウィジェット

[システム負荷 (System Load) ] ウィジェットは、アプライアンス上の (各 CPU についての) CPU の使用率、メモリ (RAM) の使用率、およびシステムの負荷 (実行を待機しているプロセスの数によって測定され、負荷平均とも呼ばれる) を現在、およびダッシュボードの時間範囲について表示します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス (Status) ] タブにデフォルトで表示されます。

ウィジェットのプリファレンスを変更して、負荷平均を表示または非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

## [システム時刻 (System Time) ] ウィジェット

[システム時刻 (System Time) ] ウィジェットは、アプライアンスのローカル システム時間、稼働時間、およびブート時間を表示します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス (Status) ] タブにデフォルトで表示されます。

ウィジェットのプリファレンスを変更して、ブート時間を非表示にするようウィジェットを設定できます。プリファレンスは、ウィジェットがアプライアンスの時計と同期する頻度も調整します。

## [ホワイト リスト イベント (White List Events) ] ウィジェット

[ホワイト リスト イベント (White List Events) ] ウィジェットは、ダッシュボードの時間範囲における 1 秒あたりの平均イベント数を、優先度別に表示します。このウィジェットは、デフォルト ダッシュボードの [相関 (Correlation) ] タブにデフォルトで表示されます。

ウィジェットの設定を変更して、さまざまな優先度のホワイト リスト イベントを表示するようウィジェットを設定できます。

ウィジェットの設定では、次のことができます。

- 優先度を持たないイベントも含めて、特定の優先度のイベントに対して別のグラフを表示するには、1 つ以上の [優先順位 (Priorities) ] チェックボックスをオンにします。
- 優先度に関係なくすべてのホワイト リスト イベントに対して追加のグラフを表示するには、[すべて表示 (Show All) ] を選択します。
- [縦方向スケール (Vertical Scale) ] を選択して、[線形 (Linear) ] (増分) または [対数 (Logarithmic) ] (10 の倍数) のスケールを選択します。

プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

グラフをクリックして特定の優先度のホワイト リスト イベントを表示することも、[すべて (All) ] グラフをクリックしてすべてのホワイト リスト イベントを表示することもできます。

いずれの場合も、イベントは、ダッシュボードの時間範囲によって制約されます。ダッシュボードを介してホワイトリストイベントにアクセスすると、Firepower Management Center に対するイベント（またはグローバル）の期間が変わります。

## ダッシュボードの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Maint

### 手順

**ステップ 1** [概要 (Overview)] > [ダッシュボード (Dashboards)] を選択して、変更するダッシュボードをメニューから選択します。

**ステップ 2** ダッシュボードを管理します。

- ダッシュボードの作成：カスタムダッシュボードを作成します。[カスタムダッシュボードの作成 \(268 ページ\)](#) を参照してください。
- ダッシュボードの削除：ダッシュボードを削除するには、削除するダッシュボードの横にある削除アイコン (🗑️) をクリックします。デフォルトのダッシュボードを削除する場合は、新しいデフォルトを定義する必要があります。そうしない場合、ダッシュボードを表示しようとするたびに、アプライアンスからダッシュボードを選択するように要求されます。
- オプションの編集：カスタムのダッシュボードオプションを編集します。[ダッシュボードオプションの編集 \(271 ページ\)](#) を参照してください。
- 時間の制約の変更：ダッシュボードの表示時間または一時停止/一時停止解除の時間を変更します。詳細は、[ダッシュボードの時刻設定の変更 \(272 ページ\)](#) を参照してください。

**ステップ 3** ダッシュボードのタブを管理します。

- タブの追加：ダッシュボードにタブを追加します。[ダッシュボードタブの追加 \(266 ページ\)](#) を参照してください。
- タブの削除：ダッシュボードのタブを削除するには、タブの右上隅にある閉じるアイコン (✖️) をクリックし、[OK] をクリックして確認します。ダッシュボードから最後のタブを削除することはできません。各ダッシュボードには少なくとも1つのタブが必要です。
- タブの名前変更：ダッシュボードのタブの名前を変更します。[ダッシュボードタブの名前の変更 \(273 ページ\)](#) を参照してください。

(注) ダッシュボードのタブの順序は変更できません。

**ステップ 4** ダッシュボードウィジェットを管理します。

- ウィジェットの追加：ダッシュボードにウィジェットを追加します。[ダッシュボードへのウィジェットの追加 \(266 ページ\)](#) を参照してください。
- プリファレンスの設定：ウィジェットのプリファレンスを設定します。[ウィジェットの設定 \(268 ページ\)](#) を参照してください。
- 表示のカスタマイズ：ウィジェットの表示をカスタマイズします。[ウィジェット表示のカスタマイズ \(271 ページ\)](#) を参照してください。
- イベントの表示：カスタム分析ウィジェットから関連するイベントを表示します。[Custom Analysis ウィジェットから関連付けられているイベントを表示する \(258 ページ\)](#) を参照してください。

**ヒント** シスコの事前定義のダッシュボード内のカスタム分析ウィジェットのすべての設定が、ウィジェットのシステムプリセットに対応しています。これらのウィジェットの1つを変更または削除した場合は、適切なプリセットをベースにして新しいカスタム分析ウィジェットを作成して復元することができます。

## ダッシュボードタブの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Maint

### 手順

- ステップ 1** 変更するダッシュボードを表示します ([ダッシュボードの表示 \(274 ページ\)](#) を参照)。
- ステップ 2** 最後の既存のタブの横にある追加アイコン (+) をクリックします。
- ステップ 3** タブの名前を入力します。
- ステップ 4** [OK] をクリックします。

## ダッシュボードへのウィジェットの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Maint



各タブには、3列のレイアウトで1つ以上のウィジェットを表示できます。ダッシュボードにウィジェットを追加するには、ウィジェットを追加するタブを選択します。ウィジェットは、自動的にウィジェットが最も少ない列に追加されます。すべてのカラムに同じ数のウィジェットがある場合、新しいウィジェットは最も左のカラムに追加されます。ダッシュボードタブには最大15個のウィジェットを追加できます。



**ヒント** 追加したウィジェットは、タブの任意の場所に移動できます。ただし、別のタブにはウィジェットを移動できません。

表示されるダッシュボードウィジェットは、使用しているアプライアンスのタイプ、ユーザーロールと（マルチドメイン環境では）現在のドメインにより異なります。すべてのユーザーロールがすべてのダッシュボードウィジェットに対してアクセス権を持っているわけではないため、多くの権限を持つユーザが作成したダッシュボードを、それよりも少ない権限を持つユーザが参照する場合、ダッシュボードのすべてのウィジェットを使用できないことがあることに注意してください。ダッシュボード上に、許可されていないウィジェットが表示されることがありますが、これらのウィジェットは無効です。

#### 手順

- ステップ1** ウィジェットを追加するダッシュボードを表示します。[ダッシュボードの表示 \(274 ページ\)](#) を参照してください。
- ステップ2** ウィジェットを追加するタブをクリックします。
- ステップ3** [ウィジェットの追加 (Add Widgets)] をクリックします。カテゴリ名をクリックして各カテゴリのウィジェットを表示することも、[すべてのカテゴリ (All Categories)] をクリックしてすべてのウィジェットを表示することもできます。
- ステップ4** 追加するウィジェットの横にある[追加 (Add)] をクリックします。[ウィジェットの追加 (Add Widgets)] ページには、追加するものも含め、各タブにあるウィジェットの数がタイプごとに表示されます。

**ヒント** （複数の RSS Feed ウィジェット、または複数の Custom Analysis ウィジェットを追加する場合など）同じタイプの複数のウィジェットを追加するには、[追加 (Add)] をもう一度クリックします。
- ステップ5** ウィジェットの追加が終了したら、[完了 (Done)] をクリックしてダッシュボードに戻ります。

#### 次のタスク

- カスタム分析ウィジェットを追加した場合は、ウィジェットの設定が必要です。[ウィジェットの設定 \(268 ページ\)](#) を参照してください。

## 関連トピック

[ウィジェットの使用可能性](#) (249 ページ)

## ウィジェットの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Maint

各ウィジェットには、動作を決定する一連のプリファレンスがあります。

### 手順

- 
- ステップ 1** プリファレンスを変更するウィジェットのタイトルバーで、プリファレンスの表示アイコン (▼) をクリックします。
- ステップ 2** 必要に応じて変更を加えます。
- ステップ 3** プリファレンスのセクションを非表示にするには、ウィジェットのタイトルバーで、プリファレンスの非表示アイコン (▲) をクリックします。
- 

## カスタム ダッシュボードの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Maint



- ヒント** 新しいダッシュボードを作成する代わりに、別のアプライアンスからダッシュボードをエクスポートし、それを自分のアプライアンスへインポートすることができます。その後でニーズに合わせて、インポートしたダッシュボードを編集することができます。
- 

### 手順

- ステップ 1** [概要 (Overview)] > [ダッシュボード (Dashboards)] > [管理 (Management)] を選択します。

**ステップ2** [ダッシュボードの作成 (Create Dashboard)] をクリックします。

**ステップ3** [カスタムダッシュボードオプション \(269 ページ\)](#) の説明に従って、カスタムダッシュボードオプションを変更します。

**ステップ4** [保存 (Save)] をクリックします。

## カスタムダッシュボードオプション

次の表に、カスタムダッシュボードを作成または編集するときに使用できるオプションを示します。

表 27: カスタムダッシュボードオプション

オプション	説明
ダッシュボードのコピー (Copy Dashboard)	カスタムダッシュボードを作成する場合は、ユーザが作成した、またはシステムで事前定義されている既存のダッシュボードをベースとして使用するよう選択できます。このオプションは、ニーズに合わせて変更できる、既存のダッシュボードのコピーを取ります。必要に応じて、[なし (None)] を選択することで、空白の新規ダッシュボードを作成できます。このオプションは、新しいダッシュボードを作成する場合のみ使用可能になります。  マルチドメイン展開では、先祖ドメインのプライベート以外のダッシュボードはコピーできます。
[名前 (Name)]	カスタムダッシュボードの固有名。
説明	カスタムダッシュボードの簡単な説明。
タブを変更する間隔 (Change Tabs Every)	ダッシュボードがそれぞれのタブを自動変更する頻度 (分単位) を指定します。ダッシュボードを一時停止した場合や、ダッシュボードのタブが1つのみの場合を除き、この設定により、指定した間隔で次のタブが表示されます。タブの自動変更を無効にするには、[タブを変更する間隔 (Change Tabs Every)] フィールドに 0 を入力します。

オプション	説明
ページを更新する間隔 (Refresh Page Every)	<p>現在のダッシュボードのタブを新しいデータで更新する頻度 (分単位) を指定します。この値は、[タブを変更する間隔 (Change Tabs Every)] の設定より大きい値にする必要があります。ダッシュボードを一時停止しない限り、この設定より、指定した間隔でダッシュボード全体が更新されます。定期的なページ更新を無効にするには、[ページを更新する間隔 (Refresh Page Every)] フィールドに 0 を入力します。ダッシュボードのページ全体を自動的に更新する頻度を決定します。</p> <p>ダッシュボード全体を更新すると、共有のダッシュボードに対して他のユーザが行ったプリファレンスまたはレイアウトの変更や、他のコンピュータ上のプライベートダッシュボードに対して、ダッシュボードが最後に更新された後で自分が行った変更を確認できます。ダッシュボードが常に表示されているネットワークオペレーションセンター (NOC) などでは、頻繁な更新が有効です。ローカルコンピュータでダッシュボードの変更を行えば、ユーザが指定する間隔で NOC のダッシュボードが自動的に更新されるため、手動による更新は必要ありません。データのアップデートを確認するためにダッシュボード全体を更新する必要はありません。個々のウィジェットはプリファレンスに従ってアップデートされます。</p> <p>(注) この設定は、個々のウィジェットの多くで使用可能なアップデート間隔とは異なります。ダッシュボードのページを更新すると個々のウィジェットのアップデート間隔はリセットされますが、[ページを更新する間隔 (Refresh Page Every)] 設定を無効にしても、ウィジェットはそれ自身のプリファレンスに従ってアップデートされます。</p>
プライベートとして保存 (Save As Private)	<p>カスタムダッシュボードは、アプライアンスのすべてのユーザが表示および変更可能か、またはユーザアカウントに関連付けて、独自の使用に限り予約可能かを決定します。ロールに関係なく、ダッシュボードへアクセスできるすべてのユーザは、共有ダッシュボードを変更できることに注意してください。特定のダッシュボードを自分のみで変更できるようにするには、そのダッシュボードをプライベートとして保存します。</p>

## ウィジェット表示のカスタマイズ

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Maint

ウィジェットは、タブ上で最小化、最大化、および再配置することができます。

### 手順

**ステップ1** ダッシュボードを表示します ([ダッシュボードの表示 \(274 ページ\)](#) を参照)。

**ステップ2** 次のように、ウィジェット表示をカスタマイズします。

- タブ上でウィジェットを再配置するには、移動するウィジェットのタイトルバーをクリックし、新しい場所へドラッグします。

(注) 別のタブにウィジェットを移動することはできません。ウィジェットを別のタブに表示する場合は、現在のタブからいったん削除してから新しいタブに追加する必要があります。

- ダッシュボードでウィジェットを最小化または最大化するには、ウィジェットのタイトルバーにある最小化 (–) アイコンまたは最大化 (□) アイコンをクリックします。
- ウィジェットをタブ上に表示する必要がなくなった場合にそのウィジェットを削除するには、ウィジェットのタイトルバーにある閉じるアイコン (✕) をクリックします。

## ダッシュボードオプションの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Maint

### 手順

**ステップ1** 編集するダッシュボードを表示します ([ダッシュボードの表示 \(274 ページ\)](#) を参照)。

**ステップ2** 変更するダッシュボードの横にある編集アイコン (🔧) をクリックします。

- ステップ3 [カスタムダッシュボードオプション \(269ページ\)](#) の説明に従ってオプションを変更します。  
 ステップ4 [保存 (Save) ]をクリックします。

## ダッシュボードの時刻設定の変更

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Maint

最短で1時間前 (デフォルト) から、最長では1年前からの期間を反映するように時間範囲を変更できます。時間範囲を変更する場合は、時間によって制約される可能性のあるウィジェットが自動でアップデートされ、新しい時間範囲が反映されます。

すべてのウィジェットを時間で制約できるわけではないことに注意してください。たとえば、ダッシュボードの時間範囲は [アプライアンス情報 (Appliance Information) ] ウィジェットには影響を与えません。このウィジェットは、アプライアンスの名前、モデル、および Firepower システム ソフトウェアの現在のバージョンが含まれている情報を提供します。

企業による Firepower システムの展開では、新しいイベントが古いイベントを置き換える頻度によっては、時間範囲を長期に変更しても、[カスタム分析 (Custom Analysis) ] ウィジェットなどのウィジェットでは役立たない場合があることに注意してください。

また、ダッシュボードを一時停止することもできます。これにより変更を表示したり、分析を中断したりせずに、ウィジェットで提供されたデータを調べることができます。ダッシュボードを一時停止すると、次のような影響があります。

- [更新間隔 (Update Every) ] ウィジェットプリファレンスに関係なく、個々のウィジェットでアップデートが停止します。
- ダッシュボードプロパティの [タブのサイクル間隔 (Cycle Tabs Every) ] 設定に関係なく、ダッシュボードのタブの自動変更が停止します。
- ダッシュボードプロパティの [ページの更新間隔 (Refresh Page Every) ] 設定に関係なく、ダッシュボードのページの更新が停止します。
- 時間範囲を変更しても影響はありません。

分析が完了したら、ダッシュボードの一時停止を解除できます。ダッシュボードの一時停止を解除すると、ページ上で該当するすべてのウィジェットが更新され、最新の時間範囲が反映されます。また、ダッシュボードのプロパティで指定した設定に従って、ダッシュボードタブの自動変更が再開され、ダッシュボード ページの更新が再開されます。

ダッシュボードに対するシステム情報のフローを中断するような接続の問題、または他の問題が発生した場合、ダッシュボードは自動的に一時停止し、問題が解決するまでエラー通知を表示します。



- (注) ダッシュボードが一時停止しているかどうかに関係なく、セッションは通常、非アクティブな状態が1時間（または設定した他の時間）続いた場合、ユーザをログアウトします。ダッシュボードを長期間パッシブにモニタリングする場合は、一部のユーザをセッションタイムアウトしないよう設定したり、システムのタイムアウト設定を変更することを検討してください。

#### 手順

- ステップ1** ウィジェットを追加するダッシュボードを表示します。[ダッシュボードの表示 \(274 ページ\)](#) を参照してください。
- ステップ2** 必要に応じて、ダッシュボードの時間範囲を変更するには、[表示経過時間 (Show the Last) ] ドロップダウンリストから時間範囲を選択します。
- ステップ3** 必要に応じて、一時停止 (||) または再生アイコン (▶) を使用して、時間範囲コントロールでダッシュボードを一時停止または一時停止解除します。

## ダッシュボードタブの名前の変更

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Maint

#### 手順

- ステップ1** 変更するダッシュボードを表示します ([ダッシュボードの表示 \(274 ページ\)](#) を参照)。
- ステップ2** 名前を変更するタブのタイトルをクリックします。
- ステップ3** タブの名前を入力します。
- ステップ4** [OK] をクリックします。

## ダッシュボードの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Maint

デフォルトでは、アプライアンスのホームページにデフォルトのダッシュボードが表示されます。デフォルトのダッシュボードを定義していない場合は、ホームページに [ダッシュボードの管理 (Dashboard Management)] ページが示され、ここで表示するダッシュボードを選択できます。

### 手順

いつでも次のいずれかの方法で操作できます。

- アプライアンスのデフォルトダッシュボードを表示するには、**[概要 (Overview)] > [ダッシュボード (Dashboards)]** を選択します。
- 特定のダッシュボードを表示するには、**[概要 (Overview)] > [ダッシュボード (Dashboards)]** を選択し、メニューからダッシュボードを選択します。
- 利用可能なすべてのダッシュボードを表示するには、**[概要 (Overview)] > [ダッシュボード (Dashboards)] > [管理 (Management)]** を選択します。個々のダッシュボードの横にある表示アイコン (🔍) を選択すると、そのダッシュボードを表示できます。





## 第 12 章

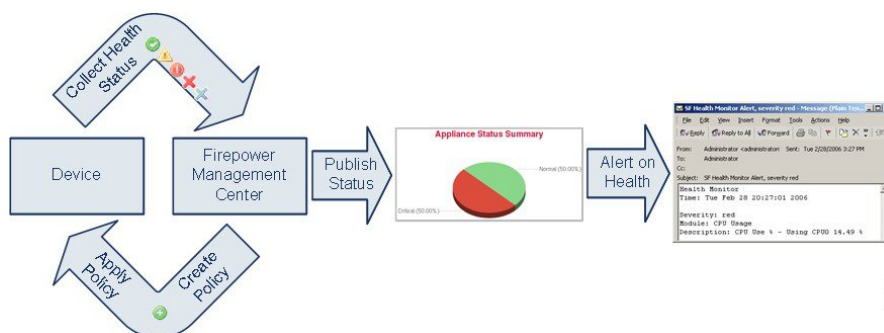
# ヘルス モニタリング

次のトピックでは、Firepower システムでヘルス モニタリングを使用する方法について説明します。

- [ヘルス モニタリングについて \(275 ページ\)](#)
- [正常性ポリシー \(284 ページ\)](#)
- [ヘルス モニタブラックリスト \(289 ページ\)](#)
- [ヘルス モニタアラート \(292 ページ\)](#)
- [ヘルス モニタの使用 \(295 ページ\)](#)
- [アプライアンスヘルス モニタの表示 \(297 ページ\)](#)
- [ヘルス イベントビュー \(300 ページ\)](#)

## ヘルス モニタリングについて

Firepower Management Center のヘルス モニタでは、さまざまなヘルスインジケータを追跡して Firepower システムのハードウェアとソフトウェアが正常に動作することを確認します。ヘルス モニタを使用して、Firepower システム展開全体の重要な機能のステータスを確認できます。



ヘルス モニタを使用すれば、正常性ポリシーとも呼ばれるテストのコレクションを作成し、正常性ポリシーを1つ以上のアプライアンスに適用できます。ヘルス モジュールとも呼ばれるテストは、指定された基準に照らしてテストするスクリプトです。テストを有効または無効にするか、テスト設定を変更することによって、正常性ポリシーを変更したり、不要になった正常

性ポリシーを削除したりできます。アプライアンスをブラックリストに登録することによって、選択したアプライアンスからのメッセージを抑制することもできます。

正常性ポリシー内のテストは設定された時間間隔で自動的に実行されます。すべてのテストを実行することも、オンデマンドで特定のテストを実行することもできます。ヘルス モニタは設定されたテスト条件に基づいてヘルス イベントを収集します。



(注) すべてのアプライアンスはハードウェア アラームのヘルス モジュール経由でハードウェアのステータスを自動的に報告します。また、Firepower Management Center はデフォルトの正常性ポリシーで設定されているモジュールを使用して自動的にステータスを報告します。アプライアンス ハートビートなどの一部の正常性モジュールは、Firepower Management Center 上で実行され Firepower Management Center の管理対象デバイスのステータスを報告します。ヘルス モジュールによっては、そのモジュールが設定されている正常性ポリシーをデバイスに適用しない限り管理対象デバイスのステータスを報告しないものもあります。

ヘルス モニタを使用してシステム全体、特定のアプライアンス、または特定のドメイン（マルチドメイン展開の場合）に関するヘルス ステータス情報にアクセスできます。[ヘルス モニタ (Health Monitor)] ページの円グラフとステータステーブルには、Firepower Management Center を含むネットワーク上のすべてのアプライアンスのステータスの視覚的なサマリが示されます。個々のアプライアンスのヘルス モニタを使用すれば、特定のアプライアンスのヘルス 詳細にドリルダウンできます。

完全にカスタマイズ可能なイベント ビューを使用すれば、ヘルス モニタによって収集されたヘルス ステータス イベントを迅速かつ容易に分析できます。このイベント ビューでは、イベントデータを検索して表示したり、調査中のイベントに関係する他の情報にアクセスしたりできます。たとえば、特定のパーセンテージの CPU 使用率の全記録を表示する場合は、CPU 使用率モジュールを検索して、パーセンテージ値を入力できます。

ヘルス イベントに対応した電子メール、SNMP、または syslog アラートを設定することもできます。ヘルス アラートは、標準アラートとヘルス ステータス レベルを関連付けたものです。たとえば、アプライアンスでハードウェアの過負荷が原因で障害が発生することは絶対ないことを確認する必要がある場合は、電子メール アラートをセットアップできます。その後、CPU、ディスク、またはメモリの使用率がそのアプライアンスに適用される正常性ポリシーで設定された警告レベルに達するたびにその電子メールアラートをトリガーとして使用するヘルス アラートを作成できます。アラートしきい値を、受け取る反復アラートの数が最小になるように設定できます。

サポートから依頼された場合に、アプライアンスのトラブルシューティングファイルを作成することもできます。

ヘルス モニタリングは管理活動であるため、管理者ユーザ ロール特権を持っているユーザのみがシステム ヘルス データにアクセスできます。

## ヘルス モジュール

ヘルス モジュールまたはヘルス テストは、正常性ポリシーに指定した条件でテストします。

表 28:ヘルス モジュール

モジュール	適用可能なアプライアンス	説明
AMP for Endpoint のステータス	Management Center	このモジュールは、最初に接続に成功した後 Firepower Management Center が AMP クラウドまたは Cisco AMP Private Cloud (AMPv) に接続できない場合、または AMPv が AMP クラウドに接続できない場合、アラートを出します。また、AMP for Endpoints 管理コンソールを使用して AMP クラウド接続の登録が解除された場合にもアラートを出します。
AMP for Firepower のステータス	Management Center	このモジュールは、以下の場合にアラートを出します。 <ul style="list-style-type: none"> <li>• Firepower Management Center が AMP クラウド、Cisco AMP Private Cloud (AMPv)、AMP Threat Grid クラウド、AMP Threat Grid オンプレミス アプライアンスに接続できない、または AMPv が AMP クラウドに接続できない。</li> <li>• 接続に使用する暗号化キーが無効である。</li> <li>• デバイスが AMP Threat Grid クラウドまたは AMP Threat Grid オンプレミスアプライアンスに接続して動的分析用のファイルを送信できない。</li> <li>• ファイル ポリシー設定に基づいてネットワーク トラフィックで過剰な数のファイルが検出された。</li> </ul> Firepower Management Center のインターネット接続が切断された場合、AMP for Firepower ステータスヘルスアラートの生成に最大 30 分かかることがあります。
アプライアンスハートビート	任意 (Any)	このモジュールは、アプライアンスハートビートがアプライアンスから届いているかどうかを確認し、アプライアンスのハートビートステータスに基づいてアラートを出します。
自動アプリケーションバイパスステータス	7000 & 8000 シリーズ	このモジュールは、アプライアンスがバイパスしきい値で設定された秒数以内に応答しなかったためにバイパスされたかどうかを確認し、バイパスが発生した場合にアラートを出します。
バックログのステータス	Management Center	このモジュールは、デバイスから Management Center に送信されるのを待機しているイベントデータのバックログのサイズが、30 分を超えて増大し続けた場合にアラートを表示します。  バックログを減らすには、帯域幅を評価し、ログに記録するイベント数を減らすことを検討してください。

モジュール	適用可能なアプライアンス	説明
クラシック ライセンス モニタ	Management Center	このモジュールは、制御、保護、URL フィルタリング、マルウェア、および VPN 用の十分なクラシック ライセンスが残っているかどうかを確認します。また、スタック内のデバイスに適合しないライセンスセットが含まれている場合にアラートを出します。モジュールに自動的に設定された警告レベルに基づいてアラートを出します。このモジュールの設定は変更できません。
CPU 使用率	任意 (Any)	このモジュールは、アプライアンス上の CPU が過負荷になっていないことを確認し、CPU 使用率がモジュールに設定されたパーセンテージを超えた場合にアラートを出します。
カードリセット	任意 (Any)	このモジュールは、リセット時に、ハードウェア障害原因で再起動されたネットワーク カードをチェックし、アラートを出します。
クラスタのステータス	脅威防御	このモジュールは、デバイスクラスタのステータスをモニタします。このモジュールは、以下の場合にアラートを出します。 <ul style="list-style-type: none"> <li>• クラスタに新しいプライマリ ユニットが選択される。</li> <li>• 新しいセカンダリ ユニットがクラスタに参加する。</li> <li>• プライマリまたはセカンダリ ユニットがクラスタから離脱する。</li> </ul>
ディスク ステータス	任意 (Any)	このモジュールは、ハードディスクと、アプライアンス上のマルウェア ストレージ パック (設置されている場合) のパフォーマンスを調査します。このモジュールは、ハードディスクと RAID コントローラ (設置されている場合) で障害が発生する恐れがある場合、または、マルウェア ストレージ パックではない追加のハードドライブが設置されている場合に、警告 (黄色) ヘルス アラートを生成します。また、設置されているマルウェア ストレージ パックを検出できなかった場合はアラート (赤色) ヘルス アラートを生成します。
ディスク使用量	任意 (Any)	このモジュールは、アプライアンスのハードドライブとマルウェア ストレージ パック上のディスク使用率をモジュールに設定された制限と比較し、その使用率がモジュールに設定されたパーセンテージを超えた時点でアラートを出します。また、モジュールしきい値に基づいて、システムが監視対象のディスク使用カテゴリ内のファイルを過剰に削除する場合、または、これらのカテゴリを除くディスク使用率が過剰なレベルに達した場合にもアラートを出します。ディスク使用率ヘルスステータスモジュールは、アプライアンス上の /パーティションと /volume パーティションのディスク使用率を監視して、ドレイン頻度を追跡するために使用します。ディスク使用率モジュールは /boot パーティションを監視対象パーティションとして列挙しますが、そのパーティションのサイズが固定のため、このモジュールはブートパーティションに基づいてアラートを出すことはしません。

モジュール	適用可能なアプライアンス	説明
ホスト制限	Management Center	このモジュールは、Firepower Management Center がモニタできるホスト数が制限に近づいているかどうかを確認し、モジュールに設定された警告レベルに基づいてアラートを出します。詳細については、 <a href="#">Firepower システムのホスト制限 (2035 ページ)</a> を参照してください。
ハードウェアアラーム	7000 & 8000 シリーズ、Threat Defense (物理)	このモジュールは、物理管理対象デバイス上のハードウェアを交換する必要があるかどうかを確認し、ハードウェアステータスに基づいてアラートを出します。また、ハードウェア関連デーモンのステータスと高可用性展開の 7000 および 8000 シリーズ デバイスのステータスについてレポートします。
HA ステータス	Management Center	このモジュールは、Firepower Management Center ハイ アベイラビリティステータスについて、モニタし、アラートを出します。Firepower Management Center のハイ アベイラビリティを確立していない場合、HA ステータスは、「HA でない (Not in HA) 」になります。  このモジュールは、ペアリングされているかどうかに関わらず、管理対象デバイスのハイ アベイラビリティ ステータスについてはモニタしたり、アラートを出したりしません。管理対象デバイスの HA ステータスは常に「HA でない (Not in HA) 」になります。[デバイス (Devices) ] > [デバイス管理 (Device Management) ] の [デバイス管理 (Device Management) ] ページを使用して、ハイ アベイラビリティ ペアのデバイスをモニタします。
ヘルス モニタ プロセス	任意 (Any)	このモジュールは、ヘルスモニタ自体のステータスを監視し、Firepower Management Center で受信された最後のステータス イベント以降の分数が警告制限または重大制限を超えた場合にアラートを出します。
インラインリンク不一致アラーム	ASA FirePOWER を除くすべての管理対象デバイス	このモジュールは、インラインセットに関連付けられたポートを監視し、インラインペアの 2 つのインターフェイスが別々の速度をネゴシエートした場合にアラートを出します。

モジュール	適用可能なアプライアンス	説明
侵入およびファイルイベント レート	すべての管理対象デバイス	<p>このモジュールは、1 秒あたりの侵入イベント数をこのモジュールに設定された制限と比較し、制限を超えた場合にアラートを出します。侵入およびファイルイベント レートが 0 の場合は、侵入プロセスがダウンしているか、管理対象デバイスがイベントを送信していない可能性があります。イベントがデバイスから送られているかどうかをチェックするには、<b>[分析 (Analysis)] &gt; [侵入 (Intrusions)] &gt; [イベント (Events)]</b> の順に選択します。</p> <p>一般に、ネットワーク セグメントのイベント レートは平均で 1 秒あたり 20 イベントです。この平均レートのネットワーク セグメントでは、<b>[1 秒あたりのイベント (重大) (Events per second (Critical))]</b> を 50 に設定し、<b>[1 秒あたりのイベント (警告) (Events per second (Warning))]</b> を 30 に設定する必要があります。システムの制限を決定するには、デバイスの <b>[統計情報 (Statistics)]</b> ページ (<b>[システム (System)] &gt; [モニタリング (Monitoring)] &gt; [統計 (Statistics)]</b>) で <b>[イベント/秒 (Events/Sec)]</b> 値を探してから、次の式を使用して制限を計算します。</p> <ul style="list-style-type: none"> <li>• 1 秒あたりのイベント (重大) = イベント/秒 * 2.5</li> <li>• 1 秒あたりのイベント (警告) = イベント/秒 * 1.5</li> </ul> <p>両方の制限に設定可能な最大イベント数は 999 であり、重大制限は警告制限より大きくする必要があります。</p>
インターフェイス ステータス	任意 (Any)	<p>このモジュールは、デバイスが現在トラフィックを収集しているかどうかを確認して、物理インターフェイスおよび集約インターフェイスのトラフィックステータスに基づいてアラートを出します。物理インターフェイスの情報には、インターフェイス名、リンクステータス、および帯域幅が含まれます。集約インターフェイスの情報には、インターフェイス名、アクティブリンクの数、および総集約帯域幅が含まれます。</p> <p>ASA FirePOWER の場合、DataPlaneInterfacex というラベルの付いたインターフェイス (ここで、xは数値) は、内部インターフェイス (ユーザ定義ではない) で、システム内部のパケットフローに関与します。</p>

モジュール	適用可能なアプライアンス	説明
リンク ステート伝達	NGIPSv と ASA FirePOWER を除くすべて	<p>このモジュールは、ペア化されたインラインセット内のリンクで障害が発生した時点特定して、リンクステート伝達モードをトリガーとして使用します。</p> <p>リンクステートがペアに伝達した場合は、そのモジュールのステータス分類が [重大 (Critical) ] に変更され、状態が次のように表示されません。</p> <p>Module Link State Propagation: ethx_ethy is Triggered</p> <p>ここで、x と y はペア化されたインターフェイス番号です。</p>
ローカルマルウェア分析	任意 (Any)	このモジュールは、デバイスがローカル マルウェア分析用に設定され、AMPクラウドからローカルマルウェア分析エンジンのシグネチャの更新をダウンロードできなかった場合、アラートを出します。
メモリ使用率	任意 (Any)	<p>このモジュールは、アプライアンス上のメモリ使用率をモジュールに設定された制限と比較し、使用率がモジュールに設定されたレベルを超えるとアラートを出します。</p> <p>メモリが 4 GB を超えるアプライアンスの場合、プリセットされたアラートしきい値は、システム問題を引き起こす可能性のあるメモリ空き容量の割合を求める式に基づいています。4 GB 未満のアプライアンスでは、警告しきい値と重大しきい値の時間間隔が非常に狭いため、[警告しきい値 % (Warning Threshold %)] の値を手動で 50 に設定することを推奨します。これにより、時間内にアプライアンスのメモリアラートを受け取って問題を解決できる可能性がさらに高まります。</p> <p>複雑なアクセス コントロール ポリシーやルールは、重要なリソースを消費し、パフォーマンスに悪影響を与える可能性があります。FirePOWER サービス ソフトウェア を含む一部のよりローエンドの ASA デバイスでは、デバイスのメモリ割り当てが最大限に使用されているため、断続的なメモリ使用率の警告が生成されることがあります。</p>
電源モジュール	物理 Management Center、7000 & 8000 シリーズ	<p>このモジュールは、デバイスの電源が交換が必要かどうかを確認し、電源ステータスに基づいてアラートを出します。</p> <p>(注) 8000 シリーズ管理対象デバイスで電源障害が発生した場合、アラートを生成するために最大 20 分かかることがあります。</p>

モジュール	適用可能なアプライアンス	説明
Process Status	任意 (Any)	このモジュールは、アプライアンス上のプロセスがプロセス マネージャの外部で停止または終了したかを確認します。プロセスが故意にプロセス マネージャの外部で停止された場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが [警告 (Warning)] に変更され、ヘルス イベント メッセージが停止されたプロセスを示します。プロセスがプロセス マネージャの外部で異常終了またはクラッシュした場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが [重大 (Critical)] に変更され、ヘルス イベント メッセージが終了したプロセスを示します。
検出の再設定	すべての管理対象デバイス	このモジュールは、デバイスの再設定が失敗した場合、アラートを出します。
RRD サーバ プロセス	Management Center	このモジュールは、時系列データを格納するラウンド ロビン サーバが正常に機能しているかどうかを確認します。このモジュールは、RRD サーバが前回の更新以降に再起動した場合にアラートを出します。また、RRD サーバの再起動を伴う連続更新回数がモジュール設定で指定された数値に達した場合に [重大 (Critical)] または [警告 (Warning)] ステータスに遷移します。
セキュリティインテリジェンス (Security Intelligence)	Management Center	<p>このモジュールは、セキュリティ インテリジェンス フィルタリングに関するさまざまな状況でアラートを出します。このモジュールは、セキュリティ インテリジェンス が使用中で次の場合にアラートを出します。</p> <ul style="list-style-type: none"> <li>• Firepower Management Center がフィードを更新できないか、フィード データが破損している、または認識可能な IP アドレスが含まれていない。</li> <li>• 管理対象デバイスが Firepower Management Center から更新されたセキュリティ インテリジェンス データを受信できない。</li> <li>• 管理対象デバイスが、メモリ問題のために、Firepower Management Center から提供されたすべてのセキュリティ インテリジェンス データをロードできない。</li> </ul> <p>セキュリティ インテリジェンス メモリ警告がヘルス モニタに表示された場合は、影響を受けるデバイスのアクセスコントロールポリシーを再適用して、セキュリティ インテリジェンス に割り当てるメモリを増やすことができます。</p>



モジュール	適用可能なアプライアンス	説明
スマート ライセンス モニタ	Management Center	<p>このモジュールは、以下の場合にアラートを出します。</p> <ul style="list-style-type: none"> <li>• Smart Licensing Agent と Smart Software Manager (SSM) の間の通信にエラーがある。</li> <li>• 製品インスタンス登録トークンの有効期限が切れている。</li> <li>• スマートライセンスの使用状況がコンプライアンスに違反している。</li> <li>• スマートライセンスの権限モードまたは評価モードの有効期限が切れている。</li> </ul>
時系列データ モニタ	Management Center	<p>このモジュールは、時系列データ（関連イベントカウントなど）が保存されるディレクトリ内の破損ファイルの存在を追跡して、ファイルが破損としてフラグが付けられ、削除された段階でアラートを出します。</p>
時刻同期ステータス	任意 (Any)	<p>このモジュールは、NTP を使用して時刻を取得するデバイスクロックと NTP サーバ上のクロックの同期を追跡して、クロックの差が 10 秒を超えた場合にアラートを出します。</p>
URL フィルタリング モニタ	Management Center	<p>このモジュールは、Firepower Management Center と管理対象デバイス間の通信、およびシステムがよくアクセスされる URL の脅威インテリジェンスを取得する Cisco Collective Security Intelligence (CSI) との通信を追跡します。Firepower Management Center が Cisco CSI との通信または Cisco CSI からの更新の取得に失敗した場合にアラートを出します。</p> <p>このモジュールは、Firepower Management Center が管理対象デバイスに URL データをプッシュできない場合にもアラートを出します。</p>
ユーザ エージェント ステータス モニタ	Management Center	<p>このモジュールは、Firepower Management Center に接続されたユーザエージェントでハートビートが検出されない場合にアラートを出します。</p>
VPN ステータス	Management Center	<p>このモジュールは、Firepower システム デバイス間の 1 つ以上の VPN トンネルがダウンしているときにアラートを出します。</p> <p>このモジュールは、以下を追跡します。</p> <ul style="list-style-type: none"> <li>• 7000 &amp; 8000 シリーズの VPN (7000 &amp; 8000 シリーズ)</li> <li>• Firepower Threat Defense のサイト間 VPN</li> </ul>

## ヘルス モニタリングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint

### 手順

**ステップ 1** [ヘルス モジュール \(276 ページ\)](#) で説明されているように、モニタするヘルス モジュールを決定します。

Firepower システムで使用しているアプライアンスの種類ごとに固有のポリシーをセットアップして、そのアプライアンスに適切なテストだけを有効にすることができます。

**ヒント** モニタリング動作をカスタマイズすることなくすぐにヘルスモニタリングを有効にするには、そのために用意されたデフォルト ポリシーを適用できます。

**ステップ 2** [正常性ポリシーの作成 \(285 ページ\)](#) で説明されているように、ヘルス ステータスを追跡するアプライアンスごとに正常性ポリシーを適用します。

**ステップ 3** (オプション) [ヘルス モニタ アラートの作成 \(293 ページ\)](#) で説明されているように、ヘルス モニタ アラートを設定します。

ヘルス ステータス レベルが特定のヘルス モジュールの特定の重大度レベルに達した段階でトリガーされる電子メール、Syslog、または SNMP アラートをセットアップできます。

## 正常性ポリシー

正常性ポリシーには、複数のモジュールに対して設定されたヘルステスト基準が含まれます。アプライアンスごとにどのヘルスモジュールを実行するかを制御したり、モジュールごとに実行するテストで使用される特定の制限を設定したりできます。

正常性ポリシーを設定するときに、そのポリシーに対して各ヘルスモジュールを有効にするかどうかを決定します。また、有効にした各モジュールが、プロセスの正常性を評価するたびに報告するヘルス ステータスを制御するための基準を選択することもできます。

システム内のすべてのアプライアンスに適用可能な1つの正常性ポリシーを作成することも、適用を計画している特定のアプライアンス用に正常性ポリシーをカスタマイズすることも、付属のデフォルト正常性ポリシーを使用することもできます。マルチドメイン展開では、先祖ドメインの管理者が子孫ドメインのデバイスに正常性ポリシーを適用できます。子孫ドメインではそのポリシーを使用するか、またはカスタマイズされたローカルポリシーと置き換えることができます。

## デフォルトの正常性ポリシー

Firepower Management Center のヘルス モニタでは、アプライアンスのヘルス モニタリングを迅速に実行できるように、デフォルトの正常性ポリシーが提供されます。デフォルト正常性ポリシーでは、実行中のプラットフォーム上で使用可能なヘルス モジュールのほとんどが自動的に有効になります。デフォルト正常性ポリシーを編集することはできませんが、コピーしてその設定に基づくカスタムポリシーを作成することができます。デフォルト正常性ポリシーは自動的に Firepower Management Center に適用されますが、正常性をモニタするすべての管理対象デバイスに適用する必要があります。

## 正常性ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint

アプライアンスで使用する正常性ポリシーをカスタマイズすることによって、新しいポリシーを作成できます。ポリシー内の設定は、最初に、新しいポリシーの基準として選択した正常性ポリシー内の設定を使用して生成されます。必要に応じて、ポリシー内のモジュールを有効または無効にし、各モジュールのアラート基準を変更できます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。先祖ドメインの管理者は、子孫ドメインのデバイスに正常性ポリシーを適用できます。子孫ドメインではこのポリシーを使用することも、カスタマイズしたローカルポリシーで置き換えることもできます。

### 手順

- ステップ 1 [システム (System)] > [ヘルス (Health)] > [ポリシー (Policy)] を選択します。
- ステップ 2 [ポリシーの作成 (Create Policy)] をクリックします。
- ステップ 3 [コピー ポリシー (Copy Policy)] ドロップダウン リストから、新しいポリシーの基準として使用する既存のポリシーを選択します。
- ステップ 4 ポリシーの名前を入力します。
- ステップ 5 ポリシーの説明を入力します。
- ステップ 6 [保存 (Save)] を選択して、ポリシー情報を保存します。
- ステップ 7 使用するモジュールを選択します。
- ステップ 8 [有効 (Enabled)] オプションに対して [オン (On)] を選択して、ヘルス ステータス テストのモジュールの使用を有効化します。
- ステップ 9 該当する場合は、[重大 (Critical)] および [警告 (Warning)] 基準を設定します。
- ステップ 10 モジュールの追加設定を行います。各モジュールで手順 7 ~ 10 を繰り返します。

**ステップ 11** 次の3つのオプションがあります。

- このモジュールに対する変更を保存して、[正常性ポリシー (Health Policy)] ページに戻るには、[ポリシーを保存して終了 (Save Policy and Exit)] をクリックします。
- このモジュールの設定を保存せずに、[正常性ポリシー (Health Policy)] ページに戻るには、[キャンセル (Cancel)] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [ポリシーを保存して終了 (Save Policy and Exit)] をクリックすると、加えたすべての変更が保存されます。[キャンセル (Cancel)] をクリックすると、すべての変更が破棄されます。

### 次のタスク

- [正常性ポリシーの適用 \(286ページ\)](#) の説明に従って、各アプライアンスに正常性ポリシーを適用します。これにより変更が適用され、影響を受けるすべてのポリシーのポリシーステータスが更新されます。

## 正常性ポリシーの適用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint

正常性ポリシーをアプライアンスに適用すると、ポリシー内で有効にしたすべてのモジュールのヘルステストが、アプライアンス上のプロセスとハードウェアの正常性を自動的に監視します。その後、ヘルステストは、ポリシー内で設定された時間間隔で実行を続け、アプライアンスのヘルスデータを収集し、そのデータを Firepower Management Center に転送します。

正常性ポリシーでモジュールを有効にしてから、ヘルステストが必要ないアプライアンスにポリシーを適用した場合、ヘルスマニタはそのヘルスマジュールのステータスを無効として報告します。

すべてのモジュールが無効になっているポリシーをアプライアンスに適用すると、適用されたすべての正常性ポリシーがアプライアンスから削除されるため、どの正常性ポリシーも適用されません。

すでにポリシーが適用されているアプライアンスに別のポリシーを適用した場合は、新しく適用されたテストに基づく新しいデータの表示が少し遅れる可能性があります。

先祖ドメインのマルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。管理者は子孫ドメインのデバイスに正常性ポリシーを適用できます。子孫ドメインはこれを使用でき、またはこれをカスタマイズされたローカルポリシーと置き換えることができます。

## 手順

**ステップ 1** [システム (System)] > [ヘルス (Health)] > [ポリシー (Policy)] を選択します。

**ステップ 2** 適用するポリシーの横にある適用アイコン (✔) をクリックします。

**ヒント** [正常性ポリシー (Health Policy)] 列の横にあるステータスアイコン (✔) は、アプライアンスの現在のヘルス ステータスを示します。

**ステップ 3** 正常性ポリシーを適用するアプライアンスを選択します。

**ステップ 4** [適用 (Apply)] をクリックして、選択したアプライアンスにポリシーを適用します。

## 次のタスク

- 必要に応じて、タスクのステータスをモニタします ([タスク メッセージの表示 \(330 ページ\)](#) を参照)。

アプライアンスのモニタリングは、ポリシーが正常に適用された直後に開始されます。

## 正常性ポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。先祖ドメインの管理者は、子孫ドメインのデバイスに正常性ポリシーを適用でき、子孫ドメインはこれを使用するか、またはカスタマイズしたローカル ポリシーに置き換えることができます。

## 手順

**ステップ 1** [システム (System)] > [ヘルス (Health)] > [ポリシー (Policy)] を選択します。

**ステップ 2** 変更するポリシーの横にある編集アイコン (✎) をクリックします。

**ステップ 3** [ポリシー名 (Policy Name)] フィールドまたは [ポリシーの説明 (Policy Description)] フィールドを必要に応じて編集します。

**ステップ 4** 変更するヘルス モジュールをクリックします。

**ステップ 5** [ヘルス モジュール \(276 ページ\)](#) の説明に従って、設定を変更します。

**ステップ 6** 次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[正常性ポリシー (Health Policy)] ページに戻るには、[ポリシーを保存して終了 (Save Policy and Exit)] をクリックします。
- このモジュールの設定を保存せずに、[正常性ポリシー (Health Policy)] ページに戻るには、[キャンセル (Cancel)] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [ポリシーを保存して終了 (Save Policy and Exit)] をクリックすると、加えたすべての変更が保存されます。[キャンセル (Cancel)] をクリックすると、すべての変更が破棄されます。

### 次のタスク

- [正常性ポリシーの適用 \(286ページ\)](#) の説明に従って、正常性ポリシーを再適用します。これにより変更が適用され、影響を受けるすべてのポリシーのポリシーステータスが更新されます。

## 正常性ポリシーの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint

不要になった正常性ポリシーを削除できます。アプライアンスに適用されているポリシーを削除した場合は、別のポリシーを適用するまでそのポリシー設定が有効のままになります。加えて、デバイスに適用されている正常性ポリシーを削除した場合、元となる関連アラート応答が無効にするまでは、そのデバイスに対して有効になっているヘルス モニタリング アラートがアクティブなままになります。

マルチドメイン導入では、現在のドメインで作成された正常性ポリシーのみを削除できます。



**ヒント** アプライアンスのヘルスモニタリングを停止するには、すべてのモジュールが無効になっている正常性ポリシーを作成し、それをアプライアンスに適用します。

### 手順

**ステップ 1** [システム (System)] > [ヘルス (Health)] > [ポリシー (Policy)] を選択します。

**ステップ 2** 削除するポリシーの横にある削除アイコン (🗑️) をクリックします。削除が成功したかどうかを示すメッセージが表示されます。

## ヘルス モニタ ブラックリスト

通常のネットワークメンテナンスの一環として、アプライアンスを無効にしたり、一時的に使用不能にしたりすることがあります。このような機能停止は意図したものであり、アプライアンスからのヘルス ステータスに Firepower Management Center 上のサマリー ヘルス ステータスを反映させる必要はありません。

ヘルス モニタ ブラックリスト機能を使用して、アプライアンスまたはモジュールに関するヘルス モニタリング ステータス レポートを無効にすることができます。たとえば、ネットワークのあるセグメントが使用できなくなることがわかっている場合は、そのセグメント上の管理対象デバイスのヘルス モニタリングを一時的に無効にして、Firepower Management Center 上のヘルスステータスにデバイスへの接続がダウンしたことによる警告状態または重大状態が表示されないようにできます。

ヘルス モニタリング ステータスを無効にしても、ヘルス イベントは生成されますが、そのステータスが無効になっているため、ヘルス モニタのヘルス ステータスには影響しません。ブラックリストからアプライアンスまたはモジュールを削除しても、ブラックリストに登録中に生成されたイベントのステータスは [無効 (Disabled) ] のままです。

アプライアンスからのヘルス イベントを一時的に無効にするには、ブラックリスト設定ページに移動して、アプライアンスをブラックリストに追加します。設定が有効になると、システムは全体のヘルス ステータスを計算するときにブラックリストに登録されているアプライアンスを含めません。[ヘルス モニタ アプライアンス ステータスの概要 (Health Monitor Appliance Status Summary) ] にはこのアプライアンスが [無効 (Disabled) ] としてリストされます。

アプライアンス上の個別のヘルス モニタリング モジュールをブラックリストに登録する方が実用的な場合があります。たとえば、Firepower Management Center 上でホスト制限に達した場合、ホスト制限ステータス メッセージをブラックリストに登録できます。

メインの [ヘルス モニタ (Health Monitor) ] ページで、ステータス行内の矢印をクリックして特定のステータスを持つアプライアンスのリストを展開表示すれば、ブラックリストに登録されたアプライアンスを区別できることに注意してください。

ブラックリストに登録されたアプライアンスまたは部分的にブラックリストに登録されたアプライアンスのビューを展開すると、ブラックリストアイコン (🔒) と注記が表示されます。



(注) Firepower Management Center では、ヘルス モニタのブラックリスト設定はローカル コンフィギュレーション設定です。そのため、Firepower Management Center 上でデバイスをブラックリストに登録してから削除しても、後で再登録すれば、ブラックリスト設定は元どおりになります。新たに再登録したデバイスはブラックリストに登録されたままです。

マルチドメイン導入では、先祖ドメインの管理者が子孫ドメインのアプライアンスやヘルス モジュールをブラックリストに登録できます。ただし、子孫ドメインの管理者は、先祖のコンフィギュレーションをオーバーライドして、自身のドメインのデバイスのブラックリストをクリアすることができます。

## アプライアンスのブラックリスト登録

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint

アプライアンスは個別に、またはグループ、モデル、関連付けられている正常性ポリシーにより、ブラックリストに登録できます。

ブラックリスト設定が有効になると、[正常性モニタアプライアンスモジュールの概要 (Health Monitor Appliance Module Summary)] と [デバイス管理 (Device Management)] ページでアプライアンスが [無効 (Disabled)] として表示されます。アプライアンスのヘルス イベントのステータスは [無効 (Disabled)] です。

個別のアプライアンスのイベントとヘルス ステータスを [無効 (Disabled)] に設定する必要がある場合、アプライアンスをブラックリストに登録できます。ブラックリスト設定が有効になると、アプライアンスが [正常性モニタアプライアンスモジュールの概要 (Health Monitor Appliance Module Summary)] に [無効 (Disabled)] として表示され、アプライアンスのヘルス イベントのステータスが [無効 (Disabled)] になります。

マルチドメイン展開では、アプライアンスを先祖ドメインのブラックリストに登録すると、子孫ドメインもすべてブラックリストに登録されたことになります。子孫ドメインは、この設定の継承をオーバーライドし、ブラックリスト指定を解除できます。Firepower Management Center はグローバル レベルでのみブラックリスト指定できます。

### 手順

**ステップ 1** [システム (System)] > [ヘルス (Health)] > [ブラックリスト (Blacklist)] を選択します。

**ステップ 2** アプライアンスグループ、モデル、またはポリシーでリストをソートするには、右側にあるドロップダウンリストを使用します。

**ヒント** [正常性ポリシー (Health Policy)] 列の横にあるステータスアイコン (🟢) は、アプライアンスの現在のヘルス ステータスを示します。[システムポリシー (System Policy)] 列の横にあるステータスアイコン (🟢) は、Firepower Management Center とデバイス間の通信ステータスを示します。

**ステップ 3** 次の 2 つの選択肢があります。

- グループ、モデル、またはポリシーカテゴリ内のすべてのアプライアンスをブラックリストに登録するには、カテゴリのチェックボックスをオンにしてから、[選択したデバイスをブラックリストに登録 (Blacklist Selected Devices)] をクリックします。



- グループ、モデル、またはポリシーカテゴリ内のすべてのアプライアンスをブラックリストから除外するには、カテゴリのチェックボックスをオンにしてから、[選択したデバイスのブラックリスト指定を解除 (Clear Blacklist on Selected Devices)] をクリックします。

## 正常性ポリシー モジュールのブラックリスト登録

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint

アプライアンス上の個別の正常性ポリシーモジュールをブラックリストに登録できます。この操作により、モジュールからのイベントによってアプライアンスのステータスが **Warning** または **Critical** に変更されないようにすることができます。

ブラックリスト設定が有効になると、アプライアンスが [ブラックリスト (Blacklist)] ページと [アプライアンス正常性モニタモジュールステータスの概要 (Appliance Health Monitor Module Status Summary)] で [部分的なブラックリスト指定 (Partially Blacklisted)] または [すべてのモジュールがブラックリスト指定 (All Modules Blacklisted)] として表示されますが、メインの [アプライアンスのステータスの概要 (Appliance Status Summary)] ページでは展開されたビューにだけ表示されます。



### ヒント

個別にブラックリストに登録したモジュールを追跡して、必要に応じてそれらを再アクティブ化できるようにしてください。誤ってモジュールを無効にすると、必要な警告または重大メッセージを見逃す可能性があります。

マルチドメイン展開では、先祖ドメインの管理者は子孫ドメインの正常性モジュールをブラックリストに登録できます。しかし、子孫ドメインの管理者は、この先祖の設定をオーバーライドし、ドメインに適用されるポリシーのブラックリスト指定を解除できます。Firepower Management Center 正常性モジュールはグローバルレベルでのみブラックリスト指定できます。

### 手順

- ステップ 1** [システム (System)] > [ヘルス (Health)] > [ブラックリスト (Blacklist)] を選択します。
- ステップ 2** 変更するアプライアンスの横にある編集アイコン (🔧) をクリックします。
- ステップ 3** ブラックリスト指定する正常性ポリシーモジュールの横にあるチェックボックスをオンにします。一部のモジュールは特定のデバイスにのみ適用できます。詳細は [ヘルスモジュール \(276 ページ\)](#) を参照してください。
- ステップ 4** [保存 (Save)] をクリックします。

## ヘルス モニタ アラート

正常性ポリシー内のモジュールのステータスが変更された場合に電子メール、SNMP、またはシステム ログ経由で通知するアラートをセットアップできます。特定のレベルのヘルスイベントが発生したときにトリガーとして使用して警告するヘルスイベントレベルと既存のアラート応答を関連付けることができます。

たとえば、アプライアンスがハード ディスク スペースを使い果たす可能性を懸念している場合は、残りのディスクスペースが警告レベルに達したときに自動的に電子メールをシステム管理者に送信できます。ハードドライブがさらにいっぱいになる場合、ハードドライブが重大レベルに達したときに2つ目の電子メールを送信できます。

マルチドメイン展開では、現在のドメインで作成されたヘルスモニタのアラートのみを表示、および変更できます。

## ヘルス モニタ アラート情報

ヘルス モニタによって生成されるアラートには次の情報が含まれます。

- アラートの重大度レベルを示す [重大度 (Severity)]。
- テスト結果がアラートをトリガーとして使用したヘルス モジュールを示す [モジュール (Module)]。
- アラートをトリガーとして使用したヘルス テスト結果を含む [説明 (Description)]。

次の表で、これらの重大度レベルについて説明します。

表 29: アラートの重大度

重大度 (Severity)	説明
クリティカル (Critical)	ヘルステスト結果がクリティカルアラートステータスをトリガーとして使用する基準を満たしました。
警告	ヘルステスト結果が警告アラートステータスをトリガーとして使用する基準を満たしました。
標準	ヘルステスト結果が通常のアラートステータスをトリガーとして使用する基準を満たしました。
エラー (Error)	ヘルステストが実行されませんでした。
回復済み (Recovered)	ヘルステスト結果がクリティカルまたは警告のアラートステータスから通常のアラートステータスに戻るための基準を満たしました。

## ヘルス モニタ アラートの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ヘルス モニタ アラートを作成するときに、重大度レベル、ヘルス モジュール、およびアラート応答の関連付けを作成します。既存のアラートを使用することも、新しいアラートをシステムヘルスの報告専用を設定することもできます。選択したモジュールが重大度レベルに達すると、アラートがトリガーされます。

既存のしきい値と重複するようにしきい値を作成または更新すると、競合が通知されます。重複したしきい値が存在する場合、ヘルス モニタは最も少ないアラートを生成するしきい値を使用し、その他のしきい値を無視します。しきい値のタイムアウト値は、5～4,294,967,295 分の間にする必要があります。

マルチドメイン導入では、現在のドメインで作成されたヘルス モニタ アラートのみを表示および変更できます。

### 始める前に

- ヘルス アラートを送信する SNMP、syslog、電子メール サーバと Firepower Management Center との通信を制御するアラート応答を設定します。[Firepower Management Center アラート応答 \(2341 ページ\)](#) を参照してください。

### 手順

- ステップ 1** [システム (System)] > [ヘルス (Health)] > [モニタ アラート (Monitor Alerts)] を選択します。
- ステップ 2** [ヘルス アラート名 (Health Alert Name)] フィールドに、ヘルス アラートの名前を入力します。
- ステップ 3** [重大度 (Severity)] リストから、アラートをトリガーするために使用する重大度レベルを選択します。
- ステップ 4** [モジュール (Module)] リストから、アラートを適用する正常性ポリシー モジュールを選択します。
- ステップ 5** [アラート (Alert)] リストから、指定した重大度レベルに達したときにトリガーするアラート応答を選択します。
- ステップ 6** オプションで、[しきい値タイムアウト (Threshold Timeout)] フィールドに、それぞれのしきい値期間が終了してしきい値がリセットされるまでの分数を入力します。

ポリシーの実行時間間隔の値がしきい値タイムアウトの値より小さい場合でも、特定のモジュールから報告される2つのヘルスイベント間の間隔のほうが常に大きくなります。たとえば、しきい値タイムアウトを8分に変更し、ポリシーの実行時間間隔が5分である場合、報告されるイベント間の間隔は10分 (5×2) になります。

ステップ7 [保存 (Save) ]をクリックして、ヘルス アラートを保存します。

## ヘルス モニタ アラートの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

既存のヘルス モニタ アラートを編集して、ヘルス モニタ アラートに関連付けられた重大度レベル、ヘルス モジュール、またはアラート応答を変更できます。

マルチドメイン展開では、現在のドメインで作成されたヘルス モニタ アラートのみを表示および変更できます。

### 手順

- ステップ1 [システム (System) ] > [ヘルス (Health) ] > [モニタ アラート (Monitor Alerts) ]を選択します。
- ステップ2 [アクティブ ヘルス アラート (Active Health Alerts) ] リストから、変更するアラートを選択します。
- ステップ3 [ロード (Load) ] をクリックして、選択したアラートの構成済みの設定をロードします。
- ステップ4 必要に応じて設定を変更します。
- ステップ5 [保存 (Save) ] をクリックして、変更したヘルス アラートを保存します。  
アラート設定が正常に保存されたかどうかを示すメッセージが表示されます。

## ヘルス モニタ アラートの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

マルチドメイン導入では、現在のドメインで作成されたヘルス モニタ アラートのみを表示および変更できます。

### 手順

- ステップ1 [システム (System) ] > [ヘルス (Health) ] > [モニタ アラート (Monitor Alerts) ]を選択します。

**ステップ 2** 削除するアクティブなヘルス アラートを選択してから、[削除 (Delete)] をクリックします。

#### 次のタスク

- アラートが継続しないようにするには、元になるアラート応答を無効にするか、または削除します。[Firepower Management Center アラート応答 \(2341 ページ\)](#) を参照してください。

## ヘルス モニタの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst

ヘルス モニタには、Firepower Management Center によって管理されているすべてのデバイスに加えて、Firepower Management Center に関して収集されたヘルス ステータスが表示されます。ヘルス モニタは以下で構成されています。

- ステータステーブル：この Firepower Management Center の管理対象アプライアンスの台数が全体のヘルス ステータス別に表示されます。
- 円グラフ：それぞれのヘルス ステータス カテゴリにおけるアプライアンスの現在のパーセンテージを示します。
- アプライアンス リスト：管理対象デバイスのヘルス状態の詳細が表示されます。

マルチドメイン展開では、先祖ドメインのヘルスモニタに、すべての子孫ドメインからのデータが表示されます。子孫ドメインには、現在のドメインからのデータのみが表示されます。

#### 手順

**ステップ 1** [システム (System)] > [ヘルス (Health)] > [モニタ (Monitor)] を選択します。

**ステップ 2** テーブルの [ステータス (Status)] カラム内の該当するステータスまたは円グラフの該当する部分を選択して、そのステータスを持つアプライアンスをリストします。

**ヒント** ステータスレベルに関する行内の矢印が下向きの場合、そのステータスのアプライアンスリストが下側のテーブルに表示されます。矢印が右向きの場合、アプライアンス リストは非表示です。

**ステップ 3** 次の選択肢があります。

- アプライアンスのヘルス モニタを表示します ([アプライアンスヘルスモニタの表示 \(297 ページ\)](#) を参照)。



- ヘルス ポリシーを作成します (正常性ポリシーの作成 (285 ページ) を参照)。
- ヘルス モニタ アラートを作成します (ヘルス モニタ アラートの作成 (293 ページ) を参照)。

## ヘルス モニタ ステータスのカテゴリ

使用可能なステータス カテゴリを、重大度別に次の表に示します。

表 30:ヘルス ステータス インジケータ

ステータス レベル	ステータス アイコン	円グラフのステータスの色	説明
エラー (Error)		黒色	アプライアンス上の1つ以上のヘルス モニタリング モジュールで障害が発生し、それ以降、正常に再実行していないことを示します。テクニカル サポート 担当者に連絡して、ヘルス モニタリング モジュールの更新プログラムを入手してください。
クリティカル (Critical)		赤	アプライアンス上の1つ以上のヘルス モジュールが重大制限を超え、問題が解決されていないことを示します。
警告		黄色	アプライアンス上の1つ以上のヘルス モジュールが警告制限を超え、問題が解決されていないことを示します。
標準		グリーン	アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作していることを示します。

ステータス レベル	ステータス アイコン	円グラフのステータスの色	説明
回復済み (Recovered)		グリーン	アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作していることを示します。これには、前にクリティカルまたは警告状態だったモジュールも含まれます。
無効		青	アプライアンスが無効またはブラックリストに登録されている、アプライアンスに正常性ポリシーが適用されていない、またはアプライアンスが現在到達不能になっていることを示します。

## アプライアンス ヘルス モニタの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst

アプライアンス ヘルス モニタは、アプライアンスのヘルス ステータスの詳細ビューを提供します。

マルチドメイン展開では、子孫ドメインのアプライアンスのヘルス ステータスを表示できません。



### ヒント

通常は、非活動状態が1時間（または設定された他の時間間隔）続くと、ユーザはセッションからログアウトされます。ヘルスステータスを長期間受動的に監視する予定の場合は、一部のユーザのセッションタイムアウトの免除、またはシステム タイムアウト設定の変更を検討してください。詳細については、[ユーザアカウント ログイン オプション \(89 ページ\)](#) と [セッションタイムアウトの設定 \(986 ページ\)](#) を参照してください。

### 手順

**ステップ 1** [システム (System)] > [ヘルス (Health)] > [モニタ (Monitor)] を選択します。

**ステップ 2** アプライアンス リストを展開します。特定のステータスを持つアプライアンスを表示するには、そのステータス行内の矢印をクリックします。または、[アプライアンス ステータスの概要 (Appliance Status Summary)] グラフで、表示するアプライアンス ステータス カテゴリの色をクリックします。

**ヒント** ステータスレベルに関する行内の矢印が下向きの場合は、そのステータスのアプライアンスリストが下側のテーブルに表示されます。矢印が右向きの場合、アプライアンス リストは非表示です。

**ステップ 3** アプライアンス リストの [アプライアンス (Appliance)] 列で、詳細を表示するアプライアンスの名前をクリックします。

**ヒント** [モジュールステータスの概要 (Module Status Summary)] グラフで、そのステータス カテゴリの [アラート詳細 (Alert Details)] の表示を切り替えるには、イベントステータス カテゴリの色をクリックします。

#### 次のタスク

- アプライアンスのすべてのヘルス モジュールを実行する場合、次を参照してください。[アプライアンスのすべてのモジュールの実行 \(298 ページ\)](#)
- アプライアンスの特定のヘルス モジュールを実行する場合、次を参照してください。[特定のヘルス モジュールの実行 \(299 ページ\)](#)
- アプライアンスのヘルス モジュール アラート グラフを生成する場合、次を参照してください。[ヘルス モジュール アラート グラフの生成 \(300 ページ\)](#)
- アプライアンスのトラブルシューティングファイルを生成する場合、次を参照してください。[高度なトラブルシューティング ファイルのダウンロード \(334 ページ\)](#)
- アプライアンスの高度なトラブルシューティングファイルを生成する場合、次を参照してください。[高度なトラブルシューティング ファイルのダウンロード \(334 ページ\)](#)
- Firepower Management Center Web インターフェイスから Firepower Threat Defense CLI コマンドを実行する場合、次を参照してください。[Web インターフェイスからの Firepower Threat Defense CLI の使用 \(335 ページ\)](#)

## アプライアンスのすべてのモジュールの実行

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst



ヘルス モジュール テストは、正常性ポリシーの作成時に設定されたポリシー実行時間間隔で自動的に実行されます。ただし、アプライアンスの最新の正常性情報を収集するためにすべてのヘルス モジュール テストをオンデマンドで実行することもできます。

マルチドメイン展開では、現在のドメイン内のアプライアンスと、子孫ドメイン内のアプライアンスに対してヘルス モジュール テストを実行できます。

### 手順

- ステップ 1** アプライアンスのヘルス モニタを表示します。[アプライアンスヘルス モニタの表示 \(297ページ\)](#) を参照してください。
- ステップ 2** [すべてのモジュールの実行 (Run All Modules)] をクリックします。ステータス バーにテストの進捗状況が表示されてから、[ヘルス モニタ アプライアンス (Health Monitor Appliance)] ページが更新されます。

(注) ヘルス モジュールを手動で実行した場合は、自動的に発生する最初の更新に、手動で実行したテストの結果が反映されないことがあります。手動で直前に実行したモジュールの値が変更されていない場合は、数秒待ってから、デバイス名をクリックしてページを更新してください。ページが自動的に再び更新されるまで待機していてもかまいません。

## 特定のヘルス モジュールの実行

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst

ヘルス モジュール テストは、正常性ポリシーの作成時に設定されたポリシー実行時間間隔で自動的に実行されます。ただし、そのモジュールの最新のヘルス情報を収集するためにヘルス モジュール テストをオンデマンドで実行することもできます。

マルチドメイン展開では、現在のドメイン内のアプライアンスと、子孫ドメイン内のアプライアンスに対してヘルス モジュール テストを実行できます。

### 手順

- ステップ 1** アプライアンスのヘルス モニタを表示します。[アプライアンスヘルス モニタの表示 \(297ページ\)](#) を参照してください。
- ステップ 2** [モジュール ステータスの概要] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

**ステップ3** イベントのリストを表示するアラートの [アラート詳細 (Alert Detail) ] 行で、[実行 (Run) ] をクリックします。

ステータスバーにテストの進捗状況が表示されてから、[ヘルス モニタ アプライアンス (Health Monitor Appliance) ] ページが更新されます。

(注) ヘルス モジュールを手動で実行した場合は、自動的に発生する最初の更新に、手動で実行したテストの結果が反映されないことがあります。直前に手動で実行したモジュールの値が変更されていない場合は、数秒待ってから、デバイス名をクリックしてページを更新してください。ページが再び自動的に更新されるまで待機していてもかまいません。

## ヘルス モジュール アラート グラフの生成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst

特定のアプライアンスの特定のヘルス テストの一定期間にわたる結果をグラフ化できます。

### 手順

**ステップ1** アプライアンスのヘルス モニタを表示します ([アプライアンスヘルス モニタの表示 \(297ページ\)](#) を参照)。

**ステップ2** [ヘルス モニタ アプライアンス (Health Monitor Appliance) ] ページの [モジュール ステータスの概要 (Module Status Summary) ] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

**ステップ3** イベントのリストを表示するアラートの [アラート詳細 (Alert Detail) ] 行で、[グラフ (Graph) ] をクリックします。

**ヒント** イベントが1つも表示されない場合は、時間範囲を調整することを考慮してください。

## ヘルス イベント ビュー

[ヘルス イベント ビュー (Health Event View) ] ページでは、ヘルス モニタがログに記録したヘルス イベントを、Firepower Management Center ログ ヘルス イベントで表示できます。完全にカスタマイズ可能なイベント ビューを使用すれば、ヘルス モニタによって収集されたヘル

スステータス イベントを迅速かつ容易に分析できます。イベント データを検索して、調査中のイベントに関係する可能性のある他の情報に簡単にアクセスしたりできます。ヘルスマジュールごとにテストされる条件を理解していれば、ヘルスイベントに対するアラートをより効率的に設定できます。

ヘルスイベント ビュー ページで多くの標準イベント ビュー機能を実行できます。

## ヘルスイベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst

[ヘルスイベントのテーブルビュー (Table View of Health Events)] ページには、指定したアプライアンス上のすべてのヘルスイベントのリストが表示されます。

Firepower Management Center 上の [ヘルスマニタ (Health Monitor)] ページからヘルスイベントにアクセスした場合は、すべての管理対象アプライアンスのすべてのヘルスイベントが表示されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。



### ヒント

このビューをブックマークすれば、イベントの [ヘルスイベント (Health Events)] テーブルを含むヘルスイベントワークフロー内のページに戻ることができます。ブックマークしたビューには、現在見ている時間範囲内のイベントが表示されますが、必要に応じて時間範囲を変更してテーブルを最新情報で更新することができます。

### 手順

[システム (System)] > [ヘルス (Health)] > [イベント (Events)] を選択します。

ヒント ヘルスイベントのテーブルビューが含まれていないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) (switch workflow)] をクリックします。[ワークフローの選択 (Select Workflow)] ページで、[ヘルスイベント (Health Events)] をクリックします。

(注) イベントが1つも表示されない場合は、時間範囲を調整することを考慮してください。

## モジュールとアプライアンス別のヘルス イベントの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst

### 手順

- 
- ステップ 1** アプライアンスのヘルス モニタを表示します ([アプライアンスヘルスモニタの表示 \(297ページ\)](#) を参照)。
- ステップ 2** [モジュール ステータスの概要 (Appliance Status Summary)] グラフで、表示するイベント ステータス カテゴリの色をクリックします。
- [アラート詳細 (Alert Detail)] リストで、表示を切り替えてイベントを表示または非表示にします。
- ステップ 3** イベントのリストを表示するアラートの [アラート詳細 (Alert Detail)] 行で、[イベント (Events)] をクリックします。
- [ヘルス イベント (Health Events)] ページが開いて、制限としてアプライアンスの名前と指定したヘルス アラート モジュールの名前を含むクエリーの結果が表示されます。イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。
- ステップ 4** 指定したアプライアンスのすべてのステータスイベントを表示する場合は、[検索制約 (Search Constraints)] を展開し、[モジュール名 (Module Name)] 制限をクリックして削除します。
- 

## ヘルス イベント テーブルの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

- 
- ステップ 1** [システム (System)] > [ヘルス (Health)] > [イベント (Events)] を選択します。
- ステップ 2** 次の選択肢があります。

- **ブックマーク**：すぐに現在のページに戻れるように、現在のページをブックマークするには、[このページのブックマーク (Bookmark This Page)] をクリックしてブックマークの名前を指定し、[保存 (Save)] をクリックします。
- **ワークフローの変更**：別のヘルスイベントワークフローを選択するには、[(ワークフローの切り替え) ((switch workflow))] をクリックします。
- **イベントの削除**：ヘルスイベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして、[削除 (Delete)] をクリックします。現在の制約されているビューですべてのイベントを削除するには、[すべて削除 (Delete All)] をクリックしてから、すべてのイベントを削除することを確認します。
- **レポートの生成**：テーブルビューのデータに基づいてレポートを生成するには、[レポートデザイナー (Report Designer)] をクリックします。
- **変更**：ヘルス テーブル ビューに表示されるイベントの時刻と日付範囲を変更します。イベントビューを時間によって制約している場合は、(グローバルかイベントに固有に関係なく) アプライアンスに設定されている時間枠の範囲外で生成されたイベントがイベントビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。
- **移動**：イベント ビュー ページを使用して移動します。
- **ブックマークの移動**：ブックマーク管理ページに移動するには、任意のイベントビューから [ブックマークの表示 (View Bookmarks)] をクリックします。
- **その他に移動**：他のイベント テーブルに移動して関連イベントを表示します。
- **ソート**：表示されたイベントをソートする、イベントテーブルに表示するカラムを変更する、または表示するイベントを制約します。
- **すべて表示**：すべてのイベントのイベントの詳細をビューに表示するには、[すべて表示 (View All)] をクリックします。
- **詳細の表示**：単一のヘルスイベントに関連付けられる詳細を表示するには、イベントの左側にある下矢印のリンクをクリックします。
- **複数表示**：複数のヘルスイベントのイベント詳細を表示するには、詳細を表示するイベントに対応する行の横にあるチェックボックスをオンにして、[表示 (View)] をクリックします。
- **ステータスの表示**：特定のステータスのすべてのイベントを表示するには、そのステータスのイベントの [ステータス (Status)] カラムのステータスアイコンをクリックします。

## 7000 および 8000 シリーズ デバイスのハードウェア アラートの詳細



- (注) 8350 ハードウェアプラットフォームには6つのファンがあり、FAN2～FAN7と表示されています。これは想定されている動作です。8350プラットフォームでFAN1またはファンの番号付けに関するハードウェアアラートを受け取った場合は、アラートを無視できます。

表 31: 7000 および 8000 シリーズ デバイスの監視対象条件

監視対象条件	黄色または赤色エラー状態の原因
デバイスの高可用性ステータス	高可用性ペアの 7000 または 8000 シリーズ デバイスが相互に通信していない（ケーブル配線の問題などで）場合は、ハードウェアアラーム モジュールが赤色に変化します。
ftwo デーモン ステータス	ftwo デーモンがダウンすると、ハードウェアアラーム モジュールのヘルスステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
検出された NFE カード	システム上で検出された NFE カードの枚数を示します。この値がアプライアンスの予想 NFE カウントと一致しない場合は、ハードウェアアラーム モジュールが赤色に変化します。
NFE ハードウェア ステータス	1 つ以上の NFE カードが通信していない場合は、ハードウェアアラーム モジュールが赤色に変化し、該当するカードがメッセージ詳細に表示されます。
NFE ハートビート	システムが NFE ハートビートを検出しなかった場合は、ハードウェアアラーム モジュールが赤色に変化し、メッセージ詳細に関連カードへの参照が追加されます。
NFE 内部リンク ステータス	NMSB カードと NFE カード間のリンクがダウンした場合は、ハードウェアアラーム モジュールが赤色に変化し、メッセージ詳細に関連ポートへの参照が追加されます。
NFE メッセージデーモン	NFE メッセージデーモンがダウンすると、ハードウェアアラーム モジュールのヘルスステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。

監視対象条件	黄色または赤色エラー状態の原因
NFE 温度	<p>NFE 温度が 97 °C を超えると、ハードウェアアラームモジュールのヘルスステータスが黄色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。</p> <p>NFE 温度が 102 °C を超えると、ハードウェアアラームモジュールのヘルスステータスが赤色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。</p>
NFE 温度ステータス	<p>特定の NFE カードの現在の温度ステータスを示します。OK の場合ハードウェアアラームモジュールは緑色を、警告の場合は黄色を、クリティカルの場合は赤色（および該当する場合は NFE カード番号）を示します。</p>
NFE TCAM デーモン	<p>NFE TCAM デーモンがダウンすると、ハードウェアアラームモジュールのヘルスステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。</p>
nfm_ipfragd (ホスト フラグ) デーモン	<p>nfm_ipfragd デーモンがダウンすると、ハードウェアアラームモジュールのヘルスステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。</p>
NFE プラットフォーム デーモン	<p>NFE プラットフォーム デーモンがダウンすると、ハードウェアアラームモジュールのヘルスステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。</p>
NMSB コミュニケーション	<p>メディアアセンブリが存在しないか、通信していない場合は、ハードウェアアラームモジュールのヘルスステータスが赤色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。</p>

監視対象条件	黄色または赤色エラー状態の原因
psls デーモン ステータス	psls デーモンがダウンすると、ハードウェアアラームモジュールのヘルスステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
Rulesd (ホストルール) デーモン	Rulesd デーモンがダウンすると、ハードウェアアラームモジュールのヘルスステータスが黄色に変化し、メッセージ詳細にデーモンへの参照 (および該当する場合は NFE カード番号) が追加されます。
scmd デーモン ステータス	scmd デーモンがダウンすると、ハードウェアアラームモジュールのヘルスステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。

## [ヘルスイベント (Health Events)] テーブル

正常性ポリシー内で有効にされたヘルスマニタモジュールが、さまざまなテストを実行してアプライアンスのヘルスステータスを特定します。ヘルスステータスが指定された基準を満たしている場合は、ヘルスイベントが生成されます。

次の表で、ヘルスイベントテーブルで表示および検索できるフィールドについて説明します。

表 32: ヘルスイベントフィールド

フィールド	説明
モジュール名 (Module Name)	表示するヘルスイベントを生成したモジュールの名前を指定します。たとえば、CPU パフォーマンスを測定するイベントを表示するには、「CPU」と入力します。検索によって、該当する CPU 使用率イベントと CPU 温度イベントが取得されます。
テスト名 (Test Name) (検索専用)	イベントを生成したヘルスマニタモジュールの名前。
時刻 (Time) (検索専用)	ヘルスイベントのタイムスタンプ。



フィールド	説明
説明	イベントを生成したヘルスマジュールの説明。 たとえば、プロセスが実行できない場合に生成されるヘルスイベントには「Unable to Execute」というラベルが付けられます。
値	イベントが生成されたヘルステストから得られた結果の値 (単位数)。  たとえば、監視対象デバイスが 80% 以上の CPU リソースを使用しているときに生成されるヘルスイベントを Firepower Management Center が生成した場合の値は 80 ~ 100 です。
単位	結果の単位記述子。アスタリスク (*) を使用してワイルドカード検索を作成できます。  たとえば、監視対象デバイスが 80% 以上の CPU リソースを使用しているときに生成されるヘルスイベントを Firepower Management Center が生成した場合の単位記述子はパーセント記号 (%) です。
ステータス (Status)	アプライアンスに報告されるステータス ([クリティカル (Critical) ]、[黄色 (Yellow) ]、[緑色 (Green) ]、または [無効 (Disabled) ])。
ドメイン (Domain)	管理対象デバイスによって報告されたヘルスイベントの場合は、ヘルスイベントを報告したデバイスのドメイン。Firepower Management Center によって報告されたヘルスイベントの場合は、Global。このフィールドは、マルチドメイン展開の場合にのみ存在します。
Device	ヘルスイベントが報告されたアプライアンス。

■ [ヘルスイベント (Health Events)] テーブル



## 第 13 章

# システムのモニタリング

以下のトピックでは、Firepower システムをモニタする方法を示します。

- システム統計 (309 ページ)
- システム統計が使用できるアプライアンス (309 ページ)
- [ホスト統計情報 (Host Statistics) ]セクション (310 ページ)
- [ディスク使用量 (Disk Usage) ]セクション (311 ページ)
- [プロセス (Processes) ]セクション (311 ページ)
- [SFDataCorrelator プロセス統計情報 (SFDataCorrelator Process Statistics) ]セクション (319 ページ)
- [侵入イベント情報 (Intrusion Event Information) ]セクション (320 ページ)
- システム統計情報の表示 (320 ページ)

## システム統計

Firepower システム Web インターフェイスの [統計情報 (Statistics) ] ページには、アプライアンスの現在の一般的ステータスに関する統計情報 (ディスク使用量とシステム プロセス)、データ コリレータ統計情報、侵入イベント情報が表示されます。

Firepower Management Center と 7000 & 8000 シリーズ デバイスの両方に関するシステム統計情報を確認できます。

## システム統計が使用できるアプライアンス

Web インターフェイスにシステム統計が用意されているアプライアンスは以下の通りです。

統計情報の種類	統計ページのセクション	Management Center	7000 & 8000 シリーズ デバイス
ホスト統計情報	[ホスト統計情報 (Host Statistics) ]セクション (310 ページ)	Yes	Yes

統計情報の種類	統計ページのセクション	Management Center	7000 & 8000 シリーズ デバイス
システムステータス とディスク使用量	[ディスク使用量 (Disk Usage) ]セクション (311 ページ)	Yes	Yes
システム プロセス ステータス	[プロセス (Processes) ]セク ション (311 ページ)	Yes	Yes
データ コリレータ 統計	[SFDataCorrelator プロセス統計 情報 (SFDataCorrelator Process Statistics) ]セクション (319 ページ)	Yes	No
侵入イベント統計	[侵入イベント情報 (Intrusion Event Information) ]セクショ ン (320 ページ)	Yes	No

## [ホスト統計情報 (Host Statistics) ]セクション

次の表に、[統計情報 (Statistics) ] ページにリストされるホスト統計情報を示します。

表 33: ホスト統計情報 (Host Statistics)

カテゴリ (Category)	説明
時刻 (Time)	システムの現在の時刻。
Uptime (アップタイム)	システムが前回起動してから経過した日数 (該当する場合)、時間数、および分数。
メモリ使用率 (Memory Usage)	使用中のシステム メモリの割合。
負荷平均 (Load Average)	直前の 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数。
ディスク使用率 (Disk Usage)	使用中のディスクの割合。詳細なホスト統計情報を表示するには、矢印をクリックします。
プロセス (Processes)	システムで実行されているプロセスの概要。

## [ディスク使用量 (Disk Usage) ]セクション

[統計情報 (Statistics) ]ページの [ディスク使用率 (Disk Usage) ]セクションは、カテゴリ別およびパーティションステータス別に、ディスク使用量のクイック概要を示します。マルウェア ストレージパックがデバイスにインストールされている場合、そのパーティションステータスも確認できます。このページを定期的にモニタして、システムプロセスおよびデータベースで十分なディスク領域が使用可能であることを確認できます。



**ヒント** Firepower Management Center で、ヘルス モニタを使用して、ディスク使用状況を監視し、ディスク容量不足の状態をアラートすることもできます。

## [プロセス (Processes) ]セクション

[統計情報 (Statistics) ]ページの [プロセス (Processes) ]セクションでは、アプライアンスで現在実行中のプロセスを表示できます。これは、一般的なプロセス情報と、実行中の各プロセスに固有の情報を提供します。Firepower Management Center の Web インターフェイスを使用すると、管理対象デバイスのプロセスのステータスを表示できます。

アプライアンスで実行されるプロセスには、デーモンと実行可能ファイルの2種類があることに注意してください。デーモンは常に実行され、実行可能ファイルは必要に応じて実行されます。

### プロセス使用状況フィールド

統計情報ページのプロセス セクションを展開すると、以下を表示できます。

#### [CPU (Cpu(s) ]

次の CPU 使用状況情報がリストされます：

- ユーザ プロセスの使用状況の割合
- システム プロセスの使用状況の割合
- nice 使用状況の割合 (高い優先度を示す、負の nice 値を持つプロセスの CPU 使用状況)。 nice 値は、システム プロセスのスケジュールされた優先度を示しており、-20 (最も高い優先度) から 19 (最も低い優先度) の範囲の値になります。
- アイドル状態の使用状況の割合

#### [メモリ (Mem) ]

以下のメモリ使用状況情報がリストされます。

- メモリ内の合計キロバイト数
- メモリ内の使用キロバイト数の合計
- メモリ内の空きキロバイト数の合計
- メモリ内のバッファに書き出されたキロバイト数の合計

### [切替 (Swap) ]

以下のスワップ使用状況情報がリストされます。

- スワップ内の合計キロバイト数
- スワップ内の使用キロバイト数の合計
- スワップ内の空きキロバイト数の合計
- スワップ内のキャッシュされたキロバイト数の合計

次の表に、プロセス セクションに表示される各列を示します。

表 34: プロセスリストカラム

カラム (Column)	説明
Pid	プロセス ID 番号
[ユーザ名 (Username) ]	プロセスを実行しているユーザまたはグループの名前
Pri	プロセスの優先度
Nice	<i>nice</i> 値。プロセスのスケジューリング優先度を示す値です。値は -20 (最も高い優先度) から 19 (最も低い優先度) までの範囲になります。
Size	プロセスで使用されるメモリ サイズ (値の後ろにメガバイトを表す m がない場合はキロバイト単位)
Res	メモリ内の常駐ページング ファイルの量 (値の後ろにメガバイトを表す m がない場合はキロバイト単位)

カラム (Column)	説明
State	<p>プロセスの状態 :</p> <ul style="list-style-type: none"> <li>• D : プロセスが中断不能スリープ状態 (通常は入出力) にある</li> <li>• N : プロセスの nice 値が正の値</li> <li>• R : プロセスが実行可能である (実行するキュー上で)</li> <li>• S : プロセスがスリープモードにある</li> <li>• T : プロセスがトレースまたは停止されている</li> <li>• W : プロセスがページングしている</li> <li>• X : プロセスがデッド状態である</li> <li>• Z : プロセスが機能していない</li> <li>• &lt; : プロセスの nice 値が負の値</li> </ul>
時刻 (Time)	プロセスが実行されてきた時間の長さ (時間数:分数:秒数)
Cpu	プロセスが使用している CPU の割合
コマンド (Command)	プロセスの実行可能ファイル名

#### 関連トピック

[システム デーモン \(313 ページ\)](#)

[実行可能ファイルおよびシステム ユーティリティ \(315 ページ\)](#)

## システム デーモン

デーモンは、アプライアンスで継続的に実行されます。これにより、サービスが使用可能になり、必要に応じてプロセスが生成されるようになります。次の表では、[プロセスのステータス (Process Status) ] ページに表示されるデーモンをリストし、その機能について簡単に説明しています。



(注) 次の表は、アプライアンスで実行される可能性があるすべてのプロセスの包括的なリストではありません。

表 35: システム デーモン

デーモン	説明
crond	スケジュールされたコマンド (cron ジョブ) の実行を管理します
dhclient	ダイナミック ホスト IP アドレッシングを管理します
fpcollect	クライアントとサーバのフィンガープリントの収集を管理します
httpd	HTTP (Apache Web サーバ) プロセスを管理します
httpsd	HTTPS (SSL を使用した Apache Web サーバ) サービスを管理し、SSL および有効な証明書の認証が機能しているかチェックし、アプリケーションへの安全な Web アクセスを提供するためにバックグラウンドで実行します
keventd	Linux カーネルのイベント通知メッセージを管理します
klogd	Linux カーネルメッセージのインターセプションおよびロギングを管理します
kswapd	Linux カーネルのスワップ メモリを管理します
kupdated	ディスクの同期を実行する、Linux カーネルの更新プロセスを管理します
mysqld	データベース プロセスを管理します
ntpd	Network Time Protocol (NTP) プロセスを管理します
午後	すべての Firepower システム プロセスを管理し、必要なプロセスを始動し、予期せず失敗したプロセスをすべて再始動します
reportd	レポートを管理します
safe_mysqld	データベースのセーフ モード運用を管理し、エラーが発生した場合にはデータベース デーモンを再始動し、ランタイム情報をファイルに記録します



デーモン	説明
SFDataCorrelator	データ転送を管理します
sfstreamer (Management Center のみ)	Event Streamer を使用するサードパーティ製クライアント アプリケーションへの接続を管理します
sfmgr	アプライアンスへの sftunnel 接続を使用して、リモートでアプライアンスを管理および設定するための RPC サービスを提供します
SFRemediated (Management Center のみ)	修復応答を管理します
sftimeserviced (Management Center のみ)	時間同期メッセージを管理対象デバイスに転送します
sfmbservice	アプライアンスへの sftunnel 接続を使用して、リモート アプライアンスで実行されている sfmb メッセージブローカプロセスへのアクセスを提供します。現在、ヘルス モニタリングでのみ使用されており、管理対象デバイスから Firepower Management Center へ正常なイベントやアラートを送信します。
sftroughd	着信ソケットで接続をリッスンしてから、正しい実行可能ファイル (通常は、Cisco メッセージブローカ sfmb) を呼び出して要求を処理します
sftunnel	リモート アプライアンスとの通信を必要とするすべてのプロセスに対し、安全な通信チャネルを提供します。
sshd	セキュア シェル (SSH) プロセスを管理し、アプライアンスへの SSH アクセスを提供するためにバックグラウンドで実行します
syslogd	システム ロギング (syslog) プロセスを管理します

## 実行可能ファイルおよびシステム ユーティリティ

システム上には、他のプロセスまたはユーザ操作によって実行される実行可能ファイルが数多く存在します。次の表に、[プロセス ステータス (Process Status)] ページで表示される実行可能ファイルについて説明します。

表 36: システムの実行可能ファイルおよびユーティリティ

実行可能ファイル	説明
awk	awk プログラミング言語で作成されたプログラムを実行するユーティリティ
bash	GNU Bourne-Again シェル
cat	ファイルを読み取り、コンテンツを標準出力に書き込むユーティリティ
chown	ユーザおよびグループのファイル権限を変更するユーティリティ
chsh	デフォルトのログイン シェルを変更するユーティリティ
SFDataCorrelator (Management Center のみ)	システムで作成されるバイナリ ファイルを分析し、イベント、接続データ、およびネットワーク マップを生成します。
cp	ファイルをコピーするユーティリティ
df	アプライアンスの空き領域の量をリストするユーティリティ
エコー	コンテンツを標準出力に書き込むユーティリティ
egrep	指定された入力を、ファイルおよびフォルダで検索するユーティリティ。標準grepでサポートされていない正規表現の拡張セットをサポートします
検索	指定された入力のディレクトリを再帰的に検索するユーティリティ
grep	指定された入力をファイルとディレクトリで検索するユーティリティ
halt	サーバを停止するユーティリティ
httpsdctl	セキュアな Apache Web プロセスを処理する
hwclock	ハードウェア クロックへのアクセスを許可するユーティリティ

実行可能ファイル	説明
ifconfig	ネットワーク構成実行可能ファイルを示します。MACアドレスが常に一定になるようにします
iptables	[アクセス権の設定 (Access Configuration) ] ページに加えられた変更に基づいてアクセス制限を処理します。
iptables-restore	iptables ファイルの復元を処理します
iptables-save	iptables に対する保存済みの変更を処理します
kill	セッションおよびプロセスを終了するために使用できるユーティリティ
killall	すべてのセッションおよびプロセスを終了するために使用できるユーティリティ
ksh	Korn シェルのパブリック ドメインバージョン
ロガー	コマンドラインから syslog デーモンにアクセスする方法を提供するユーティリティ
md5sum	指定したファイルのチェックサムとブロック数を印刷するユーティリティ
mv	ファイルを移動 (名前変更) するユーティリティ
myisamchk	データベース テーブルの検査および修復を示します
mysql	データベース プロセスを示します。複数のインスタンスが表示されることがあります
openssl	認証証明書の作成を示します
perl	perl プロセスを示します
ps	標準出力にプロセス情報を書き込むユーティリティ
sed	1 つ以上のテキスト ファイルの編集に使用されるユーティリティ

実行可能ファイル	説明
sfheartbeat	アプライアンスがアクティブであることを示す、ハートビートブロードキャストを識別します。ハートビートはデバイスと Firepower Management Center の間の接続を維持するために使用されます
sfmb	メッセージブローカ プロセスを示します。Firepower Management Center とデバイスとの間の通信を処理します。
sh	Korn シェルのパブリック ドメインバージョン
shutdown	アプライアンスをシャットダウンするユーティリティ
sleep	指定された秒数のあいだプロセスを中断するユーティリティ
smtpclient	電子メールイベント通知機能が有効な場合に、電子メール送信を処理するメールクライアント
snmptrap	SNMP 通知機能が有効な場合に、指定された SNMP トラップサーバに SNMP トラップデータを転送します
snort	Snort が動作していることを示します
ssh	アプライアンスへのセキュア シェル (SSH) 接続を示します
sudo	sudo プロセスを示します。これにより、admin 以外のユーザが実行可能ファイルを実行できるようになります
top	上位の CPU プロセスに関する情報を表示するユーティリティ
touch	指定したファイルへのアクセス時刻や変更時刻を変更するために使用できるユーティリティ
vim	テキストファイルの編集に使用されるユーティリティ
wc	指定したファイルの行、ワード、バイトのカウントを実行するユーティリティ

## 関連トピック

[システムのアクセス リストの設定 \(958 ページ\)](#)

## [SFDataCorrelator プロセス統計情報 (SFDataCorrelator Process Statistics) ]セクション

Firepower Management Center では、現在の日付のデータ コリレータとネットワーク検出プロセスに関する統計情報を表示できます。管理対象デバイスがデータの取得、復号化、および分析を実行する際に、ネットワーク検出プロセスはデータをフィンガープリントおよび脆弱性データベースと関連付けてから、Firepower Management Center で実行中のデータ コリレータで処理されるバイナリ ファイルを生成します。データ コリレータはバイナリ ファイルの情報を分析し、イベントを生成し、ネットワーク マップを作成します。

ネットワーク検出とデータ コリレータに表示される統計情報は、デバイスごとに 0:00 から 23:59 までの間に収集された統計情報を使用した、当日の平均です。

次の表に、データ コリレータ プロセスに表示される統計情報を示します。

表 37: データ コリレータ プロセスの統計情報

カテゴリ (Category)	説明
イベント/秒 (Events/Sec)	データ コリレータが受信し処理する検出イベントの 1 秒当たりの数
接続/秒 (Connections/Sec)	データ コリレータが受信し処理する接続の 1 秒当たりの数
CPU 使用率 — ユーザ (%) (CPU Usage — User (%))	当日のユーザプロセスで使用される CPU 時間の平均割合
CPU 使用率 — システム (%) (CPU Usage — System (%))	当日のシステムプロセスで使用される CPU 時間の平均割合
VmSize (KB)	当日のデータ コリレータに割り当てられたメモリの平均サイズ (キロバイト単位)
VmRSS (KB)	当日のデータ コリレータで使用されるメモリの平均量 (キロバイト単位)

## [侵入イベント情報 (IntrusionEventInformation)] セクション

Firepower Management Center デバイスと管理対象デバイスのどちらでも、[統計情報 (Statistics)] ページで、侵入イベントに関するサマリ情報を確認できます。表示される情報には、前回の侵入イベントの日時、過去 1 時間および過去 1 日に発生したイベントの合計数、データベース内のイベントの合計数などがあります。



(注) [統計情報 (Statistics)] ページの [侵入イベント情報 (Intrusion Event Information)] セクションにある情報は、Firepower Management Center に送信された侵入イベントではなく、管理対象デバイスに保存されている侵入イベントに基づいています。管理対象デバイスが侵入イベントをローカルに格納できない（または格納しないように設定されている）場合、侵入イベント情報はこのページに表示されません。

次の表に、[統計情報 (Statistics)] ページの [侵入イベント情報 (Intrusion Event Information)] セクションに表示される統計情報を示します。

表 38: 侵入イベント情報 (Intrusion Event Information)

統計	説明
前回のアラート (Last Alert Was)	前回のイベントが発生した日時
過去 1 時間のイベントの合計 (Total Events Last Hour)	過去 1 時間に発生したイベントの合計数
過去 1 日のイベントの合計 (Total Events Last Day)	過去 24 時間に発生したイベントの合計数
データベース内のイベントの合計 (Total Events in Database)	イベント データベース内のイベントの合計数

## システム統計情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin/Maint
脅威 (侵入イベント データ用)	保護 (侵入イベント データ用)			

Firepower Management Center では、Web インターフェイスはアプライアンスとその管理対象となるすべてのデバイスの統計情報を表示します。7000 および 8000 シリーズ デバイスでは、システムはそのデバイスの統計情報のみを表示します。

## 手順

- 
- ステップ 1** [システム (System)] > [モニタリング (Monitoring)] > [統計 (Statistics)] を選択します。
- ステップ 2** 必要に応じ、Firepower Management Center で、[デバイスの選択 (Select Device(s))] リストからデバイスを選択し、[デバイスの選択 (Select Devices)] をクリックします。
- ステップ 3** 使用可能な統計を表示します ([システム統計が使用できるアプライアンス \(309 ページ\)](#) を参照)。
- ステップ 4** オプションで、[ディスク使用率 (Disk Usage)] セクションで以下を実行できます。
- [カテゴリ別 (By Category)] 積み上げ横棒で、ディスク使用量カテゴリの上にポインタを移動すると、以下が (順番に) 表示されます。
    - そのカテゴリが使用する使用可能なディスク領域の割合
    - ディスク上の実際のストレージ領域
    - そのカテゴリで使用可能なディスク領域の合計
  - [パーティション別 (By Partion)] の横にある下矢印をクリックして展開します。マルウェア ストレージ パックがインストールされている場合は、`/var/storage` パーティションの使用状況が表示されます。
- ステップ 5** オプションで、[プロセス (Processes)] の横にある矢印をクリックすると、[プロセス使用状況 フィールド \(311 ページ\)](#) で説明されている情報が表示されます。
-







## 第 14 章

# システムのトラブルシューティング




以下のトピックは、Firepower システムで発生する可能性のある問題を診断する方法について説明します。

- [システム メッセージ \(323 ページ\)](#)
- [システム メッセージの管理 \(327 ページ\)](#)
- [トラブルシューティング用のヘルス モニタ レポート \(332 ページ\)](#)
- [Web インターフェイスからの Firepower Threat Defense CLI の使用 \(335 ページ\)](#)
- [機能固有のトラブルシューティング \(336 ページ\)](#)

## システム メッセージ

Firepower システムで発生した問題を突き止める必要がある場合、調査の出発点となるのはメッセージセンターです。メッセージセンターでは、Firepower システムがシステムのアクティビティとステータスに関して継続的に生成するメッセージを表示できます。

メッセージセンターを開くには、メインメニューの[展開 (Deploy)] ボタンの右隣にある[システム ステータス (System Status)] アイコンをクリックします。このアイコンは、システムの状態によって以下のように表示されます。

-  : 1 つ以上のエラーと任意の数の警告がシステム上に存在することを示します。
-  : 1 つ以上の警告がシステム上に存在することを示します。エラーは発生していません。
-  : 警告とエラーはいずれもシステム上に存在していないことを示します。

アイコンに数字が表示されている場合、その数字は現在のエラー メッセージまたは警告メッセージの数を示します。

メッセージセンターを閉じるには、Firepower システム Web インターフェイス内でメッセージセンターの外側をクリックします。

メッセージセンターに加え、Web インターフェイスには、ユーザのアクティビティおよび進行中のシステムアクティビティに応じて即時にポップアップ通知が表示されます。ポップアップ通知のなかには 5 秒経過すると自動的に非表示になるものや、非表示アイコン (×) をクリックして明示的に表示を消さなければならない「スティッキー」通知もあります。通知リス

トの最上部にある [表示を消す (Dismiss) ] リンクをクリックすると、すべての通知をまとめて非表示にすることができます。



#### ヒント

スティッキー以外のポップアップ通知の上にマウスのカーソルを合わせると、その通知はスティッキーになります。

システムはユーザのライセンス、ドメイン、アクセス ロールに基づいて、どのメッセージをポップアップ通知やメッセージセンターに表示するか決定します。

## メッセージタイプ

Message Center では、システムのアクティビティとステータスをレポートするメッセージが 3 つのタブに編成されて表示されます。

### 展開 (Deployments)

このタブには、システムの各アプライアンスの設定展開に関連する現在のステータスがドメイン別にグループ化されて表示されます。Firepower システムでは、次の展開ステータス値がこのタブでレポートされます。



- [実行中 (Running) ] (🌀 の表示が回転中) : 設定は展開の処理中です。
- [成功 (Success) ] (✔) : 設定は正常に展開されました。
- [警告 (Warning) ] (⚠) : 警告展開ステータスは、警告システム ステータスアイコン (⚠) とともに表示されるメッセージ数に含まれます。
- [失敗 (Failure) ] (❌) : 設定は展開に失敗しました。 [失効ポリシー \(363 ページ\)](#) を参照してください。失敗した展開は、エラー システム ステータス アイコン (❌) とともに表示されるメッセージ数に含まれます。




### ヘルス (Health)

このタブには、システムの各アプライアンスの現在のヘルス ステータス情報がドメイン別にグループ化されて表示されます。ヘルス ステータスは、 [ヘルス モニタリングについて \(275 ページ\)](#) に記載されているように、ヘルス モジュールによって生成されます。

Firepower システムでは、次のヘルス ステータス値がこのタブでレポートされます。

- [警告 (Warning) ] (⚠) : アプライアンス上のヘルス モジュールが警告制限を超え、問題が解決されていないことを示します。[ヘルス モニタリング (Health Monitoring) ] ページには、これらの状態が黄色い三角形のアイコン (⚠) で示されます。警告ステータスは、警告システム ステータス アイコン (⚠) とともに表示されるメッセージ数に含まれます。
- [重大 (Critical) ] (❌) : アプライアンス上のヘルス モジュールが重大制限を超え、問題が解決されていないことを示します。[ヘルス モニタリング (Health Monitoring) ]








ページには、これらの状態が  アイコンで示されます。重大ステータスは、エラーシステムステータスアイコン () とともに表示されるメッセージ数に含まれます。

- [エラー (Error) ] ( ) : アプライアンス上のヘルスモニタリングモジュールに障害が発生し、それ以降、正常に再実行されていないことを示します。[ヘルスモニタリング (Health Monitoring) ] ページには、これらの状態が  アイコンで示されます。エラーステータスは、エラーシステムステータスアイコン () とともに表示されるメッセージ数に含まれます。

[ヘルス (Health) ] タブのリンクをクリックして、[ヘルスモニタリング (Health Monitoring) ] ページで関連の詳細情報を表示できます。現在のヘルスステータス状態がない場合、[ヘルス (Health) ] タブにメッセージは表示されません。

## タスク

Firepower システムでは、完了するまで時間がかかる可能性がある特定のタスク (構成のバックアップやインストールの更新など) を実行できます。このタブには、これらの長時間実行タスクのステータスが表示され、自分が開始したタスクや、適切なアクセス権がある場合は、システムの他のユーザが開始したタスクが含まれることがあります。このタブには、各メッセージの最新の更新時間に基づいて時系列の逆順にメッセージが表示されます。一部のタスクステータスメッセージには、問題となっているタスクについての詳細情報へのリンクが含まれています。Firepower システムでは、次のタスクステータス値がこのタブでレポートされます。

- [待機中 (Waiting) ] ( ) : 別の進行中のタスクが完了するまで実行を待機しているタスクを示します。このメッセージタイプでは、更新の経過表示バーが表示されます。
- [実行中 (Running) ] ( の表示が回転中) : 進行中のタスクを示します。このメッセージタイプでは、更新の経過表示バーが表示されます。
- [再試行中 (Retrying) ] ( ) : 自動的に再試行しているタスクを示します。なお、すべてのタスクの再試行が許可されるわけではありません。このメッセージタイプでは、更新の経過表示バーが表示されます。
- [成功 (Success) ] ( ) : 正常に完了したタスクを示します。
- [失敗 (Failure) ] ( ) : 正常に完了しなかったタスクを示します。失敗したタスクは、エラーシステムステータスアイコン () とともに表示されるメッセージ数に含まれます。
- [停止 (Stopped) ] ( ) : システムアップデートのために中断されたタスクを示します。停止したタスクを再開することはできません。

新しいタスクが開始されると、新しいメッセージがこのタブに表示されます。タスクが完了すると (成功、失敗、または停止のステータス) 、タスクを削除するまで、このタブには最終ステータスを示すメッセージが引き続き表示されます。[タスク (Tasks) ] タブおよびメッセージデータベースがいっぱいにならないように、メッセージを削除することをお勧めします。

## メッセージ管理

メッセージセンターから、以下を実行できます。

- ポップアップ通知の動作を設定します（これらを表示するかどうかを選択します）。
- システム データベースの追加のタスクのステータス メッセージを表示します（削除されていないもので利用可能なものがある場合）。
- 個々のタスクのステータスメッセージを削除します。（これは、削除されたメッセージを確認できるすべてのユーザに影響します）。
- タスクのステータスメッセージを一括で削除します。（これは、削除されたメッセージを確認できるすべてのユーザに影響します）。



---

### ヒント

シスコは、表示に加えてデータベースの不要なデータを削除するために、累積されたタスクのステータスメッセージを [タスク (Task) ] タブから定期的に削除することを推奨します。データベースのメッセージ数が 100,000 に到達すると、削除したタスクのステータスメッセージが自動的に削除されます。

---

## システム メッセージの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	展開 (Deployment) : 管理者/[設定をデバイスに展開する (Deploy Configuration to Devices) ] 権限を持つカスタム ユーザ ロール [ヘルス (Health) ] : 管理者/[ヘルス (Health) ] 権限を持つカスタム ユーザ ロール 他人によって開始されたタスク : 管理者/[他のユーザのタスクを確認する (View Other Users' Tasks) ] 権限があるカスタム ユーザ ロール 自分が開始したタスク : 任意

### 手順

**ステップ 1** [システム ステータス (System Status) ] アイコンをクリックして、メッセージセンターを表示します。

**ステップ 2** 次の選択肢があります。

- [展開 (Deployments) ] タブをクリックして、設定の展開に関連するメッセージを表示します。 [展開メッセージの表示 \(328 ページ\)](#) を参照してください。

- [ヘルス (Health) ] タブをクリックして、Firepower Management Center とそれに登録したデバイスの状況に関連するメッセージを表示します。ヘルスメッセージの表示 (329 ページ) を参照してください。
- [タスク (Tasks) ] タブをクリックして、長時間実行タスクに関連するメッセージを表示または管理します。タスクメッセージの表示 (330 ページ) またはタスクメッセージの管理 (331 ページ) を参照してください。
- Message Center の右上隅にある歯車アイコン (⚙) をクリックして、ポップアップ通知の動作を設定します。通知動作の設定 (332 ページ) を参照してください。

## 展開メッセージの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	[設定をデバイスに展開する (Deploy Configuration to Devices) ] 権限を持つ管理者/ユーザ ロール

### 手順

**ステップ 1** [システム ステータス (System Status) ] アイコンをクリックして、メッセージセンターを表示します。

**ステップ 2** [展開 (Deployments) ] タブをクリックします。

**ステップ 3** 次の選択肢があります。

- 現在のすべての展開ステータスを表示するには、[合計 (total) ] をクリックします。
- 任意の展開ステータスに関するメッセージのみを表示するには、そのステータスの値をクリックします。
- 展開の経過時間、開始時刻および停止時刻を表示するには、メッセージの時間経過インジケータ (たとえば、[1分5秒 (1m 5s) ]) の上にカーソルを置きます。

### 関連トピック

[設定変更の導入 \(350 ページ\)](#)

## ヘルス メッセージの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	[ヘルス (Health)] の権限を持つ管理者/ユーザ ロール

### 手順

**ステップ 1** [システム ステータス (System Status)] アイコンをクリックして、メッセージセンターを表示します。

**ステップ 2** [ヘルス (Health)] タブをクリックします。

**ステップ 3** 次の選択肢があります。

- 現在のすべてのヘルス ステータスを表示するには、[合計 (total)] をクリックします。
- 任意のステータスに関するメッセージのみを表示するには、そのステータスの値をクリックします。
- メッセージが最も最近更新された時刻を表示するには、そのメッセージの相対時間インジケータ (たとえば [3 日前 (3 day(s) ago)]) の上にカーソルを置きます。
- 特定のメッセージの詳細なヘルス ステータス情報を表示するには、メッセージをクリックします。
- [ヘルス モニタリング (Health Monitoring)] ページの完全なヘルス ステータスを表示するには、タブの下部にある [ヘルス モニタ (Health Monitor)] をクリックします。

### 関連トピック

[ヘルス モニタリングについて \(275 ページ\)](#)

## タスク メッセージの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	他人によって開始されたタスク： [他のユーザのタスクを確認する (View Other Users' Tasks) ] 権限がある管理/カスタム ユーザ ロール  自分が開始したタスク：任意

### 手順

**ステップ 1** [システム ステータス (System Status) ] アイコンをクリックして、メッセージセンターを表示します。

**ステップ 2** [タスク (Tasks) ] タブをクリックします。

**ステップ 3** 次の選択肢があります。

- 現在のすべてのタスクのステータスを表示するには、[合計 (total) ] をクリックします。
- 任意のステータスのタスクに関するメッセージのみを表示するには、そのステータスの値をクリックします。

(注) 停止したタスクのメッセージは、タスクのステータスメッセージの合計リストにのみ表示されます。停止したタスクではフィルタリングできません。

- メッセージが最も最近更新された時刻を表示するには、そのメッセージの相対時間インジケータ (たとえば [3 日前 (3 day(s) ago) ]) の上にカーソルを置きます。
- タスクに関する詳細を表示するには、メッセージ内のリンクをクリックします。
- さらにタスクのステータスメッセージが表示可能な場合は、メッセージリストの下部にある [さらにメッセージを取得する (Fetch more messages) ] をクリックして取得します。



## タスク メッセージの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	他人によって開始されたタスク： [他のユーザのタスクを確認する (View Other Users' Tasks) ] 権限がある管理/カスタム ユーザ ロール  自分が開始したタスク：任意

### 手順

**ステップ 1** [システム ステータス (System Status) ] アイコンをクリックして、メッセージセンターを表示します。

**ステップ 2** [タスク (Tasks) ] タブをクリックします。

**ステップ 3** 次の選択肢があります。

- さらにタスクのステータス メッセージが表示可能な場合は、メッセージ リストの下部にある [さらにメッセージを取得する (Fetch more messages) ] をクリックして取得します。
- 完了したタスク (ステータスが停止、成功、または失敗のタスク) に関する 1 つのメッセージを削除するには、メッセージの横にある削除アイコン (✖) をクリックします。
- すべての完了しているタスク (ステータスが停止、成功、または失敗のタスク) に関するメッセージをすべて削除するには、[総数 (total) ] でメッセージをフィルタリングして、[すべての完了タスクの削除 (Remove all completed tasks) ] をクリックします。
- すべての正常に完了したタスクに関するメッセージをすべて削除するには、[成功 (success) ] でメッセージをフィルタリングして、[すべての成功タスクの削除 (Remove all successful tasks) ] をクリックします。
- すべての失敗したタスクに関するメッセージをすべて削除するには、[失敗 (failure) ] でメッセージをフィルタリングして、[すべての失敗タスクの削除 (Remove all failed tasks) ] をクリックします。

## 通知動作の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)



(注) この設定は、すべてのポップアップ通知に影響を及ぼし、ログインセッション間で保持されません。

### 手順

- ステップ 1** [システム ステータス (System Status)] アイコンをクリックして、メッセージセンターを表示します。
- ステップ 2** メッセージセンターの右上にある歯車アイコン (⚙️) をクリックします。
- ステップ 3** ポップアップ通知の表示を有効または無効にするには、[通知を表示 (Show notifications)] スライダをクリックします。
- ステップ 4** スライダを非表示にするには、歯車アイコン (⚙️) を再度クリックします。
- ステップ 5** [システム ステータス (System Status)] アイコンを再度クリックして、メッセージセンターを閉じます。

## トラブルシューティング用のヘルス モニタ レポート

アプライアンスで問題が発生したときに、問題の診断に役立つように、サポートからトラブルシューティングファイルを提供するように依頼されることがあります。システムは、特定の機能分野を対象とした情報を含むトラブルシューティングファイルと、高度なトラブルシューティングファイル（このファイルはサポートと連携して取得します）を生成することができます。次の表に示すオプションのいずれかを選択して、特定の機能のトラブルシューティングファイルの内容をカスタマイズできます。

一部のオプションは報告対象のデータの点で重複していますが、トラブルシューティングファイルには、オプションの選択に関係なく冗長コピーは含まれません。

表 39: 選択可能なトラブルシューティングオプション

オプション	報告内容
Snort のパフォーマンスと設定 (Snort Performance and Configuration)	アプライアンス上の Snort に関連するデータと構成設定

オプション	報告内容
ハードウェアパフォーマンスとログ (Hardware Performance and Logs)	アプライアンス ハードウェアのパフォーマンスに関連するデータとログ
システムの設定、ポリシー、ログ (System Configuration, Policy, and Logs)	アプライアンスの現在のシステム設定に関連する構成設定、データ、およびログ
検知機能の構成、ポリシー、ログ (Detection Configuration, Policy, and Logs)	アプライアンス上の検知機能に関連する構成設定、データ、およびログ
インターフェイスとネットワーク関連データ (Interface and Network Related Data)	アプライアンスのインラインセットとネットワーク設定に関連する構成設定、データ、およびログ
検知、認識、VDB データ、およびログ (Discovery, Awareness, VDB Data, and Logs)	アプライアンス上の現在の検出設定と認識設定に関連する構成設定、データ、およびログ
データおよびログのアップグレード (Upgrade Data and Logs)	アプライアンスの以前のアップグレードに関連するデータおよびログ
全データベースのデータ (All Database Data)	トラブルシューティングレポートに含まれるすべてのデータベース関連データ
全ログのデータ (All Log Data)	アプライアンス データベースによって収集されたすべてのログ
ネットワーク マップ情報 (Network Map Information)	現在のネットワーク トポロジデータ

## 特定のシステム機能のトラブルシューティング ファイルの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst

カスタマイズしたトラブルシューティングファイルを生成およびダウンロードして、そのファイルをサポートに送信できます。

マルチドメイン展開では、子孫ドメイン内のデバイスに対するトラブルシューティングファイルの生成およびダウンロードが可能です。

### 手順

- ステップ 1** アプライアンスのヘルスモニタを表示します。[アプライアンスヘルスモニタの表示 \(297ページ\)](#) を参照してください。

- ステップ 2** [トラブルシューティング ファイルの生成 (Generate Troubleshooting Files) ] をクリックします。
- ステップ 3** [全データ (All Data) ] を選択して生成可能なすべてのトラブルシューティング データを生成することも、個別のボックスをオンにすることもできます。詳細については、[タスク メッセージの表示 \(330 ページ\)](#) を参照してください。
- ステップ 4** [OK] をクリックします。
- ステップ 5** Message Center でタスクのメッセージを表示します。[タスク メッセージの表示 \(330 ページ\)](#) を参照してください。
- ステップ 6** 生成されたトラブルシューティング ファイルに対応するタスクを探します。
- ステップ 7** アプライアンスがトラブルシューティング ファイルを生成して、タスク ステータスが [完了 (Completed) ] に変わったら、[クリックして生成されたファイルを取得 (Click to retrieve generated files) ] をクリックします。
- ステップ 8** ブラウザのプロンプトに従ってファイルをダウンロードします。(トラブルシューティングファイルは、1 つの .tar.gz ファイルでダウンロードされます)。
- ステップ 9** サポートの指示に従って、トラブルシューティング ファイルを Cisco に送信してください。

## 高度なトラブルシューティング ファイルのダウンロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst

マルチドメイン展開では、子孫ドメイン内のデバイスに対するトラブルシューティングファイルの生成およびダウンロードが可能です。グローバルドメインの場合のみ、Firepower Management Center からファイルをダウンロードできます。

### 手順

- ステップ 1** アプライアンスのヘルス モニタを表示します ([アプライアンスヘルス モニタの表示 \(297 ページ\)](#) を参照)。
- ステップ 2** [高度なトラブルシューティング (Advanced Troubleshooting) ] をクリックします。
- ステップ 3** [ファイルのダウンロード (File Download) ] タブで、サポートから提供されたファイル名を入力します。
- ステップ 4** [ダウンロード (Download) ] をクリックします。
- ステップ 5** ブラウザのプロンプトに従ってファイルをダウンロードします。
- (注) 管理対象デバイスでは、システムはファイル名の前にデバイス名を付加してファイル名を変更します。

ステップ 6 サポートの指示に従って、トラブルシューティング ファイルを Cisco に送信してください。

## Web インターフェイスからの Firepower Threat Defense CLI の使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Firepower Threat Defense	任意 (Any)	Admin/Maint/Any Security Analyst

Firepower Management Center Web インターフェイスから、選択した Firepower Threat Defense コマンドラインインターフェイス (CLI) コマンドを実行できます。これらのコマンドは、ping、packet-tracer、traceroute、show (show サブコマンドの history と banner を除く) です。

マルチドメイン環境では、子孫ドメインの管理対象デバイスの Firepower Management Center Web インターフェイスを使用して、Firepower Threat Defense CLI コマンドを入力できます。



(注) Firepower Management Center ハイ アベイラビリティを使用した展開では、この機能はアクティブ Firepower Management Center でのみ使用できます。

Firepower Threat DefenseCLI の詳細については、『*Command Reference for Firepower Threat Defense*』を参照してください。

### 手順

- ステップ 1 アプライアンスのヘルス モニタを表示します ([アプライアンスヘルスモニタの表示 \(297ページ\)](#) を参照)。
- ステップ 2 [高度なトラブルシューティング (Advanced Troubleshooting)] をクリックします。
- ステップ 3 [脅威に対する防御 CLI (Threat Defense CLI)] タブをクリックします。
- ステップ 4 [コマンド (Command)] ドロップダウン リストで、コマンドを選択します。
- ステップ 5 オプションで、[パラメータ (Parameters)] テキスト ボックスにコマンドパラメータを入力します。
- ステップ 6 [実行 (Execute)] をクリックして、コマンド出力を表示します。

## 機能固有のトラブルシューティング

機能固有のトラブルシューティングのヒントやテクニックについては、次の表を参照してください。

表 40: 機能固有のトラブルシューティング トピック

機能	関連するトラブルシューティング情報
LDAP 外部認証	<a href="#">LDAP 認証接続のトラブルシューティング (122 ページ)</a>
7000 および 8000 シリーズ デバイスのハイ アベイラビリティ状態共有	<a href="#">トラブルシューティングのためのデバイスのハイ アベイラビリティの状態共有統計情報 (619 ページ)</a>
ユーザ ルール条件	<a href="#">ユーザ制御のトラブルシューティング (405 ページ)</a>
ユーザ アイデンティティ ソース	<a href="#">ユーザ エージェント アイデンティティ ソースのトラブルシューティング (2125 ページ)</a> <a href="#">ISE アイデンティティ ソースのトラブルシューティング (2130 ページ)</a> <a href="#">TS エージェント アイデンティティ ソースのトラブルシューティング (2132 ページ)</a> <a href="#">キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング (2142 ページ)</a>
レルムとユーザデータのダウンロード	<a href="#">レルムとユーザのダウンロードのトラブルシューティング (2182 ページ)</a>
ネットワーク検出	<a href="#">ネットワーク検出戦略のトラブルシューティング (2174 ページ)</a>
カスタムセキュリティ グループ タグ (SGT) のルール条件	<a href="#">カスタム SGT 条件のトラブルシューティング (408 ページ)</a>
SSL ルール	<a href="#">SSL ルールのトラブルシューティング (1487 ページ)</a>
Firepower Threat Defense syslog	<a href="#">Syslog の設定 (1050 ページ)</a>
侵入パフォーマンス統計	<a href="#">侵入パフォーマンス統計情報のロギング設定 (1832 ページ)</a>
7000 および 8000 シリーズ、NGIPSv、および ASA with FirePOWER サービスのコマンドラインインターフェイス (CLI)	<a href="#">generate-troubleshoot (2855 ページ)</a>



## 第 **IV** 部

### 導入管理

- [ドメイン管理 \(339 ページ\)](#)
- [ポリシー管理 \(349 ページ\)](#)
- [ルール管理：共通の特性 \(369 ページ\)](#)
- [再利用可能なオブジェクト \(421 ページ\)](#)







## 第 15 章

# ドメイン管理

次のトピックでは、ドメインを使用してマルチテナンシーを管理する方法について説明します。

- [ドメインを使用したマルチテナンシーの概要 \(339 ページ\)](#)
- [ドメインの管理 \(343 ページ\)](#)
- [新しいドメインの作成 \(344 ページ\)](#)
- [ドメイン間のデータの移動 \(345 ページ\)](#)
- [ドメイン間のデバイスの移動 \(346 ページ\)](#)

## ドメインを使用したマルチテナンシーの概要

Firepower システムでは、ドメインを使用したマルチテナンシーを実装できます。ドメインは、管理対象デバイス、構成、およびイベントへのユーザアクセスをセグメント化します。最上位の [グローバル (Global) ] ドメインの下に、2 つまたは 3 つのレベルで最大 50 個のサブドメインを作成できます。

Firepower Management Center にログインすると、現在のドメインと呼ばれる単一ドメインにログインします。ユーザアカウントによっては、他のドメインに切り替えることができます。

ユーザロールによる制限に加えて、現在のドメインレベルによってさまざまな Firepower システム設定の変更が制限される場合もあります。システム ソフトウェア アップデートなどのほとんどの管理タスクは、グローバル ドメインに制限されます。

その他のタスクは、サブドメインがないドメインであるリーフドメインに制限されます。たとえば、各管理対象デバイスをリーフドメインと関連付け、そのリーフドメインのコンテキストからデバイス管理タスクを実行する必要があります。



**ヒント** このガイドの各タスク トピックには、タスクを実行できるドメイン レベルを示すサポートされるドメイン数という値があります。

各リーフ ドメインは、そのリーフ ドメインのデバイスで集められた検出データに基づいて独自のネットワーク マップを作成します。管理対象デバイスによって報告されたイベント（接続、侵入、マルウェアなど）もデバイスのリーフ ドメインに関連付けられます。

### 1 ドメイン レベル : グローバル

マルチテナンシーを設定しない場合、すべてのデバイス、構成、およびイベントはグローバル ドメインに属します。グローバル ドメインは、このシナリオの場合はリーフ ドメインでもあります。ドメイン管理を除き、サブドメインを追加するまでは、ドメイン固有の構成および分析オプションは非表示になります。

### 2 ドメイン レベル : グローバル、セカンドレベル

2レベルのマルチドメイン展開では、グローバル ドメインには直接の子孫ドメインのみがあります。たとえば、マネージドセキュリティサービスプロバイダー（MSSP）は、1つの Firepower Management Center を使用して複数の顧客のネットワーク セキュリティを管理できます。

- MSSPの管理者は、グローバル ドメインにログインして、すべての顧客の展開を管理できます。
- 各顧客の管理者は、サブドメインと呼ばれるセカンドレベルにログインして、その組織に適用されるデバイス、構成、およびイベントのみを管理できます。これらのローカル管理者は、MSSP の他の顧客の展開を表示したり、その環境に影響を与えることはできません。

### 3 ドメイン レベル : グローバル、セカンドレベル、サードレベル

3レベルのマルチドメイン展開では、グローバル ドメインにはサブドメインがあり、そのうち少なくとも1つに独自のサブドメインがあります。前の例を拡張するには、MSSP 顧客（すでにサブドメインに制限されている）がその展開をさらにセグメント化しようとしているシナリオを考えてみます。この顧客は、2つのクラスのデバイス（ネットワークエッジに配置されているデバイスと内部に配置されているデバイス）を個別に管理しようとしています。

- 顧客の管理者はセカンドレベルのサブドメインにログインして、顧客の展開全体を管理できます。
- 顧客のエッジ ネットワークの管理者は、サードレベル（リーフ）ドメインにログインして、ネットワークエッジに展開されているデバイスに適用されるデバイス、構成、およびイベントのみを管理できます。同様に、顧客の内部ネットワークの管理者は、別のサードレベル ドメインにログインして、内部のデバイス、構成、およびイベントを管理できます。エッジと内部の管理者は、互いの展開を表示できません。

## ドメインの用語

このマニュアルでは、ドメインおよびマルチドメイン展開を説明する際に次の用語を使用します。

### グローバルドメイン

マルチドメイン展開でのトップレベルドメイン。マルチテナンシーを設定しない場合、すべてのデバイス、設定、およびイベントはグローバルドメインに属します。グローバルドメインの Administrators は、Firepower システム全体の導入を管理できます。

### サブドメイン

第2または第3レベルのドメイン。

### 第2レベルドメイン

グローバルドメインの子。第2レベルドメインは、リーフドメインにするか、サブドメインを持つことができます。

### 第3レベルドメイン

第2レベルドメインの子。第3レベルドメインは常にリーフドメインです。

### リーフドメイン

サブドメインを持たないドメイン。各デバイスはリーフドメインに属している必要があります。

### 子孫ドメイン

階層の現在のドメインから下のドメイン。

### 子ドメイン

ドメインの直接子孫。

### 先祖ドメイン

現在のドメインより上にある同じ系統のドメイン。

### 親ドメイン

ドメインの直接先祖。

### 兄弟ドメイン

同じ親を持つドメイン。

### 現在のドメイン

現在ログインしているドメイン。システムでは、Web インターフェイスの右上のユーザ名の前に現在のドメイン名が表示されます。ユーザロールが制限されている場合を除き、現在のドメインの設定を編集できます。

## ドメインのプロパティ

ドメインのプロパティを変更するには、そのドメインの親ドメインの Administrator アクセス権が必要です。

### 名前 (Name) と説明 (Description)

各ドメインには、その階層内に一意の名前が必要です。説明は任意です。

### 親ドメイン (Parent Domain)

第2および第3レベルのドメインには親ドメインがあります。ドメインを作成した後にドメインの親を変更することはできません。

### デバイス

リーフドメインにのみデバイスを含めることができます。つまり、1つのドメインにはサブドメインまたはデバイスを含めることができますが、両方を含めることはできません。非リーフドメインが直接デバイスを制御している展開を保存することはできません。

ドメインエディタで、ドメイン階層の現在の場所に応じて、Webインターフェイスに使用可能な選択されたデバイスが表示されます。

### ホスト制限 (Host Limit)

Firepower Management Center がモニタでき、ネットワークマップに保存できるホストの数。モデルによって異なります。マルチドメイン展開では、リーフドメインは使用可能なモニタされたホストのプールを共有しますが、個別のネットワークマップを持っています。

各リーフドメインがネットワークマップに値を入力できるように、ホスト制限を各サブドメインレベルで設定できます。ドメインのホスト制限を **0** に設定すると、ドメインは一般的なプールで共有します。

ホスト制限を設定すると、各ドメインレベルで異なる効果があります。

- リーフ：リーフドメインの場合、ホスト制限は単に、リーフドメインがモニタできるホスト数の制限です。
- 第2レベル：第3レベルのリーフドメインを管理する第2レベルのドメインの場合、ホスト制限は、リーフドメインがモニタできるホストの総数を表します。リーフドメインは、使用可能なホストのプールを共有します。
- グローバル：グローバルドメインの場合、ホスト制限は、Firepower Management Center がモニタできるホストの総数に等しくなります。変更することはできません。

サブドメインのホスト制限の合計を、親ドメインのホスト制限より多くすることができます。たとえば、グローバルドメインのホスト制限が 150,000 の場合、複数のサブドメインを設定して、それぞれのホスト制限を 100,000 にすることができます。これらのドメインのいずれか（すべてではない）が 100,000 のホストをモニタできます。

ホスト制限に到達した後に新しいホストを検出すると、ネットワーク検出ポリシーが制御を行います。新しいホストをドロップするか、または長期間非アクティブになっているホストを置換することができます。各リーフドメインには独自のネットワーク検出ポリシーがあるため、各リーフドメインは、システムが新しいホストを検出すると、独自の動作を制御します。

ドメインのホスト制限を軽減した場合に、そのネットワークマップに新しい制限より多くのホストが含まれている場合、システムは最も長い間非アクティブになっているホストを削除します。

#### 関連トピック

[Firepower システムのホスト制限](#) (2035 ページ)

[ネットワーク検出のデータ ストレージ設定](#) (2170 ページ)

## ドメインの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ドメインのプロパティを変更するには、そのドメインの親ドメインへの管理者アクセス権が必要です。

#### 手順

**ステップ 1** [システム (System)] > [ドメイン (Domains)] を選択します。

**ステップ 2** 次のようにドメインを管理します。

- 追加: [ドメインの追加 (Add Domain)] をクリックするか、または親ドメインの横にある [サブドメインの追加 (Add Subdomain)] アイコンをクリックします ([新しいドメインの作成 \(344 ページ\)](#) を参照)。
- 編集: 変更するドメインの横にある編集アイコン (✎) をクリックします ([ドメインのプロパティ \(341 ページ\)](#) を参照)。
- 削除: 削除する空のドメインの横にある削除アイコン (🗑️) をクリックして、選択内容を確認します。宛先ドメインを編集することによって、削除するドメインからデバイスを移動します。

**ステップ 3** ドメイン構造への変更を行い、すべてのデバイスをリーフ ドメインに関連付けたら、[保存 (Save)] をクリックして変更を実行します。

**ステップ 4** プロンプトが表示されたら、追加の変更を行います。

- リーフ ドメインを親ドメインに変更した場合は、古いネットワーク マップを移動または削除します ([ドメイン間のデータの移動 \(345 ページ\)](#) を参照)。
- ドメイン間でデバイスを移動し、新しいポリシーおよびセキュリティ ゾーンまたはインターフェイス グループを割り当てる必要がある場合は、[ドメイン間のデバイスの移動 \(346 ページ\)](#) を参照してください。

## 次のタスク

- 新しいドメインのユーザロールとポリシー（アクセス制御、ネットワーク検出など）を設定します。必要に応じてデバイスのプロパティを更新します。
- 設定変更を展開します。[設定変更の導入（350 ページ）](#)を参照してください。

## 新しいドメインの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルおよびセカンドレベル	Admin

最上位の [グローバル (Global)] ドメインの下に、2つまたは3つのレベルで最大 50 個のサブドメインを作成できます。

ドメイン設定を実装する前に、リーフドメインにすべてのデバイスを割り当てる必要があります。リーフドメインにサブドメインを追加すると、ドメインはリーフドメインではなくなるので、デバイスを再度割り当てる必要があります。

## 手順

- ステップ 1** グローバルまたはセカンドレベルドメインで、[システム (System)] > [ドメイン (Domains)] を選択します。
- ステップ 2** [ドメインの追加 (Add Domain)] をクリックするか、または親ドメインの横にある [サブドメインの追加 (Add Subdomain)] アイコンをクリックします。
- ステップ 3** [名前 (Name)] と [説明 (Description)] に入力します。
- ステップ 4** [親ドメイン (Parent Domain)] を選択します。
- ステップ 5** [デバイス (Devices)] タブで、ドメインに追加する [使用可能なデバイス (Available Devices)] を選択し、[ドメインに追加 (Add to Domain)] をクリックするか、または [選択されたデバイス (Selected Devices)] のリストにドラッグアンドドロップします。
- ステップ 6** 必要に応じて、[詳細設定 (Advanced)] タブをクリックして、新しいドメインがモニタできるホスト数を制限します ([ドメインのプロパティ \(341 ページ\)](#) を参照)。
- ステップ 7** [保存 (Save)] をクリックして、ドメイン管理ページに戻ります。  
デバイスが非リーフドメインに割り当てられている場合は、システムによって警告が表示されます。これらのデバイスに新しいドメインを作成するには、[新しいドメインの作成 (Create New Domain)] をクリックします。デバイスを既存のドメインに移動する予定がある場合は、[未割り当てのままにする (Keep Unassigned)] をクリックします。
- ステップ 8** ドメイン構造への変更を行い、すべてのデバイスをリーフドメインに関連付けたら、[保存 (Save)] をクリックして変更を実行します。

**ステップ9** プロンプトが表示されたら、追加の変更を行います。

- リーフ ドメインを親ドメインに変更した場合は、古いネットワーク マップを移動または削除します（[ドメイン間のデータの移動（345 ページ）](#) を参照）。
- ドメイン間でデバイスを移動し、新しいポリシーおよびセキュリティ ゾーンまたはインターフェイス グループを割り当てる必要がある場合は、[ドメイン間のデバイスの移動（346 ページ）](#) を参照してください。

#### 次のタスク

- 新しいドメインのユーザロールとポリシー（アクセス制御、ネットワーク検出など）を設定します。必要に応じてデバイスのプロパティを更新します。
- 設定変更を展開します。[設定変更の導入（350 ページ）](#) を参照してください。

## ドメイン間のデータの移動

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

イベントおよびネットワーク マップがリーフ ドメインに関連付けられているため、リーフ ドメインを親ドメインに変更する場合は、2つの選択肢があります。

- ネットワーク マップおよび関連付けられているイベントを新しいリーフ ドメインに移動します。
- ネットワーク マップは削除しますが、イベントは保持します。この場合、システムが必要に応じてまたは設定されているようにイベントをプルーニングするまで、イベントは親ドメインに関連付けられたままとなります。または、古いイベントを手動で削除できます。

#### 始める前に

- 以前のリーフ ドメインが現在の親ドメインになるドメイン設定を実行します（[ドメインの管理（343 ページ）](#) を参照）。

#### 手順

**ステップ1** 現在親ドメインである以前のリーフ ドメインそれぞれに対し、2つの選択肢があります。

- **親ドメイン**のイベントおよびネットワーク マップを継承するには、新しいリーフ ドメインを選択します。

- 親ドメインのネットワーク マップを削除するが、古いイベントは保持する場合は、[なし (None) ] を選択します。

ステップ2 [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ドメイン間のデバイスの移動

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルおよびセカンドレベル	Admin

ドメイン間でデバイスを移動すると、デバイスに適用された設定とポリシーに影響する可能性があります。システムは実行できる内容を自動的に保持および更新し、実行できない内容を削除します。

具体的には次のとおりです。

- 移動したデバイスに割り当てられた正常性ポリシーが新しいドメインでアクセス不能の場合、新しい正常性ポリシーを選択できます。
- 移動したデバイスに割り当てられたアクセス コントロール ポリシーが有効でない場合、または新しいドメインでアクセスできない場合は、新しいポリシーを選択します。すべてのデバイスに、割り当てられたアクセス コントロール ポリシーが必要です。
- 移動したデバイス上のインターフェイスが、新しいドメインでアクセスできないセキュリティゾーンに属している場合は、新しいゾーンを選択できます。
- インターフェイスは、以下から削除されます。
  - 新しいドメインでアクセス不能で、アクセス コントロール ポリシーで使用されていないセキュリティゾーン。
  - すべてのインターフェイスグループ。

デバイスでポリシーの更新が必要だが、ゾーン間でインターフェイスを移動する必要がない場合は、ゾーン設定が最新であることを示すメッセージが表示されます。たとえば、デバイスのインターフェイスが共通の先祖ドメインに設定されているセキュリティゾーンに属している場合は、サブドメインからサブドメインにデバイスを移動する場合はゾーン設定を更新する必要はありません。



### 始める前に

- デバイスをドメインからドメインに移動し、次に新しいポリシーとセキュリティゾーンを割り当てる必要があるドメイン構成を実装します（[ドメインの管理（343 ページ）](#) を参照）。

### 手順

- 
- ステップ 1** [デバイスの移動 (Move Devices) ] ダイアログボックスの [設定するデバイスの選択 (Select Device(s) to Configure) ] の下で、設定するデバイスをオンにします。
- 同じ正常性ポリシーとアクセス コントロール ポリシーを割り当てるには、複数のデバイスをオンにします。
- ステップ 2** デバイスに適用する [アクセス コントロール ポリシー (Access Control Policy) ] を選択するか、または新しいポリシーを作成するには [新しいポリシー (New Policy) ] を選択します。
- ステップ 3** デバイスに適用する [正常性ポリシー (Health Policy) ] を選択するか、またはデバイスに正常性ポリシーを適用しないままにするには [なし (None) ] を選択します。
- ステップ 4** インターフェイスを新しいゾーンに割り当てるようにプロンプトが表示された場合は、リストされている各インターフェイスに [新しいセキュリティゾーン (New Security Zone) ] を選択するか、または後で割り当てるには [なし (None) ] を選択します。
- ステップ 5** すべての影響を受けるデバイスを設定した後、[保存 (Save) ] をクリックしてポリシーとゾーンの割り当てを保存します。
- ステップ 6** [保存 (Save) ] をクリックして、ドメイン構成を実装します。
- 

### 次のタスク

- 移動の影響を受けた移動済みデバイスでその他の設定を更新します。
- 設定変更を展開します。[設定変更の導入（350 ページ）](#) を参照してください。





## 第 16 章

# ポリシー管理

ここでは、Firepower Management Center でさまざまなポリシーを管理する方法について説明します。

- [ポリシーの導入 \(349 ページ\)](#)
- [ポリシーの比較 \(360 ページ\)](#)
- [ポリシー レポート \(362 ページ\)](#)
- [失効ポリシー \(363 ページ\)](#)
- [限定的な導入のパフォーマンスに関する考慮事項 \(364 ページ\)](#)

## ポリシーの導入

導入を設定した後、およびその設定を変更したときは、影響を受けるデバイスにその変更を導入する必要があります。導入のステータスは、メッセージセンターで確認できます。

導入を行うと、以下のコンポーネントが更新されます。

- デバイスとインターフェイスの設定
- デバイス関連ポリシー：NAT、VPN、QoS、プラットフォーム設定
- アクセスコントロールおよび関連するポリシー：DNS、ファイル、アイデンティティ、侵入、ネットワーク分析、プレフィルタ、SSL
- ネットワーク検出ポリシー
- 侵入ルールの更新
- これらの要素のいずれかに関連付けられている設定とオブジェクト

システムにポリシーを自動的に導入させるには、導入タスクをスケジュールするか、あるいは侵入ルールの更新をインポートする際に導入するようにシステムを設定します。特に、侵入ポリシーの更新によって侵入およびネットワーク分析に関するシステム定義の基本ポリシーを変更できるようにしている場合は、ポリシーの導入を自動化すると役立ちます。侵入ルール更新によって、アクセスコントロールポリシーの前処理およびパフォーマンスの詳細設定オプションのデフォルト値が変更されることもあります。

マルチドメイン展開では、ユーザアカウントが属するいずれのドメインにも変更を導入できます。

- 導入先を先祖ドメインに切り替えると、変更がすべてのサブドメインに同時に導入されます。
- 導入先をリーフドメインに切り替えると、変更はそのドメインだけに導入されます。

## 設定変更の導入

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Network Admin/Security Approver

展開を設定した後、およびその設定を変更したときは、その変更を影響を受けるデバイスに展開します。



**注意** 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。このインスペクション中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。[Snort®の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。Firepower 7010、7020、および 7030 の管理対象デバイスでは、設定変更の展開に最大 5 分かかる場合があります。利用できない時間を最小限にするために、導入は変更時間帯に実行します。

### 始める前に

- 設定変更の展開に関するガイドラインを確認してください ([設定変更の展開に関する注意事項 \(353 ページ\)](#) を参照)。
- すべての管理対象デバイスが同じバージョンのセキュリティゾーンオブジェクトを使用していることを確認してください。セキュリティゾーンオブジェクトを編集している場合：同期させるすべてのデバイスでインターフェイスのゾーン設定を編集するまでは、デバイスに設定変更を展開しないでください。すべての管理対象デバイスに同時に展開する必要があります。 ([セキュリティゾーンオブジェクトのリビジョンの同期 \(584 ページ\)](#) を参照してください。)

### 手順

**ステップ 1** Firepower Management Center メニューバーで、[展開 (Deploy)] をクリックします。

[ポリシーの展開 (Deploy Policies)] ダイアログに、設定の期限が切れているデバイスがリストされます。ダイアログの上部の [バージョン (Version)] は、最後に設定変更を行った時期を示します。デバイス テーブルの [現在のバージョン (Current Version)] 列は、変更を各デバイスに最後に展開した時期を示します。

**ステップ 2** 設定変更を展開するデバイスを特定して選択します。

- [ソート (Sort)] : 列ヘッダーをクリックすることで、デバイス リストをソートします。
- [展開 (Expand)] : デバイス リストを展開して展開される設定変更を表示するには、プラス アイコン (+) をクリックします。システムは、期限切れのポリシーをインデックス (🔍) アイコンでマーキングします。
- [フィルタ (Filter)] : デバイス リストをフィルタリングします。ディスプレイの列ヘッダーの右上隅にある矢印をクリックし、[フィルタ (Filter)] テキスト ボックスにテキストを入力し、Enter を押します。

**ステップ 3** (オプション) 展開の開始前にルールの競合がないかチェックするには、[ルールの競合のチェック (Check for rule conflicts)] を有効にします。

特定の順序でルールを評価するポリシーでは、以前のルールが常に最初にトラフィックに一致するため、ルールがトラフィックに全く一致しない場合に競合が発生します。ルールの競合が展開を妨げることはありませんが、有効な展開の構築には適切なルールの作成と順序付けが必要です。展開プロセスで、アクセス コントロール ポリシーのルールの競合をチェックできます。しかし、複雑な展開では、ルールの競合のチェックに時間がかかる場合があります。

**ステップ 4** [展開 (Deploy)] をクリックします。

**ステップ 5** 変更の展開時にエラーまたは警告が出された場合には、次の選択肢があります。

- [続行 (Proceed)] : 警告状態を解決せずに展開を続行します。ルールの競合のチェックを有効にした場合、警告には検出されたルールの競合が含まれています。システムがエラーを確認した場合は続行できません。
- [キャンセル (Cancel)] : 展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

---

### 次のタスク

- 必要に応じて、展開のステータスをモニタします ([展開メッセージの表示 \(328 ページ\)](#) を参照)。
- 設定の展開に失敗した場合は、解決策について [設定変更の展開に関する注意事項 \(353 ページ\)](#) を参照してください。

### 関連トピック

[Snort® の再起動シナリオ \(354 ページ\)](#)

## デバイスへの強制導入

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Network Admin/Security Approver

通常は設定を変更すると構成設定に失効のマークが付きますが、そのようにしなくてもデバイスに設定を導入できます。



**注意** 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。このインスペクション中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。[Snort®の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。Firepower 7010、7020、および 7030 の管理対象デバイスでは、設定変更の展開に最大 5 分かかる場合があります。利用できない時間を最小限にするために、導入は変更時間帯に実行します。

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 強制導入するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [デバイス (Device)] タブをクリックします。

**ステップ 4** [全般 (General)] セクション見出しの横にある編集アイコン (✎) をクリックします。

**ステップ 5** [強制導入 (Force Deploy)] 矢印 (➡) をクリックします。

**ステップ 6** 必要に応じてデバイス リストを展開して、導入される構成設定を表示します。

システムは、期限切れのポリシーをインデックス (🔍) アイコンでマーキングします。

**ステップ 7** [展開 (Deploy)] をクリックします。

**ステップ 8** 構成設定の展開時にエラーまたは警告が出された場合には、次の選択肢があります。

- [続行 (Proceed)] をクリックして、エラーまたは警告条件を解決しないで導入を続行します。このボタンは、システムが導入の警告のみを特定した場合に有効になります。システムが導入のエラーを特定した場合には無効になります。

- [キャンセル (Cancel) ] をクリックして、展開を実行せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

### 次のタスク

- 必要に応じて、展開のステータスをモニタします ([展開メッセージの表示 \(328 ページ\)](#) を参照)。
- 設定の展開に失敗した場合は、解決策について [設定変更の展開に関する注意事項 \(353 ページ\)](#) を参照してください。

### 関連トピック

[Snort® の再起動シナリオ \(354 ページ\)](#)

## 設定変更の展開に関する注意事項

設定変更を管理対象デバイスに展開する際は、次の点に留意してください。



**重要** 利用できない時間を最小限にするために、展開は変更時間帯に実行します。

### 展開の結果



**注意** 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。このインスペクション中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。Firepower 7010、7020、および 7030 の管理対象デバイスでは、設定変更の展開に最大 5 分かかる場合があります。

- アプリケーション制御の実行時に必要なディテクタが無効になっている場合、システムは、ポリシーの展開時にシステムによって提供される適切なディテクタを自動的に有効にします。何もない場合、システムは、アプリケーションに対し直近で変更されたユーザ定義のディテクタを有効にします。
- ネットワーク検出ポリシーに変更を展開する場合、システムは、監視対象ネットワーク内のホストのネットワーク マップから MAC アドレス、TTL、およびホップ情報を削除してから、再検出を行います。また、影響を受ける管理対象デバイスは、まだ Firepower Management Center に送信されていない検出データを破棄します。

## トラブルシューティング

- インライン設定をパッシブに展開されたデバイスに適用しないでください。またその逆も同様です。
- デバイスの機能を超えないように注意してください。

複雑なアクセスコントロールポリシーやルールは、重要なリソースを消費し、パフォーマンスに悪影響を与える可能性があります。アクセスコントロールポリシーを展開すると、システムはすべてのルールをまとめて評価し、ネットワークトラフィックを評価するためにターゲットデバイスが使用する拡張基準セットを作成します。

ターゲットデバイスでサポートされるアクセスコントロールルールまたは呼び出し侵入ポリシーの最大数を超えると、システムが警告を表示します。この最大数は、ポリシーの複雑性、物理メモリ、デバイスのプロセッサ数などの、さまざまな要因によって異なります。

- デバイスが設定した機能に対して正しいモデルであり、正しいライセンスと最小バージョンの Firepower システムを使用していることを確認します。たとえば、異なるバージョンの Firepower システムを実行しているスタック構成の 7000 または 8000 シリーズ デバイスをターゲットにすることはできません。

## 自動展開

次のように自動的に展開するようにシステムを設定できます。

- 侵入ルール更新の完了後
- スケジュールされたタスクの使用

## 関連トピック

[Snort®の再起動シナリオ](#) (354 ページ)

# Snort®の再起動シナリオ

管理対象デバイス上の侵入検知および防御エンジンは、*Snort* プロセスと呼ばれます。Snort プロセスがトラフィックインスペクション中に再起動すると、プロセスが再開するまでインスペクションが中断されます。この中断中に、トラフィックがドロップされるか、追加の検査なしで受け渡されるかは、[Snort®の再起動によるトラフィックの動作](#) (356ページ) で説明されているように、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。また、Snort プロセスが再起動するかどうかに関係なく、展開時にリソース需要が高まった結果、いくつかのパケットがインスペクションを実行せずにドロップされることがあります。

次の表に示すいずれかのシナリオでは、Snort プロセスが再起動されます。



表 41: Snort 再起動のシナリオ

再起動のシナリオ	詳細情報
Snort プロセスの再起動が必要な特定の設定を展開した場合。	展開またはアクティブ化された際に Snort プロセスを再起動する設定 (357 ページ)
Snort プロセスを直ちに再起動するように設定を変更した場合。	変更により Snort プロセスがただちに再起動する場合 (360 ページ)
現在展開されている自動アプリケーションバイパス (AAB) 設定のトラフィックをアクティブにした場合。	自動アプリケーションバイパスの設定 (559 ページ)

#### 関連トピック

[アクセスコントロールポリシーの詳細設定 \(1338 ページ\)](#)

[展開またはアクティブ化された際に Snort プロセスを再起動する設定 \(357 ページ\)](#)

## ポリシー適用中のトラフィックの検査

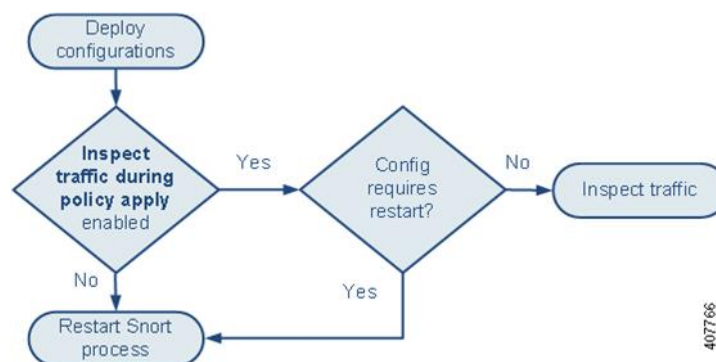
[ポリシー適用時にトラフィックを検査 (Inspect traffic during policy apply)] は、管理対象デバイスが設定変更の展開時にトラフィックを検査できるようにするための詳細アクセスコントロールポリシーの一般設定です。これは、展開する設定で Snort プロセスの再起動が不要な場合に限ります。このオプションは、次のように設定できます。

- [有効 (Enabled)] : 特定の設定で Snort 処理を再起動する必要な場合を除き、トラフィックは展開時に検査されます。

展開する設定に Snort の再起動が必要でなければ、システムは現在展開されているアクセスコントロールポリシーを使用してトラフィックを検査し、導入中に、展開しているアクセスコントロールポリシーに切り替えます。

- [無効 (Disabled)] : 展開時にトラフィックは検査されません。Snort プロセスは展開時に必ず再起動されます。

次の図に、[ポリシー適用時にトラフィックを検査 (Inspect traffic during policy apply)] を有効にした場合と無効にした場合の Snort の再起動の仕組みを示します。





**注意** 展開する際にリソースを要求すると、いくつかの packets がインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。このインスペクション中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。[Snort®の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

## Snort®の再起動によるトラフィックの動作

次の表に、Snort プロセスが再起動した場合のさまざまなデバイスのトラフィックの処理方法を示します。

表 42: 再起動によるトラフィックへの影響 (管理対象デバイスのモデル別)

デバイス モデル	インターフェイスの設定	再起動によるトラフィックの動作
7000 および 8000 シリーズ、 NGIPSv、Firepower Threat Defense、Firepower Threat Defense Virtual	インライン、[フェールセーフ (Failsafe)] が有効または無効	インスペクションなしで受け渡される  [フェールセーフ (Failsafe)] が無効で、Snort がビジーでもダウンしていない場合、いくつかの packets がドロップされることがあります。
	インライン、タップ モード	すぐに packets を出力し、バイパス Snort をコピーする
	パッシブ	中断なし、インスペクションなし
7000 および 8000 シリーズ	ルーテッド、スイッチド、トランスペアレント	ドロップされる
Firepower Threat Defense	ルーテッド、トランスペアレント	ドロップされる

デバイス モデル	インターフェイスの設定	再起動によるトラフィックの動作
ASA FirePOWER	フェールオープン ([トラフィック許可 (Permit Traffic) ]) 状態のルーテッドまたはトランスペアレント	インスペクションなしで受け渡される
	フェールクローズ ([トラフィック クローズ (Close Traffic) ]) 状態のルーテッドまたはトランスペアレント	ドロップされる



- (注) 再起動中に Snort プロセスがダウンした場合のトラフィック処理に加え、フェールセーフ オプションの設定に応じて、トラフィックをインスペクションなしで通過させたり、または Snort プロセスがビジーのときにトラフィックをドロップしたりすることもできます。[Firepower システムのインラインセット \(593 ページ\)](#) を参照してください。

## 展開またはアクティブ化された際に Snort プロセスを再起動する設定

AAB 以外の構成を展開すると、常に Snort プロセスが再起動されます。AAB の展開自体には再起動が伴いませんが、パケットの遅延が大きすぎると、現在展開されている AAB 設定がアクティブになり、Snort プロセスが部分的に再起動されます。

### アクセス コントロール ポリシー (Access Control Policy)

- アクセスコントロールルールの URL カテゴリ/レピュテーションの最初の条件を追加または最後の条件を削除します。
- 現在使用されていない侵入ポリシーを追加するか、または侵入ポリシーの最後のインスタンスを削除することで、アクティブな侵入ポリシーの総数を変更します。アクセスコントロールルールで侵入ポリシーをデフォルトのアクションまたはデフォルトの侵入ポリシーとして使用できます。

### アクセス コントロール ポリシーの詳細設定

- [ポリシー適用時にトラフィックのインスペクションを実行する (Inspect traffic during policy apply) ] が無効な場合に展開します。
- [ファイルとマルウェアの設定 (Files and Malware Settings) ] で、デフォルト以外の値を設定します。
- SSL ポリシーを追加または削除します。
- アダプティブ プロファイルを有効または無効にします。

- [ログセッション/プロトコル配信 (Log Session/Protocol Distribution) ] トラブルシューティング オプションを有効または無効にします。

### セキュリティ インテリジェンス (Security Intelligence)

- 複数のセキュリティ インテリジェンス ホワイトリストまたはブラックリスト ネットワークまたはネットワーク オブジェクトを追加または削除します。Snort プロセスが再開されるかどうかは、インスペクションに使用可能なメモリに応じて、デバイスごとに異なります。

### SSL ポリシー (SSL Policy)

- SSL ルールのカテゴリ/レピュテーションの最初の条件を追加または最後の条件を削除します。

### ファイル ポリシー (File Policy)

- [アーカイブを検査する (Inspect Archives) ] を有効または無効にします。
- ファイルルールで [ファイルを検出 (Detect Files) ] または [ファイルをブロック (Block Files) ] を選択します。
- [ファイルを検出 (Detect Files) ] または [ファイルをブロック (Block Files) ] ルールで、[ストア ファイル (Store files) ] を有効または無効にします。
- [マルウェア クラウドのルックアップ (Malware Cloud Lookup) ] または [マルウェアをブロック (Block Malware) ] ルールアクションと、分析オプション ([Spero 分析または MSEXE (Spero Analysis or MSEXE) ]、[ダイナミック分析 (Dynamic Analysis) ] または [ローカルマルウェア分析 (Local Malware Analysis) ]) またはストアファイルオプション ([マルウェア (Malware) ]、[不明 (Unknown) ]、[クリーン (Clean) ] または [カスタム (Custom) ]) を組み合わせた最初のアクティブ ファイルルールを追加するか、または最後のアクティブ ファイルルールを削除します。

### アイデンティティ ポリシー (Identity Policy)

- SSL 復号化が無効になっている場合 (つまり、アクセス コントロール ポリシーに SSL ポリシーが含まれていない場合) は、最初のアクティブ認証ルールを追加するか、または最後のルールを削除します。

アクティブな認証ルールに [アクティブ認証 (Active Authentication) ] ルールアクションが含まれるか、[パッシブ認証でユーザを識別できない場合にアクティブ認証を使用 (Use active authentication if passive authentication cannot identify user) ] が選択された [パッシブ認証 (Passive Authentication) ] ルールアクションが含まれます。

## ネットワーク分析ポリシー

- 現在使用されていないネットワーク分析ポリシーを追加するか、またはネットワーク分析ポリシーの最後のインスタンスを削除することで、ネットワーク分析ポリシーの総数を変更します。ネットワーク分析ポリシーは、ネットワーク分析ルールと一緒に使用することもできれば、デフォルトのネットワーク分析ポリシーとして使用することもできます。
- IMAP、POP または SMTP プリプロセッサの値を変更します。値は、[Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth] または [Unix-to-Unix Decoding Depth] のいずれかです。

## ネットワーク ディスカバリ (Network Discovery)

- ネットワーク検出ポリシーを使用して、HTTP、FTP、または MDNS プロトコル経由で権限のないトラフィックベースのユーザ検出を有効または無効にします。

## デバイス管理

- ルーティング：7000 または 8000 シリーズ デバイスにルーテッドインターフェイス ペアまたは仮想ルータを追加します。
- VPN：7000 または 8000 シリーズ デバイスで VPN を追加または削除します。



---

**注意** システムは、7000 または 8000 シリーズ デバイスの VPN を追加または削除したときに Snort プロセスが再起動することを警告しません。

---

- MTU：デバイス上のすべての非管理インターフェイスのうちの最大 MTU 値を変更します。
- 従来型デバイスの高可用性：高可用性状態共有オプションを変更します。
- 自動アプリケーションバイパス (AAB)：現在展開されている AAB 構成は、Snort プロセスの誤動作またはデバイスの誤設定により、単一のパケットが過度の処理時間を使用した場合にアクティブになります。その結果、Snort プロセスが部分的に再起動され、非常に大きい遅延が緩和されるか、または完全なトラフィックの停止が防止されます。この部分的な再起動により、デバイスがトラフィックをどのように処理するかに応じて、いくつかのパケットがインスペクションなしで通過するか、またはドロップされます。

## 侵入ルールの更新

- 侵入ルールの更新をインポートした後に展開します。

### システムの更新プログラム

- まれに、システムの更新プログラムが再起動は不要だが、Snort バイナリを更新する場合に、Snort プロセスが再起動されます。
- 脆弱性データベース (VDB) 更新をインストールするか、VDB 更新のインストール後にアクセス コントロール ポリシーを初めて展開します。

### 関連トピック

[設定変更の導入](#) (350 ページ)

[Snort® の再起動シナリオ](#) (354 ページ)

## 変更により Snort プロセスがただちに再起動する場合

以下の変更を行うと、展開プロセスを経ることなく Snort プロセスが直ちに再起動されます。再起動がトラフィックにどのように影響するかは、管理対象デバイスのモデルおよびトラフィックの処理方法によって異なります。詳細については、[Snort® の再起動によるトラフィックの動作](#) (356 ページ) を参照してください。

- アプリケーションまたはアプリケーションディテクタに関する次の操作のいずれかを実行します。
  - システムまたはカスタム アプリケーションディテクタを有効または無効にします。
  - アクティブ化されたカスタム ディテクタを削除します。
  - アクティブ化されたカスタム ディテクタを保存して再アクティブ化します。
  - ユーザ定義のアプリケーションを作成します。

すべての管理対象デバイスで Snort プロセスが再起動します。

- Firepower Threat Defense ハイ アベイラビリティ ペアの作成または解除：プライマリ デバイスとセカンダリ デバイスで Snort プロセスが再起動します。
- 脆弱性データベース (VDB) 更新をインストールするか、VDB 更新のインストール後にアクセス コントロール ポリシーを初めて展開します。
- 7000 または 8000 シリーズ ユーザインターフェイスで Snort プロセスを再起動します ([システム (System) ]> [設定 (Configuration) ]> [プロセス (Process) ])。確認メッセージが表示され、キャンセルすることができます。

## ポリシーの比較

変更後のポリシーが組織の標準に準拠することを確認したり、システムパフォーマンスを最適化したりする目的で、2つのファイルポリシーの間の違いや、保存済みポリシーと実行中のポリシーの間の違いを調べることができます。

比較できるポリシーのタイプは次のとおりです。

- DNS
- ファイル
- ヘルス
- アイデンティティ
- 侵入
- ネットワーク分析
- SSL

比較ビューには、両方のポリシーが並べて表示されます。2つのポリシー間の差異は、次のように強調表示されます。

- 青色は強調表示された設定が2つのポリシーで異なることを示し、差異は赤色で示されません。
- 緑色は強調表示された設定が一方のポリシーには存在するが、他方には存在しないことを示します。

## ポリシーの比較

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	任意 (Any)	機能に応じて異なる	機能に応じて異なる

### 手順

**ステップ 1** 比較するポリシーの管理ページにアクセスします。

- [DNS] : [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [DNS]
- [ファイル (File)] : [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [マルウェアとファイル (Malware & File)]
- [状況 (Health)] : [システム (System)] > [ヘルス (Health)] > [ポリシー (Policy)]
- [ID (Identity)] : [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [ID (Identity)]
- [侵入 (Intrusion)] : [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]
- [ネットワーク分析 (Network Analysis)] : [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access

**Control** ] > [ **侵入 (Intrusion)** ]、次に [ **ネットワーク分析ポリシー (Network Analysis Policy)** ] をクリックします。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

• [ **SSL** ] : [ **ポリシー (Policies)** ] > [ **アクセス コントロール (Access Control)** ] > [ **SSL** ]

**ステップ 2** [ **ポリシーの比較 (Compare Policies)** ] をクリックします。

**ステップ 3** [ **比較対象 (Compare Against)** ] ドロップダウンリストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[ **他のポリシー (Other Policy)** ] を選択します。
- 同じポリシーの 2 つのリビジョンを比較するには、[ **その他のリビジョン (Other Revision)** ] を選択します。
- 現在のアクティブポリシーを他のポリシーに対して比較するには、[ **実行中の設定 (Running Configuration)** ] を選択します。

**ステップ 4** 選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較する場合、[ **ポリシー A (Policy A)** ] ドロップダウンリストと [ **ポリシー B (Policy B)** ] ドロップダウンリストから比較するポリシーを選択します。
- 実行中の設定を別のポリシーと比較する場合、[ **ポリシー B (Policy B)** ] ドロップダウンリストから 2 番目のポリシーを選択します。

**ステップ 5** [ **OK** ] をクリックします。

**ステップ 6** 比較の結果を確認します。

- [ **比較ビューア (Comparison Viewer)** ] : 比較ビューアを使用して、ポリシーの違いを個別に検索するには、タイトルバーの上にある [ **前へ (Previous)** ] または [ **次へ (Next)** ] をクリックします。
- [ **比較レポート (Comparison Report)** ] : 2 つのポリシーの違いを示す PDF レポートを生成するには、[ **比較レポート (Comparison Report)** ] をクリックします。

## ポリシー レポート

ほとんどのポリシーには、2 種類のレポートを生成することができます。単一のポリシーに関するレポートには、現在保存されているポリシー設定の詳細が記載されます。一方、比較レポートには、2 つのポリシー間の違いだけがリストされます。単一ポリシー レポートは、ヘルス ポリシーを除くすべてのポリシー タイプについて生成できます。



(注) 侵入ポリシー レポートには基本ポリシーの設定とポリシー階層の設定が結合され、どちらが基本ポリシーまたはポリシー レイヤのどちらに基づく設定であるかは区別されません。



## 現在のポリシー レポートの生成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	任意 (Any)	機能に応じて異なる	機能に応じて異なる

### 手順

**ステップ 1** レポートを生成するポリシーの管理ページにアクセスします。

- [アクセス制御 (Access Control) ] : [ポリシー (Policies) ] > [アクセスコントロール (Access Control) ]
- [DNS] : [ポリシー (Policies) ] > [アクセスコントロール (Access Control) ] > [DNS]
- [ファイル (File) ] : [ポリシー (Policies) ] > [アクセスコントロール (Access Control) ] > [マルウェアとファイル (Malware & File) ]
- [ヘルス (Health) ] : [システム (System) ] > [ヘルス (Health) ] > [ポリシー (Policy) ]
- [ID (Identity) ] : [ポリシー (Policies) ] > [アクセスコントロール (Access Control) ] > [ID (Identity) ]
- [侵入 (Intrusion) ] : [ポリシー (Policies) ] > [アクセスコントロール (Access Control) ] > [侵入 (Intrusion) ]
- [デバイスの NAT (NAT for 7000 & 8000 シリーズ devices) ] : [デバイス (Devices) ] > [NAT]
- [ネットワーク分析 (Network Analysis) ] : [ポリシー (Policies) ] > [アクセスコントロール (Access Control) ]、次に [ネットワーク分析ポリシー (Network Analysis Policy) ] をクリックします。または [ポリシー (Policies) ] > [アクセスコントロール (Access Control) ] > [侵入 (Intrusion) ]、次に [ネットワーク分析ポリシー (Network Analysis Policy) ] をクリックします。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

- [SSL] : [ポリシー (Policies) ] > [アクセスコントロール (Access Control) ] > [SSL]

**ステップ 2** レポートの生成対象とするポリシーの横にあるレポートアイコン (📄) をクリックします。

## 失効ポリシー

Firepower システムは、失効したポリシーに赤色のステータス テキストでマークを付けます。このテキストには、ポリシーの更新を必要とするターゲットデバイスの数が示されます。失効ステータスをクリアするには、ポリシーをデバイスに再展開する必要があります。

ポリシーの再展開が必要な設定変更には次のものがあります。

- アクセスコントロールポリシー自体の変更：アクセスコントロールルール、デフォルトアクション、ポリシーターゲット、セキュリティインテリジェンスフィルタリング、前処理などの詳細オプションの変更。
- アクセスコントロールポリシーが呼び出すポリシーの変更：SSLポリシー、ネットワーク分析ポリシー、侵入ポリシー、ファイルポリシー、アイデンティティポリシー、またはDNSポリシー。
- 呼び出されるアクセスコントロールポリシーで使用される再利用可能オブジェクトまたは設定の変更：
  - ネットワーク、ポート、VLAN タグ、URL、地理位置情報オブジェクト
  - セキュリティインテリジェンスリストおよびフィード
  - アプリケーションフィルタまたはディテクタ
  - 侵入ポリシーの変数セット
  - ファイルリスト
  - 復号関連のオブジェクトとセキュリティゾーン
- システムソフトウェア、侵入ルール、または脆弱性データベース（VDB）の更新。

Web インターフェイスの複数の場所からこれらの設定の一部を変更できることに留意してください。たとえば、オブジェクトマネージャ（**[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]**）を使用してセキュリティゾーンを変更できますが、デバイスの設定（**[デバイス (Devices)] > [デバイス管理 (Device Management)]**）でインターフェイスのタイプを変更すると、ゾーンも変更され、ポリシーの再展開が必要になります。

次の更新では、ポリシーの再展開は必要ありません。

- セキュリティインテリジェンスフィードへの自動更新およびコンテキストメニューを使用したセキュリティインテリジェンスのグローバルブラックリストおよびホワイトリストへの追加
- URL フィルタリングデータへの自動更新
- スケジュールされた位置情報データベース（GeoDB）の更新

## 限定的な導入のパフォーマンスに関する考慮事項

システムはホスト、アプリケーション、ユーザ検出データを使用することで、ネットワークの完全な最新プロファイルを作成できます。また、システムが侵入検知および防御システム（IPS）として機能して、ネットワークトラフィックを分析して侵入およびエクスプロイトを検出し、オプションで問題のあるパケットをドロップすることもできます。

検出とIPSを組み合わせることで、ネットワークアクティビティにコンテンツが提供され、次のような多くの機能を利用することができます。

- 侵害の影響フラグと表示。これによって、どのホストが特定の 익스プロイト、攻撃、またはマルウェアに対して脆弱であるかが示されます。
- アダプティブプロファイルの更新と Firepower の推奨事項。これによって、宛先ホストに応じてトラフィックを個別に検査できます。
- 相関。これによって、影響を受けるホストに応じて別々に侵入（およびその他のイベント）に応答できます。

ただし、組織がIPSまたは検出のみを実行することを目的としている場合は、システムのパフォーマンスを最適化できる設定がいくつかあります。

## 侵入防御のない検出

検出機能では、ネットワークトラフィックをモニタして、ネットワーク上のホストの数とタイプ（ネットワーク デバイスを含む）だけでなく、それらのホスト上のオペレーティング システム、アクティブなアプリケーション、およびオープンポートを判断できます。管理対象デバイスをネットワークのユーザアクティビティをモニタするように設定することもできます。検出データを使用して、トラフィック プロファイリングを実行し、ネットワーク コンプライアンスを評価し、ポリシー違反に応答できます。

基本的な展開（検出と単純なネットワークベースのアクセス制御のみ）では、アクセスコントロールポリシーの設定時にいくつかの重要なガイドラインに従うことで、デバイスのパフォーマンスを向上させることができます。



- (注) それが一にすべてのトラフィックを許可する場合であっても、アクセスコントロールポリシーを使用する必要があります。ネットワーク検出ポリシーが実行できるのは、アクセスコントロールポリシーが通過を許可したトラフィックを検査することのみです。

最初に、アクセスコントロールポリシーは複雑な処理を必要とせず、単純なネットワークベースの基準のみを使用してネットワークトラフィックを処理することを確認します。次の**すべての**ガイドラインを実装する必要があります。これらのオプションのいずれかを誤って設定すると、パフォーマンス上の利点がなくなります。

- セキュリティ インテリジェンス機能を使用**しないで**ください。入力されたグローバル ホワイトリストまたはブラックリストをポリシーのセキュリティ インテリジェンスの設定から削除します。
- モニタアクションまたはインタラクティブブロックアクションにアクセスコントロールルールを**含まない**でください。許可、信頼、およびブロックルールのみを使用します。許可されたトラフィックは検出によって検査できますが、信頼されたトラフィックとブロックされたトラフィックは検査できないことに留意してください。

- アプリケーション、ユーザ、URL、ISE 属性、または位置情報ベースのネットワーク条件にアクセス コントロール ルールを含めないでください。単純なネットワークベースの条件（ゾーン、IP アドレス、VLAN タグ、およびポート）のみを使用します。
- ファイル、マルウェア、または侵入インスペクションを実行するアクセス コントロール ルールを含めないでください。つまり、ファイルポリシーまたは侵入ポリシーをアクセス コントロール ルールに関連付けしないでください。
- アクセス コントロール ポリシーのデフォルトの侵入ポリシーが [アクティブなルールなし (No Rules Active) ] に設定されていることを確認します。
- ポリシーのデフォルトアクションとして [ネットワーク検出のみ (Network Discovery Only) ] を選択します。侵入インスペクションを実行するポリシーのデフォルトアクションを選択しないでください。

アクセス コントロール ポリシーと組み合わせて、ネットワーク検出ポリシーを設定して適用できます。このポリシーは、システムが検出データについて検査をするネットワークセグメント、ポート、およびゾーンを指定し、ホスト、アプリケーション、およびユーザがセグメント、ポート、およびゾーンで検出されるかどうかを指定します。

#### 関連トピック

[デフォルトの侵入ポリシー](#) (1837 ページ)

## ディスカバリのない侵入防御

侵入検知および防御機能によって、侵入とエクスプロイトの有無についてネットワークトラフィックを分析できます。またオプションで違反パケットをドロップできます。侵入インスペクションを実行するがディスカバリ（検出）データを利用する必要がない場合は、ディスカバリを無効にして、デバイスのパフォーマンスを向上させることができます。



- (注) アプリケーション、ユーザ、または URL の制御を実行する場合は、パフォーマンス上の利点を得るためにディスカバリを無効にすることは**できません**。システムがディスカバリデータを保存しないようにすることはできますが、システムはそれらの機能を実行するためにディスカバリデータを収集して検査する**必要があります**。

ディスカバリを無効にするには、次の**すべての**ガイドラインを実行します。いずれかでも誤って設定すると、パフォーマンス上の利点がなくなります。

- アクセス コントロール ポリシーでは、デバイスが適切にライセンス済みであっても、アプリケーション条件、ユーザ条件、URL 条件、ISE 属性条件、または地理位置情報ベースのネットワーク条件を持つルールを含めないでください。単純なネットワークベースの条件（ゾーン、IP アドレス、VLAN タグ、およびポート）のみを使用します。
- ネットワーク検出ポリシーからすべてのルールを削除します。

アクセスコントロールポリシーとネットワーク検出ポリシーを展開すると、新しいディスカバリがターゲットデバイスで停止します。システムは、ネットワーク検出ポリシーで指定されたタイムアウト期間に応じて、ネットワークマップ内の情報を段階的に削除します。また、すべてのディスカバリデータを即座に消去することもできます。





## 第 17 章

# ルール管理：共通の特性

以下のトピックでは、Firepower Management Center でさまざまなポリシーのルールの共通特性を管理する方法について説明します。

- [ルールの概要 \(369 ページ\)](#)
- [ルール条件タイプ \(371 ページ\)](#)
- [ルールの検索 \(409 ページ\)](#)
- [デバイス別のフィルタリングルール \(410 ページ\)](#)
- [ルールとその他のポリシーの警告 \(411 ページ\)](#)
- [ルールのパフォーマンスに関するガイドライン \(412 ページ\)](#)

## ルールの概要

さまざまなポリシー内のルールで、ネットワークトラフィックをきめ細かく制御できます。システムは最初の一致のアルゴリズムを使用して、指定した順番でルールに照らし合わせてトラフィックを評価します。

これらのルールはポリシー全体で一貫していない他の設定を含んでいる場合もありますが、次のような多くの基本的な特性や設定メカニズムは共通です。

- **条件**：ルールの条件は各ルールが処理するトラフィックを指定します。各ルールには複数の条件を設定できます。トラフィックがルールに一致するには、すべての条件に一致する必要があります。
- **アクション**：ルールのアクションによって、一致するトラフィックの処理方法が決まります。選択できる [アクション (Action)] リストがルールにない場合でも、ルールには関連付けられたアクションが1つある点に注意してください。たとえば、カスタムネットワーク分析ルールはそのルールの「アクション」としてネットワーク分析ポリシーを使用します。別の例としては、QoS ルールの場合、どの QoS ルールでもトラフィックのレート制限という同じ動作をするため、明示的なアクションはありません。
- **位置**：ルールの位置は評価の順番を決定します。ポリシーを使ってトラフィックを評価すると、システムは指定した順序でトラフィックとルールを照合します。通常は、システムによるトラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初のルールに従って行われます (トラフィックフローの追跡と記録を行うがトラフィックフ

ローには影響しないモニタールールは例外です)。適切なルールの順序を指定することで、ネットワークトラフィックの処理に必要なリソースが削減され、ルールのプリエンブションを回避できます。

- **カテゴリ**：いくつかのルールタイプを整理するために、各親ポリシーでカスタムのルールカテゴリを作成できます。
- **ロギング**：多くのルールでは、ルールが処理する接続をシステムがロギングするかどう  
か、およびロギングの処理方法は、ロギングの設定によって制御されます。一部のルール  
(IDルールやネットワーク分析ルールなど)にはロギング設定は含まれません。これは、  
ルールが接続の最終的な性質を決定するわけではなく、またそのルールが接続をロギング  
するために特別に設計されているわけではないためです。別の例としては、QoSルールに  
はロギングの設定は含まれていません。これは、レート制限されているというだけの理由  
で接続をロギングすることはできないためです。
- **コメント**：一部のルールタイプでは、変更を保存するたびにコメントを追加できます。た  
とえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載  
することができます。



#### ヒント

多くのポリシーエディタでは、右クリックメニューで編集、削除、移動、有効化、無効化など、数多くのルール管理オプションへのショートカットを提供しています。

#### 共通の特性を持つルール

この章では、以下のルールや設定に見られる多くの共通の側面について説明しています。共通していない設定の情報については、以下を参照してください。

- **アクセスコントロールルール**：[アクセスコントロールルール \(1343 ページ\)](#)
- **トンネルとプレフィルタルール**：[トンネルとプレフィルタルールのコンポーネント \(1408 ページ\)](#)
- **SSL ルール**：[SSL ルールの作成および変更 \(1472 ページ\)](#)
- **DNS ルール**：[DNS ルールの作成および編集 \(1389 ページ\)](#)
- **ID ルール**：[アイデンティティルールの作成 \(2193 ページ\)](#)
- **ネットワーク分析ルール**：[ネットワーク分析ルールの設定 \(1842 ページ\)](#)
- **QoS ルール**：[QoS ルールの設定 \(722 ページ\)](#)
- **インテリジェントアプリケーションバイパス (IAB)**：[インテリジェントアプリケーションバイパス \(1415 ページ\)](#)
- **アプリケーションフィルタ**：[アプリケーションフィルタ \(439 ページ\)](#)



### 共通の特性のないルール

次のルールの設定は、この章では説明していません。

- 侵入ルール：ルールを使用した侵入ポリシーの調整 (1619 ページ)
- ファイルルール：ファイルルール (1542 ページ)
- 関連ルール：関連ルールの設定 (2227 ページ)
- NATルール (クラシック)：7000 および 8000 シリーズデバイス用の NAT (1079 ページ)
- NATルール (Firepower Threat Defense)：Firepower Threat Defense 用のネットワーク アドレス変換 (NAT) (1101 ページ)
- 8000 シリーズファストパスルール：高速パスルールの設定 (8000 シリーズ) (561 ページ)

## ルール条件タイプ

次の表は、この章に記述している一般的なルールの条件について説明し、使用設定を列挙します。

条件	トラフィック制御方法	対応しているルール/設定
<a href="#">インターフェイス条件 (374 ページ)</a>	送信元インターフェイスと宛先インターフェイス、対応している場合にはトンネルゾーン	アクセスコントロールルール トンネルルール プレフィルタルール SSLルール DNSルール アイデンティティルール ネットワーク分析ルール QoSルール
<a href="#">ネットワーク条件 (377 ページ)</a>	送信元 IP アドレスと宛先 IP アドレス、対応している場合には地理的な場所や発信側のクライアント	アクセスコントロールルール プレフィルタルール SSLルール DNSルール アイデンティティルール ネットワーク分析ルール QoSルール

条件	トラフィック制御方法	対応しているルール/設定
トンネルエンドポイント条件 (380 ページ)	プレーンテキスト用、送信元のトンネルエンドポイント宛先のトンネルエンドポイント、パススルートンネル	トンネルルール
VLAN 条件 (382 ページ)	VLAN タグ	アクセスコントロールルール トンネルルール プレフィルタルール SSL ルール DNS ルール アイデンティティルール ネットワーク分析ルール
ポートおよび ICMP コードの条件 (382 ページ)	送信元ポート、宛先ポート、プロトコル、ICMP コード	アクセスコントロールルール プレフィルタルール SSL ルール アイデンティティルール QoS ルール
カプセル化の条件 (385 ページ)	カプセル化プロトコル (非暗号化)	トンネルルール
アプリケーション条件 (アプリケーション制御) (386 ページ)	アプリケーションまたはアプリケーション特性 (タイプ、リスク、ビジネスの関連性、カテゴリ、タグ)	アクセスコントロールルール SSL ルール アイデンティティルール QoS ルール アプリケーションフィルタ インテリジェントアプリケーションバイパス (IAB)
URL 条件 (URL フィルタリング) (393 ページ)	URL、対応している場合には、URL の特性 (カテゴリおよびレピュテーション)	アクセスコントロールルール SSL ルール QoS ルール

条件	トラフィック制御方法	対応しているルール/設定
ユーザ条件、レلم条件、および ISE 属性条件 (ユーザ制御) (401 ページ)	ホストのログイン権限のあるユーザまたはそのユーザのレلم、グループ、または ISE 属性	アクセスコントロールルール SSL ルール (ISE 属性なし) QoS ルール
カスタム SGT 条件 (406 ページ)	カスタムセキュリティグループタグ (SGT)	アクセスコントロールルール

## ルール条件の仕組み

ルール条件では、各ルールで処理するトラフィックを指定します。各ルールに複数の条件を設定し、トラフィックがルールに一致するにはすべての条件を満たす必要があります。使用可能な条件タイプは、ルールタイプによって異なります。

ルールエディタには、条件タイプごとに独自のタブがあります。一致させるトラフィック特性を選択して条件を作成します。一般に、左側の使用可能な項目のリスト (1 つまたは 2 つ) から基準を選択し、それらの基準を右側の選択済み項目のリスト (1 つまたは 2 つ) に追加します。たとえば、アクセスコントロールルールの URL 条件では、URL カテゴリとレピュテーション基準を組み合わせて、ブロックする Web サイトのグループを 1 つ作成できます。

条件を作成しやすくするために、レلم、ISE 属性、さまざまなタイプのオブジェクトやオブジェクトグループなど、さまざまなシステム提供の構成やカスタム構成を使用して、トラフィックを照合できます。多くの場合、ルール基準は手動で指定できます。

### 送信元と宛先の基準

ルールに送信元と宛先の基準 (ゾーン、ネットワーク、ポート) が含まれる場合、通常は一方または両方の基準を制約として使用できます。両方を使用する場合、一致するトラフィックの発信元は、指定した送信元のゾーン、ネットワーク、またはポートのいずれかであり、宛先のゾーン、ネットワーク、またはポートのいずれかから送出される必要があります。

### 条件ごとの項目

最大 50 個の項目を各条件に追加できます。送信元と宛先の基準を含むルールでは、それぞれ最大 50 個使用できます。選択した項目のいずれかに一致するトラフィックが条件に一致します。

### 単純なルールの仕組み

ルールエディタには、次の一般的な選択肢があります。条件の作成の詳細な手順については、各条件タイプのトピックを参照してください。

- 項目の選択 (Choose Item) : 項目をクリックするか、そのチェックボックスにマークを付けます。多くの場合、Ctrl または Shift キーを使用して複数の項目を選択するか、右クリックして [すべて選択 (Select All)] を選択できます。

- 検索 (Search) : 検索フィールドに基準を入力します。入力するとリストが更新されます。項目名が検索され、オブジェクトとオブジェクトグループについては、その値が検索されます。リロード (🔄) またはクリア (✖) をクリックして検索をクリアします。
- 事前定義された項目の追加 (Add Predefined Item) : 1つ以上の使用可能な項目を選択し、[追加 (Add)] ボタンをクリックするか、ドラッグアンドドロップします。無効な項目 (重複、無効な組み合わせなど) は追加できません。
- 手動項目の追加 (Add Manual Item) : [選択済み (Selected)] 項目リストの下のフィールドをクリックし、有効な値を入力して [追加 (Add)] をクリックします。ポートを追加すると、ドロップダウンリストからプロトコルも選択できます。
- オブジェクトの作成 (Create Object) : 追加アイコン (➕) をクリックし、作成する条件ですぐに使用できる新しい再利用可能オブジェクトを作成し、オブジェクトマネージャで管理できます。この方法を使用してアプリケーションフィルタをその場で追加した場合、別のユーザ作成フィルタが含まれるフィルタを保存することはできません。
- 削除 (Delete) : 項目の削除アイコン (🗑) をクリックするか、1つ以上の項目を選択し、右クリックして [選択項目の削除 (Delete Selected)] を選択します。

## インターフェイス条件

インターフェイスルールの条件は送信元インターフェイスと宛先インターフェイスによってトラフィックを制御します。

ルールタイプと導入環境でのデバイスにより、セキュリティゾーンやインターフェイスグループと呼ばれる定義済みのインターフェイスオブジェクトを使用してインターフェイス条件を構築できます。インターフェイスオブジェクトはネットワークをセグメント化して複数のデバイス間でインターフェイスをグループ化することによってトラフィックフローを制御し、分類しやすくします。[インターフェイスオブジェクト：インターフェイスグループとセキュリティゾーン \(437 ページ\)](#) を参照してください。



### ヒント

インターフェイスによってルールを制約するのは、システムパフォーマンスを改善するための最適な方法の1つです。ルールがデバイスのすべてのインターフェイスを除外する場合、そのルールはそのデバイスのパフォーマンスに影響しません。

インターフェイスオブジェクト内のすべてのインターフェイスが同じタイプ (すべてインライン、パッシブ、スイッチド、ルーテッド、または ASA FirePOWER) である必要があるのと同様に、インターフェイス条件で使用されているすべてのインターフェイスオブジェクトは同じタイプである必要があります。パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブ展開では宛先インターフェイスでルールを制約することはできません。

### トンネルゾーンとセキュリティゾーン

一部の設定では、セキュリティゾーンの代わりにトンネルゾーンを使用してインターフェイス条件を制約できます。トンネルゾーンではプレフィルタを使用して、カプセル化された接続の特定のタイプに合わせて後続のトラフィック処理を調整できます。



- (注) トンネルゾーンの制約がサポートされる設定の場合、再区分された接続、つまり割り当てられたトンネルゾーンを持つ接続はセキュリティゾーンの制約と一致しません。詳細については、[トンネルゾーンおよびプレフィルタリング \(1410 ページ\)](#) を参照してください。

### インターフェイス条件を持つルール

ルールタイプ	セキュリティゾーンのサポート	トンネルゾーンのサポート	インターフェイスグループのサポート
アクセスコントロール	Yes	Yes	No
トンネルとプレフィルタ	Yes	該当なし。プレフィルタポリシー内でトンネルゾーンを割り当てます	Yes
SSL	Yes	No	No
DNS (送信元のみ)	Yes	No	No
ID (Identity)	Yes	No	No
ネットワーク分析	Yes	No	No
QoS (ルーテッドのみ、必須)	Yes	No	Yes

### 例：セキュリティゾーンを使用したアクセス制御

ホストにインターネットへの無制限接続を提供しつつ、それでも着信トラフィックで侵入およびマルウェアの有無を検査することでホストを保護したいという展開を想定します。

最初に、内部と外部の2つのセキュリティゾーンを作成します。次に、1つ以上のデバイスでインターフェイスのペアをこれらのゾーンに割り当てます。この際、1つのインターフェイスは内部ゾーンの各ペアに割り当て、1つは外部ゾーンに割り当てます。内部側のネットワークに接続されたホストは、保護されている資産を表します。



- (注) 内部（または外部）のすべてのインターフェイスを1つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティポリシーが意味をなすグループ化を選択します。

次に、宛先ゾーンの条件が内部に設定されているアクセスコントロールルールを設定します。この単純なルールでは、内部ゾーンのいずれかのインターフェイスからデバイスを離れるトラフィックが照合されます。一致するトラフィックを侵入やマルウェアについて検査するには、ルールアクションとして[許可 (Allow)]を選択し、そのルールを侵入ポリシーとファイルポリシーに関連付けます。

## インターフェイス条件の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 始める前に

- (アクセスコントロールのみ) セキュリティゾーンではなくトンネルゾーンによってトラフィックを制約する場合は、関連付けられたプレフィルタポリシーがそれらのゾーンを割り当てるようにします。[アクセス制御への他のポリシーの関連付け \(1340ページ\)](#) を参照してください。

### 手順

**ステップ1** ルールエディタで、インターフェイス条件のタブをクリックします。

- インターフェイスグループおよびセキュリティゾーン（トンネル、プレフィルタ、QoS）：[\[インターフェイスオブジェクト \(Interface Objects\)\]](#) タブをクリックします。
- セキュリティゾーン（アクセスコントロール、SSL、DNS、アイデンティティ、ネットワーク分析）：[\[ゾーン \(Zones\)\]](#) タブをクリックします。
- トンネルゾーン（アクセスコントロール）：[\[ゾーン \(Zones\)\]](#) タブをクリックします。

**ステップ2** [\[使用可能なインターフェイスオブジェクト \(Available Interface Objects\)\]](#) または [\[利用可能なゾーン \(Available Zones\)\]](#) リストから追加するインターフェイスを見つけて選択します。

(アクセスコントロールのみ) 再ゾーン分割されたトンネルでの接続を一致させるには、セキュリティゾーンではなくトンネルゾーンを選択します。同じルールでトンネルゾーンとセキュリティゾーンを使用することはできません。詳細については、[トンネルゾーンおよびプレフィルタリング \(1410ページ\)](#) を参照してください。

**ステップ3** [送信元に追加 (Add to Source) ]または[宛先に追加 (Add to Destination) ]をクリックするか、またはドラッグアンドドロップします。

**ステップ4** ルールを保存するか、編集を続けます。

---

#### 次のタスク

- (アクセスコントロールのみ) プレフィルタ中にトンネルを再ゾーン分割した場合、完全なカバレッジを確保する必要がある場合は追加のルールを設定します。再ゾーン分割されたトンネルでの接続は、セキュリティゾーン制約があるルールに一致しません。詳細については、[トンネルゾーンの使用 \(1411 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ネットワーク条件

ネットワーク ルールの条件では、内部ヘッダーを使用して、送信元と宛先の IP アドレスを基準にトラフィックを制御します。外部ヘッダーを使用するトンネルルールでは、ネットワーク条件の代わりにトンネルエンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々の IP アドレスまたはアドレス ブロックを手動で指定することもできます。



(注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

---

#### ネットワーク条件での地理位置情報

ルールによっては、送信元または宛先の地理的位置を使用してトラフィックを照合することもできます。ルールのタイプが地理位置情報をサポートするものであれば、ネットワーク条件と地理位置情報条件を混在させることができます。トラフィックのフィルタリングに最新の地理位置情報データが使用されるよう、地理位置情報データベース (GeoDB) を定期的に更新することを強くお勧めします。

#### ネットワーク条件での元のクライアント (プロキシトラフィックのフィルタリング)

一部のルールでは、発信元クライアントに基づいてプロキシトラフィックを処理できます。送信元ネットワーク条件を使用してプロキシサーバを指定し、次に元のクライアント制約を追加して元のクライアント IP アドレスを指定します。システムはパケットの X-Forwarded-For (XFF)、True-Client-IP、またはカスタム定義 HTTP ヘッダー フィールドを使用して、元のクライアント IP を判別します。

プロキシの IP アドレスがルールの送信元ネットワークの制約と一致する場合、トラフィックはルールに一致し、元のクライアントの IP アドレスは、ルールの元のクライアント制約に一致します。たとえば、特定の元のクライアントアドレスからのトラフィックを許可するものの、それが特定のプロキシを使用している場合のみに限定するには、以下の3つのアクセスコントロールルールを作成します。

アクセスコントロールルール 1：特定の IP アドレス（209.165.201.1）からの非プロキシトラフィックをブロックします。

送信元ネットワーク：209.165.201.1  
元のクライアントネットワーク：none または any  
アクション：ブロック

アクセスコントロールルール 2：同じ IP アドレスからのプロキシトラフィックを許可します。ただし、そのトラフィックのプロキシサーバが、選択したもの（209.165.200.225 または 209.165.200.238）である場合に限りです。

送信元ネットワーク：209.165.200.225 および 209.165.200.238  
元のクライアントネットワーク：209.165.201.1  
アクション：許可

アクセスコントロールルール 3：同じ IP アドレスからのプロキシトラフィックを、それが他のプロキシサーバを使用する場合はブロックします。

送信元ネットワーク：any  
元のクライアントネットワーク：209.165.201.1  
アクション：ブロック

#### ネットワーク条件を使用したルール

ルールタイプ	地理位置情報による制約のサポート	元のクライアントによる制約のサポート
アクセスコントロール	Yes	Yes
プレフィルタ	No	No
SSL	Yes	No
DNS（送信元ネットワークのみ）	No	No
ID（Identity）	Yes	No
ネットワーク分析	No	No
QoS	Yes	No



## ネットワーク条件の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** ルールエディタで、[ネットワーク (Networks)] タブをクリックします。

**ステップ 2** [利用可能なネットワーク (Available Networks)] リストから追加する定義済みネットワークを見つけて選択します。

ルールが地理位置情報をサポートしている場合は、ネットワークと地理位置情報の基準を同じルールに混在させることができます。

- [ネットワーク (Networks)] : [ネットワーク (Networks)] サブタブをクリックして、ネットワークを選択します。
- [地理位置情報 (Geolocation)] : [地理位置情報 (Geolocation)] サブタブをクリックして、地理位置情報オブジェクトを選択します。

**ステップ 3** (オプション) ルールが元のクライアント制約をサポートしている場合は、[送信元ネットワーク (Source Networks)] で、プロキシされたトラフィックを元のクライアントに基づいて処理するようにルールを設定します。

- [送信元/プロキシ (Source/Proxy)] : [送信元 (Source)] サブタブをクリックして、プロキシサーバを指定します。
- [元のクライアント (Original Client)] : [元のクライアント (Original Client)] サブタブをクリックして、ネットワークを元のクライアント制約として追加します。プロキシ接続では、元のクライアントの IP アドレスは、ルールに一致するネットワークの 1 つと一致する必要があります。

**ステップ 4** [送信元に追加 (Add to Source)]、[元のクライアントに追加 (Add to Original Client)]、または [宛先に追加 (Add to Destination)] をクリックするか、またはドラッグアンドドロップします。

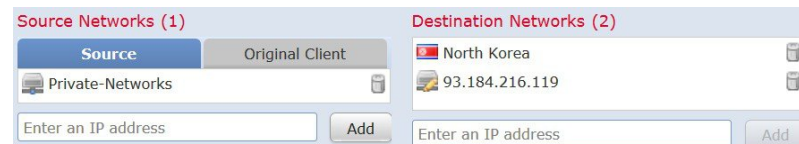
**ステップ 5** 手動で指定するネットワークを追加します。送信元、元のクライアント、または宛先 IP アドレスかアドレスブロックを入力し、[追加 (Add)] をクリックします。

(注) システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

**ステップ 6** ルールを保存するか、編集を続けます。

#### 例：アクセスコントロールルールのネットワーク条件

次の図は、内部ネットワークから発生し、北朝鮮または 93.184.216.119 (example.com) のリソースにアクセスしようとする接続をブロックするアクセスコントロールルールのネットワーク条件を示しています。



この例で、「Private Networks」と呼ばれるネットワークオブジェクトグループ（図に示されていない IPv4 および IPv6 プライベート ネットワークのネットワーク オブジェクトから構成されます）は、内部ネットワークを表します。また、example.com の IP アドレスを手動で指定し、システムが提供する北朝鮮の地理位置情報オブジェクトを使用して北朝鮮の IP アドレスを表しています。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## トンネルエンドポイント条件

トンネルエンドポイント条件は、トンネルルールに固有のものです。この条件は、他のルールタイプのネットワーク条件と似ています。

トンネルエンドポイント条件は、特定のタイプのプレーンテキスト、パススルートンネル（[カプセル化の条件 \(385 ページ\)](#)）を制御します。この制御は、それらの送信元と宛先の IP アドレスによって、外側のカプセル化ヘッダーを使用して行います。これらは、トンネルエンドポイントの IP アドレス、つまり、トンネルのいずれかの側のネットワーク デバイスのルーテッドインターフェイスです。

トンネルルールはデフォルトでは双方向で、送信元エンドポイントのいずれかと宛先エンドポイントのいずれかとの間の一致するすべてのトンネルを処理します。ただし、送信元から宛先へのトラフィックのみに一致する単方向トンネルルールを設定できます。[トンネルとプレフィルタ ルールのコンポーネント \(1408 ページ\)](#) を参照してください。

事前定義済みのネットワーク オブジェクトを使用してトンネルエンドポイント条件を作成したり、個々の IP アドレスまたはアドレス ブロックを手動で指定したりできます。



- (注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

## トンネル エンドポイント条件の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

- ステップ 1** ルールエディタで、[トンネル エンドポイント (Tunnel Endpoints)] タブをクリックします。
- ステップ 2** [利用可能なトンネル エンドポイント (Available Tunnel Endpoints)] リストから追加する定義済みネットワークを見つけて選択します。
- トンネル エンドポイントは、トンネルの両側にあるネットワーク デバイスのルーテッドインターフェイスの IP アドレスであるため、ネットワーク オブジェクトを使用してトンネル エンドポイント条件を作成できます。
- ステップ 3** [送信元に追加 (Add to Source)] または [宛先に追加 (Add to Destination)] をクリックするか、またはドラッグ アンド ドロップします。
- トンネルルールはデフォルトでは双方向であるため、2つのエンドポイント間のすべてのトラフィックを処理できます。ただし、送信元からのトンネルのみを照合するよう選択した場合、トンネルルールは、送信元から宛先へのトラフィックのみに一致します。
- ステップ 4** 手動で指定するエンドポイントを追加します。送信元か宛先の IP アドレス、またはアドレスブロックを入力し、[追加 (Add)] をクリックします。
- (注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。
- ステップ 5** ルールを保存するか、編集を続けます。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## VLAN 条件

VLANルール条件によって、VLANタグ付きトラフィックが制御されます。システムでは、プレフィルタ ポリシー（そのルールで最も外側の VLAN タグを使用する）を除き、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

事前定義のオブジェクトを使用して VLAN 条件を作成でき、また **1 ~ 4094** の VLAN タグを手動で入力することもできます。VLAN タグの範囲を指定するには、ハイフンを使用します。



- (注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の VLAN タグを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

### VLAN 条件が含まれたルール

次のルール タイプでは、VLAN 条件がサポートされます。

- アクセス コントロール
- トンネルとプレフィルタ（最も外側の VLAN タグを使用）
- SSL
- DNS
- アイデンティティ
- ネットワーク分析

## ポートおよび ICMP コードの条件

ポート条件を使用することで、トラフィックの送信元および宛先のポートに応じてそのトラフィックを制御できます。ルールのタイプによって、「ポート」は次のいずれかを表します。

- TCP と UDP : TCP および UDP トラフィックは、トランスポート層プロトコルに基づいて制御できます。システムは、カッコ内に記載されたプロトコル番号 + オプションの関連ポートまたはポート範囲を使用してこの設定を表します。例 : TCP(6)/22。
- ICMP : ICMP および ICMPv6 (IPv6 ICMP) トラフィックは、そのインターネット層プロトコルと、オプションでタイプおよびコードに基づいて制御できます。例 : ICMP(1):3:3
- ポートなし : ポートを使用しない他のプロトコルを使用してトラフィックを制御できません。

### 送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポートプロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。たとえば、DNS over TCP および DNS over UDP の両方を 1 つのアクセスコントロールルールの送信元ポート条件として追加できます。

### ポート条件を使用した非 TCP トラフィックの照合

非 TCP トラフィックを照合するためのポート条件を設定することはできますが、いくつかの制約事項があります。

- **アクセスコントロールルール**：クラシックデバイスの場合、GRE でカプセル化されたトラフィックをアクセスコントロールルールに照合するには、宛先ポート条件として GRE（47）プロトコルを使用します。GRE 制約ルールには、ネットワークベースの条件（ゾーン、IP アドレス、ポート、VLAN タグ）のみを追加できます。また、GRE 制約ルールが設定されたアクセスコントロールポリシーでは、システムが外側のヘッダーを使用して**すべての**トラフィックを照合します。Firepower Threat Defense デバイスの場合、GRE でカプセル化されたトラフィックを制御するには、プレフィルタポリシーでトンネルルールを使用します。
- **SSL ルール**：SSL ルールは TCP ポート条件のみをサポートします。
- **アイデンティティルール**：システムは非 TCP トラフィックに対してアクティブ認証を適用できません。アイデンティティルールのアクションが [アクティブ認証 (Active Authentication)] の場合、あるいは [パッシブ認証でユーザを識別できない場合はアクティブ認証を使用する (Use active authentication if passive authentication cannot identify user)] オプションをオンにする場合は、TCP ポート制約のみを使用してください。アイデンティティルールアクションが [パッシブ認証 (Passive Authentication)] または [認証なし (No Authentication)] である場合、非 TCP トラフィックに基づいてポート条件を作成できます。



**注意** SSL復号が無効の場合（つまりアクセスコントロールポリシーにSSLポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作（356 ページ）](#)を参照してください。

アクティブ認証ルールには [アクティブ認証 (Active Authentication)] ルールアクションが含まれているか、または [パッシブ認証でユーザを識別できない場合はアクティブ認証を使用する (Use active authentication if passive authentication cannot identify user)] が選択された [パッシブ認証 (Passive Authentication)] ルールアクションが含まれています。

- ICMP エコー：タイプ 0 が設定された宛先 ICMP ポート、またはタイプ 129 が設定された宛先 ICMPv6 ポートは、要求されていないエコー応答だけと照合されます。ICMP エコー要求への応答として送信される ICMP エコー応答は無視されます。ルールですべての ICMP エコーに一致させるには、ICMP タイプ 8 または ICMPv6 タイプ 128 を使用してください。

### ポート条件を使用したルール

次のルールは、ポート条件をサポートします。

- アクセス コントロール
- プレフィルタ
- SSL (TCP トラフィックのみをサポート)
- アイデンティティ (アクティブ認証は TCP トラフィックのみをサポート)
- QoS

## ポート条件の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

## 手順

- 
- ステップ1** ルールエディタで、[ポート (Ports)] タブをクリックします。
- ステップ2** [利用可能なポート (Available Ports)] リストから追加する定義済みポートを見つけて選択します。
- ステップ3** [送信元に追加 (Add to Source)] または [宛先に追加 (Add to Destination)] をクリックするか、またはドラッグアンドドロップします。
- ステップ4** 手動で指定する送信元ポートまたは宛先ポートを追加します。
- [送信元 (Source)]: プロトコルを選択し、0 から 65535 までのポートを1つ入力して [追加 (Add)] をクリックします。
  - [宛先 (ICMP 以外) (Destination (non-ICMP))]: プロトコルを選択または入力します。プロトコルを指定しない場合、または [TCP] か [UDP] を選択した場合は、0 から 65535 までのポートを1つ入力します。[追加 (Add)] をクリックします。
  - [宛先 (ICMP) (Destination (ICMP))]: [プロトコル (Protocol)] ドロップダウンリストから [ICMP] または [IPv6-ICMP] を選択し、表示されるポップアップウィンドウでタイプおよび関連するコードを選択します。ICMP タイプとコードの詳細については、Internet Assigned Numbers Authority (IANA) の Web サイトを参照してください。
- ステップ5** ルールを保存するか、編集を続けます。
- 

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## カプセル化の条件

カプセル化の条件は、トンネルルールに固有です。

この条件では、カプセル化プロトコルによって特定のタイプのプレーンテキスト、パススルートンネルを制御します。ルールを保存する前に、一致するプロトコルを1つ以上選択する必要があります。次のオプションを選択できます。

- GRE (47)
- IP-in-IP (4)
- IPv6-in-IP (41)
- Teredo (UDP (17) /3455)

## アプリケーション条件（アプリケーション制御）

システムはIPトラフィックを分析する際、ネットワークで一般的に使用されているアプリケーションを識別および分類できます。このディスカバリベースのアプリケーション認識は、アプリケーション制御、つまりアプリケーショントラフィック制御機能の基本です。

システム提供のアプリケーションフィルタは、アプリケーションの基本特性（タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ）にしたがってアプリケーションを整理することで、アプリケーション制御に役立ちます。システム提供のフィルタの組み合わせやアプリケーションの任意の組み合わせをもとに、ユーザ定義の再利用可能フィルタを作成できます。

アプリケーションフィルタと個別に指定されたアプリケーションの両方を使用することで、完全なカバレッジを確保できます。

アプリケーション制御の一部として、コンテンツ規制を適用するアクセスコントロールルール（セーフサーチやYouTube EDUなど）を使用することもできます。

### アプリケーションフィルタの利点

アプリケーションフィルタにより、迅速にアプリケーション制御を設定できます。たとえば、システム提供のフィルタを使って、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセスコントロールルールを簡単に作成できます。ユーザがそれらのアプリケーションの1つを使用しようとする、システムがセッションをブロックします。

アプリケーションフィルタを使用することで、ポリシーの作成と管理は簡単になります。この方法によりアプリケーショントラフィックが期待どおりに制御されます。シスコは、システムと脆弱性データベース（VDB）の更新を通して、頻繁にアプリケーションディテクタを更新しています。このため、アプリケーショントラフィックは常に最新のディテクタによってモニタされます。また、独自のディテクタを作成し、どのような特性のアプリケーションを検出するかを割り当て、既存のフィルタを自動的に追加することもできます。

### アプリケーション条件の設定

次の表に示す設定を行い、アプリケーション制御を実行します。この表には、設定する内容により、アプリケーション制御にどのような制約を設けることができるかも示します。

設定 (Configuration)	タイプ、リスク、関連性、カテゴリ	タグ	ユーザ定義のフィルタ	コンテンツ規制
アクセスコントロールルール	Yes	Yes	Yes	Yes



設定 (Configuration)	タイプ、リスク、関連性、カテゴリ	タグ	ユーザ定義のフィルタ	コンテンツ規制
SSL ルール	Yes	No : SSL プロトコルタグによって、自動的に暗号化アプリケーショントラフィックに制約される	No	No
ID ルール (アクティビティ認証からアプリケーションを免除)	Yes	No : ユーザーエージェント除外タグによって、自動的に制約される	No	No
QoS ルール	Yes	Yes	Yes	No
オブジェクトマネージャ内のユーザ定義のアプリケーションフィルタ	Yes	Yes	No : ユーザー定義のフィルタのネストは不可	No
インテリジェントアプリケーションバイパス (IAB)	Yes	Yes	Yes	No

関連トピック

[概要 : アプリケーション検出 \(2097 ページ\)](#)

## アプリケーション条件とフィルタの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

アプリケーションの条件またはフィルタを作成するには、使用可能なアプリケーションのリストから、トラフィックを制御するアプリケーションを選択します。オプションとして (推奨)、フィルタを使用して使用可能なアプリケーションを抑制します。フィルタと個別に指定されたアプリケーションを同じ条件で使用できます。



## 始める前に

- アクセス コントロール ルールでアプリケーション制御を実行するためには、[適応型プロファイルの設定 \(2016 ページ\)](#) で説明されているように、アダプティブプロファイルを有効 (デフォルト状態) にする **必要があります**。

## 手順

**ステップ 1** ルール エディタまたは設定エディタを起動します。

- アクセス コントロール、SSL、QoS ルール条件：ルール エディタで [アプリケーション (Applications)] タブをクリックします。
- アイデンティティルール条件：ルールエディタで [レルムおよび設定 (Realms & Settings)] タブをクリックし、アクティブ認証を有効にします。[アイデンティティルールの作成 \(2193 ページ\)](#) を参照してください。
- アプリケーション フィルタ：オブジェクト マネージャの [アプリケーション フィルタ (Application Filters)] ページで、アプリケーション フィルタを追加または編集します。フィルタの一意の **名前** を指定します。
- インテリジェント アプリケーション バイパス (IAB)：アクセス コントロール ポリシー エディタで [詳細 (Advanced)] タブをクリックし、IAB の設定を編集して、[バイパス可能なアプリケーションおよびフィルタ (Bypassable Applications and Filters)] をクリックします。

**ステップ 2** (オプション) セーフサーチ () または YouTube EDU () のグレー表示のアイコンおよび設定関連のオプションをクリックして、アクセス コントロール ルールのコンテンツ制限機能を有効にします。

その他の設定要件については、[アクセス コントロール ルールを使用したコンテンツ制限の実施 \(1427 ページ\)](#) を参照してください。

たいいていの場合、コンテンツ制限を有効にすると、条件の [選択されたアプリケーションおよびフィルタ (Selected Applications and Filters)] リストに適切な値が入力されます。コンテンツ制限を有効にするときに、コンテンツ制限に関係するアプリケーションまたはフィルタがすでにリスト内に存在している場合には、システムはリストに自動的に値を入力することはしません。

アプリケーションを絞り込んで選択内容をフィルタする手順を続行するか、またはスキップしてルールの保存に進みます。

**ステップ 3** [使用可能なアプリケーション (Available Applications)] リストから追加するアプリケーションを見つけて選択します。

[使用可能なアプリケーション (Available Applications)] に表示されるアプリケーションを抑制するには、1つ以上の **アプリケーション フィルタ** を選択するか、個別のアプリケーションを検索します。使用可能なアプリケーションを抑制した後に、**フィルタに一致するすべてのアプリケーション** を追加したり、個別のアプリケーションを選択および追加したりできます。

**ヒント** サマリー情報とインターネットの検索リンクを表示するには、アプリケーションの横の情報アイコン (i) をクリックします。ロック解除アイコン (🔓) は、システムが復号されたトラフィックでのみ識別できるアプリケーションを示します。

フィルタを単独または組み合わせて選択すると、[使用可能なアプリケーション (Available Applications)] リストが更新され、条件を満たすアプリケーションのみが表示されます。システムによって提供されるフィルタは組み合わせて選択できますが、ユーザ定義フィルタはできません。

- 同じ特性 (リスク、ビジネス関連性など) の複数のフィルタ : アプリケーショントラフィックは1つのフィルタのみに一致する必要があります。たとえば、中リスクフィルタと高リスクフィルタの両方を選択すると、[使用可能なアプリケーション (Available Applications)] リストにすべての中リスク アプリケーションと高リスク アプリケーションが表示されます。
- 異なるアプリケーション特性のフィルタ : アプリケーショントラフィックは、両方のフィルタタイプに一致する必要があります。たとえば、高リスク フィルタとビジネスとの関連性が低いフィルタの両方を選択すると、[使用可能なアプリケーション (Available Applications)] リストに両方の条件を満たすアプリケーションのみが表示されます。

**ステップ 4** [ルールに追加 (Add to Rule)] をクリックするか、ドラッグアンドドロップします。

**ヒント** フィルタとアプリケーションをさらに追加する前に、[フィルタのクリア (Clear Filters)] をクリックして現在の選択をクリアします。

Web インターフェイスでは、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。

**ステップ 5** ルールまたは設定を保存するか、編集を続けます。

---

#### 例 : アクセス コントロール ルールのアプリケーション条件

次の図は、MyCompany のユーザ定義アプリケーションフィルタ、リスクが高くビジネスとの関連性が低いすべてのアプリケーション、ゲームアプリケーション、および個々に選択されたいくつかのアプリケーションをブロックするアクセスコントロールルールのアプリケーション条件を示しています。



次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

## アプリケーションの特性

システムは、次の表に示す基準を使用して、検出された各アプリケーションの特性を判別します。これらの特性をアプリケーションフィルタとして使用します。

表 43: アプリケーションの特性

特性	説明	例
タイプ (Type)	<p>アプリケーションプロトコルは、ホスト間の通信を意味します。</p> <p>クライアントは、ホスト上で動作しているソフトウェアを意味します。</p> <p>Web アプリケーションは、HTTP トラフィックの内容または要求された URL を意味します。</p>	<p>HTTP と SSH はアプリケーションプロトコルです。</p> <p>Web ブラウザと電子メールクライアントはクライアントです。</p> <p>MPEG ビデオと Facebook は Web アプリケーションです。</p>
リスク (Risk)	<p>アプリケーションが組織のセキュリティポリシーに違反することがある目的で使用される可能性。</p>	<p>ピアツーピアアプリケーションはリスクが極めて高いと見なされます。</p>
ビジネスとの関連性 (Business Relevance)	<p>アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。</p>	<p>ゲームアプリケーションはビジネスとの関連性が極めて低いと見なされません。</p>
カテゴリ (Category)	<p>アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも1つのカテゴリに属します。</p>	<p>Facebook はソーシャルネットワーキングのカテゴリに含まれます。</p>

特性	説明	例
タグ	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。	ビデオストリーミング Web アプリケーションには、ほとんどの場合、high bandwidth と displays ads というタグが付けられます。

## アプリケーション制御の制限

### アダプティブ プロファイルが有効になっていることの確認

アダプティブ プロファイルが無効な場合（デフォルト状態）、アクセス コントロール ルールは、アプリケーション制御を実行できません。

### アプリケーション ディテクタの自動有効化

ディテクタが検出対象のアプリケーションに対して有効でない場合、システムは、そのアプリケーションに対応するシステム提供のすべてのディテクタを自動的に有効にします。存在しない場合、システムはそのアプリケーション対応で最近変更されたユーザ定義のディテクタを有効にします。

### アプリケーション 識別の速度

システムは、次が実行されるまで、インテリジェント アプリケーション バイパス (IAB) とレート制限を含めアプリケーション制御を実行できません。

- モニタ対象の接続がクライアントとサーバの間で確立され、
- システムがセッションでアプリケーションを識別する

この識別は 3～5 パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に行われる必要があります。

早期のトラフィックがその他のすべての基準に一致するが、アプリケーション識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、SSL ハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッショントラフィックに適切なアクションを適用します。

アクセス コントロールの場合、これらの受け渡されたパケットは、アクセス コントロール ポリシーのデフォルトの侵入ポリシー（デフォルトアクション侵入ポリシーでもほぼ一致するルール of 侵入ポリシーでもない）によりインスペクションが実行されます。

### アプリケーションや他のルールより前に配置される URL ルール

URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルールより前に配置します。特に、URL ルールがブロック ルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。

- その他のルールがアプリケーション条件を含んでいる。

- 検査対象のトラフィックが暗号化されている。

### 暗号化および復号トラフィックのアプリケーション制御

システムは暗号化トラフィックと復号トラフィックを識別し、フィルタ処理することができます。

- 暗号化トラフィック：システムは、SMTPS、POPS、FTPS、TelnetS、IMAPSを含むStartTLSで暗号化されたアプリケーショントラフィックを検出できます。さらに、TLS ClientHelloメッセージのServer Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。これらのアプリケーションにSSL Protocol タグが付けられます。SSL ルールでは、これらのアプリケーションのみを選択できます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。
- 復号トラフィック：システムは、復号されたトラフィック（暗号化されたまたは暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションにdecrypted traffic タグを割り当てます。

### アプリケーションのアクティブ認証の免除

アイデンティティ ポリシーでは、特定のアプリケーションのアクティブ認証を免除し、トラフィックにアクセス コントロールの続行を許可できます。これらのアプリケーションには、User-Agent Exclusion タグが付けられます。アイデンティティ ルールでは、これらのアプリケーションのみを選択できます。

### ペイロードのないアプリケーショントラフィック パケットの処理

アクセスコントロールを実行している場合、システムは、アプリケーションが識別された接続内にペイロードがないパケットに対してデフォルト ポリシー アクションを適用します。

### 参照されるアプリケーショントラフィックの処理

アドバタイズメントトラフィックなどのWebサーバによって参照されるトラフィックを処理するには、参照しているアプリケーションではなく、参照されるアプリケーションを照合します。

### 複数のプロトコルを使用するアプリケーショントラフィックの制御 (Skype)

システムは、Skypeの複数のタイプのアプリケーショントラフィックを検出できます。Skypeのトラフィックを制御するには、個々のアプリケーションを選択するのではなく、[アプリケーションフィルタ (Application Filters)] リストから[Skype] タグを選択します。これにより、システムは同じ方法でSkypeのすべてのトラフィックを検出してコントロールできるようになります。

### コンテンツ制限機能用にサポートされる検索エンジン

システムは、特定の検索エンジンの場合のみ、セーフサーチフィルタリングをサポートします。システムは、これらの検索エンジンからのアプリケーショントラフィックに safesearch supported タグを割り当てます。

#### 関連トピック

[デフォルトの侵入ポリシー](#) (1837 ページ)

[アプリケーション検出に関する特殊な考慮事項](#) (2102 ページ)

## URL 条件 (URL フィルタリング)

URL 条件は、ネットワークのユーザがアクセスできる Web サイトを制御します。この機能は、URL フィルタリングと呼ばれます。

- カテゴリおよびレピュテーションベースの URL フィルタリング：URL フィルタリングライセンスでは、URL の一般的な分類 (カテゴリ) とリスク レベル (レピュテーション) に基づいて Web サイトへのアクセスを制御することができます。
- 手動 URL フィルタリング：任意のライセンスで、個々の URL、URL のグループおよび URL リストとフィードを手動で指定し、Web トラフィックのきめ細かいカスタム制御を実現できます。

Web サイトをブロックするときは、ユーザのブラウザにデフォルト動作を許可するか、またはシステムによって提供される一般的なページまたはカスタム HTTP 応答ページを表示できます。インタラクティブブロッキングは、警告ページをクリックスルーすることで Web サイトのブロックをバイパスする機会をユーザに与えます。詳細については、[HTTP 応答ページとインタラクティブブロッキング](#) (1369 ページ) を参照してください。

#### URL 条件を伴うルール

次の表に、URL 条件をサポートするルールと、各ルールタイプがサポートするフィルタリングのタイプを一覧します。

ルールタイプ	カテゴリとレピュテーションのサポートフィルタリングの有無	手動フィルタリングのサポート
アクセスコントロール	Yes	Yes
SSL	Yes	なし。代わりに識別名条件を使用
QoS	Yes	Yes

### レピュテーションベースの URL フィルタリング

URL フィルタリングライセンスでは、要求された URL のカテゴリおよびレピュテーションに基づいて、Web サイトへのアクセスを制御できます。

- **カテゴリ**：URL の一般的な分類。たとえば `ebay.com` はオークションカテゴリ、`monster.com` は求職カテゴリに属します。1 つの URL は複数のカテゴリに属することができます。
- **レピュテーション**：この URL が、組織のセキュリティ ポリシーに違反するかもしれない目的で使用される可能性がどの程度であるか。レピュテーションは、高リスク（レベル 1）からウェルノウン（レベル 5）の範囲です。



(注) イベントで URL カテゴリおよびレピュテーション情報を表示するには、URL 条件を使用して少なくとも 1 つのルールを作成する必要があります。また、Cisco Collective Security Intelligence (CSI) との通信を有効にして、最新の脅威インテリジェンスを取得する必要があります。

### レピュテーションベースの URL フィルタリングの利点

URL カテゴリとレピュテーションによって、URL フィルタリングをすぐに設定できます。たとえば、アクセス コントロールを使用して、乱用薬物カテゴリの高リスク URL をブロックできます。または、QoS を使用して、ストリーミング メディア カテゴリのサイトからのトラフィックをレート制限することができます。

カテゴリおよびレピュテーションデータを使用すると、ポリシーの作成と管理がより簡単になります。この方法では、システムが Web トラフィックを期待どおりに確実に制御します。脅威インテリジェンスは、新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは確実に最新の情報を使用して要求された URL をフィルタ処理します。セキュリティに対する脅威を表すサイトや望ましくないコンテンツが表示されるサイトは、ユーザーが新しいポリシーを更新したり展開したりするペースを上回って次々と現れては消える可能性があります。

システムはどのように適応するのか、いくつかの例を示します。

- アクセス コントロールルールですべてのゲーム サイトをブロックする場合、新しいドメインが登録されてゲームに分類されると、これらのサイトをシステムで自動的にブロックできます。同様に、QoS ルールですべてのストリーミング メディア サイトをレート制限する場合、システムは新しいストリーミング メディア サイトへのトラフィックを自動的に制限できます。
- アクセス コントロールルールですべてのマルウェア サイトをブロックし、あるブログ ページがマルウェアに感染すると、システムはその URL をブログからマルウェアに再分類して、そのサイトをブロックすることができます。
- アクセス コントロールルールでリスクの高いソーシャル ネットワーキング サイトをブロックし、だれかがプロフィールページに悪意のあるペイロードへのリンクが含まれるリンクを掲載すると、システムはそのページのレピュテーションを無害なサイトから高リスクに変更してブロックすることができます。

### 関連トピック

[集成型セキュリティ インテリジェンスの通信設定オプション](#)（1559 ページ）

[Snort® の再起動シナリオ](#)（354 ページ）



## 手動 URL フィルタリング

アクセス コントロール ルールおよび QoS ルールでは、個々の URL、URL のグループ、または URL のリストとフィールドを手動でフィルタリングすることで、カテゴリとレピュテーションベースの URL のフィルタリングを補足したり、選択的にオーバーライドしたりできます。



- (注) 多数の URL をフィルタリングする場合、個別の、またはグループ化された URL オブジェクトを使用する代わりに、URL リストを使用します。詳細については、[セキュリティインテリジェンスのリストとフィールド \(464 ページ\)](#) を参照してください。

特殊なライセンスなしでこのタイプの URL フィルタリングを実行することができます。手動 URL フィルタリングは SSL ルールではサポートされません。その代わりに、識別名の条件を使用します。

たとえば、アクセス コントロールを使用して組織に適していない Web サイトのカテゴリをブロックできます。ただし、カテゴリに適切な Web サイトが含まれていて、そこにアクセスを提供する必要がある場合は、そのサイトに手動で許可ルールを作成し、カテゴリのブロックルールの前に配置できます。

特定の URL を手動でフィルタリングする場合、影響を受ける可能性のある他のトラフィックについて慎重に検討してください。ネットワーク トラフィックが URL 条件に一致するかどうか判断するために、システムは単純な部分文字列マッチングを実行します。要求された URL が文字列の一部に一致すると、URL が一致したと見なされます。

たとえば `example.com` へのすべてのトラフィックを許可する場合、ユーザは次の URL を含むサイトを参照できます。

- `http://example.com/`
- `http://example.com/newexample`
- `http://www.example.com/`

別の例として、`ign.com` (ゲーム サイト) を明示的にブロックする場合を考えてください。部分文字列マッチングにより `ign.com` 自体だけでなく `verisign.com` もブロックされることになり、意図しない動作が生じる可能性があります。

### 関連トピック

[セキュリティインテリジェンスのリストとフィールド \(464 ページ\)](#)

## URL 条件の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
URL フィルタリング (カテゴリ/レピュテーション) 任意 (手動)	URL フィルタリング (カテゴリ/レピュテーション) 任意 (手動)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

URL 条件を作成するときに、トラフィックを制御する URL カテゴリを選択します。必要に応じて、URL カテゴリをレピュテーションで制約できます。

アクセス コントロールおよび QoS ルールでは、事前定義された URL オブジェクト、URL リストとフィード、および手動のルールごとの URL を使用して個々の URL をフィルタ処理することもできます。これらの URL はレピュテーションで制約できません。手動 URL フィルタリングは SSL ルールではサポートされません。その代わりに、識別名の条件を使用します。



### 注意

アクセス コントロールまたは SSL (ただし QoS ではない) ルールの URL またはカテゴリ/レピュテーションの最初の条件を追加するかまたは最後の条件を削除すると設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### 手順

**ステップ 1** ルールエディタで、URL 条件のタブをクリックします。

- アクセス コントロールまたは QoS : [URL (URLs) ] タブをクリックします。
- SSL : [カテゴリ (Category) ] タブをクリックします。

**ステップ 2** 制御する URL を見つけて選択します。

- カテゴリ : URL の URL カテゴリを選択するか、デフォルトの [任意 (Any) ] のままにします。アクセス コントロールまたは QoS ルールでは、[カテゴリ (Category) ] サブタブをクリックしてカテゴリを選択します。
- URL オブジェクト、リスト、およびフィード : 定義済みの URL オブジェクトおよび URL リストとフィードを選択します。アクセス コントロールまたは QoS ルールでは、[URL (URLs) ] サブタブをクリックして URL を選択します。

**ステップ 3** (オプション) レピュテーションを選択して URL カテゴリを制約します。

レピュテーション レベルを選択すると、ルールアクションに応じて、選択したレベルよりも重大または重大でない他のレピュテーションも含まれます。ルールアクションを変更すると、URL 条件のレピュテーション レベルが自動的に変更されます。

- [より重大でないレピュテーションを含める (Includes less severe reputations) ] : ルールで Web トラフィックを許可または信頼する場合。たとえば、無害なサイト (レベル 4) を許可するようアクセスコントロールルールを設定した場合、有名 (レベル 5) サイトも自動的に許可されます。
- [より重大なレピュテーションを含める (Includes more severe reputations) ] : ルールで Web トラフィックをレート制限、復号、ブロック、またはモニタする場合。たとえば、疑わしいサイト (レベル 2) をブロックするようアクセスコントロールルールを設定した場合、高リスク (レベル 1) のサイトも自動的にブロックされます。

**ステップ 4** [ルールに追加 (Add to Rule) ] をクリックするか、ドラッグアンドドロップします。

**ステップ 5** (オプション) アクセスコントロールまたは QoS ルールでは、URL を入力し、[追加 (Add) ] をクリックして、手動で指定する URL を追加します。

URL または IP アドレスを入力できます。このフィールドでは、ワイルドカードはサポートされません。

**ステップ 6** ルールを保存するか、編集を続けます。

**例 : アクセスコントロールルールの URL 条件**

次の図は、すべてのマルウェアサイト、すべての高リスクサイト、およびすべての有害なソーシャルネットワーキングサイトをブロックするアクセスコントロールルールの URL 条件を示しています。また、単一サイト example.com (URL オブジェクトによって表されます) もブロックされます。



次の表では、条件を作成する方法を要約します。

ブロックする URL	カテゴリまたは URL オブジェクト	レピュテーション
マルウェア サイト (レピュテーションに関係なく)	マルウェア サイト (Malware Sites)	任意 (Any)
高リスクの URL (レベル 1)	任意 (Any)	1 - 高リスク (High Risk)

ブロックする URL	カテゴリまたは URL オブジェクト	レピュテーション
無害 (benign) よりも大きいリスクがあるソーシャルネットワークワーキング サイト (レベル 1 ~ 3)	ソーシャル ネットワーク (Social Network)	3-セキュリティリスクのある無害なサイト (Benign sites with security risks)
example.com	example.com という名前の URL オブジェクト	none

### 次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

## HTTPS トラフィックのフィルタリング

暗号化されたトラフィックをフィルタリングするには、システムはSSLハンドシェイク時に渡される情報 (トラフィックを暗号化するために使用される公開キー証明書のサブジェクト共通名) に基づいて、要求された URL を決定します。

HTTPS フィルタリングは、HTTP フィルタリングとは異なり、サブジェクト共通名内のサブドメインを無視します。アクセスコントロールまたは QoS ポリシーで HTTPS URL を手動でフィルタリングする場合は、サブドメイン情報を含めないでください。たとえば、www.example.com ではなく、example.com を使用します。

また、HTTPS フィルタリングは URL リストもサポートしていません。代わりに、URL オブジェクトとグループを使用する必要があります。



### ヒント

SSL ポリシーでは、特定の URL に対するトラフィックの処理と復号は、識別名の SSL ルール条件を定義することで行えます。証明書のサブジェクト識別名にある共通名属性には、サイトの URL が含まれています。HTTPS トラフィックを復号すると、アクセスコントロールルールが復号されたセッションを評価できるようになるため、URL フィルタリングが改善します。

### 暗号化プロトコルによるトラフィックの制御

アクセスコントロールまたは QoS ポリシー内で URL フィルタリングを実行する場合、暗号化プロトコル (HTTP または HTTPS) は無視されます。これは、手動およびレピュテーションベース両方の URL 条件で発生します。つまり、URL フィルタリングは、次の Web サイトへのトラフィックを同じように扱います。

- http://example.com/
- https://example.com/

HTTP または HTTPS トラフィックのみに一致するルールを設定するには、アプリケーション条件をルールに追加します。たとえば、あるサイトへの HTTPS アクセスを許可する一方で、HTTP アクセスを許可しないようにできます。そのためには、2つのアクセスコントロールルールを作成し、それぞれにアプリケーションと URL の条件を割り当てます。

最初のルールは Web サイトへの HTTPS トラフィックを許可します。

Action: Allow  
Application: HTTPS  
URL: example.com

2番目のルールは同じ Web サイトへの HTTP アクセスをブロックします。

Action: Block  
Application: HTTP  
URL: example.com

## URL フィルタリングの制限

### URL 識別の速度

システムは以下の動作の前に URL をフィルタリングできません。

- モニタ対象の接続がクライアントとサーバの間で確立される。
- システムがセッションで HTTP または HTTPS アプリケーションを識別する。
- システムが要求された URL を識別する (ClientHello メッセージまたはサーバ証明書からの暗号化されたセッションの場合)。

この識別は3～5パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に行われる必要があります。

早期のトラフィックがその他のすべてのルール条件に一致するが、識別が不完全な場合、システムは、パケットの受け渡しと接続の確立 (または、SSL ハンドシェイクの完了) を許可します。システムは識別を完了した後、残りのセッショントラフィックに適切なルールアクションを適用します。

アクセス制御の場合、これらの受け渡されたパケットは、デフォルトアクション侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもなく、アクセス制御ポリシーのデフォルトの侵入ポリシーによりインスペクションが実行されます。

### アプリケーションや他のルールより前に配置される URL ルール

URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルールより前に配置します。特に、URL ルールがブロックルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。

- その他のルールがアプリケーション条件を含んでいる。
- 検査対象のトラフィックが暗号化されている。

### カテゴリまたはレピュテーションが不明な URL

URL のカテゴリまたはレピュテーションが不明な場合、Web サイトの閲覧は、カテゴリまたはレピュテーションベースの URL 条件を持つルールには一致しません。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

### 手動 URL フィルタリング

特定の URL を手動でフィルタリングする場合は、影響を受ける可能性のある他のトラフィックを慎重に考慮してください。ネットワーク トラフィックが URL 条件に一致するかどうか判別するために、システムは単純な部分文字列マッチングを実行します。要求された URL が文字列の任意の部分に一致する場合、URL は一致するとみなされます。

### 暗号化された Web トラフィックの URL フィルタリング

暗号化された Web トラフィックに対して URL フィルタリングを実行すると、システムは次のように動作します。

- 暗号化プロトコルを無視します。ルールに URL 条件はあるがプロトコルを指定するアプリケーション条件がない場合、ルールは HTTPS および HTTP 両方のトラフィックを照合します。
- URL リストを使用しません。代わりに、URL オブジェクトとグループを使用する必要があります。
- トラフィックを暗号化するために使用する公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合し、サブジェクト共通名に含まれるサブドメインを無視します。
- アクセス制御ルール（または、その他の設定）によってブロックされている暗号化された接続の場合は HTTP 応答ページを表示しません。[HTTP 応答ページの制限 \(1370 ページ\)](#)を参照してください。

### URL での検索クエリ パラメータ

システムでは、URL 条件の照合に URL 内の検索クエリ パラメータを使用しません。たとえば、すべてのショッピング トラフィックをブロックする場合を考えます。amazon.com を探すために Web 検索を使用してもブロックされませんが、amazon.com を閲覧しようとするするとブロックされます。

### 選択したデバイス モデルのメモリ制限

メモリの制約上、一部のモデルでは、小規模でそれほど細分化されていないカテゴリとレピュテーションによってほとんどの URL フィルタリングが実行されます。たとえば、親 URL のサブサイトがそれぞれ異なる URL カテゴリとレピュテーションを持っている場合でも、一部のデバイスでは、親 URL のデータのみが保存される場合があります。これらのデバイスによって処理される Web トラフィックの場合、システムはクラウドルックアップを実行して、ローカルデータベースにないサイトのカテゴリとレピュテーションを判断できます。

メモリが少ないデバイスには、7100 ファミリと次の ASA モデルが含まれます：ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X。NGIPSv で、カテゴリおよびレピュテーション ベースの URL フィルタリングを実行するための正しいメモリ量を割り当てる方法について、詳しくは *Firepower System Virtual Installation Guide* を参照してください。

#### 関連トピック

[デフォルトの侵入ポリシー](#)（1837 ページ）

## ユーザ条件、レلم条件、およびISE属性条件（ユーザ制御）

Firepower システムによって収集された権限のあるユーザアイデンティティデータを使用してユーザ制御を実行することができます。

アイデンティティソースはユーザがログインまたはログアウトする際、またはMicrosoft Active Directory (AD) またはLDAP のクレデンシャルを使用して認証する際にユーザをモニタします。次に、この収集されたアイデンティティデータを使用して、モニタ対象ホストに関連付けられているログインしている権限のあるユーザに基づいてトラフィックを処理するルールを設定できます。ユーザは、そのユーザがログオフする（アイデンティティソースによって報告される）か、レلمがセッションをタイムアウトするか、システムのデータベースからそのユーザデータが削除されるまで、ホストに関連付けられたままになります。

Firepower システムのご使用のバージョンでサポートされる権限のあるユーザアイデンティティソースについては、[ユーザアイデンティティソースについて](#)（2121 ページ）を参照してください。

ユーザ制御を実行するために、次のルール条件を使用できます。

- ユーザ条件およびレلم条件：ホストのログインしている権限のあるユーザに基づいてトラフィックを照合します。トラフィックは、レلم、個々のユーザ、またはそれらのユーザが属しているグループに基づいて制御できます。
- ISE 属性条件：ユーザの、ISE が割り当てたセキュリティグループタグ (SGT)、デバイスタイプ（エンドポイントプロファイルとも呼ばれる）、またはロケーション IP（エンドポイントロケーションとも呼ばれる）に基づいてトラフィックを照合します。ISE をアイデンティティソースとして設定する必要があります。



(注) 一部のルールでは、カスタム SGT 条件が ISE によって割り当てられなかった SGT 属性にタグ付けされたトラフィックを照合できます。これはユーザ制御とはみなされず、ISE をアイデンティティソースとして使用していない場合にのみ機能します。[カスタム SGT 条件](#)（406 ページ）を参照してください。

## ユーザ条件を持つルール

ルールタイプ	ユーザ条件およびレルム条件のサポート	ISE 属性条件のサポート
アクセス コントロール	Yes	Yes
SSL	Yes	No
QoS	Yes	Yes

## 関連トピック

[ユーザエージェントのアイデンティティ ソース \(2123 ページ\)](#)

[ISE アイデンティティ ソース \(2126 ページ\)](#)

[ターミナルサービス \(TS\) エージェントのアイデンティティ ソース \(2131 ページ\)](#)

[キャプティブ ポータルのアイデンティティ ソース \(2133 ページ\)](#)

## ユーザ制御の前提条件

## アイデンティティ ソース/認証方式の設定

実行する認証タイプのアイデンティティ ソースを設定します。詳細については、[ユーザアイデンティティ ソースについて \(2121 ページ\)](#) を参照してください。

ユーザエージェント、TS エージェント、または ISE デバイスのモニタ対象に多くのユーザグループを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、Firepower Management Center のユーザ制限が原因で、システムがグループに基づいてユーザマッピングをドロップすることがあります。その結果、レルム、ユーザ、またはユーザグループの条件のルールが、一致することが想定されているトラフィックと一致しなくなる可能性があります。

## レルムの設定

監視対象の各 AD または LDAP サーバ (ISE、ユーザエージェント、および TS エージェントサーバを含む) のレルムを設定し、ユーザのダウンロードを実行します。詳細については、[レルムの作成 \(2185 ページ\)](#) を参照してください。

レルムを設定するときには、アクティビティを監視するユーザおよびユーザ・グループを指定します。ユーザグループを含めると、自動的に、すべてのセカンダリグループのメンバーを含む、そのグループのすべてのメンバーが含まれます。ただし、セカンダリグループをルール条件として使用する場合は、セカンダリグループをレルム構成に明示的に含める必要があります。

レルムごとに、ユーザデータの自動ダウンロードを有効にすると、ユーザおよびユーザグループの信頼できるデータを更新することができます。



### アイデンティティ ポリシーの作成

レルムを認証方式に関連付けるアイデンティティポリシーを作成し、そのポリシーをアクセス制御に関連付けます。詳細については、[アイデンティティポリシーの作成 \(2192 ページ\)](#) を参照してください。

デバイスのユーザ制御（アクセス制御、SSL、QoS）を実行するポリシーは、アイデンティティポリシーを共有します。そのアイデンティティポリシーによって、それらのデバイス上のトラフィックに影響するルールで使用できるレルム、ユーザ、およびグループが決まります。

QoS ルールでユーザ条件を設定する前に、QoS ポリシーの対象となるデバイスが、デバイスに適用されたアクセス制御ポリシーで定義されている正しいアイデンティティポリシーを使用していることを確認する必要があります。同じデバイスに適用された QoS ポリシーとアクセス制御ポリシーは明示的にリンクされていないため、QoS ルールエディタで無効なレルム、ユーザ、およびグループを選択することが可能です。これらの無効な要素は、Firepower Management Center に存在するが、QoS 対象のデバイスには適用されないアイデンティティポリシーから取得された要素です。これらの要素を使用すると、実際に適用されるまで、無効な選択をしたことが判別されません。

## ユーザおよびレルム条件の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

レルム、またはそのレルム内のユーザとユーザ グループでルールを制約できます。

### 始める前に

- [ユーザ条件、レルム条件、および ISE 属性条件 \(ユーザ制御\) \(401 ページ\)](#) で説明されているユーザ制御の前提条件を満たしてください。

### 手順

- ステップ 1** ルール エディタで、[ユーザ (Users) ] タブをクリックします。
- ステップ 2** (オプション) [利用可能なレルム (Available Realms) ] リストから使用するレルムを見つけて選択します。
- ステップ 3** (オプション) [有効なユーザ (Available Users) ] リストからユーザとグループを選択して、ルールをさらに制約します。
- ステップ 4** [ルールに追加 (Add to Rule) ] をクリックするか、ドラッグアンドドロップします。
- ステップ 5** ルールを保存するか、編集を続けます。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ISE 属性条件の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 始める前に

- [ユーザ条件、レulum条件、および ISE 属性条件 \(ユーザ制御\) \(401 ページ\)](#) に記載されているユーザ制御の前提条件を満たします。

### 手順

**ステップ 1** ルール エディタで、ISE 属性条件のタブをクリックします。

- アクセス コントロール : [SGT/ISE 属性 (SGT/ISE Attributes) ] タブをクリックします。
- QoS : [ISE 属性 (ISE Attributes) ] タブをクリックします。

ISE 属性条件を制約するために、ISE 割り当てセキュリティグループタグ (SGT) を使用できます。アクセス コントロールルールでカスタム SGT を使用するには、[カスタム SGT 条件 \(406 ページ\)](#) を参照してください。

**ステップ 2** [使用可能な属性 (Available Attributes) ] リストから、使用する ISE 属性を見つけて選択します。

- [セキュリティグループタグ (SGT) (Security Group Tag (SGT)) ]
- [デバイス タイプ (Device Type) ] (エンドポイント プロファイルとも呼ばれます)
- [ロケーション IP (Location IP) ] (エンドポイント ロケーションとも呼ばれます)

**ステップ 3** [使用可能な ISE メタデータ (Available ISE Metadata) ] [使用可能なメタデータ (Available Metadata) ] リストから属性メタデータを選択して、さらにルールを制約します。または、デフォルトの [すべて (any) ] のままにします。

**ステップ 4** [ルールに追加 (Add to Rule) ] をクリックするか、ドラッグ アンド ドロップします。

**ステップ 5** (オプション) [ロケーション IP アドレスの追加 (Add a Location IP Address) ] フィールドで、IP アドレスによりルールを制約し、[追加 (Add) ] をクリックします。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

**ステップ 6** ルールを保存するか、編集を続けます。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ユーザ制御のトラブルシューティング

ユーザ ルールの予期しない動作に気付いたら、ルール、アイデンティティ ソース、またはレルムの設定を調整することを検討してください。その他の関連するトラブルシューティング情報については、以下を参照してください。

- [ユーザエージェントアイデンティティ ソースのトラブルシューティング \(2125 ページ\)](#)
- [ISE アイデンティティ ソースのトラブルシューティング \(2130 ページ\)](#)
- [TS エージェントアイデンティティ ソースのトラブルシューティング \(2132 ページ\)](#)
- [キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング \(2142 ページ\)](#)
- [レルムとユーザのダウンロードのトラブルシューティング \(2182 ページ\)](#)

#### レルム、ユーザ、またはユーザグループを対象とするルールがトラフィックと一致しない

ユーザ エージェント、TS エージェント、または ISE デバイスのモニタ対象に多くのユーザグループを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、Firepower Management Center のユーザ制限が原因で、システムがユーザレコードをドロップすることがあります。その結果、ユーザ条件のルールが、一致することが想定されているトラフィックと一致しない可能性があります。

#### ユーザグループまたはユーザグループ内のユーザを対象とするルールが、一致することが想定されているトラフィックと一致しない

ユーザグループ条件を含むルールを設定する場合は、LDAP または Active Directory サーバでユーザグループを設定する必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、システムはユーザグループ制御を実行できません。

#### セカンダリグループ内のユーザを対象とするルールが、一致することが想定されているトラフィックと一致しない

Active Directory サーバのセカンダリグループのメンバーであるユーザを含めるか除外するユーザグループ条件を含むルールを設定する場合、サーバは報告するユーザの数を制限していることがあります。

デフォルトでは、Active Directory サーバはセカンダリグループから報告するユーザの数を制限します。この制限は、セカンダリグループ内のすべてのユーザが Firepower Management Center

に報告され、ユーザ条件を含むルールでの使用に適するようにカスタマイズする必要があります。

#### ルールが、初めて表示されたユーザと一致しない

システムは、以前に表示されていないユーザからのアクティビティを検出すると、サーバからそれらのユーザに関する情報を取得します。システムがこの情報を正常に取得するまで、このユーザに表示されるアクティビティは、一致するルールによって**処理されません**。代わりに、ユーザセッションが、一致する次のルール（または該当する場合はポリシーのデフォルトアクション）によって処理されます。

たとえば、次のような状況が考えられます。

- ユーザグループのメンバーであるユーザが、ユーザグループ条件を含むルールに一致しない。
- ユーザデータの取得に使用されたサーバが Active Directory サーバである場合、ユーザエージェント、TS エージェント、または ISE デバイスによって報告されたユーザがルールと一致しない。

これにより、システムがユーザデータをイベントビューおよび分析ツールに表示するのが遅れる可能性があることに注意してください。

#### ルールがすべての ISE ユーザと一致しない

これは想定されている動作です。Active Directory ドメインコントローラで認証された ISE ユーザに対してユーザ制御を実行することができます。LDAP、RADIUS、または RSA ドメインコントローラで認証された ISE ユーザに対するユーザ制御は実行できません。

## カスタム SGT 条件

ID ソースとして Cisco ISE を設定しない場合、ISE によって指定されていないセキュリティグループタグ (SGT) 使用してトラフィックを制御できます。SGT は、信頼ネットワーク内での、トラフィックの送信元の権限を指定します。

カスタム SGT ルールの条件では、システムが ISE サーバとの接続によって取得した ISE SGT ではなく、手動で作成された SGT オブジェクトを使ってトラフィックをフィルタ処理します。この手動で作成された SGT オブジェクトは、制御するトラフィックの SGT 属性に対応しません。カスタム SGT を使用したトラフィック制御は、ユーザ制御とは見なされません。

#### カスタム SGT 条件を持つルール

カスタム SGT 条件をサポートするのはアクセスコントロールルールのみです。

## ISE SGT とカスタム SGT ルール条件との比較

ルールの中には、割り当てられた SGT に基づいてトラフィックを制御するために使用できるものがあります。ルールのタイプ、およびアイデンティティソースの設定によって、ISE 割り

当てる SGT またはカスタム SGT のいずれかを使用して、トラフィックを割り当て済み SGT 属性と照合することができます。



- (注) ISE SGT を使用してトラフィックを照合する場合、パケットに SGT 属性が割り当てられていないとしても、パケットの送信元 IP アドレスが ISE 内で既知であれば、そのパケットは ISE SGT ルールと照合されます。

条件タイプ	要件	ルールエディタにリストされている SGT
ISE SGT	ISE アイデンティティソース	ISE サーバをクエリして取得され、メタデータが自動的に更新される SGT
カスタム SGT	ISE アイデンティティソースなし	ユーザが作成するスタティック SGT オブジェクト

#### 関連トピック

[ユーザ条件、レムルム条件、および ISE 属性条件 \(ユーザ制御\)](#) (401 ページ)

## カスタムセキュリティグループタグ (SGT) から ISE セキュリティグループタグ (SGT) への自動遷移

カスタム SGT に一致するルールを作成し、ISE を ID ソースに設定すると、システムは次の動作をします。

- オブジェクトマネージャの [セキュリティグループタグ (Security Group Tag)] オプションを無効にします。システムは既存の SGT オブジェクトをそのまま保持しますが、それらの変更や、新しいオブジェクトの追加はできません。
- カスタム SGT 条件の既存のルールを保持します。ただし、これらのルールはトラフィックの照合を行いません。また、既存のルールにカスタム SGT 基準を追加することや、カスタム SGT 条件を含む新しいルールを作成することはできません。

ISE を設定する場合は、カスタム SGT 条件を含む既存のルールは削除するか、無効にすることを推奨します。SGT 属性を持つトラフィックを照合するには、代わりに ISE 属性条件を使用します。

#### 関連トピック

[ユーザ制御用 ISE の設定](#) (2128 ページ)

## カスタム SGT 条件の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

次の手順では、ISEによって割り当てられていないSGT属性がタグ付けされたトラフィックをフィルタ処理する方法を説明します。これはユーザ制御とみなされず、アイデンティティソースとしてISEを使用していない場合にのみ機能します。[ISE SGT とカスタム SGT ルール条件との比較 \(406 ページ\)](#) を参照してください。

### 始める前に

- ISE 接続を無効にします。カスタム SGT の照合は、アイデンティティソースとしてISEを使用する場合、機能しません。
- 一致させる SGT に対応するセキュリティグループタグオブジェクトを設定します。[セキュリティグループタグオブジェクトの作成 \(441 ページ\)](#) を参照してください。

### 手順

- 
- ステップ 1** ルールエディタで、[SGT/ISE 属性 (SGT/ISE Attributes)] タブをクリックします。
- ステップ 2** [使用可能な属性 (Available Attributes)] リストから [セキュリティグループタグ (Security Group Tag)] を選択します。
- ステップ 3** [使用可能なメタデータ (Available Metadata)] リストで、カスタム SGT オブジェクトを見つけて選択します。
- [すべて (Any)] を選択すると、ルールは SGT 属性があるすべてのトラフィックと一致します。たとえば、この値は、TrustSec 向けに構成されていないホストからのトラフィックをブロックするアクセスコントロールルールが必要な場合に選択できます。
- ステップ 4** [ルールに追加 (Add to Rule)] をクリックするか、ドラッグアンドドロップします。
- ステップ 5** ルールを保存するか、編集を続けます。
- 

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## カスタム SGT 条件のトラブルシューティング

予期しないルールの動作に気付いたら、カスタム SGT オブジェクトの設定を調整することを検討してください。

### 使用不可のセキュリティ グループ タグ オブジェクト

カスタム SGT オブジェクトが使用できるのは、ISE をアイデンティティ ソースとして設定していない場合のみです。詳細については、[カスタム セキュリティ グループ タグ \(SGT\) から ISE セキュリティ グループ タグ \(SGT\) への自動遷移 \(407 ページ\)](#) を参照してください。

## ルールの検索

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

多くのポリシーでは、ルールとルール内の検索が可能です。システムは、入力内容をルールの名前および条件値と照合します。これには、オブジェクトとオブジェクトグループが含まれます。

セキュリティ インテリジェンスまたは URL のリストまたはフィールドに含まれる値は検索できません。

### 手順

- ステップ 1** ポリシー エディタで、[ルール (Rules)] タブをクリックします。
- ステップ 2** [ルールの検索 (Search Rules)] プロンプトをクリックし、検索文字列のすべてまたは一部を入力してから Enter キーを押します。  
照合ルールごとに、一致する値のカラムが強調表示されます。ステータスメッセージには、現行の一致および合計一致数が表示されます。
- ステップ 3** 目的のルールを見つけます。

照合ルールの間を移動する場合は、次の一致アイコン (▼) または前の一致アイコン (▲) をクリックします。

### 次のタスク

- 新しい検索を開始する前に、クリア アイコン (✕) をクリックして、検索と強調表示をクリアします。

## デバイス別のフィルタリングルール

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	機能に応じて異なる	任意 (Any)	Admin/Access Admin/Network Admin

一部のポリシーエディタでは、該当デバイスによってルールの表示をフィルタ処理することができます。

システムは、ルールがそのデバイスに影響するかどうかを判断するために、ルールのインターフェイス制約を使用します。インターフェイス（セキュリティゾーンまたはインターフェイスグループ条件）でルールを制約すると、インターフェイスが置かれている場所のデバイスがそのルールの影響を受けます。インターフェイス制約のないルールは、すべてのインターフェイスに適用されるので、すべてのデバイスに適用されることになります。

QoS ルールは、常にインターフェイスで制約されます。

### 手順

**ステップ 1** ポリシーエディタで、[ルール (Rules)] タブをクリックし、[デバイスでフィルタ処理 (Filter by Device)] をクリックします。

ターゲット デバイスとデバイス グループのリストが表示されます。

**ステップ 2** 1つまたは複数のチェックボックスをオンにして、これらのデバイスまたはグループに適用されるルールだけを表示します。または、[すべて (All)] をオンにしてリセットし、すべてのルールを表示します。

**ヒント** ポインタをルール基準に合わせると、その値が表示されます。基準がデバイス特有のオーバーライドを持つオブジェクトを表し、そのデバイスだけでルールリストをフィルタ処理する場合、システムはオーバーライド値を表示します。基準がドメイン特有のオーバーライドを持つオブジェクトを表し、そのドメインのデバイスでルールリストをフィルタ処理する場合、システムはオーバーライド値を表示します。

**ステップ 3** [OK] をクリックします。

### 関連トピック

[アクセス コントロール ルールの作成および編集 \(1350 ページ\)](#)

[プレフィルタリングの設定 \(1405 ページ\)](#)

[QoS ルールの設定 \(722 ページ\)](#)

[脅威に対する防御のための NAT の設定 \(1117 ページ\)](#)





## ルールとその他のポリシーの警告


ポリシーおよびルールエディタでは、トラフィックの分析やフローに悪影響を与える可能性のある設定をアイコンで示します。問題に応じて、システムはユーザがそのようなポリシーを展開しようとするときに警告するか、導入を完全に阻止します。



**ヒント** 警告、エラー、または情報のテキストを確認するには、マウスのポインタをアイコンの上に置きます。

表 44: ポリシーのエラーアイコン

アイコン	説明	例
 error	ルールまたは設定にエラーがある場合、影響を受けるルールを無効にしても、問題を修正するまではポリシーを展開できません。	カテゴリおよびレピュテーションベースの URL フィルタリングを実行するルールは、URL フィルタリング ライセンスのないデバイスをターゲットにする時点まで有効です。その時点で、ルールの横にエラーアイコンが表示され、ポリシーを展開できなくなります。ポリシーを展開するには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、URL フィルタリングライセンスを有効にする必要があります。
 警告	ルールに関する警告またはその他の警告が表示されていても、ポリシーを展開することはできます。しかし、警告でマークされている誤った設定は有効になりません。  警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。	プリエンプトされるルール、または誤った設定によりトラフィックを照合できないルールは有効になりません。誤った設定には、空のオブジェクトグループ、一致するアプリケーションがないアプリケーションフィルタ、除外された LDAP ユーザ、無効なポートなどを使用した条件が含まれます。  一方、警告アイコンがライセンスエラーまたはモデルの不一致を示している場合は、問題を修正するまでそのポリシーを展開することはできません。

アイコン	説明	例
 情報	情報アイコンは、トラフィックのフローに影響する可能性がある設定に関する有用な情報を表示します。これらの問題によってポリシーの展開が阻止されることはありません。	アプリケーション制御およびURLフィルタリングが適用されている場合、システムは接続でアプリケーショントラフィックまたは Web トラフィックを識別するまで、その接続の最初の数パケットと一部のルールとの照合をスキップすることがあります。これにより接続を確立することができ、アプリケーションと HTTP 要求を識別できるようになります。

#### 関連トピック

[アプリケーション制御の制限](#) (391 ページ)

[URL フィルタリングの制限](#) (399 ページ)

## ルールのパフォーマンスに関するガイドライン

Firepower システムでは、さまざまなポリシーに含まれるルールが、ネットワーク トラフィックをきめ細かく制御します。ルールを適切に設定して順序付けることは、効果的な導入を確立する上で不可欠な要素です。それぞれの組織と導入に固有のポリシーとルールセットがありますが、ニーズに対処しながらもパフォーマンスを最適化するために従うべき一般的なガイドラインがいくつかあります。

パフォーマンスの最適化は、リソースを大量に消費する分析を実行する場合は特に重要です。複雑なポリシーやルールは、重要なリソースを消費し、パフォーマンスに悪影響を与える可能性があります。設定の変更を展開すると、システムはすべてのルールをまとめて評価し、ターゲットデバイスでネットワーク トラフィックを評価するために使用する拡張基準セットを作成します。それらの基準がターゲットデバイスのリソース（物理メモリ、プロセッサなど）を上回っている場合、そのデバイスに展開することはできません。



- (注) 常に、ルールを組織のニーズに適した順序に配置する必要があります。すべてのトラフィックに適用する必要がある最優先順位のルールをポリシーの先頭近くに配置します。ただし、ルールに優先順位を付けなければ、アプリケーション条件または URL 条件を設定したルールが一致する可能性が高くなります。これは、システムは接続においてアプリケーショントラフィックまたは Web トラフィックを識別するまで、その接続の最初の数パケットと一部のルールとの照合をスキップすることがあるためです。これにより接続を確立することができ、アプリケーションと HTTP 要求を識別できるようになります。

#### 関連トピック

[アプリケーション制御の制限](#) (391 ページ)

[URL フィルタリングの制限](#) (399 ページ)

## ルールの簡素化および絞り込みのガイドライン

### 簡素化：設定しすぎない

処理するトラフィックの照合が1つの条件で十分な場合には、2つの条件を使用しないでください。

個々のルール条件を最小化します。できる限り少ない個々の要素をルールの条件に使用します。たとえば、ネットワーク条件では、個々のIPアドレスではなくIPアドレスブロックを使用します。ポート条件では、ポート範囲を使用します。アプリケーション制御およびURLフィルタリングを実行する場合はアプリケーションフィルタとURLカテゴリおよびレピュテーションを使用し、ユーザ制御を実行する場合はLDAP ユーザグループを使用します。

要素をオブジェクトに組み合わせても、パフォーマンスは向上しません。たとえば、50個のIPアドレスを1つのネットワークオブジェクトに含めて使用することにパフォーマンス的なメリットはなく、条件にこれらのIPアドレスを個別に含めるよりも単に構成上のメリットがあるだけです。

### 絞り込み：特にインターフェイスによってリソース消費ルールを絞り込んで制約する

できる限り、ルールの条件を使用してリソース消費ルールが処理するトラフィックを絞り込んで定義します。絞り込まれたルールは、広範な条件を持つルールが多様なタイプのトラフィックを照合し、後でより多くの特定のルールをプリエンブション処理できるという理由からも重要です。以下は、リソース消費ルールの例です。

- トラフィックを復号するSSLルール：復号だけでなく、復号されたトラフィックの更なる分析にもリソースが必要です。絞り込みを細かくし、また可能な場合は、暗号化トラフィックをブロックするか、復号しないようにします。
- ディープインスペクションを呼び出すアクセスコントロールルール：特に複数のカスタム侵入ポリシーと変数セットを使用している場合、侵入ファイルやマルウェアのインスペクションにはリソースが必要です。ディープインスペクションは必要な場所でのみ呼び出されることを確認してください。

最大のパフォーマンスによるメリットを得るため、インターフェイスによってルールを制約します。ルールがデバイスのすべてのインターフェイスを除外する場合、そのルールはそのデバイスのパフォーマンスに影響しません。

## ルールの順序指定のガイドライン

### ルールのプリエンブション

ルールのプリエンブションが発生するのは、評価する順番が前のルールがトラフィックと一致するために、その後のルールが全くトラフィックと一致しない場合です。ルールの条件により、そのルールが他のルールをプリエンブション処理するかどうかが決まります。次の例では、最初のルールが管理トラフィックを許可するため、2番目のルールがそのトラフィックをブロックできません。

アクセス コントロール ルール 1 : 管理ユーザを許可

アクセス コントロール ルール 2 : 管理ユーザをブロック

どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。次の例では、最初の SSL ルールでの VLAN 範囲に 2 番目のルールでの VLAN が含まれるため、最初のルールが 2 番目のルールをプリエンブション処理します。

SSL ルール 1 : VLAN 22 ~ 33 を復号しない

SSL ルール 2 : VLAN 27 をブロック

次の例では、VLAN が設定されていないルール 1 はあらゆる VLAN と一致します。そのため、ルール 1 がルール 2 をプリエンブション処理し、ルール 2 での VLAN 2 の照合は行われません。

アクセス コントロール ルール 1 : 送信元ネットワーク 10.4.0.0/16 を許可

アクセス コントロール ルール 2 : 送信元ネットワーク 10.4.0.0/16、VLAN 2 を許可

あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールがプリエンブション処理されます。

QoS ルール 1: VLAN 1 URL www.netflix.com をレート制限

QoS ルール 2: VLAN 1 URL www.netflix.com をレート制限

条件が 1 つでも異なる場合は、後続のルールがプリエンブション処理されることはありません。

QoS ルール 1: VLAN 1 URL www.netflix.com をレート制限

QoS ルール 2: VLAN 2 URL www.netflix.com をレート制限

#### 例 : プリエンブションを避けるための SSL ルールの順序付け

ここで 1 つのシナリオとして、信頼できる CA (Good CA) が悪意のあるエンティティ (Bad CA) に間違っ て CA 証明書を発行してしまい、その証明書を取消していない状況を考えてみましょう。信頼できない CA によって発行された証明書で暗号化されたトラフィックは SSL ポリシーを使用してブロックしたいものの、信頼できる CA の信頼チェーン内にあるそれ以外のトラフィックは許可したいとします。CA 証明書とすべての中間 CA 証明書をアップロードした後、ルールを以下の順序で設定した SSL ポリシーを構成します。

SSL ルール 1 : 発行元 CN=www.badca.com をブロック

SSL ルール 2 : 発行元 CN=www.goodca.com を復号しない

上記のルールを逆の順序にすると、不正な CA で信頼されたトラフィックを含め、正当な CA で信頼されたすべてのトラフィックが最初に一致することになります。どのトラフィックも後続の不正な CA ルールに一致しないため、悪意のあるトラフィックはブロックされずに許可される可能性があります。

## ルールのアクションとルールの順序

ルールのアクションによって、一致したトラフィックの処理方法が決まります。パフォーマンスを向上させるには、リソースを集約的に使用するルールを実行する前に、トラフィックの追加処理を実行または保証しないルールを配置してください。これにより、システムはさらに検査する必要のあるトラフィックだけを転送できます。

以下の例は、一連のルールがすべて同等に重要であり、プリエンプションが問題にならない場合に、さまざまなポリシーでルールを順序付ける方法を示しています。

### 最適な順序：SSL ルール

復号にはリソースが必要になるだけでなく、復号後のトラフィックの分析も必要になります。したがって、トラフィックを復号する SSL ルールを最後に配置します。

1. [モニタ (Monitor)] : 一致する接続をログに記録するだけで、トラフィックに対して他のアクションは実行しないルール。
2. [ブロック (Block)]、[リセットしてブロック (Block with reset)] : それ以上のインスペクションを行わずにトラフィックをブロックするルール。
3. [復号しない (Do not decrypt)] : 暗号化トラフィックを復号しないまま、暗号化セッションをアクセスコントロールルールに渡すルール。これらのセッションのペイロードにディープインスペクションは適用されません。
4. [復号-既知のキー (Decrypt - Known Key)] : 既知の秘密キーを使用して着信トラフィックを復号するルール。
5. [復号-再署名 (Decrypt-Resign)] : サーバ証明書に再署名することによって発信トラフィックを復号するルール。

### 最適な順序：アクセスコントロールルール

複数のカスタム侵入ポリシーと変数セットを使用している場合は特に、侵入、ファイル、マルウェアのインスペクションにリソースが必要です。したがって、ディープインスペクションを呼び出すアクセスコントロールルールを最後に配置します。

1. [モニタ (Monitor)] : 一致する接続をログに記録するだけで、トラフィックに対して他のアクションは実行しないルール。
2. [信頼 (Trust)]、[ブロック (Block)]、[リセットしてブロック (Block with reset)] : それ以上のインスペクションを行わずにトラフィックを処理するルール。信頼できるトラフィックは、アイデンティティポリシーが課す認証要件、およびレート制限の対象となることに注意してください。
3. [許可 (Allow)]、[インタラクティブブロック (ディープインスペクションなし) (Interactive Block (no deep inspection))] : それ以上のインスペクションを行わずにトラフィックのディスカバリを許可するルール。許可されるトラフィックは、アイデンティティポリシーが課す認証要件、およびレート制限の対象となることに注意してください。

4. [許可 (Allow) ]、[インタラクティブ ブロック (ディープ インспекションあり) (Interactive Block (deep inspection)) ]: 禁止されているファイル、マルウェア、エクスポイトのディープ インспекションを実行するファイル ポリシーまたは侵入ポリシーに関連付けられているルール。

## コンテンツ規制ルールの順序

SSL とアクセス コントロール ポリシーの両方でルールのプリエンプションを避けるため、YouTube 規制を制御するルールは、セーフサーチ規制を制御するルールの上に配置します。

アクセス コントロール ルールに対してセーフサーチを有効にする場合、システムは検索エンジンのカテゴリを [選択したアプリケーションとフィルタ (Selected Applications and Filters) ] リストに追加します。このアプリケーション カテゴリには YouTube が含まれます。そのため、YouTube トラフィックは、評価の優先順位が上のルールで YouTube EDU が有効にされていない限り、セーフサーチ ルールに一致します。

同様のルールのプリエンプションは、セーフサーチ サポート フィルタを持つ SSL ルールを、評価順序内で特定の YouTube アプリケーション条件を持つ SSL ルールよりも高い順序に配置した場合に生じます。

### 関連トピック

[コンテンツ制限について](#) (1425 ページ)

## SSL ルールの順序

### 証明書がピンングされたサイトからのトラフィックの許可

証明書のピンングを行うと、SSLセッションが確立される前に、サーバの公開キー証明書が、サーバにすでに関連付けられているブラウザの証明書と一致しているかどうかを、クライアントのブラウザが強制的に確認します。[復号 - 再署名 (Decrypt - Resign) ] アクションにはサーバ証明書を変更してからクライアントに渡すという動作が含まれているため、ブラウザがすでにその証明書をピンングしている場合は、変更された証明書が拒否されます。

たとえば、クライアント ブラウザが、証明書ピンングを使用するサイト **windowsupdate.microsoft.com** に接続されており、そのトラフィックと一致する SSL ルールを [復号 - 再署名 (Decrypt - Resign) ] アクションを使用して設定すると、システムはサーバ証明書に再署名してから、クライアントサーバに渡します。この変更されたサーバ証明書は、ブラウザでピンングした windowsupdate.microsoft.com の証明書と一致しないため、クライアントブラウザは接続を拒否します。

このトラフィックを許可するには、サーバ証明書の共通名または識別名と一致させるために、[復号しない (Do not decrypt) ] アクションを使用して SSL ルールを設定します。SSL ポリシーでは、このルールを、トラフィックと一致するすべての [復号 - 再署名 (Decrypt - Resign) ] ルールの前に配置してください。Web サイトに正常に接続された後で、クライアントブラウザから、ピンングされた証明書を取得できます。また、接続が成功したか失敗したかに関わらず、ログに記録された接続イベントから証明書を表示できます。

### ClientHello の変更の優先順位付け

ClientHello の変更を優先順位付けするには、ServerHello またはサーバ証明書条件に一致するルールの前に、ClientHello メッセージで使用可能な条件に一致するルールを配置します。

管理対象デバイスが SSL ハンドシェイクを処理するときに、ClientHello メッセージを変更して、復号の可能性を高めることができます。たとえば、Firepower システムは圧縮されたセッションを復号できないので、圧縮メソッドを削除できます。

システムは [復号 - 再署名 (Decrypt - Resign) ] アクションを含む SSL ルールに最終的に一致させることができる場合、ClientHello メッセージを変更するのみです。システムが新しいサーバへの暗号化セッションを最初に検出したときは、サーバ証明書データを ClientHello の処理には使用できません。これは復号されていない最初のセッションとなる可能性があります。同じクライアントからの後続の接続で、システムはサーバ証明書条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号の可能性を最大化できます。

ServerHello またはサーバ証明書条件 (証明書、識別名、証明書のステータス、暗号スイート、バージョン) と一致するルールを、ClientHello 条件 (ゾーン、ネットワーク、VLAN タグ、ポート、ユーザ、アプリケーション、URL カテゴリ) と一致するルールの前に配置する場合、ClientHello の変更をプリエンプション処理し、復号されないセッションの数を増やすことができます。

## URL ルールの順序

URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルールより前に配置します。特に、URL ルールがブロックルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。

- アプリケーション条件が含まれている場合。
- 検査対象のトラフィックが暗号化されている場合。

## 侵入ポリシーの急増を回避するためのガイドライン

アクセスコントロールポリシーでは、1つの侵入ポリシーを各許可ルール、インタラクティブブロックルール、およびデフォルトアクションと関連付けることができます。侵入ポリシーと変数セットの固有のペアはすべて、1つのポリシーと見なされます。

ただし、ターゲットデバイスでサポートされるアクセスコントロールルールや侵入ポリシーには最大数があります。この最大数は、ポリシーの複雑性、物理メモリ、デバイスのプロセッサ数などの、さまざまな要因によって異なります。

デバイスでサポートされる最大を超えるとアクセスコントロールポリシーは展開できず、再評価する必要があります。いくつかの侵入ポリシーまたは変数セットを統合すると、複数のアクセスコントロールルールに1つの侵入ポリシーと変数セットのペアを関連付けることができます。一部のデバイスでは、すべての侵入ポリシーに関して1つの変数セットだけを使用できる場合や、デバイス全体でただ1つの侵入ポリシー/変数セットペアだけを使用できる場合があります。

## 大規模接続（フロー）のオフロード

データセンターの Firepower 9300 シャーシ上で Firepower Threat Defense を展開する場合は、超高速パスにオフロードするトラフィックを識別して、トラフィックが NIC 自身でスイッチングされるようにできます。これは、フローオフロードと呼ばれます。オフロードによって、大容量ファイルの転送など、データ集約型アプリケーションのパフォーマンスを向上させることができます。

- ハイパフォーマンスコンピューティング（HPC）調査サイト。ここでは、Firepower Threat Defense デバイスがストレージと高コンピューティングステーション間で展開されます。1つの調査サイトが NFS 経由の FTP ファイル転送またはファイル同期を使用してバックアップを行うと、大量のデータトラフィックがすべての接続に影響を与えます。NFS を介する FTP ファイル転送およびファイル同期のオフロードによって、他のトラフィックへの影響が軽減されます。
- 主にコンプライアンス目的で使用される High Frequency Trading（HFT）。ここでは、Firepower Threat Defense デバイスがワークステーションと Exchange 間で展開されます。セキュリティは通常は問題にはなりません、遅延は大きな問題です。

Firepower 9300 シャーシでは、以下の基準を満たす接続をオフロードできます。

- プレフィルタポリシーにより FastPath される。
- IPv4 アドレスのみ。
- TCP、UDP、GRE のみ。
- 標準または 802.1Q タグ付きイーサネットフレームのみ。
- スイッチドまたはルーテッドインターフェイスのみ。パッシブ、インライン、インラインタップインターフェイスではサポートされません。

オフロードに適格なフローを識別するには、**FastPath** アクションを適用するプレフィルタポリシールールを作成します。TCP/UDP にはプレフィルタルールを使用し、GRE にはトンネルルールを使用します。ちなみに、セキュリティゾーン、送信元と宛先のネットワーク、およびポートのマッチングのみに基づいて [信頼 (Trust)] アクションを適用するようにアクセスコントロールルールを設定し、[セキュリティインテリジェンス (Security Intelligence)] を無効にする場合、これらのルールをマッチングするフローも、オフロードに適格なフローになります。

接続が確立されると、オフロードに適格な接続であれば、さらなる処理が Firepower Threat Defense ソフトウェアではなく NIC で行われます。オフロードされたフローは、引き続き制限付きステートフルインスペクション（基本的な TCP フラグおよびオプションのチェックなど）を受信します。システムは必要に応じてさらなる処理のためにファイアウォールシステムへのパケットを選択的に増やすことができます。

オフロードされたフローのリバースフローもオフロードされます。



## フローオフロードの制限事項

すべてのフローをオフロードできるわけではありません。オフロードの後でも、フローを特定の条件下でのオフロードから除外することができます。次に、制限事項の一部を示します。

### オフロードできないフロー

次のタイプのフローはオフロードできません。

- IPv6 アドレッシングを使用するフロー。
- TCP、UDP、GRE 以外のプロトコルに対するフロー。
- パッシブ、インラインまたはインライン タップ モードで設定されたインターフェイス上のフロー。ルーテッド インターフェイスおよびスイッチ インターフェイスがサポートされている唯一のタイプです。
- Snort またはその他のインスペクション エンジンによるインスペクションが必要なフロー。FTP など場合によっては、コントロールチャネルはオフロードできませんがセカンダリ データ チャネルはオフロードできます。
- IPsec および VPN 接続。
- 暗号化または復号を必要とするフロー。
- マルチキャスト フロー。
- AAA 関連のフロー。
- Vpath、VXLAN 関連のフロー。
- URL フィルタリング。
- Tracer フロー。
- セキュリティ グループでタグ付けされたフロー。
- クラスタで非対称フローが発生した場合に備えて、別のクラスタ ノードから転送されるリバース フロー。
- クラスタ内の一元化されたフロー（フローのオーナーがマスターでない場合）。

### オフロードを無効にする条件

フローがオフロードされた後、フロー内のパケットは次の条件を満たす場合に Firepower Threat Defense デバイス に返され、さらに処理されます。

- タイムスタンプ以外の TCP オプションが含まれている。
- フラグメント化されている。





## 第 18 章

# 再利用可能なオブジェクト

以下のトピックでは、Firepower システムで再利用可能オブジェクトを管理する方法について説明します。

- [再利用可能オブジェクトの概要 \(422 ページ\)](#)
- [オブジェクト マネージャ \(424 ページ\)](#)
- [ネットワーク オブジェクト \(433 ページ\)](#)
- [ポート オブジェクト \(435 ページ\)](#)
- [トンネル ゾーン \(439 ページ\)](#)
- [アプリケーションフィルタ \(439 ページ\)](#)
- [VLAN タグ オブジェクト \(440 ページ\)](#)
- [セキュリティ グループ タグ オブジェクト \(441 ページ\)](#)
- [URL オブジェクト \(442 ページ\)](#)
- [地理位置情報オブジェクト \(443 ページ\)](#)
- [変数セット \(444 ページ\)](#)
- [セキュリティ インテリジェンスのリストとフィード \(464 ページ\)](#)
- [シンクホール オブジェクト \(475 ページ\)](#)
- [ファイル リスト \(476 ページ\)](#)
- [暗号スイート リスト \(483 ページ\)](#)
- [識別名オブジェクト \(484 ページ\)](#)
- [PKI オブジェクト \(487 ページ\)](#)
- [SLA モニタ オブジェクト \(499 ページ\)](#)
- [プレフィックス リスト \(501 ページ\)](#)
- [ルート マップ \(504 ページ\)](#)
- [アクセス リスト \(508 ページ\)](#)
- [AS パスのオブジェクト \(511 ページ\)](#)
- [コミュニティ リスト \(512 ページ\)](#)
- [ポリシー リスト \(514 ページ\)](#)
- [VPN オブジェクト \(516 ページ\)](#)

## 再利用可能オブジェクトの概要

柔軟性と Web インターフェイスの使いやすさを向上させるために、Firepower システムでは、名前を値に関連付ける再利用可能な構成である名前付きオブジェクトを使用します。その値を使用する場合は、代わりに名前付きオブジェクトを使用します。多くのポリシーとルール、イベント検索、レポート、ダッシュボードなど、Web インターフェイスのさまざまな場所でのオブジェクトの使用がサポートされています。よく使用される構成を表す多くの事前定義されたオブジェクトが提供されています。

オブジェクトを作成および管理するには、オブジェクトマネージャを使用します。オブジェクトを使用する多くの構成では、必要に応じて、その場でオブジェクトを作成することもできます。オブジェクトマネージャを使用して、次の操作も実行できます。

- 単一の構成で複数のオブジェクトを参照するための、オブジェクトのグループ化。 [オブジェクトグループ \(426 ページ\)](#) を参照してください。
- 選択したデバイス、またはマルチドメイン展開の場合は選択したドメインのオブジェクト値のオーバーライド。 [オブジェクトのオーバーライド \(429 ページ\)](#) を参照してください。

アクティブなポリシーで使用されるオブジェクトを編集した後に、変更を有効にするには、変更した構成を再展開する必要があります。アクティブなポリシーで使用されているオブジェクトは削除できません。

### オブジェクトタイプ

次の表に、Firepower システムで作成できるオブジェクト、各オブジェクトタイプがグループ化可能かどうか、およびオーバーライドを許可するように構成できるかどうかを示します。

オブジェクトタイプ (Object Type)	グループ化可能	オーバーライドを許可
ネットワーク	Yes	Yes
[ポート (Port) ]	Yes	Yes
インターフェイス : <ul style="list-style-type: none"> <li>• セキュリティゾーン</li> <li>• インターフェイスグループ</li> </ul>	No	No
トンネルゾーン	No	No
アプリケーションフィルタ	No	No
VLAN タグ	Yes	Yes
セキュリティグループタグ (SGT)	No	No

オブジェクトタイプ (Object Type)	グループ化可能	オーバーライドを許可
URL	Yes	Yes
位置情報 (GeoLocation)	No	No
変数セット	No	No
セキュリティインテリジェンス：ネットワーク、DNS、URL のリストとフィード	No	No
シンクホール	No	No
ファイルリスト	No	No
暗号スイートリスト	No	No
識別名 (Distinguished Name)	Yes	No
公開キー インフラストラクチャ (PKI) : <ul style="list-style-type: none"> <li>• 内部および信頼できる CA</li> <li>• 内部および外部証明書</li> </ul>	Yes	No
SLA モニタ	No	No
プレフィックス リスト：IPv4 および IPv6	No	Yes
ルート マップ	No	Yes
アクセス リスト：標準および拡張	No	Yes
AS パス	No	Yes
コミュニティ リスト (Community List)	No	Yes
ポリシー リスト	No	Yes

### オブジェクトおよびマルチテナンシー

マルチドメイン展開では、グローバルおよび子孫ドメインでオブジェクトを作成できます。ただし、グローバルドメインでのみ作成できるセキュリティグループタグ (SGT) オブジェクトを除きます。現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。また、編集できない先祖ドメインで作成されたオブジェクトも表示されますが、セキュリティゾーンとインターフェイスグループを除きます。



- (注) セキュリティゾーンとインターフェイスグループは、リーフレベルで設定したデバイスインターフェイスに関連するため、子孫ドメイン内の管理者は、先祖ドメインで作成されたゾーンとグループを表示および編集できます。サブドメインのユーザは、先祖ゾーンとグループからインターフェイスを追加および削除できますが、ゾーン/グループを削除または名前変更することはできません。

オブジェクト名は、ドメイン階層内で一意である必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

グループ化をサポートするオブジェクトの場合、現在のドメインのオブジェクトを先祖ドメインから継承されたオブジェクトとグループ化できます。

オブジェクトのオーバーライドにより、ネットワーク、ポート、VLAN タグ、URL などの特定のオブジェクトタイプのデバイス固有またはドメイン固有の値を定義できます。マルチドメイン展開では、先祖ドメイン内のオブジェクトのデフォルト値を定義できますが、子孫ドメイン内の管理者は、そのオブジェクトのオーバーライドの値を追加できます。

## オブジェクトマネージャ

オブジェクトマネージャを使用すると、オブジェクトおよびオブジェクトグループを作成、管理することができます。

オブジェクトマネージャには、ページあたり 20 のオブジェクトまたはグループが表示されます。オブジェクトまたはグループのタイプが 20 を超える場合は、ページ下部のナビゲーションリンクを使用して追加ページを表示します。特定のページにアクセスしたり、更新アイコン (🔄) にアクセスしてビューを更新したりすることもできます。

デフォルトでは、オブジェクトとグループはページで、アルファベット順に名前でもリストされます。ただし、表示されている任意の列でオブジェクトまたはグループの各タイプをソートできます。ページのオブジェクトは、名前または値でフィルタすることもできます。

## オブジェクトの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

## 手順

- ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ 2** リストからオブジェクトタイプを選択します ([再利用可能オブジェクトの概要 \(422 ページ\)](#) を参照)。
- ステップ 3** 編集するオブジェクトの横にある編集アイコン (✎) をクリックします。
- 代わりに表示アイコン (👁) が表示される場合、オブジェクトは先祖ドメインに属しており、上書きを許可しないように設定されており、オブジェクトを変更する権限がありません。
- ステップ 4** 必要に応じてオブジェクト設定を変更します。
- ステップ 5** 変数セットを編集する場合は、セット内の変数を管理します ([変数の管理 \(460 ページ\)](#) を参照)。
- ステップ 6** オーバーライドを許可するように設定できるオブジェクトの場合、次の操作をします。
- このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可 (Allow Overrides)] チェックボックスをオンにします ([オブジェクトのオーバーライドの許可 \(431 ページ\)](#) を参照)。現在のドメインに属しているオブジェクトに対してのみ、この設定を変更できます。
  - このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド (Override)] セクションを展開し、[追加 (Add)] をクリックします ([オブジェクトのオーバーライドの追加 \(431 ページ\)](#) を参照)。
- ステップ 7** [保存 (Save)] をクリックします。
- ステップ 8** 変数セットを編集するときそのセットがアクセス コントロール ポリシーで使用されている場合、[はい (Yes)] をクリックして変更の保存を確認します。

## 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## オブジェクトまたはオブジェクトグループのフィルタ処理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

マルチドメインの導入環境では、現在ドメインと親ドメインで作成されたオブジェクトが表示され、それらをフィルタ処理できます。

## 手順

**ステップ1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ2** [フィルタ処理 (Filter)] フィールドのフィルタ条件を入力します。

ページは入力に従って更新され、一致する項目が表示されます。

次のメタ文字を使用できます。

- アスタリスク (\*) 文字は、ある文字の 0 回以上のオカレンスに一致します。
- キャレット記号 (^) は文字列の先頭部分と一致します。
- ドル記号 (\$) は文字列の末尾と一致します。

## オブジェクトのソート

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

## 手順

**ステップ1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ2** 列の見出しをクリックします。反対方向でソートするには、見出しを再度クリックします。

## オブジェクトグループ

オブジェクトをグループ化すると、複数のオブジェクトを1つの設定で参照できます。システムでは、Web インターフェイスでオブジェクトおよびオブジェクトグループを交互に使用することができます。たとえば、ポート オブジェクトを使用する場合はいつでも、ポート オブジェクトグループも使用できます。

ネットワーク、ポート、VLAN タグ、URL、およびPKI オブジェクトをグループ化できます。ネットワーク オブジェクトグループはネストすることができます。つまり、ネットワーク オ



オブジェクトグループを別のネットワークオブジェクトグループに追加できます。許容されるネストレベルは最大10です。

同じタイプのオブジェクトおよびオブジェクトグループには、同じ名前を付けることはできません。マルチドメイン展開では、オブジェクトグループの名前をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ポリシーで使用されるオブジェクトグループ（たとえば、アクセスコントロールポリシーで使用されるネットワークオブジェクトグループ）を編集する場合、変更を適用するためには、変更後の設定を再展開する必要があります。

グループを削除しても、グループ内のオブジェクトは削除されず、相互の関連性だけが削除されます。さらに、アクティブポリシーで使用中のグループは削除できません。たとえば、保存されたアクセスコントロールポリシーのVLAN条件で使用しているVLANタグのグループは削除できません。

## 再利用可能オブジェクトのグループ化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

先祖ドメインから継承したオブジェクトを持つ現在のドメイン内のオブジェクトをグループ化できます。

### 手順

- ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ 2** グループ化するオブジェクトタイプが、[ネットワーク (Network)]、[ポート (Port)]、[URL]、[VLAN タグ (VLAN Tag)] の場合は、次のように操作します。
  - a) オブジェクトタイプのリストからオブジェクトタイプを選択します。
  - b) [追加 [オブジェクトタイプ] (Add [Object Type])] ドロップダウンリストから [グループの追加 (Add Group)] を選択します。
- ステップ 3** グループ化するオブジェクトタイプが [識別名 (Distinguished Name)] の場合は、次のように操作します。
  - a) [識別名 (Distinguished Name)] ノードを展開します。
  - b) [オブジェクトグループ (Object Groups)] を選択します。

c) [識別名グループの追加 (Add Distinguished Name Group)] をクリックします。

**ステップ 4** グループ化するオブジェクトタイプが [PKI] の場合は、次のように操作します。

- a) [PKI] ノードを展開します。
- b) 次のいずれかを実行します。

- 内部 CA グループ (Internal CA Groups)
- 信頼できる CA グループ (Trusted CA Groups)
- 内部証明書グループ (Internal Cert Groups)
- 外部証明書グループ (External Cert Groups)

c) [[オブジェクトタイプ] グループの追加 (Add [Object Type] Group)] ボタンをクリックします。

**ステップ 5** 一意の [名前 (Name)] を入力します。

**ステップ 6** リストから 1 つ以上のオブジェクトを選択して、[追加 (Add)] をクリックします。

次のことも実行できます。

- 含める既存のオブジェクトを検索するには、フィルタ フィールド (🔍) を使用します。これは入力に従って更新され、一致する項目を表示します。検索文字列をクリアするには、検索フィールドの上にある再ロードアイコン (🔄) をクリックするか、検索フィールド内のクリアアイコン (✖) をクリックします。
- 既存のオブジェクトがニーズを満たさない場合、すぐにオブジェクトを作成するには、追加アイコン (+) をクリックします。

**ステップ 7** 必要に応じて、[ネットワーク (Network)]、[ポート (Port)]、[URL]、および [VLAN タグ (VLAN Tag)] グループに対し、次の操作を実行します。

- [説明 (Description)] を入力します。
- [オーバーライドを許可する (Allow Overrides)] チェックボックスをオンにして、このオブジェクトグループのオーバーライドを許可します。[オブジェクトのオーバーライドの許可 \(431 ページ\)](#) を参照してください。

**ステップ 8** [保存 (Save)] をクリックします。

---

### 次のタスク

- アクティブなポリシーがオブジェクトグループを参照する場合は、設定の変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## オブジェクトのオーバーライド

オブジェクトをオーバーライドすることにより、オブジェクトの代替値を定義できます。指定したデバイスに対して、システムはこの代替値を使用します。

ほとんどのデバイスに有効な定義を設定したオブジェクトを作成した後、異なる定義を必要とする少数のデバイスについて、オーバーライドを使用してオブジェクトに対する変更内容を指定できます。また、すべてのデバイスに対してオーバーライドする必要があるオブジェクトを作成し、そのオブジェクトを使用してすべてのデバイスに適用する単一のポリシーを作成することもできます。オブジェクトオーバーライドでは、デバイス全体で使用する共有ポリシーの小さなセットを作成し、個々のデバイスの必要に応じてポリシーを変更できます。

たとえば、社内のさまざまな部門へのICMPトラフィックを拒否する場合があります。それぞれの部門は、異なるネットワークに接続されています。これを実行するには、**Departmental Network** という名前のネットワーク オブジェクトを含むルールを使用して、アクセス コントロールポリシーを定義します。このオブジェクトのオーバーライドを許可することによって、関連する各デバイスで、デバイスが接続されている実際のネットワークを指定するオーバーライドを作成できます。

マルチドメイン展開では、先祖ドメインのオブジェクトのデフォルト値を定義して、子孫ドメインの管理者がそのオブジェクトのオーバーライド値を追加できるようにすることができます。たとえば、マネージドセキュリティサービスプロバイダー (MSSP) では、単一の **Firepower Management Center** を使用して複数の顧客のネットワーク セキュリティを管理する場合があります。この場合、MSSP の管理者は、すべての顧客の導入で使用するオブジェクトをグローバルドメインに定義できます。各顧客の管理者は子孫ドメインにログインして、それぞれの組織に応じてそのオブジェクトをオーバーライドできます。これらのローカル管理者がMSSPの他の顧客のオーバーライド値を表示したり、影響を与えたりすることはできません。

オブジェクト オーバーライドのターゲットを特定のドメインに絞ることもできます。その場合、ユーザがデバイス レベルで値をオーバーライドしない限り、システムはターゲット ドメインのすべてのデバイスにオブジェクト オーバーライド値を使用します。

オブジェクトマネージャで、オーバーライド可能なオブジェクトを選択し、そのオブジェクトに対するデバイスレベルまたはドメインレベルのオーバーライドのリストを定義できます。

オブジェクト オーバーライドを使用できるオブジェクト タイプは以下に限られます。

- ネットワーク
- [ポート (Port) ]
- VLAN タグ
- URL
- SLA モニタ
- プレフィックス リスト
- ルート マップ
- アクセス リスト

- AS パス
- コミュニティ リスト (Community List)
- ポリシー リスト

オブジェクト マネージャでは、オーバーライド可能なオブジェクトのオブジェクト タイプには [オーバーライド (Override) ] 列が表示されます。この列の有効な値は以下のとおりです。

- 緑のチェックマーク：このオブジェクトにはオーバーライドを作成できます。オーバーライドはまだ追加されていません。
- 赤の X：このオブジェクトにはオーバーライドを作成できません。
- 数値：このオブジェクトに追加されているオーバーライドの数を表します（たとえば、「2」は2つのオーバーライドが追加されていることを意味します）。

## オブジェクトオーバーライドの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** [オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択します。

**ステップ 2** オブジェクトタイプのリストから選択します (再利用可能オブジェクトの概要 (422 ページ) を参照)。

**ステップ 3** 編集するオブジェクトの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、オブジェクトは先祖ドメインに属しており、上書きを許可しないように設定されており、オブジェクトを変更する権限がありません。

**ステップ 4** オブジェクト オーバーライドを管理します。

- 追加：オブジェクトオーバーライドを追加します (オブジェクトのオーバーライドの追加 (431 ページ) を参照)。
- 許可：オブジェクトオーバーライドを許可します (オブジェクトのオーバーライドの許可 (431 ページ) を参照)。
- 削除：オブジェクトエディタで、削除するオーバーライドの横にある削除アイコン (🗑) をクリックします。

- 編集：オブジェクト オーバーライドを編集します（[オブジェクト オーバーライドの編集 \(432 ページ\)](#) を参照）。

## オブジェクトのオーバーライドの許可

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

- ステップ 1** オブジェクト エディタで、[オーバーライドを許可 (Allow Overrides)] チェックボックスをオンにします。
- ステップ 2** [保存 (Save)] をクリックします。

### 次のタスク

- オブジェクトのオーバーライド値を追加します（[オブジェクトのオーバーライドの追加 \(431 ページ\)](#) を参照）。

## オブジェクトのオーバーライドの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 始める前に

- オブジェクトのオーバーライドを許可します（[オブジェクトのオーバーライドの許可 \(431 ページ\)](#) を参照）。

### 手順

- ステップ 1** オブジェクト エディタで、[オーバーライド (Override)] セクションを展開します。
- ステップ 2** [追加 (Add)] をクリックします。

**ステップ3** [ターゲット (Targets) ] タブで、[使用可能なデバイスとドメイン (Available Devices and Domains) ] リストからドメインまたはデバイスを選択し、[追加 (Add) ] をクリックします。

**ステップ4** [オーバーライド (Override) ] タブで、[名前 (Name) ] を入力します。

**ステップ5** 必要に応じて、[説明 (Description) ] を入力します。

**ステップ6** オーバーライド値を入力します。

例：

ネットワーク オブジェクトについては、ネットワーク値を入力します。

**ステップ7** [追加 (Add) ] をクリックします。

**ステップ8** [保存 (Save) ] をクリックします。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## オブジェクトオーバーライドの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

既存のオーバーライドの説明と値を変更できます。ただし、既存のターゲットリストは変更できません。代わりに、既存のオーバーライドを置き換える、新しいターゲットに対する新しいオーバーライドを追加する必要があります。

### 手順

**ステップ1** オブジェクトエディタで、[オーバーライド (Override) ] セクションを展開します。

**ステップ2** 変更するオーバーライドの横にある編集アイコン (✎) をクリックします。

**ステップ3** 必要に応じて、[説明 (Description) ] を変更します。

**ステップ4** オーバーライド値を変更します。

**ステップ5** [保存 (Save) ] をクリックして、オーバーライドを保存します。

**ステップ6** [保存 (Save) ] をクリックして、オブジェクトを保存します。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## ネットワーク オブジェクト

ネットワーク オブジェクトは1つ以上の IP アドレスを表します。ネットワーク オブジェクトおよびグループを、アクセス コントロール ポリシー、ネットワーク変数、侵入ルール、アイデンティティルール、ネットワーク検出ルール、イベント検索、レポートなど、システムの Web インターフェイスのさまざまな場所で使用できます。

ネットワーク オブジェクトを必要とするオプションを設定する際は、リストが自動的にフィルタリングされて、そのオプションに有効なネットワーク オブジェクトだけが表示されます。たとえば、オプションのなかにはホスト オブジェクトが必要なものと、サブネットが必要なものがあります。

ネットワーク オブジェクトには、以下のいずれかのタイプを指定できます。

### ホスト

単一の IP アドレス。

IPv4 の例 :

209.165.200.225

IPv6 の例 :

2001:DB8::0DB8:800:200C:417A または 2001:DB8:0:0:0DB8:800:200C:417A

### ネットワーク (Network)

アドレス ブロック (別名サブネット)。

IPv4 の例 :

209.165.200.224/27

IPv6 の例 :

2001:DB8:0:CD30::/60

### アドレス範囲 (Address Range)

IP アドレスの範囲。

IPv4 の例 :

209.165.200.225-209.165.200.250

IPv6 の例 :

2001:db8:0:cd30::1-2001:db8:0:cd30::1000

## グループ

ネットワークオブジェクトまたは他のネットワークグループからなるグループ。

次に例を示します。

```
209.165.200.225
209.165.201.1
209.165.202.129
```

あるネットワークオブジェクトグループを別のネットワークオブジェクトグループに追加することで、ネストされたグループを作成できます。グループをネストできるレベルは、最大で 10 レベルです。

## ネットワークオブジェクトの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ 2** オブジェクトタイプのリストから [ネットワーク (Network)] を選択します。

**ステップ 3** [ネットワークを追加 (Add Network)] ドロップダウンメニューで、[オブジェクトの追加 (Add Object)] を選択します。

**ステップ 4** 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

**ステップ 5** 必要に応じて、[説明 (Description)] を入力します。

**ステップ 6** [ネットワーク (Network)] フィールドに、適切な値を入力します。[ネットワークオブジェクト \(433 ページ\)](#) を参照してください。

**ステップ 7** オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可 (Allow Overrides)] チェックボックスをオンにします ([オブジェクトのオーバーライドの許可 \(431 ページ\)](#) を参照)。
- このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド (Override)] セクションを展開し、[追加 (Add)] をクリックします ([オブジェクトのオーバーライドの追加 \(431 ページ\)](#) を参照)。



ステップ 8 [保存 (Save) ] をクリックします。

#### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## ポートオブジェクト

ポートオブジェクトは、異なるプロトコルをそれぞれ少し異なる方法で表します。

#### TCP および UDP

ポートオブジェクトは、カッコ内にプロトコル番号が記載されたトランスポート層プロトコルと、オプションの関連ポートまたはポート範囲を表します。例：TCP(6)/22。

#### ICMP および ICMPv6 (IPv6-ICMP)

ポートオブジェクトはインターネット層プロトコルと、オプションでタイプおよびコードを表します。例：ICMP(1):3:3

ICMP または IPV6-ICMP ポートオブジェクトは、タイプ、および該当する場合はコードを基準に制限できます。ICMPのタイプとコードの詳細については、次のURLを参照してください。

- <http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml>
- <http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml>

#### その他

ポートオブジェクトは、ポートを使用しない他のプロトコルを表します。

Firepower システムには、ウェルノウンポート用にデフォルトのポートオブジェクトが用意されています。これらのデフォルトオブジェクトを変更または削除することはできません。デフォルトオブジェクトに加え、カスタムポートオブジェクトを作成できます。

ポートオブジェクトおよびグループは、アクセスコントロールポリシー、アイデンティティルール、ネットワーク検出ルール、ポート変数、イベント検索など、システムのWebインターフェイスのさまざまな場所で使用できます。たとえば、組織が特定のポート範囲を使用するカスタムクライアントを使用していて、システムで過剰なイベントや誤解を与えるイベントが発生した場合、それらのポートをモニタ対象から除外するようネットワーク検出ポリシーを設定できます。

ポートオブジェクトを使用する際は、次のガイドラインに従ってください。

- アクセスコントロールルールの送信元ポート条件にはTCP/UDP以外のプロトコルを追加できません。さらに、送信元ポートと宛先ポートの両方のポート条件をルールで設定する場合、トランスポートプロトコルを混在させることはできません。

- 送信元ポート条件で使用されるポート オブジェクト グループにサポート対象外のプロトコルを追加した場合、設定を展開しても、その条件が使用されているルールは管理対象デバイスで適用されません。
- TCP と UDP の両方のポートを含むポート オブジェクトを作成してから、ルールの送信元ポート条件としてそのポートオブジェクトを追加した場合、宛先ポートを追加することはできません。その逆もまた同様です。

## ポートオブジェクトの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** [オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択します。

**ステップ 2** オブジェクト タイプのリストから [ポート (Port) ] を選択します。

**ステップ 3** [ポートの追加 (Add Port) ] ドロップダウン リストで、[オブジェクトの追加 (Add Object) ] を選択します。

**ステップ 4** 名前を入力します。

**ステップ 5** [プロトコル (Protocol) ] を選択します。

**ステップ 6** 選択したプロトコルに応じて、[ポート (Port) ] で制限するか、または ICMP の [タイプ (Type) ] および [コード (Code) ] を選択します。

1 から 65535 のポートを入力できます。ポート範囲を指定するには、ハイフンを使用します。[すべて (All) ] のプロトコルと一致させることを選択した場合は、[その他 (Other) ] ドロップダウン リストを使用して、ポートでオブジェクトを制限する必要があります。

**ステップ 7** オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可 (Allow Overrides) ] チェックボックスをオンにします ([オブジェクトのオーバーライドの許可 \(431 ページ\)](#) を参照)。
- このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド (Override) ] セクションを展開し、[追加 (Add) ] をクリックします ([オブジェクトのオーバーライドの追加 \(431 ページ\)](#) を参照)。

**ステップ 8** [保存 (Save) ] をクリックします。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## インターフェイスオブジェクト：インターフェイスグループとセキュリティゾーン

インターフェイスオブジェクトは、ネットワークをセグメント化してトラフィックフローを制御し、分類しやすくします。インターフェイスオブジェクトは単にインターフェイスをグループ化します。これらのグループは複数のデバイスにまたがる場合があります。また、単一のデバイスに複数のインターフェイスオブジェクトを設定することもできます。

インターフェイスオブジェクトには次の2つのタイプがあります。

- セキュリティゾーン：インターフェイスは、1つのセキュリティゾーンにのみ属することができます。
- インターフェイスグループ：インターフェイスは複数のインターフェイスグループ（および1つのセキュリティゾーン）に属することができます。

Firepower Threat Defense NAT ポリシー、プレフィルタポリシー、および QoS ポリシーでインターフェイスグループを使用できます。

トンネルゾーンはインターフェイスオブジェクトではありませんが、特定の設定ではセキュリティゾーンの代わりにトンネルゾーンを使用できます。 [トンネルゾーンおよびプレフィルタリング \(1410 ページ\)](#) を参照してください。

インターフェイスオブジェクト内のすべてのインターフェイスが同じタイプ（すべてインライン、パッシブ、スイッチド、ルーテッド、または ASA FirePOWER）である必要があります。インターフェイスオブジェクトを作成した後、それに含まれるインターフェイスのタイプを変更することはできません。

オブジェクトマネージャのインターフェイスオブジェクトのページでは、管理対象デバイスで設定されているセキュリティゾーンとインターフェイスグループの一覧が表示されます。また、このページには、各インターフェイスオブジェクトのタイプも表示され、各インターフェイスオブジェクトを展開すると、どのデバイスのどのインターフェイスが各オブジェクトに属するかを表示できます。

### モデル固有の注意事項および警告

7000 または 8000 シリーズ デバイスの初期設定時に、システムはデバイス用に選択した検出モードに基づいてセキュリティゾーンを作成します。たとえば、パッシブ展開ではシステムはパッシブゾーンを作成し、インライン展開では外部ゾーンと内部ゾーンを作成します。Firepower Management Center にデバイスを登録すると、これらのセキュリティゾーンが Management Center に追加されます。

ASA FirePOWER セキュリティ コンテキストの変更（シングル コンテキスト モードからマルチコンテキストモードへの変更、またはその逆の変更）をすると、割り当てられているセキュリティゾーンからデバイスのすべてのインターフェイスがシステムによって削除されます。

### インターフェイスオブジェクトとマルチテナンシー

マルチドメイン展開では、どのレベルでもインターフェイスオブジェクトを作成できます。先祖ドメインで作成されたインターフェイスオブジェクトには別のドメインのデバイスに存在するインターフェイスが含まれる場合があります。この状況において、オブジェクトマネージャ内の先祖のインターフェイスオブジェクトの設定を表示するサブドメインユーザには、当該ドメインのインターフェイスのみが確認できます。

ロールによって制限されない限り、サブドメインのユーザは先祖ドメインで作成されたインターフェイスオブジェクトを表示および編集できます。サブドメインのユーザは、これらのインターフェイスオブジェクトにインターフェイスの追加や削除を行えます。ただし、インターフェイスオブジェクトの削除や名称変更はできません。子孫ドメインで作成されたインターフェイスオブジェクトの表示や編集はできません。

## セキュリティゾーンおよびインターフェイスグループオブジェクトの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	セキュリティゾーン：任意 インターフェイスグループ： Firepower Threat Defense	任意 (Any)	Admin/Access Admin/Network Admin



#### ヒント

空のインターフェイスオブジェクトを作成し、後からインターフェイスを追加できます。インターフェイスを追加するには、インターフェイスに名前が付いている必要があります。[デバイス (Devices)] > [デバイス管理 (Device Management)] でインターフェイスを設定しているときに、セキュリティゾーンを作成することもできます（インターフェイスグループは作成できません）。

#### 始める前に

- 各種インターフェイスオブジェクトの使用要件および制限を理解します。[インターフェイスオブジェクト：インターフェイスグループとセキュリティゾーン \(437ページ\)](#) を参照してください。
- 必要なインターフェイスオブジェクトを慎重に決定します。既存のセキュリティゾーンをインターフェイスグループに、またはその逆に変更することはできません。代わりに、新しいインターフェイスオブジェクトを作成する必要があります。

## 手順

- ステップ1 [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ2 オブジェクトタイプのリストから、[インターフェイス (Interface)] を選択します。
- ステップ3 [追加 (Add)] > [セキュリティゾーン (Security Zone)] または [追加 (Add)] > [インターフェイスグループ (Interface Group)] をクリックします。
- ステップ4 名前を入力します。
- ステップ5 [インターフェイスタイプ (Interface Type)] を選択します。
- ステップ6 [デバイス (Device)] > [インターフェイス (Interfaces)] ドロップダウンリストから、追加するインターフェイスを含むデバイスを選択します。
- ステップ7 1つ以上のインターフェイスを選択します。
- ステップ8 [追加 (Add)] をクリックして、デバイス別にグループ化された、選択したインターフェイスを追加します。
- ステップ9 [保存 (Save)] をクリックします。

## 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

# トンネルゾーン

トンネルゾーンとは、特別な分析のために明示的にタグ付けする特定のタイプのプレーンテキスト、パススルートンネルを表します。トンネルゾーンは、一部の設定でインターフェイスの制約として使用できますが、インターフェイスオブジェクトではありません。

詳細については、[トンネルゾーンおよびプレフィルタリング \(1410 ページ\)](#) を参照してください。

# アプリケーションフィルタ

システム提供のアプリケーションフィルタは、アプリケーションの基本特性 (タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ) にしたがってアプリケーションを整理することで、アプリケーション制御に役立ちます。オブジェクトマネージャで、システム提供のフィルタの組み合わせやアプリケーションの任意の組み合わせをもとに、ユーザ定義の再利用可能アプリケーションフィルタを作成、管理できます。詳細については、[アプリケーション条件 \(アプリケーション制御\) \(386 ページ\)](#) を参照してください。

## VLAN タグオブジェクト

設定した個々の VLAN タグオブジェクトは、1つの VLAN タグまたはタグの範囲を表します。

複数の VLAN タグオブジェクトをグループ化できます。グループは複数のオブジェクトを表します。つまり、1つのオブジェクトで VLAN タグの範囲を使用することは、この意味ではグループとはみなされません。

VLAN タグオブジェクトとグループは、ルールやイベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、特定の VLAN だけに適用されるアクセスコントロールルールを作成することができます。

### VLAN タグオブジェクトの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin Access Admin Network Admin

#### 手順

- ステップ 1 [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ 2 オブジェクトタイプのリストから [VLAN タグ (VLAN Tag)] を選択します。
- ステップ 3 [VLAN タグの追加 (Add VLAN Tag)] ドロップダウンリストで、[オブジェクトの追加 (Add Object)] を選択します。
- ステップ 4 [名前 (Name)] を入力します。
- ステップ 5 [説明 (Description)] を入力します。
- ステップ 6 [VLAN タグ (VLAN Tag)] フィールドに値を入力します。VLAN タグの範囲を指定するには、ハイフンを使用します。
- ステップ 7 オブジェクトのオーバーライドを管理します。
  - このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可 (Allow Overrides)] チェックボックスをオンにします ([オブジェクトのオーバーライドの許可 \(431 ページ\)](#) を参照)。
  - このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド (Override)] セクションを展開し、[追加 (Add)] をクリックします ([オブジェクトのオーバーライドの追加 \(431 ページ\)](#) を参照)。
- ステップ 8 [保存 (Save)] をクリックします。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## セキュリティグループタグオブジェクト

セキュリティグループタグ (SGT) オブジェクトは、単一の SGT 値を指定します。ルールで SGT オブジェクトを使用して、Cisco ISE で割り当てられたものではない SGT 属性を持つトラフィックを制御できます。SGT オブジェクトをグループ化またはオーバーライドすることはできません。

### 関連トピック

- [カスタムセキュリティグループタグ \(SGT\) から ISE セキュリティグループタグ \(SGT\) への自動遷移 \(407 ページ\)](#)
- [カスタム SGT 条件 \(406 ページ\)](#)
- [ISE SGT とカスタム SGT ルール条件との比較 \(406 ページ\)](#)

## セキュリティグループタグオブジェクトの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	グローバルだけ	Admin/Access Admin/Network Admin

### 始める前に

- ISE 接続を無効にします。アイデンティティソースとして ISE を使用している場合は、カスタム SGT オブジェクトを作成することはできません。

### 手順

- ステップ 1 [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ 2 オブジェクトタイプのリストから [セキュリティグループタグ (Security Group Tag)] を選択します。
- ステップ 3 [セキュリティグループタグの追加 (Add Security Group Tag)] をクリックします。
- ステップ 4 名前を入力します。
- ステップ 5 必要に応じて、[説明 (Description)] を入力します。
- ステップ 6 [タグ (Tag)] フィールドに、単一の SGT を入力します。

ステップ7 [保存 (Save) ]をクリックします。

#### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

#### 関連トピック

[カスタムセキュリティグループタグ \(SGT\) から ISE セキュリティグループタグ \(SGT\) への自動遷移 \(407 ページ\)](#)

[カスタム SGT 条件 \(406 ページ\)](#)

[ISE SGT とカスタム SGT ルール条件との比較 \(406 ページ\)](#)

## URL オブジェクト

設定した各 URL オブジェクトは、単一の URL または IP アドレスを表します。URL オブジェクトとグループは、アクセス コントロール ポリシーやイベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、特定の Web サイトをブロックするアクセス コントロール ルールを作成することができます。

URL オブジェクトを作成する際に、特に暗号化トラフィックを復号またはブロックする SSL インспекションを設定しない場合は、次の事項に留意してください。

- アクセス コントロール ルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は含めないでください。たとえば、`www.example.com` ではなく、`example.com` を使用します。
- URL 条件を含むアクセス コントロール ルールを使用して Web トラフィックを照合する場合、システムは暗号化プロトコル (HTTP 対 HTTPS) を無視します。つまり、アプリケーション条件を使用してルールを調整しない限り、Web サイトをブロックすると、その Web サイトへの HTTP と HTTPS の両方のトラフィックがブロックされます。URL オブジェクトを作成する場合は、オブジェクトの作成時にプロトコルを指定する必要はありません。たとえば、`http://example.com/` ではなく、`example.com` を使用します。

## URL オブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin



## 手順

- ステップ1 [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ2 オブジェクト タイプのリストから [URL] を選択します。
- ステップ3 [URL の追加 (Add URL)] ドロップダウンリストで、[オブジェクトの追加 (Add Object)] を選択します。
- ステップ4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。
- ステップ5 必要に応じて、[説明 (Description)] を入力します。
- ステップ6 [URL] に、URL または IP アドレスを入力します。
- ステップ7 オブジェクトのオーバーライドを管理します。
  - このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可 (Allow Overrides)] チェックボックスをオンにします ([オブジェクトのオーバーライドの許可 \(431 ページ\)](#) を参照)。
  - このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド (Override)] セクションを展開し、[追加 (Add)] をクリックします ([オブジェクトのオーバーライドの追加 \(431 ページ\)](#) を参照)。
- ステップ8 [保存 (Save)] をクリックします。

## 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

# 地理位置情報オブジェクト

設定済みの位置情報 (ジオロケーション) オブジェクトは、モニタ対象ネットワーク上のトラフィックの送信元または宛先としてシステムで識別された 1 つ以上の国または大陸を表します。アクセスコントロールポリシー、SSL ポリシー、イベント検索など、システムの Web インターフェイスのさまざまな場所で地理位置情報オブジェクトを使用できます。たとえば、特定の国が送信元/宛先であるトラフィックをブロックするアクセスコントロールルールを作成できます。

常に最新の情報を使用してネットワークトラフィックをフィルタ処理できるように、地理位置情報データベース (GeoDB) を定期的に更新することを強くお勧めします。

## 地理位置情報オブジェクトの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ 2** オブジェクトタイプのリストから [地理位置情報 (Geolocation)] を選択します。

**ステップ 3** [位置情報の追加 (Add Geolocation)] をクリックします。

**ステップ 4** 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

**ステップ 5** 地理位置情報オブジェクトに含める国および大陸のチェックボックスを選択します。大陸を選択すると、その大陸内のすべての国、および GeoDB 更新によってその大陸に今後追加されるすべての国が選択されます。大陸の下でいずれかの国を選択解除すると、その大陸が選択解除されます。国と大陸を任意に組み合わせて選択できます。

**ステップ 6** [保存 (Save)] をクリックします。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## 変数セット

変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーで変数を使用して、ルール抑制、アダプティブプロファイルの更新、および動的 (ダイナミック) ルール状態で IP アドレスを表すこともできます。



**ヒント** プリプロセスルールは、侵入ルールで使用されるネットワーク変数で定義されたホストにかかわらず、イベントをトリガーできます。

変数セットを使用して、変数を管理、カスタマイズ、およびグループ化します。システム提供のデフォルトの変数セットを使用することも、独自のカスタムセットを作成することもできます。いずれのセット内でも、定義済みのデフォルト変数を変更したり、ユーザ定義変数を追加および変更したりできます。

Firepower システムで提供する共有オブジェクトルールと標準テキストルールのほとんどで、定義済みのデフォルト変数を使用してネットワークとポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 `$HOME_NET` を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 `$EXTERNAL_NET` を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Web サーバに対するエクスプロイトを検出するルールは、`$HTTP_SERVERS` 変数および `$HTTP_PORTS` 変数を使用します。

ルールがより効率的なのは、変数がユーザのネットワーク環境をより正確に反映する場合です。少なくとも、デフォルトセットにあるデフォルト変数は変更する必要があります。`$HOME_NET` などの変数がネットワークを正しく定義し、`$HTTP_SERVERS` にネットワーク上のすべての Web サーバが含まれていれば、処理は最適化され、疑わしいアクティビティがないかどうかすべての関連システムがモニタされます。

変数を使用するには、変数セットをアクセス コントロールルールまたはアクセス コントロール ポリシーのデフォルトアクションに関連付けられている侵入ポリシーにリンクします。デフォルトでは、デフォルトの変数セットは、アクセス コントロール ポリシーによって使用されるすべての侵入ポリシーにリンクされています。

変数を任意のセットに追加すると、それはすべてのセットに追加されます。つまり、各変数セットは、システムで現在設定されているすべての変数のコレクションになります。どの変数セット内でも、ユーザ定義変数を追加し、任意の変数の値をカスタマイズすることができます。

Firepower システムでは、初めに定義済みのデフォルト値で構成された単一のデフォルトの変数セットを提供します。デフォルトセット内の各変数は、最初はそのデフォルト値に設定されています。定義済みの変数の場合、このデフォルト値は Cisco Talos Security Intelligence and Research Group (Talos) によって設定され、ルール更新で提供される値です。

定義済みのデフォルト変数は、そのデフォルト値に設定されたままにすることもできますが、定義済みの変数のサブセットを変更することを推奨します。

変数はデフォルトセットでのみ使用できますが、多くの場合、1つ以上のカスタム設定を追加し、異なるセットで異なる変数の値を設定し、場合によっては新しい変数を追加することによって、最大限に活用できます。

複数のセットを使用する場合は、デフォルトのセットにある任意の変数の現在値によって、他のすべてのセットの変数のデフォルト値が決まることに注意してください。

[オブジェクトマネージャ (Object Manager)] ページで [変数セット (Variable Sets)] を選択した場合、オブジェクトマネージャには、デフォルトの変数セットと、作成したすべてのカスタムセットがリストされます。

新しくインストールされたシステムでは、デフォルトの変数セットは、Cisco で定義済みのデフォルト変数だけで構成されています。

各変数セットには、システムによって提供されるデフォルト変数と、任意の変数セットから追加したすべてのカスタム変数が含まれます。デフォルト設定は編集できますが、デフォルトセットの名前を変更したり、削除したりすることはできないことに注意してください。

マルチドメイン展開では、システムはサブドメインごとにデフォルトの変数セットを生成します。



**注意** アクセスコントロールまたは侵入ポリシーをインポートすると、デフォルトの変数セットにある既存のデフォルト変数が、インポートされたデフォルト変数でオーバーライドされます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。

#### 関連トピック

[変数の管理](#) (460 ページ)

[変数セットの管理](#) (459 ページ)

## 侵入ポリシー内の変数セット

Firepower システムは、デフォルトではアクセス コントロール ポリシーで使用されるすべての侵入ポリシーにデフォルトの変数セットをリンクします。侵入ポリシーを使用するアクセスコントロールポリシーを展開すると、その侵入ポリシー内で有効にした侵入ルールでは、リンクされた変数セットの変数値が使用されます。

アクセス コントロール ポリシー内の侵入ポリシーで使用されるカスタム変数セットを変更すると、システムの [アクセス コントロール ポリシー (Access Control Policy) ] ページで、そのポリシーのステータスが「失効 (out-of-date)」と表示されます。変数セットの変更内容を実装するには、アクセスコントロールポリシーを再度展開する必要があります。デフォルトセットを変更すると、侵入ポリシーを使用するすべてのアクセス コントロール ポリシーのステータスが「失効 (out-of-date)」と表示され、変更内容を実装するにはすべてのアクセス コントロール ポリシーを再度展開する必要があります。

## 変数

変数は、次のカテゴリのいずれかに属します。

### デフォルト変数

Firepower システムから提供される変数。デフォルト変数の名前変更または削除はできません。また、デフォルト値を変更することもできません。ただし、デフォルト変数のカスタマイズしたバージョンを作成できます。

### カスタマイズされた変数

作成した変数。この変数には、次の変数があります。

- カスタマイズされたデフォルト変数

デフォルト変数の値を編集すると、システムはその変数を [デフォルトの変数 (Default Variables)] 領域から [カスタマイズされた変数 (Customized Variables)] 領域に移動します。デフォルトセットの変数値によってカスタムセットの変数のデフォルト値が決まるため、デフォルトセットのデフォルト変数をカスタマイズすると、他のすべてのセットの変数のデフォルト値が変更されます。

#### • ユーザ定義変数

独自の変数を追加および削除したり、異なる変数セット内の値をカスタマイズしたり、カスタマイズされた変数をそのデフォルト値にリセットしたりできます。ユーザ定義変数をリセットすると、それは [カスタマイズされた変数 (Customized Variables)] 領域に残ります。

ユーザ定義変数は、次のいずれかのタイプにできます。

- ネットワーク変数は、ネットワークトラフィックのホストの IP アドレスを指定します。
- ポート変数は、ネットワークトラフィックの TCP または UDP ポートを指定するもので、いずれかのタイプを意味する値 `any` を指定することもできます。

たとえば、カスタム標準テキストルールを作成する場合、独自のユーザ定義変数を追加して、トラフィックをより正確に反映したり、ショートカットとしてルール作成プロセスを単純化したりすることもできます。また、「緩衝地帯」(つまり DMZ) でのみトラフィックを検査するルールを作成する場合、公開されているサーバの IP アドレスが値にリストされる `$DMZ` という変数を作成することもできます。こうして、この地帯で作成された任意のルールで `$DMZ` 変数を使用できます。

#### 拡張変数

特定の条件下で Firepower システムから提供される変数。この変数が含まれる展開は非常に限定的です。

## 定義済みデフォルト変数

デフォルトでは、Firepower System は、1 つのデフォルト変数セットを提供します。このセットは、定義済みのデフォルト変数から構成されています。Cisco Talos Security Intelligence and Research Group (Talos) では、ルール更新を使用し、新しい侵入ルールや更新された侵入ルール、他の侵入ポリシーエレメント (デフォルト変数など) を提供します。

システムが提供する侵入ルールの多くが定義済みのデフォルト変数を使用していることから、これらの変数に関する適切な値を設定します。変数セットを使用してネットワーク上のトラフィックを特定する方法によっては、任意またはすべての変数セットにあるこれらのデフォルト変数の値を変更できます。



**注意** アクセスコントロールまたは侵入ポリシーをインポートすると、デフォルトの変数セットにある既存のデフォルト変数が、インポートされたデフォルト変数でオーバーライドされます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。

次の表では、システムによって提供される変数について説明し、通常、いずれの変数に変更されるかを示します。変数をご使用のネットワークに合わせて調整する方法を決定するには、プロフェッショナル サービスまたはサポートにお問い合わせください。

表 45: システム提供変数

変数名	説明	変更しますか
\$AIM_SERVERS	既知の AOL インスタント メッセンジャ (AIM) サーバを定義し、これらはチャットベースのルールや AIM エクスプロイトを検索するルールで使用されます。	不要。
\$DNS_SERVERS	ドメインネームサービス (DNS) サーバを定義します。DNS サーバに特に影響するルールを作成する場合、\$DNS_SERVERS 変数を宛先または送信元 IP アドレスとして使用できます。	現在のルールセットでは不要です。
\$EXTERNAL_NET	Firepower System が非保護ネットワークとして表示されるネットワークを定義し、外部ネットワークを定義する多くのルールで使用されます。	はい。\$HOME_NET を適切に定義してから、\$EXTERNAL_NET の値として \$HOME_NET を除外する必要があります。
\$FILE_DATA_PORTS	ネットワークストリームでファイルを検出する侵入ルールで使用される非暗号化ポートを定義します。	不要。
\$FTP_PORTS	ネットワーク上の FTP サーバのポートを定義し、FTP サーバのエクスプロイトルールに使用されます。	はい。FTP サーバがデフォルトポート以外のポートを使用する場合 (web インターフェイスのデフォルトポートを表示できます)。
\$GTP_PORTS	パケット デコーダが GTP (General Packet Radio Service (GPRS) トンネリングプロトコル) PDU 内部でペイロードを取得するデータ チャネルポートを定義します。	不要。

変数名	説明	変更しますか
\$HOME_NET	関連した侵入ポリシーがモニタするネットワークを定義し、内部ネットワークを定義するために多くのルールで使用されます。	内部ネットワークのIPアドレスを指定する場合は変更します。
\$HTTP_PORTS	ネットワーク上のWebサーバのポートを定義し、Webサーバのエクスプロイトルールに使用されます。	はい。webサーバがデフォルトポート以外のポートを使用する場合（webインターフェイスのデフォルトポートを表示できます）。
\$HTTP_SERVERS	ネットワーク上のWebサーバを定義します。Webサーバのエクスプロイトルールで使用されます。	HTTPサーバを実行する場合は変更します。
\$ORACLE_PORTS	ネットワーク上でOracleデータベースサーバのポートを定義し、Oracleデータベースでの攻撃をスキャンするルールで使用されます。	Oracleサーバを実行する場合は変更します。
\$SHELLCODE_PORTS	システムにシェルコードのエクスプロイトをスキャンさせるポートを定義し、シェルコードを使用するエクスプロイトを検出するルールで使用されます。	不要。
\$SIP_PORTS	ネットワーク上のSIPサーバのポートを定義し、SIPのエクスプロイトルールに使用されます。	不要。
\$SIP_SERVERS	ネットワーク上のSIPサーバを定義し、SIP対象エクスプロイトを指定するルールで使用されます。	はい。SIPサーバを実行している場合は、\$HOME_NETを適切に定義してから、\$SIP_SERVERSの値として\$HOME_NETを含める必要があります。
\$SMTP_SERVERS	ネットワーク上でSMTPサーバを定義し、メールサーバをターゲットとするエクスプロイトを解決するルールで使用されます。	SMTPサーバを実行する場合は変更します。
\$SNMP_SERVERS	ネットワーク上でSNMPサーバを定義し、SNMPサーバでの攻撃をスキャンするルールで使用されます。	SNMPサーバを実行する場合は変更します。

変数名	説明	変更しますか
\$SNORT_BPF	その後バージョン 5.3.0 以降にアップグレードされるバージョン 5.3.0 以前の Firepower System ソフトウェア リリースのシステム上に存在する場合のみに表示されるレガシー拡張変数を特定します。	変更しません。この変数は表示または削除のみが可能です。削除後に、編集または復元することはできません。
\$SQL_SERVERS	ネットワーク上のデータベースサーバを定義し、データベース対象エクスプロイトを指定するルールで使用されます。	はい。SQL サーバを実行する場合は変更します。
\$SSH_PORTS	ネットワーク上の SSH サーバのポートを定義し、SSH サーバのエクスプロイトルールに使用されます。	はい。デフォルトポート以外の SSH サーバのポートを使用する場合（web インターフェイスでのデフォルトポートを表示できます）。
\$SSH_SERVERS	ネットワーク上の SSH サーバを定義し、SSH 対象エクスプロイトを指定するルールで使用されます。	はい。SSH サーバを実行している場合は、\$HOME_NET を適切に定義してから、\$SSH_SERVERS の値として \$HOME_NET を含める必要があります。
\$TELNET_SERVERS	ネットワーク上の既知の Telnet サーバを定義し、Telnet サーバ対象エクスプロイトを指定するルールで使用されます。	Telnet サーバを実行する場合は変更します。
\$USER_CONF	Web インターフェイスを介して利用可能な場合を除き、1 つ以上の特徴を設定できる一般的なツールを提供します。  \$USER_CONF の設定が競合または重複していると、システムは停止します。	機能の説明で指示されている場合や、サポートによる指示があった場合を除き、変更しません。

## ネットワーク変数

ネットワーク変数で表される IP アドレスを、侵入ポリシーで有効にした侵入ルール、侵入ポリシールール抑制、動的ルール状態、およびアダプティブ プロファイルの更新で使用することができます。ネットワーク変数とネットワーク オブジェクトおよびネットワーク オブジェクトグループとの相違点として、ネットワーク変数は侵入ポリシーおよび侵入ルールに固有のもので、一方、ネットワーク オブジェクトおよびグループを使用すると、アクセスコントロールポリシー、ネットワーク変数、侵入ルール、ネットワーク検出ルール、イベント検索、レポートなど、システムの Web インターフェイスのさまざまな場所で IP アドレスを表すことができます。



次の設定でネットワーク変数を使用して、ネットワーク上のホストの IP アドレスを指定できます。

- 侵入ルール：侵入ルールの [送信元 IP (Source IPs) ] および [宛先 IP (Destination IPs) ] 見出しフィールドを使用すると、パケット インスペクションを、特定の送信元または宛先 IP アドレスを持つパケットに制限することができます。
- 抑制：送信元または宛先の侵入ルール抑制の [ネットワーク (Network) ] フィールドを使用すると、特定の 1 つの IP アドレスまたは IP アドレス範囲が侵入ルールやプリプロセッサをトリガーした場合の侵入イベント通知を抑制できます。
- 動的ルール状態：送信元または宛先の動的ルール状態の [ネットワーク (Network) ] フィールドを使用すると、指定時間内に発生した侵入ルールやプリプロセッサルールの一致数が多すぎる場合に、それを検出できます。
- アダプティブ プロファイルの更新：アダプティブ プロファイルの更新が有効にされている場合、アダプティブ プロファイルの [ネットワーク (Networks) ] フィールドに、パッチ展開でパケット フラグメントおよび TCP ストリームのリアセンブルを改善する必要があるホストが示されます。

このセクションで示されるフィールドで変数を使用する場合、侵入ポリシーにリンクされた変数セットは、侵入ポリシーを使用するアクセスコントロールポリシーで処理されるネットワークトラフィックでの変数値を決定します。

次のネットワーク設定を任意に組み合わせて変数に追加できます。

- 使用可能なネットワーク リストから選択したネットワーク変数、ネットワーク オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせ
- [新規変数 (New Variable) ] または [変数の編集 (Edit Variable) ] ページから追加した個々のネットワークオブジェクト (独自の変数や、他の既存の変数、さらに今後の変数にこれらを追加できます)
- リテラルの単一 IP アドレスまたはアドレス ブロック

それぞれを個別に追加することにより、複数のリテラル IP アドレスとアドレス ブロックをリストできます。IPv4 および IPv6 アドレスとアドレス ブロックを単独で、または任意に組み合わせてリストできます。IPv6 アドレスを指定するときには、RFC 4291 で定義された任意のアドレス指定規則を使用できます。

追加する変数での包含ネットワークのデフォルト値は any で、これは任意の IPv4 または IPv6 アドレスを示します。除外ネットワークのデフォルト値は none です。これは「ネットワークなし」を意味します。また、リテラル値の中でアドレス :: を指定すると、包含ネットワークリストで任意の IPv6 アドレスを指定でき、除外リストでは IPv6 アドレスなしを指定できます。

除外リストにネットワークを追加すると、指定されたアドレスおよびアドレスブロックが除外されます。つまり、除外された IP アドレスやアドレスブロックを除き、任意の IP アドレスに一致させることができます。

たとえば、リテラルアドレス 192.168.1.1 を除外すると 192.168.1.1 以外の任意の IP アドレスが指定され、2001:db8:ca2e::fa4c を除外すると 2001:db8:ca2e::fa4c 以外の任意の IP アドレスが指定されます。

リテラルネットワークまたは使用可能なネットワークを任意に組み合わせて、除外で使用できます。たとえば、リテラル値 192.168.1.1 および 192.168.1.5 を除外すると、192.168.1.1 と 192.168.1.5 以外の任意の IP アドレスが含まれます。つまり、システムはこの構文を「192.168.1.1 でなく、しかも 192.168.1.5 でない」と解釈し、大カッコ内に列挙されたものを除くすべての IP アドレスに一致させます。

ネットワーク変数を追加または編集するときには、次の点に注意してください。

- 論理的に言って、値 any を除外することはできません。any を除外すると「アドレスなし」を意味することになります。たとえば、除外ネットワークリストに、値 any を持つ変数を追加することはできません。
- ネットワーク変数は、指定された侵入ルールおよび侵入ポリシー機能に関するトラフィックを識別します。プリプロセッサルールは、侵入ルールで使われているネットワーク変数で定義されたホストとは無関係に、イベントをトリガーできることに注意してください。
- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、アドレスブロック 192.168.5.0/24 を包含し、192.168.6.0/24 を除外することはできません。

## ポート変数

ポート変数は、侵入ポリシーで有効になった侵入ルールの [送信元ポート (Source Port)] および [宛先ポート (Destination Port)] ヘッダー フィールドで使用できる TCP ポートと UDP ポートを表します。ポート変数とポート オブジェクトおよびポート オブジェクト グループとの相違点は、ポート変数が侵入ルール固有のものであることです。TCP や UDP 以外のプロトコル用にポート オブジェクトを作成して、ポート変数、アクセス コントロール ポリシー、ネットワーク検出ルール、イベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。

侵入ルールの [送信元ポート (Source Port)] および [宛先ポート (Destination Port)] ヘッダー フィールドでポート変数を使用すると、パケットインスペクションを特定の送信元または宛先 TCP/UDP ポートを持つパケットに制限することができます。

これらのフィールドで変数を使用した場合、アクセス コントロール ルールまたはポリシーに関連付けられた侵入ポリシーにリンクされる変数セットは、アクセス コントロール ポリシーが展開されるネットワーク トラフィックでのこれらの変数の値を決定します。

次のポート設定を任意に組み合わせて変数に追加できます。

- 使用可能なポート リストから選択したポート変数およびポート オブジェクトの任意の組み合わせ

使用可能なポート リストには、ポート オブジェクト グループが表示されず、したがってこれらを変数に追加できないことに注意してください。

- [新規変数 (New Variable) ] または [変数の編集 (Edit Variable) ] ページから追加した個々のポートオブジェクト (独自の変数や、他の既存の変数、さらに今後の変数にこれらを追加できます)

有効な変数値は TCP および UDP ポートのみです (どちらのタイプでも値 any を含む)。新しい変数のページまたは変数の編集ページを使用して、有効な変数値ではない有効なポートオブジェクトを追加した場合、オブジェクトはシステムに追加されますが、使用可能なオブジェクトリストには表示されません。オブジェクトマネージャを使用して、変数で使われるポートオブジェクトを編集する場合、有効な変数値にのみ値を変更できます。

- 単一のリテラルポート値とポート範囲

ポート範囲はダッシュ (-) を使って区切る必要があります。下位互換性のために、コロンで指定されるポート範囲もサポートされていますが、作成するポート変数ではコロンを使用できません。

複数のリテラルポートの値および範囲をリストするには、それぞれを個別に追加して任意に組み合わせることができます。

ポート変数を追加または編集するときには、次の点に注意してください。

- 追加する変数での包含ポートのデフォルト値は any で、これは任意のポートまたはポート範囲を示します。除外ポートのデフォルト値は none で、これは「ポートなし」を示します。



---

**ヒント** 値 any を持つ変数を作成するには、特定の値を追加せずに変数に名前を付けて保存します。

---

- 論理的に言って、値 any を除外することはできません。any を除外すると「ポートなし」を意味することになります。たとえば、値 any を持つ変数を除外ポートリストに追加した場合、変数セットを保存することはできません。
- 除外リストにポートを追加すると、指定されたポートおよびポート範囲が除外されます。つまり、除外されたポートまたはポート範囲を除き、任意のポートに一致させることができます。
- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、ポート範囲 10 から 50 を包含し、ポート 60 を除外することはできません。

## 拡張変数

拡張変数を使用すると、他の方法では Web インターフェイスで設定できない機能を設定することができます。現在、Firepower システムで使用可能な拡張変数は 2 つのみで、そのうち USER\_CONF 拡張変数のみ編集可能です。

## USER\_CONF

USER\_CONF は、Web インターフェイスで通常設定できない1つ以上の機能を設定するための汎用ツールです。



**注意** 機能の説明またはサポート担当の指示に従う場合を除き、拡張変数USER\_CONFを使用して侵入ポリシー機能を設定しないでください。競合または重複する設定が存在すると、システムが停止します。

USER\_CONFを編集するときには、1行に合計4096文字まで入力できます。行は自動的に折り返します。変数の最大長 8192 文字、またはディスク スペースなどの物理制限に達するまで、任意の数の有効な指示または行数を含めることができます。コマンドディレクティブでは、完全な引数の後にバックスラッシュ (\) 行連結文字を使用します。

USER\_CONF をリセットすると、空になります。

## SNORT\_BPF

SNORT\_BPF はレガシー拡張変数です。バージョン 5.3.0 以降にアップグレードされる前の旧バージョンの Firepower システム ソフトウェアリリースのときにシステムでこの変数が設定された場合にのみ、これが表示されます。この変数は表示または削除のみが可能です。削除後に、編集または復元することはできません。

この変数を使用すると、Berkeley Packet Filter (BPF) を適用して、システムに到達する前のトラフィックをフィルタできました。SNORT\_BPF に備わっていたフィルタリング機能を今後も適用するには、この変数の代わりにアクセス コントロールルールを使用してください。この変数は、システム アップグレード前に存在していた設定でのみ表示されます。

## 変数のリセット

変数セットの新しい変数ページまたは変数の編集ページで、変数をデフォルト値にリセットできます。次の表に、変数をリセットするときの基本原則を要約します。

表 46: 変数のリセット値

リセットする変数のタイプ	それが含まれるセットタイプ	リセット後の値
デフォルト	デフォルト	ルール更新値
ユーザ定義	デフォルト	任意
デフォルトまたはユーザ定義	カスタム	現在のデフォルトセット値 (変更/未変更にかかわらず)

カスタムセットの変数をリセットすると、単にデフォルトセット内のその変数の現在値にリセットされます。

逆に、デフォルトセットの変数の値をリセットまたは変更すると、すべてのカスタムセット内のその変数のデフォルト値が常に更新されます。リセットアイコンがグレー表示され、その

変数をリセットできないことを示している場合、そのセットでは変数のカスタマイズ値が存在しないことを意味します。カスタムセット内の変数の値をすでにカスタマイズした場合を除き、デフォルトセットの変数を変更すると、変数セットがリンクされた侵入ポリシーで使われている値が更新されます。



(注) デフォルトセット内の変数を変更するときには、その変更により、リンクされたカスタムセットの変数を使用する侵入ポリシーがどのような影響を受けるか評価するのが適切です（特に、カスタムセット内の変数値をカスタマイズしていない場合）。

変数セット内のリセットアイコン (🔄) の上にポインタを置くと、リセット値を確認できます。カスタマイズされた値とリセット値が同じである場合は、次のいずれかを示しています。

- カスタムセットまたはデフォルトセットの中で、値 any を持つ変数を追加した
- カスタムセットの中で、明示的な値を持つ変数を追加し、設定した値をデフォルト値として使用することを選択した

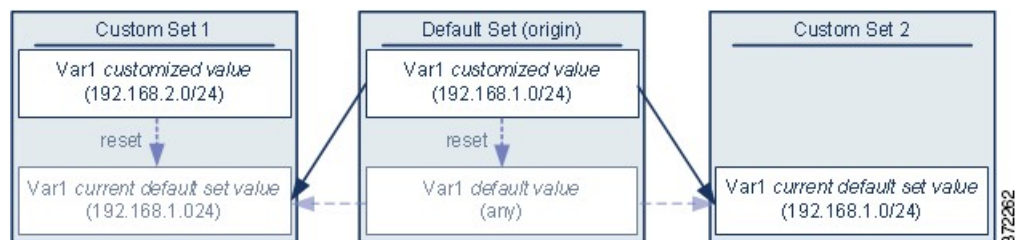
## セットに変数を追加する

変数セットに変数を追加すると、他のすべてのセットにもその変数が追加されます。カスタムセットから変数を追加する場合は、設定値をデフォルトセットのカスタマイズ値として使用するかどうかを選択する必要があります。

- 設定値（たとえば、192.168.0.0/16）を使用する場合、変数は、デフォルト値 any を持つカスタマイズ値として設定値を使用するデフォルトセットに追加されます。デフォルトセットの現在の値によって他のセットのデフォルト値が決まるため、他のカスタムセットの初期のデフォルト値は設定値（この例では 192.168.0.0/16）になります。
- 設定値を使用しない場合、変数はデフォルト値 any のみを使用してデフォルトセットに追加され、こうして、他のカスタムセットの初期のデフォルト値は any になります。

### 例：デフォルトセットへのユーザ定義変数の追加

次の図は、値が 192.168.1.0/24 のデフォルトセットにユーザ定義の変数 var1 を追加した場合のセットのインタラクションを示しています。



任意のセットで var1 の値をカスタマイズできます。var1 がカスタマイズされていない Custom Set 2 では、この値は 192.168.1.0/24 です。Custom Set 1 では、var1 のカスタマイズ値

例：カスタムセットへのユーザ定義変数の追加

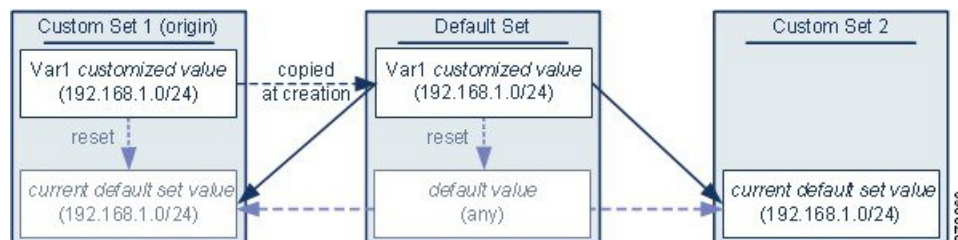
192.168.2.0/24はデフォルト値をオーバーライドします。デフォルトセットのユーザ定義変数をリセットすると、すべてのセットのそのデフォルト値が any にリセットされます。

この例では、Custom Set 2 で var1 を更新しなかった場合、デフォルトセットで var1 をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 var1 が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

この例では示されていませんが、セット間のインタラクションは、デフォルトセットのデフォルト変数をリセットすると現在のルール更新で Cisco によって設定された値に、そのデフォルト変数がリセットされること以外は、ユーザ定義変数およびデフォルト変数で同じであることに注意してください。

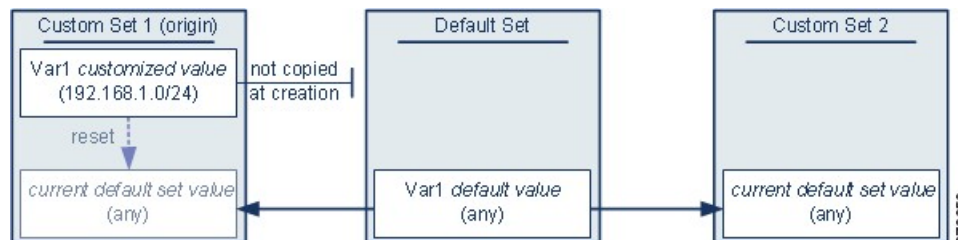
例：カスタムセットへのユーザ定義変数の追加

次の2つの例は、カスタムセットにユーザ定義変数を追加した場合の変数セットのインタラクションについて示しています。新しい変数を保存すると、設定値を他のセットのデフォルト値として使用するかどうかを尋ねるプロンプトが出されます。次の例では、設定値を使用するという選択がなされています。



Custom Set 1 からの var1 の発信元を除き、この例は var1 をデフォルトセットに追加した上述の例と同じであることに注意してください。var1 のカスタマイズ値 192.168.1.0/24 を Custom Set 1 に追加すると、値はデフォルト値 any を持つカスタマイズ値としてデフォルトセットにコピーされます。その後、var1 の値とインタラクションは、var1 をデフォルトセットに追加した場合と同じになります。前述の例と同様、デフォルトセットで var1 をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 var1 が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

次の例では、前述の例にあるように値が 192.168.1.0/24 の var1 を Custom Set 1 に追加しますが、var1 の設定値を他のセットのデフォルト値として**使用しない**ことを選択します。



このアプローチでは、var1 をデフォルト値 any を持つすべてのセットに追加します。var1 を追加したら、任意のセットでその値をカスタマイズできます。このアプローチの利点は、デフォルトセットで var1 を最初にカスタマイズしないことによって、デフォルトセットの値を

カスタマイズし、var1 をカスタマイズしていない Custom Set 2 などのセット内の現在の値を意図せずに変更してしまうリスクが軽減されます。

## 変数のネスト

循環したネストにならない限り、変数をネストすることができます。否定形の変数をネストすることはできません。

### 有効なネストされた変数

以下の例では、SMTP\_SERVERS、HTTP\_SERVERS、OTHER\_SERVERS がネストしても有効な変数です。

変数	タイプ (Type)	含まれるネットワーク	除外されるネットワーク
SMTP_SERVERS	カスタマイズされたデフォルト	10.1.1.1	—
HTTP_SERVERS	カスタマイズされたデフォルト	10.1.1.2	—
OTHER_SERVERS	ユーザ定義	10.2.2.0/24	—
HOME_NET	カスタマイズされたデフォルト	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

### 無効なネストされた変数

以下の例では、HOME\_NET はネストすると無効な変数です。HOME\_NET をネストすると、変数の循環になるためです。つまり、OTHER\_SERVERS の定義には HOME\_NET が含まれるため、HOME\_NET はそれ自体でネストすることになります。

変数	タイプ (Type)	含まれるネットワーク	除外されるネットワーク
SMTP_SERVERS	カスタマイズされたデフォルト	10.1.1.1	—
HTTP_SERVERS	カスタマイズされたデフォルト	10.1.1.2	—
OTHER_SERVERS	ユーザ定義	10.2.2.0/24 HOME_NET	—

変数	タイプ (Type)	含まれるネットワーク	除外されるネットワーク
HOME_NET	カスタマイズされたデフォルト	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

#### ネストでサポートされない否定形の変数

否定形の変数のネストはサポートされないため、以下の例に示されているように、保護ネットワークの外部にある IP アドレスを表す変数 NONCORE\_NET を使用することはできません。

変数	タイプ (Type)	含まれるネットワーク	除外されるネットワーク
HOME_NET	カスタマイズされたデフォルト	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
EXTERNAL_NET	カスタマイズされたデフォルト	—	HOME_NET
DMZ_NET	ユーザ定義	10.4.0.0/16	—
NOT_DMZ_NET	ユーザ定義	—	DMZ_NET
NONCORE_NET	ユーザ定義	EXTERNAL_NET NOT_DMZ_NET	—

#### ネストでサポートされない否定形の変数の代替手段

上記の例の代替手段として、以下に示す変数 NONCORE\_NET を作成することで、保護ネットワークの外部にある IP アドレスを表すことができます。

変数	タイプ (Type)	含まれるネットワーク	除外されるネットワーク
HOME_NET	カスタマイズされたデフォルト	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
DMZ_NET	ユーザ定義	10.4.0.0/16	—
NONCORE_NET	ユーザ定義	—	HOME_NET DMZ_NET



## 変数セットの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

### 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ 2** オブジェクトタイプのリストから [変数セット (Variable Set)] を選択します。

**ステップ 3** 変数セットを管理します。

- 追加：カスタムの変数セットを追加するには、[変数セットの追加 (Add Variable Set)] をクリックします。 [変数セットの作成 \(460 ページ\)](#) を参照してください。
- 削除：カスタムの変数セットを削除するには、変数セットの横にある削除アイコン (🗑️) をクリックして、[はい (Yes)] をクリックします。デフォルトの変数セットまたは先祖ドメインに属している変数セットは削除できません。

(注) 削除する変数セットで作成された変数は、別のセットで削除されたり他の方法で影響を受けることはありません。

- 編集：変数セットを編集するには、変更する変数セットの横にある編集アイコン (✎) をクリックします。 [オブジェクトの編集 \(424 ページ\)](#) を参照してください。
- フィルタ処理：変数セットを名前でもフィルタリングするには、名前を入力を開始します。入力中にページが更新され、一致する名前が表示されます。名前のフィルタリングをクリアするには、フィルタ フィールドにあるクリアアイコン (✖) をクリックします。
- 変数の管理：変数セットに含まれる変数を管理するには、 [変数の管理 \(460 ページ\)](#) を参照してください。

## 変数セットの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ2** オブジェクトタイプのリストから [変数セット (Variable Set)] を選択します。

**ステップ3** [変数セットの追加 (Add Variable Set)] をクリックします。

**ステップ4** 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

**ステップ5** 必要に応じて、[説明 (Description)] を入力します。

**ステップ6** セット内の変数を管理します ([変数の管理 \(460 ページ\)](#) を参照)。

**ステップ7** [保存 (Save)] をクリックします。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## 変数の管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

## 手順

**ステップ1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ2** オブジェクト タイプのリストから [変数セット (Variable Set)] を選択します。

**ステップ3** 編集する変数セットの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ4** 変数を管理します。

- 表示：変数の完全な値を表示するには、変数の横の [値 (Value)] 列内の値にポインタを重ねます。
- 追加：変数を追加するには、[追加 (Add)] をクリックします。 [変数の追加 \(462 ページ\)](#) を参照してください。
- 削除：変数の横にある削除アイコン (🗑️) をクリックします。変数の追加後に変数セットを保存した場合は、[はい (Yes)] をクリックして、変数の削除を確認します。

次の変数は削除できません。

- デフォルトの変数
- 侵入ルールや別の変数で使用されているユーザ定義変数
- 先祖ドメインに属している変数
- 編集：編集する変数の横にある編集アイコン (✎) をクリックします。 [変数の編集 \(463 ページ\)](#) を参照してください。
- リセット：変更した変数をデフォルト値にリセットするには、変更した変数の横にあるリセットアイコン (↺) をクリックします。リセットアイコンがグレー表示の場合は、次のいずれかが当てはまります。
  - 現在の値がすでにデフォルト値になっている。
  - 設定が先祖ドメインに属している。

**ヒント** アクティブなリセットアイコンの上にポインタを移動して、デフォルト値を表示します。

**ステップ5** [保存 (Save)] をクリックして、変数セットを保存します。その変数セットがアクセスコントロール ポリシーで使用されている場合は、[はい (Yes)] をクリックして変更を保存することを確認します。

デフォルトセットの現在の値によって他のすべてのセットのデフォルト値が決まるため、デフォルトセットの変数を変更またはリセットすると、デフォルト値がカスタマイズされていない他のセットの現在の値が変更されます。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（[設定変更の導入 \(350 ページ\)](#) を参照）。

## 変数の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** 変数セット エディタで、[追加 (Add)] をクリックします。

**ステップ 2** [名前 (Name)] に一意の変数名を入力します。

**ステップ 3** [タイプ (Type)] ドロップダウン リストから、[ネットワーク (Network)] または [ポート (Port)] を選択します。

**ステップ 4** 変数の値を指定します。

- 使用可能ネットワークまたはポートのリストの項目を包含リストまたは除外リストに移動する場合は、1 つまたは複数の項目を選択してドラッグアンドドロップするか、[包含 (Include)] または [除外 (Exclude)] をクリックします。

**ヒント** ネットワーク変数またはポート変数の包含リストと除外リストにあるアドレスやポートが重複している場合、除外されているアドレスまたはポートが優先されません。

- 1 つのリテラル値を入力し、[追加 (Add)] をクリックします。ネットワーク変数の場合、単一の IP アドレスまたはアドレスブロックを入力できます。ポート変数の場合、単一ポートまたはポート範囲を追加できます。ポート範囲は上限値と下限値をハイフン (-) で区切ります。複数のリテラル値を入力する場合は、必要に応じてこの手順を繰り返します。
- 包含リストまたは除外リストから項目を削除するには、項目の横にある削除アイコン (🗑️) をクリックします。

(注) ネットワーク変数の場合、包含または除外する項目のリストは、リテラル文字列や既存の変数、オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせで構成できます。

**ステップ5** [保存 (Save) ]をクリックして変数を保存します。カスタムセットから新しい変数を追加する場合、次のオプションがあります。

- [はい (Yes) ]をクリックすると、設定値を使用する変数がデフォルトセットのカスタマイズ値として追加され、結果として他のカスタムセットのデフォルト値として追加されません。
- [いいえ (No) ]をクリックすると、変数はデフォルトセットのデフォルト値 any として追加され、結果として他のカスタムセットのデフォルト値として追加されます。

**ステップ6** [保存 (Save) ]をクリックして変数セットを保存します。変更内容が保存され、変数セットにリンクされているアクセスコントロールポリシーに失効ステータスが表示されます。

#### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## 変数の編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

カスタム変数とデフォルト変数の両方を編集できます。

既存の変数の [名前 (Name) ] と [タイプ (Type) ] の値は変更できません。

#### 手順

**ステップ1** 変数セット エディタで変更する変数の横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

**ステップ2** 変数を変更します。

- 利用可能なネットワークまたはポートのリストから、含める項目のリストまたは除外する項目のリストに項目を移動するには、1つ以上の項目を選択してからドラッグアンドドロップするか、または [含める (Include) ] か [除外 (Exclude) ] をクリックします。

**ヒント** ネットワーク変数またはポート変数の包含リストと除外リストにあるアドレスやポートが重複している場合、除外されているアドレスまたはポートが優先されません。

- 1つのリテラル値を入力し、[追加 (Add) ] をクリックします。ネットワーク変数の場合、単一のIPアドレスまたはアドレスブロックを入力できます。ポート変数の場合、単一ポートまたはポート範囲を追加できます。ポート範囲は上限値と下限値をハイフン (-) で区切ります。複数のリテラル値を入力する場合は、必要に応じてこの手順を繰り返します。
- 含めるリストまたは除外リストから項目を削除するには、項目の横にある削除アイコン (🗑️) をクリックします。

(注) ネットワーク変数の場合、包含または除外する項目のリストは、リテラル文字列や既存の変数、オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせで構成できます。

**ステップ 3** [保存 (Save) ] をクリックして変数を保存します。

**ステップ 4** [保存 (Save) ] をクリックして変数セットを保存します。変数セットがアクセスコントロールポリシーで使用されている場合、[はい (Yes) ] をクリックして変更の保存を確認します。変更内容が保存され、変数セットにリンクされているアクセスコントロールポリシーに失効ステータスが表示されます。

#### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## セキュリティインテリジェンスのリストとフィード

セキュリティインテリジェンスのリストとフィードは、以下を収集することでトラフィックをすばやくフィルタリングするのに役立ちます。

- IPアドレスとアドレスブロック：アクセスコントロールポリシーでセキュリティインテリジェンスの一部としてブラックリスト化およびホワイトリスト化するのに使用します。
- ドメイン名：DNSポリシーでセキュリティインテリジェンスの一部としてブラックリスト化およびホワイトリスト化するのに使用します。
- URL：アクセスコントロールポリシーでセキュリティインテリジェンスの一部としてブラックリスト化およびホワイトリスト化するのに使用します。また、セキュリティインテリジェンス後に分析およびトラフィック処理フェーズが実行されるアクセスコントロールルールおよびQoSルールで、URLリストを使用することもできます。

## 一覧

リストは、手動で管理される静的コレクションです。

デフォルトで、アクセスコントロールポリシーとDNSポリシーは、セキュリティインテリジェンスの一部としてグローバルブラックリストおよびホワイトリストを使用します。[今すぐホワイトリストに登録 (Whitelist Now)] および [今すぐブラックリストに登録 (Blacklist Now)] アクションを使用することで、再展開することなくセキュリティインテリジェンスリストを作成して実装できます。[今すぐブラックリストに登録 (Blacklist Now)]、[今すぐホワイトリストに登録 (Whitelist Now)]、およびグローバルリスト (466 ページ) を参照してください。

カスタムリストは、フィードやグローバルリストを増補および微調整できます。ただし、カスタムリストを実装するには再展開する必要があります。

## フィード

フィードは、HTTP または HTTPS で一定期間更新する動的コレクションです。

定期的に更新される Cisco Intelligence Feed を使用すると、Talos からの最新の脅威インテリジェンスに基づいてネットワークトラフィックをフィルタリングできます。また、サードパーティのフィードを使用することもできます。あるいは、カスタム内部フィードを使用すると、複数の Firepower Management Center からなる大規模な導入で企業全体のブラックリストを簡単に保衛できます。

システムがフィードを更新する際は、変更が伝搬されるまで数分かかりますが、再展開の必要はありません。システムがフィードをインターネットから更新するタイミングを厳密に制御したい場合は、そのフィードの自動更新を無効にすることができます。ただし、自動更新を行えば、最新の関連するデータであることが確実にになります。



- (注) システムはカスタム フィードのダウンロード時にピア SSL 証明書の検証を実行しません。また、システムは、証明書のバンドルまたは自己署名証明書を使用したリモートピアの検証もサポートしていません。

## リストとフィードの書式設定

各リストまたはフィードは、500MB 未満の単純なテキスト ファイルでなければなりません。リスト ファイルの拡張子は .txt でなければなりません。1 行につきエントリまたはコメントを 1 つ (IP アドレス 1 つ、URL 1 つ、ドメイン名 1 つ) 含めます。



- ヒント 含めることができるエントリの数は、ファイルの最大サイズによって制限されます。たとえば、コメントがなく URL の長さの平均が 100 文字 (Punycode または Unicode 表現と改行のパーセントを含む) の URL リストには、524 万を超えるエントリを含めることができます。

DNS リストエントリ内では、ドメインラベルとしてアスタリスク (\*) ワイルドカード文字を指定できます。その場合、すべてのラベルがワイルドカードと一致します。たとえば、`www.example.*` のエントリは `www.example.com` と `www.example.co` の両方に一致します。

ソース ファイル内にコメント行を含める場合は、シャープ (#) 文字で開始する必要があります。コメントが含まれるソース ファイルをアップロードすると、システムによってアップロード中にコメントが削除されます。ダウンロードするソース ファイルには、コメントを除くすべてのエントリが含まれます。

システムが破損したフィードまたは認識不能なエントリがあるフィードをダウンロードした場合、システムは古いフィードデータを引き続き使用します（これが初回のダウンロードである場合を除く）。ただし、システムがフィード内のエントリを1つでも認識できる場合、システムは認識できるエントリを使用します。

## セキュリティ インテリジェンス オブジェクトのクイック リファレンス

オブジェクトタイプ (Object Type)	機能の編集	編集後に再度展開しますか?
デフォルト (カスタム入力) ホワイトリストとブラックリスト: グローバル、子孫、ドメイン固有	コンテキストメニューを使用してエントリを追加。 オブジェクト マネージャを使用してエントリを削除。	エントリを追加後、いいえ。 エントリを削除後、はい。
カスタム ホワイトリストとブラックリスト	オブジェクト マネージャを使用して新しいリストと交換リストをアップロード。	○
システム提供インテリジェンス フィード	オブジェクト マネージャを使用して更新頻度を無効または変更。	なし
カスタム フィード	オブジェクト マネージャを使用して完全に変更。	なし
シンクホール	オブジェクト マネージャを使用して完全に変更。	○

### [今すぐブラックリストに登録 (Blacklist Now)]、[今すぐホワイトリストに登録 (Whitelist Now)]、およびグローバル リスト

Firepower Management Center のコンテキストメニュー ([コンテキストメニュー \(32 ページ\)](#) を参照) では、セキュリティインテリジェンスを使って、すばやくブラックリストやホワイトリストに登録することができます。たとえば、エクスプロイトの試行に関連した侵入イベント



でルーティング可能な IP アドレスのセットに気付いた場合、それらの IP アドレスを即座にブラックリストに入れることができます。変更内容が伝達されるまでに数分かかる場合がありますが、再度展開する必要はありません。

[今すぐブラックリストに登録 (Blacklist Now) ] と [今すぐホワイトリストに登録 (Whitelist Now) ] のコンテキストメニュー オプションは、IP アドレス、URL、DNS 要求ホットスポットに使用可能です。コンテキストメニューでブラックリストまたはホワイトリストに登録すると、選択した項目が該当するデフォルトグローバルリストに追加されます。デフォルトでは、アクセスコントロールポリシーと DNS ポリシーがすべてのセキュリティゾーンに適用されるグローバルリストを使用します。ポリシーごとに、これらのリストを使用しないように選択することができます。



(注) これらのオプションは、セキュリティインテリジェンスにのみ適用されます。セキュリティインテリジェンスは、すでにファーストパスされたトラフィックをブラックリストに登録することはできません。同様に、セキュリティインテリジェンスでホワイトリストに登録しても、それに一致するトラフィックが自動的に信頼されることもファーストパスされることもありません。詳細については、[セキュリティインテリジェンスについて \(1375ページ\)](#) を参照してください。

コンテキストメニュー オプション	対象項目	対象グローバル リスト
[今すぐブラックリストに追加 (Blacklist Now) ] [今すぐホワイトリストに追加 (Whitelist Now) ]	IP アドレス	[グローバルブラックリスト (Global Blacklist) ] [グローバルホワイトリスト (Global Whitelist) ]
[今すぐ URL に HTTP/S 接続をブラックリストする (Blacklist HTTP/S Connections to URL Now) ] [今すぐ URL に HTTP/S 接続をホワイトリストする (Whitelist HTTP/S Connections to URL Now) ]	URL	[URL グローバルブラックリスト (Global Blacklist for URL) ] [URL グローバルホワイトリスト (Global Whitelist for URL) ]
[今すぐドメインに HTTP/S 接続をブラックリストする (Blacklist HTTP/S Connections to Domain Now) ] [今すぐドメインに HTTP/S 接続をホワイトリストする (Whitelist HTTP/S Connections to Domain Now) ]	ドメイン全体	[URL グローバルブラックリスト (Global Blacklist for URL) ] [URL グローバルホワイトリスト (Global Whitelist for URL) ]

コンテキストメニューオプション	対象項目	対象グローバルリスト
[今すぐドメインに DNS 要求をブラックリストにする (Blacklist DNS Requests to Domain Now) ]	ドメイン全体の DNS 要求	[DNS グローバルブラックリスト (Global Blacklist for DNS) ]
[今すぐドメインに DNS 要求をホワイトリストにする (Whitelist DNS Requests to Domain Now) ]		[DNS グローバルホワイトリスト (Global Whitelist for DNS) ]

マルチドメイン展開では、グローバルリストだけでなくドメインリストにも項目を登録することで、ブラックリストやホワイトリストを適用する Firepower システム ドメインを選択することができます。セキュリティインテリジェンスリストとマルチテナンシー (468 ページ) を参照してください。

セキュリティインテリジェンスリストにエントリを追加すると、アクセス制御に影響が出るため、次のうちいずれか1つが必須です。

- 管理者 (Administrator) アクセス
- デフォルト ロールの組み合わせ：ネットワーク管理者 (Network Admin) またはアクセス管理者 (Access Admin) に加えてセキュリティアナリスト (Security Analyst) およびセキュリティ承認者 (Security Approver)
- アクセス コントロール ポリシーの変更 (Modify Access Control Policy) と設定をデバイスに展開 (Deploy Configuration to Devices) の両方のアクセス許可を持つカスタム ロール。

## セキュリティ インテリジェンス リストとマルチテナンシー

マルチドメイン展開では、グローバルドメインは、グローバルなブラックリストとホワイトリストを所有しています。グローバルリストに対して項目を追加または削除できるのは、グローバル管理者のみです。サブドメイン ユーザがネットワーク、ドメイン名、および URL をホワイトリストとブラックリストに追加できるように、マルチテナンシーでは次のものが追加されます。

- ドメインリスト：コンテンツが特定のサブドメインにのみ適用されるホワイトリストまたはブラックリスト。グローバルリストは、グローバルドメインのドメインリストです。
- 子孫ドメインリスト：現在のドメインの子孫のドメインリストを集約するホワイトリストまたはブラックリスト。

### ドメイン リスト

グローバルリストに（編集ではなく）アクセスできることに加えて、各サブドメインには独自の名前付きリストがあり、そのコンテンツはそのサブドメインにのみ適用されます。たとえば、Company A という名前のサブドメインは、次のリストを所有するとします。

- ドメインブラックリスト - Company A およびドメイン ホワイトリスト - Company A

- DNS のドメインブラックリスト - Company A、および DNS のドメインホワイトリスト - Company A
- URL のドメインブラックリスト - Company A、および URL のドメインホワイトリスト - Company A

現在のドメインより上位の管理者は、これらのリストに入力できます。コンテキストメニューを使用して、現在のドメインとすべての子孫ドメインの項目をブラックリストまたはホワイトリストに追加できます。ただし、ドメインリストから項目を削除できるのは、関連付けられたドメインの管理者のみです。

たとえば、グローバル管理者はグローバルドメインと Company A のドメインの同じ IP アドレスをブラックリストに追加できますが、それを Company B のドメインのブラックリストには追加できません。このアクションにより、同じ IP アドレスが次のリストに追加されます。

- (グローバル管理者のみが削除できる) グローバルブラックリスト
- (Company A の管理者のみが削除できる) ドメインブラックリスト - Company A

システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

### 子孫ドメインリスト

子孫ドメインリストは、現在のドメインの子孫のドメインリストを集約するホワイトリストまたはブラックリストです。リーフドメインには、子孫ドメインリストはありません。

子孫ドメインリストが便利なのは、上位レベルのドメインの管理者が一般的なセキュリティインテリジェンス設定を適用できる一方で、サブドメインユーザは独自の展開で項目をブラックリストやホワイトリストに追加できるためです。

たとえば、グローバルドメインには、次の子孫ドメインリストがあります。

- 子孫ブラックリスト - グローバルおよび子孫のホワイトリスト - グローバル
- URL の子孫ブラックリスト - グローバル、および子孫の URL のホワイトリスト - グローバル
- URL の子孫ブラックリスト - グローバル、および子孫の URL のホワイトリスト - グローバル



(注) 子孫ドメインリストは、手動で入力されたリストではなく象徴的な集約であるため、オブジェクトマネージャには表示されません。それを使用できる場所、つまり、アクセスコントロールポリシーと DNS ポリシーに表示されます。

## セキュリティ インテリジェンス フィードの更新頻度の変更

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

システムが提供するフィードは削除できませんが、更新頻度を変更（または無効に設定）できます。デフォルトで、フィードは2時間ごとに更新されます。

マルチドメイン展開では、システムが提供するフィードはグローバルドメインに属し、このドメインの管理者のみが変更できます。ユーザは、各自が使用するドメインに属するカスタムフィードの更新頻度を更新できます。

### 手順

- 
- ステップ 1** [オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択します。
- ステップ 2** [セキュリティ インテリジェンス (Security Intelligence) ] ノードを展開し、更新頻度を変更するフィードのタイプを選択します。
- ステップ 3** 更新するフィードの横にある編集アイコン (✎) をクリックします。
- 代わりに表示アイコン (🔍) が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。
- ステップ 4** [更新頻度 (Update Frequency) ] を編集します。
- ステップ 5** [保存 (Save) ] をクリックします。
- 

## カスタム セキュリティ インテリジェンス フィード

カスタムまたはサードパーティのセキュリティ インテリジェンス フィードを使用すると、インターネット上で定期的に更新される他の信頼できるホワイトリストおよびブラックリストによって、システムが提供するインテリジェンスフィードを拡張することができます。内部フィードをセットアップすることもできます。これは、1つのソースリストを使用して導入環境で複数の Firepower Management Center を更新する場合に役立ちます。



- (注) セキュリティインテリジェンス フィードでは、/0 ネットマスクを使ってアドレスブロックをホワイトリスト登録またはブラックリスト登録することはできません。ポリシーですべてのトラフィックをモニタまたはブロックする場合は、[モニタ (Monitor)] または [ブロック (Block)] ルールアクションを含むアクセスコントロールルールを使用し、デフォルト値 any を [送信元ネットワーク (Source Networks)] および [宛先ネットワーク (Destination Networks)] それぞれに設定します。

フィードを設定する場合は、URL を使用して場所を指定します。この URL は Punycode によりエンコードできません。デフォルトで、システムは設定した間隔でフィードソース全体をダウンロードし、管理対象デバイスを自動更新します。

md5 チェックサムを使用して、更新フィードをダウンロードするかどうか判断するようにシステムを設定することもできます。システムが最後にフィードをダウンロードした後にチェックサムが変更されていない場合、再ダウンロードする必要はありません。特に内部フィードが大きい場合には、md5 チェックサムを使用することができます。md5 チェックサムは、チェックサムのみを含む単純なテキストファイルに保存する必要があります。コメントはサポートされていません。

手動でセキュリティインテリジェンス フィードを更新すると、インテリジェンス フィードを含め、すべてのフィードが更新されます。

## セキュリティインテリジェンス フィードの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

- ステップ 1 [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ 2 [セキュリティインテリジェンス (Security Intelligence)] ノードを展開し、追加するフィードタイプを選択します。
- ステップ 3 上記で選択したフィードタイプに適したオプションをクリックします。
  - [ネットワーク リストとフィードの追加 (Add Network Lists and Feeds)]
  - [DNS リストとフィードの追加 (Add DNS Lists and Feeds)]
  - [URL リストとフィードの追加 (Add URL Lists and Feeds)]
- ステップ 4 フィードの名前を [名前 (Name)] に入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

**ステップ5** [タイプ (Type) ] ドロップダウンリストから [フィード (Feed) ] を選択します。

**ステップ6** [フィード URL (Feed URL) ] を入力します。

**ステップ7** オプションで、[MD5 URL] を入力します。

**ステップ8** [更新頻度 (Update Frequency) ] を選択します。

**ステップ9** [保存 (Save) ] をクリックします。

フィードの更新を無効にした場合を除き、システムはフィードをダウンロードして検証しようとしています。

## 手動によるセキュリティインテリジェンスフィードの更新

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (セキュリティインテリジェンス)	保護 (セキュリティインテリジェンス)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ1** [オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択します。

**ステップ2** [セキュリティインテリジェンス (Security Intelligence) ] ノードを展開し、フィードタイプを選択します。

**ステップ3** [フィードの更新 (Update Feeds) ] をクリックして、確認します。

**ステップ4** [OK] をクリックします。

フィードの更新をダウンロードして検証した後、Firepower Management Center はすべての変更内容を管理対象デバイスに通知します。導入環境では、更新されたフィードを使用してトラフィックのフィルタリングが開始されます。

## カスタムセキュリティインテリジェンスリスト

セキュリティインテリジェンスリストは、IPアドレス、アドレスブロック、URL、またはドメイン名の単純なスタティックリストで、ユーザがシステムに手動でアップロードします。カスタムリストは、単一の Firepower Management Center の管理対象デバイスで、フィードやグローバルリストの1つを増やしたり、微調整したりする場合に役立ちます。

たとえば、信頼できるフィードが重要なリソースへのアクセスを誤ってブロックしているものの、このフィードが全体的に部門にとって有用である場合、IP アドレス フィード オブジェクトをアクセス コントロール ポリシーのブラックリストから削除する代わりに、誤って分類された IP アドレスだけが含まれるカスタム ホワイトリストを作成できます。



- (注) セキュリティインテリジェンスリストでは、/0 ネットマスクを使ってアドレスブロックをホワイトリスト登録またはブラックリスト登録することはできません。ポリシーですべてのトラフィックをモニタまたはブロックする場合は、[モニタ (Monitor)] または [ブロック (Block)] ルールアクションを含むアクセス コントロールルールを使用し、デフォルト値 any を [送信元ネットワーク (Source Networks)] および [宛先ネットワーク (Destination Networks)] それぞれに設定します。

リスト エントリのフォーマットについて、次の点に注意してください。

- アドレスブロックのネットマスクは、IPv4 および IPv6 の場合、それぞれ 0 から 32、または 0 から 128 までの整数になります。
- ドメイン名に含まれる Unicode は Punycode 形式でエンコードされる必要があります。大文字と小文字は区別されません。
- ドメイン名の文字の大文字と小文字は区別されません。
- URL に含まれる Unicode はパーセントエンコーディング形式でエンコードする必要があります。
- URL サブディレクトリの文字の大文字と小文字は区別されます。
- シャープ記号 (#) で始まるリスト エントリは、コメントと見なされます。

リスト エントリの照合について、次の点に注意してください。

- URL または DNS リストにより高位レベルのドメインが存在する場合、システムはそれより低いレベルのドメインを一致とします。たとえば、DNS リストに example.com を追加すると、システムは www.example.com と test.example.com の両方を一致とします。
- システムは DNS または URL リスト エントリに対して DNS ルックアップを (フォワードルックアップ、リバースルックアップともに) 行いません。たとえば、URL リストに http://192.168.0.2 を追加し、これがルックアップすれば http://www.example.com であつたとします。この場合、システムは http://192.168.0.2 のみ一致とし、http://www.example.com は一致となりません。
- URL リストに末尾がスラッシュ (/) 記号で終わる URL を追加した場合、そのエントリに一致するのは完全に一致する URL のみとなります。
- URL または DNS リストに末尾にスラッシュ記号のない URL を追加した場合、そのエントリと同じプレフィックスを持つ URL は一致となります。たとえば、URL リストに www.example.com を追加すると、システムは www.example.com と www.example.com/example の両方を一致とします。

## 新しいセキュリティインテリジェンスリストの Firepower Management Center へのアップロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

セキュリティインテリジェンスリストを変更するには、ソースファイルを変更して、新しいコピーをアップロードする必要があります。Webインターフェイスを使用してファイルの内容を変更することはできません。ソースファイルへのアクセス権がない場合は、システムからコピーをダウンロードします。

### 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ 2** [セキュリティインテリジェンス (Security Intelligence)] ノードを展開し、リストのタイプを選択します。

**ステップ 3** 上記の手順で選択したリストに該当するオプションをクリックします。

- [ネットワークリストとフィードの追加 (Add Network Lists and Feeds)]
- [DNS リストとフィードの追加 (Add DNS Lists and Feeds)]
- [URL リストとフィードの追加 (Add URL Lists and Feeds)]

**ステップ 4** 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

**ステップ 5** [タイプ (Type)] ドロップダウンリストから、[リスト (List)] を選択します。

**ステップ 6** [参照 (Browse)] をクリックしてリストの .txt ファイルを位置指定し、[アップロード (Upload)] をクリックします。

**ステップ 7** [保存 (Save)] をクリックします。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。



## セキュリティ インテリジェンス リストの更新

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

### 手順

- ステップ 1 [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ 2 [セキュリティ インテリジェンス (Security Intelligence)] ノードを展開し、リストのタイプを選択します。
- ステップ 3 更新するリストの横にある編集アイコン (✎) をクリックします。  
代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 4 編集するリストのコピーが必要な場合、[ダウンロード (Download)] をクリックし、ブラウザのプロンプトに従ってリストをテキスト ファイルとして保存します。
- ステップ 5 必要に応じてリストを変更します。
- ステップ 6 [セキュリティ インテリジェンス (Security Intelligence)] ポップアップ ウィンドウで、[参照 (Browse)] をクリックして、変更されたリストを参照し、[アップロード (Upload)] をクリックします。
- ステップ 7 [保存 (Save)] をクリックします。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## シンクホール オブジェクト

シンクホールオブジェクトとは、シンクホール内のすべてのドメイン名のルーティング不可アドレスか、またはサーバに解決されない IP アドレスのいずれかを付与する DNS サーバを表します。DNS ポリシー ルール内のシンクホール オブジェクトを参照して、一致するトラフィック

クをシンクホールにリダイレクトすることができます。オブジェクトには、IPv4 アドレスと IPv6 アドレスの両方を割り当てる必要があります。

## シンクホールオブジェクトの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ 2** オブジェクトタイプのリストから [シンクホール (Sinkhole)] を選択します。

**ステップ 3** [シンクホールの追加 (Add Sinkhole)] をクリックします。

**ステップ 4** 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

**ステップ 5** シンクホールの [IPv4 アドレス (IPv4 Address)] と [IPv6 アドレス (IPv6 Address)] を入力します。

**ステップ 6** 次の選択肢があります。

- シンクホールサーバへのトラフィックをリダイレクトする場合は、[シンクホールへの接続のログ (Log Connections to Sinkhole)] を選択します。
- 非解決 IP アドレスにトラフィックをリダイレクトする場合は、[シンクホールへの接続をブロックしてログ (Block and Log Connections to Sinkhole)] を選択します。

**ステップ 7** 侵入の痕跡 (IoC) のタイプをシンクホールに割り当てるには、[タイプ (Type)] ドロップダウンからいずれかのタイプを選択します。

**ステップ 8** [保存 (Save)] をクリックします。

## ファイルリスト

AMP for Firepower を使用しており、AMP クラウドがファイルの性質を誤って特定した場合は、このファイルをファイルリストに追加して、今後さらに検出できます。このファイルは、SHA-256 ハッシュ値を使用して指定されます。各ファイルリストには、一意の SHA-256 値を最大 10000 個まで含めることができます。

ファイル リストには 2 種類の事前定義済みカテゴリがあります。

### クリーン リスト

このリストにファイルを追加すると、システムは AMP クラウドがクリーンな性質を割り当てた場合と同様にファイルを扱います。

### カスタム検出リスト

このリストにファイルを追加すると、システムは AMP クラウドがマルウェアの性質を割り当てた場合と同様にファイルを扱います。

マルチドメイン展開では、各ドメインにクリーンリストとカスタム検出リストが存在します。下位レベルのドメインでは、先祖のリストを表示できますが、変更できません。

これらのリストに含まれているファイルに手動でブロッキング動作を指定するため、システムはこれらのファイルの性質について AMP クラウドに照会しません。ファイルの SHA 値を計算するには、[マルウェア クラウドルックアップ (Malware Cloud Lookup)] アクションと [マルウェア ブロック (Block Malware)] アクションのどちらか、および一致するファイルタイプを使用して、ファイル ポリシー内のルールを設定する必要があります。



**注意** クリーンリストにマルウェアを含めないでください。クリーンリストによって、AMP クラウドおよびカスタム検出リストの両方がオーバーライドされます。

## ファイル リストのソース ファイル

SHA-256 値のリストと説明を含むコンマ区切り値 (CSV) ソース ファイルをアップロードすることによって、複数の SHA-256 値をファイルリストに追加できます。Firepower Management Center はその内容を検証し、有効な SHA-256 値をファイルリストに入れます。

ソースファイルは、ファイル名拡張子.csvの単純なテキストファイルである必要があります。見出しはポンド記号 (#) で始まる必要があります。これはコメントとして処理され、アップロードされません。各エントリには、1つの SHA-256 値の後に説明が含まれる必要があります、LF または CR+LF 改行文字で終わる必要があります。システムはエントリ内のこれ以外の情報をすべて無視します。

次の点に注意してください。

- ファイル リストからソース ファイルを削除すると、それに関連付けられているすべての SHA-256 ハッシュもファイルリストから削除されます。
- ソース ファイルのアップロードに成功した結果、10000 個を超える個別の SHA-256 値がファイルリストに含まれる場合は、複数のファイルをファイルリストにアップロードすることはできません。
- システムは、アップロード時に 256 文字を超える説明を最初の 256 文字で切り捨てます。説明にコンマを含める場合は、エスケープ文字 (\) を使用する必要があります。説明が含まれていない場合、代わりにソース ファイル名が使用されます。

- 重複しないすべての SHA-256 値がこのファイルリストに追加されます。すでにファイルリストに存在する SHA-256 値を含むソースファイルをアップロードした場合、新しくアップロードされた値によって既存の SHA-256 値が変更されることはありません。SHA-256 値に関連するキャプチャ済みファイル、ファイルイベント、またはマルウェア イベントを表示するとき、個々の SHA-256 値から脅威名または説明が得られます。
- システムはソース ファイル内の無効な SHA-256 値をアップロードしません。
- アップロードされた複数のソース ファイル内に同じ SHA-256 値に関するエントリが含まれる場合、システムは最も新しい値を使用します。
- 1 つのソース ファイル内に同じ SHA-256 値のエントリが複数含まれる場合、システムは最後のものを使用します。
- オブジェクト マネージャ内でソース ファイルを直接編集することはできません。変更を行うには、最初にソース ファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。
- ソース ファイルに関連付けられたエントリ数とは、個別の SHA-256 値の数です。ファイルリストからソース ファイルを削除すると、ファイルリストに含まれる SHA-256 エントリの合計数は、ソース ファイル内の有効なエントリ数だけ減少します。

## ファイルリスト別の SHA-256 値の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア	マルウェア	Firepower	任意 (Any)	Admin/Network Admin/Access Admin

ファイルの SHA-256 値を送信して、それをファイルリストに追加できます。重複する SHA-256 値は追加できません。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

### 始める前に

- イベント ビューからファイルまたはマルウェア イベントを右クリックし、コンテキストメニューで [フルテキストの表示 (Show Full Text)] を選択し、ファイルの SHA-256 値全体をコピーし、ファイルリストに貼り付けます。

## 手順

- ステップ1** [オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択します。
- ステップ2** オブジェクト タイプのリストから [ファイル リスト (File List) ] を選択します。
- ステップ3** ファイルの追加場所となるクリーン リストまたはカスタム検出リストの横の編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

- ステップ4** [追加元 (Add by) ] ドロップダウンリストから [SHA 値の入力 (Enter SHA Value) ] を選択します。
- ステップ5** [説明 (Description) ] フィールドにソース ファイルの説明を入力します。
- ステップ6** [SHA-256] フィールドにファイル全体の値を入力し、または貼り付けます。システムでは値の部分的な一致はサポートされません。
- ステップ7** [追加 (Add) ] をクリックします。
- ステップ8** [保存 (Save) ] をクリックします。

## 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。



- (注) 設定の変更が展開されたら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。

## ファイル リストへの個々のファイルのアップロード

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア	マルウェア	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

ファイル リストに追加するファイルのコピーがある場合、分析用にファイルを Firepower Management Center にアップロードできます。システムはファイルの SHA-256 値を計算し、ファイルをリストに追加します。SHA-256 を計算するとき、システムはファイル サイズを制限しません。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

### 手順

- ステップ1 [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ2 オブジェクトタイプのリストから [ファイルリスト (File List)] を選択します。
- ステップ3 ファイルの追加場所となるクリーンリストまたはカスタム検出リストの横の編集アイコン (✎) をクリックします。  
代わりに表示アイコン (🔍) が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。
- ステップ4 [追加 (Add by)] ドロップダウンリストから、[SHA の計算 (Calculate SHA)] を選択します。
- ステップ5 オプションで、[説明 (Description)] フィールドにファイルの説明を入力します。説明を入力しない場合、アップロード時にファイル名が説明として使用されます。
- ステップ6 [参照 (Browse)] をクリックし、アップロードするファイルを選択します。
- ステップ7 [SHA の計算と追加 (Calculate and Add SHA)] をクリックします。
- ステップ8 [保存 (Save)] をクリックします。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。



(注) 設定の変更を導入すると、その後システムはそのリストのファイルを AMP クラウドでクエリしなくなります。

## ファイルリストへのソースファイルのアップロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア	マルウェア	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

### 手順

- ステップ 1 [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ 2 [ファイルリスト (File List)] をクリックします。
- ステップ 3 ソースファイルからの値の追加先となるファイルリストの横にある編集アイコン (✎) をクリックします。  
  
代わりに表示アイコン (🔍) が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。
- ステップ 4 [追加方法 (Add by)] ドロップダウンリストで [SHA のリスト (List of SHAs)] を選択します。
- ステップ 5 オプションで、[説明 (Description)] フィールドにソースファイルの説明を入力します。説明を入力しない場合、システムはファイル名を使用します。
- ステップ 6 [参照 (Browse)] をクリックしてソースファイルを参照してから、[リストのアップロードと追加 (Upload and Add List)] をクリックします。
- ステップ 7 [保存 (Save)] をクリックします。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。



(注) ポリシーを展開したら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。

## ファイルリストの SHA-256 値の編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア	マルウェア	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

ファイルリストの個々の SHA-256 値を編集または削除することができます。オブジェクトマネージャ内でソースファイルを直接編集できないことに注意してください。変更を行うには、最初にソースファイルを直接変更し、システム上のコピーを削除した後、変更済みソースファイルをアップロードする必要があります。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

## 手順

**ステップ 1** [オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択します。

**ステップ 2** [ファイルリスト (File List) ] をクリックします。

**ステップ 3** ファイルの変更対象となるクリーン リストまたはカスタム検出リストの横の編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

**ステップ 4** 次の操作を実行できます。

- 変更する SHA-256 値の横にある編集アイコン (✎) をクリックし、必要に応じて [SHA-256] または [説明 (Description) ] の値を変更します。
- 削除する SHA-256 値の横にある削除アイコン (🗑) をクリックします。

**ステップ 5** [保存 (Save) ] をクリックし、リストのファイル エントリを更新します。

**ステップ 6** [保存 (Save) ] をクリックして、ファイル リストを保存します。

## 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。



(注) 設定の変更が展開されたら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。



## ファイルリストからのソースファイルのダウンロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア	マルウェア	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

### 手順

- ステップ1 [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ2 オブジェクトタイプのリストから [ファイルリスト (File List)] を選択します。
- ステップ3 ソースファイルのダウンロード対象となるクリーンリストまたはカスタム検出リストの横の編集アイコン (✎) をクリックします。  
  
代わりに表示アイコン (🔍) が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。
- ステップ4 ダウンロードするソースファイルの横にある表示アイコン (🔍) をクリックします。
- ステップ5 [SHA リストのダウンロード (Download SHA List)] をクリックし、プロンプトに従ってソースファイルを保存します。
- ステップ6 [閉じる (Close)] をクリックします。

## 暗号スイート リスト

暗号スイートリストは複数の暗号スイートからなるオブジェクトです。定義済み暗号スイートの値は、SSLまたはTLS暗号化セッションのネゴシエートに使われる暗号スイートを表しています。暗号スイートおよび暗号スイートリストをSSLルールで使用すると、クライアントとサーバが暗号スイートを使ってSSLセッションをネゴシエートしたかどうかに基づいて暗号化トラフィックを制御できます。SSLルールに暗号スイートリストを追加すると、リスト内のいずれかの暗号スイートでネゴシエートされたSSLセッションがルールに一致します。



- (注) Web インターフェイスでは暗号スイートリストと同じ場所で暗号スイートを使用できますが、暗号スイートを追加、変更、削除することはできません。

## 暗号スイート リストの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ 2** オブジェクトタイプのリストから [暗号スイート リスト (Cipher Suite List)] を選択します。

**ステップ 3** [暗号スイートの追加 (Add Cipher Suites)] をクリックします。

**ステップ 4** 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

**ステップ 5** [使用可能な暗号 (Available Ciphers)] リストから、1 つ以上の暗号スイートを選択します。

**ステップ 6** [追加 (Add)] をクリックします。

**ステップ 7** オプションで、[選択された暗号 (Selected Ciphers)] リストで、削除する暗号スイートの隣にある削除アイコン (🗑️) をクリックします。

**ステップ 8** [保存 (Save)] をクリックします。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## 識別名オブジェクト

それぞれの識別名オブジェクトは、公開鍵証明書のサブジェクトまたは発行元にリストされた識別名を表します。SSL ルールで識別名オブジェクトとグループを使用すると、サブジェクトまたは発行元として識別名を含むサーバ証明書を使ってクライアントとサーバが SSL セッションをネゴシエートしたかどうかに基づき、暗号化トラフィックを制御できます。

識別名オブジェクトには、共通名属性 (CN) を含めることができます。「CN=」なしで共通名を追加すると、システムはオブジェクトを保存する前に「CN=」を追加します。

さらに、次の表に示す属性を含む識別名を追加することもできます。属性はカンマで区切って使用します。

表 47: 識別名の属性

属性 (Attribute)	説明	使用可能な値
C	国コード (Country Code)	2つの英字
CN	Common Name	最大 64 文字の英数字、バックスラッシュ (/)、ハイフン (-)、引用符 (")、アスタリスク (*)、スペース文字
O	Organization	最大 64 文字の英数字、バックスラッシュ (/)、ハイフン (-)、引用符 (")、アスタリスク (*)、スペース文字
OU	組織	最大 64 文字の英数字、バックスラッシュ (/)、ハイフン (-)、引用符 (")、アスタリスク (*)、スペース文字

ワイルドカードとして1つ以上のアスタリスク (\*) を属性に定義できます。共通名属性では、ドメイン名ラベルごとに1つ以上のアスタリスクを定義できます。ワイルドカードはそのラベル内でのみ照合されますが、ワイルドカードを使用して複数のラベルを定義できます。例については、以下の表を参照してください。

表 48: 共通名属性のワイルドカードの例

属性 (Attribute)	一致	一致しない
CN="*ample.com"	example.com	mail.example.com example.text.com ampleexam.com
CN="exam*.com"	example.com	mail.example.com example.text.com ampleexam.com
CN="*xamp*.com"	example.com	mail.example.com example.text.com ampleexam.com

属性 (Attribute)	一致	一致しない
CN="*.example.com"	mail.example.com	example.com example.text.com ampleexam.com
CN="*.com"	example.com ampleexam.com	mail.example.com example.text.com
CN="*.*.com"	mail.example.com example.text.com	example.com ampleexam.com

## 識別名オブジェクトの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPsvを除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ 2** [識別名 (Distinguished Name)] ノードを展開し、[個別オブジェクト (Individual Objects)] を選択します。

**ステップ 3** [識別名の追加 (Add Distinguished Name)] をクリックします。

**ステップ 4** 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

**ステップ 5** [DN] フィールドに、識別名または共通名の値を入力します。次の選択肢があります。

- 識別名を追加する場合は、[識別名オブジェクト \(484 ページ\)](#) に示されている属性をカンマで区切って含めることができます。
- 共通名を追加する場合は、複数のラベルとワイルドカードを含めることができます。

**ステップ 6** [保存 (Save)] をクリックします。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## PKI オブジェクト

### SSL アプリケーションの PKI オブジェクト

PKI オブジェクトは、導入をサポートするために必要な公開鍵証明書、およびペアになった秘密鍵を表します。内部 CA オブジェクトおよび信頼できる CA オブジェクトは、認証局 (CA) 証明書で構成されます。また、内部 CA オブジェクトには、証明書とペアになった秘密鍵も含まれます。内部証明書オブジェクトおよび外部証明書オブジェクトは、サーバ証明書で構成されます。また、内部証明書オブジェクトには、証明書とペアになった秘密鍵も含まれます。

信頼できる認証局オブジェクトと内部証明書オブジェクトを使用して ISE への接続を設定する場合、ISE をアイデンティティ ソースとして使用できます。

内部証明書オブジェクトを使用してキャプティブポータルを設定する場合、システムはキャプティブポータルデバイスがユーザの Web ブラウザに接続する際に、デバイスのアイデンティティを検証できます。

信頼できる認証局オブジェクトを使用してレルムを設定する場合、LDAP または AD サーバへのセキュア接続を設定できます。

SSL ルールで PKI オブジェクトを使用する場合、以下のものを使用して暗号化されたトラフィックを照合することができます。

- 外部証明書オブジェクト内の証明書
- 信頼できる CA オブジェクトの CA によって署名された証明書、または信頼できる CA チェーン内で署名された証明書

SSL ルールで PKI オブジェクトを使用する場合、以下のものを復号できます。

- 発信トラフィック：内部 CA オブジェクトを使ってサーバ証明書を再署名することによって復号します
- 受信トラフィック：内部証明書オブジェクトにある既知の秘密鍵を使用して復号します

証明書とキーの情報を手動で入力し、その情報を含むファイルをアップロードします。場合によっては、新しい CA 証明書や秘密キーを生成することができます。

オブジェクト マネージャで PKI オブジェクトのリストを表示すると、システムは証明書のサブジェクト識別名をオブジェクト値として表示します。証明書の完全なサブジェクト識別名を表示するには、値の上にポインタを移動してください。証明書に関する他の詳細を表示するには、PKI オブジェクトを編集します。



- (注) Firepower Management Center および管理対象デバイスは、内部 CA オブジェクトと内部証明書オブジェクトに保存されるすべての秘密キーを、保存前にランダムに生成されたキーを使って暗号化します。パスワード保護されている秘密キーをアップロードすると、アプライアンスはユーザ提供のパスワードを使って秘密キーを復号し、ランダムに生成されたキーを使ってそれを再暗号化してから保存します。

## 内部認証局オブジェクト

設定されたそれぞれの内部認証局 (CA) オブジェクトは、組織で制御される CA の CA 公開鍵証明書を表します。このオブジェクトは、オブジェクト名、CA 証明書、およびペアになった秘密鍵からなります。SSL ルールで内部 CA オブジェクトとグループを使用すると、内部 CA によってサーバ証明書に再署名することにより、発信する暗号化トラフィックを復号できます。



- (注) [復号 - 再署名 (Decrypt - Resign) ] SSL ルールで内部 CA オブジェクトを参照する場合、ルールが暗号化セッションに一致すると、SSL ハンドシェイクのネゴシエート中は証明書を信頼できないという警告がユーザのブラウザに表示されることがあります。これを回避するには、信頼できるルート証明書のクライアントまたはドメインリストに内部 CA オブジェクト証明書を追加します。

次の方法で内部 CA オブジェクトを作成できます。

- RSA ベースまたは楕円曲線ベースの既存の CA 証明書と秘密キーをインポートする
- 新しい RSA ベースの自己署名 CA 証明書と秘密キーを生成する
- RSA ベースの未署名の CA 証明書と秘密キーを生成する内部 CA オブジェクトを使用する前に、証明書に署名するために証明書署名要求 (CSR) を別の CA に送信する必要があります。

署名付き証明書を含む内部 CA オブジェクトを作成した後で、CA 証明書と秘密鍵をダウンロードできるようになります。システムは、ダウンロードされた証明書と秘密キーをユーザ提供のパスワードで暗号化します。

システムで生成された場合でも、ユーザによって作成された場合でも、内部 CA オブジェクトの名前は変更できますが、他のオブジェクト プロパティは変更できません。

使用中の内部 CA オブジェクトは削除できません。さらに、SSL ポリシーで使用される内部 CA オブジェクトを編集すると、関連するアクセスコントロールポリシーが失効します。変更を反映させるには、アクセスコントロールポリシーを再度展開する必要があります。

## CA 証明書と秘密キーのインポート

X.509 v3 CA 証明書と秘密キーをインポートすることによって、内部 CA オブジェクトを設定できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則 (DER)
- プライバシー強化電子メール (PEM)

秘密キーファイルがパスワード保護されている場合は、復号パスワードを提供できます。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書またはキーの情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。



(注) ルールに [復号 - 再署名 (Decrypt - Resign)] アクションを設定すると、そのルールでは、設定されているルール条件に加えて、参照される内部 CA 証明書の暗号化アルゴリズムのタイプに基づいてトラフィックが照合されます。たとえば、楕円曲線ベースのアルゴリズムで暗号化された発信トラフィックを復号するには、楕円曲線ベースの CA 証明書をアップロードする必要があります。

## CA 証明書と秘密キーのインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

### 手順

- ステップ 1 [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ 2 [PKI] ノードを展開して、[内部 CA (Internal CAs)] を選択します。
- ステップ 3 [CA のインポート (Import CA)] をクリックします。
- ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

- ステップ 5** [証明書データ (Certificate Data) ]フィールドの上部にある[参照 (Browse) ]をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。
- ステップ 6** [キー (Key) ]フィールドの上部にある[参照 (Browse) ]をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。
- ステップ 7** アップロードファイルがパスワード保護されている場合は、[暗号化および次のパスワード: (Encrypted, and the password is:)] チェックボックスをオンにして、パスワードを入力します。
- ステップ 8** [保存 (Save) ]をクリックします。

#### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## CA 証明書および秘密キーの生成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPsv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

識別情報を提供することで、RSA ベースの自己署名 CA 証明書と秘密キーを生成するように内部 CA オブジェクトを設定できます。

生成される CA 証明書の有効期間は 10 年です。[有効期間の開始 (Valid From) ]の日付は、生成の一週間前です。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

#### 手順

- ステップ 1** [オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ]を選択します。
- ステップ 2** [PKI] ノードを展開し、[内部 CA (Internal CAs) ]を選択します。
- ステップ 3** [CA の生成 (Generate CA) ]をクリックします。
- ステップ 4** 名前を入力します。



マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

**ステップ 5** ID 属性を入力します。

**ステップ 6** [自己署名 CA の生成 (Generate self-signed CA)] をクリックします。

## 新しい署名付き証明書

署名付き証明書を CA から取得することによって、内部 CA オブジェクトを設定できます。これは、次の 2 段階からなります。

- 内部 CA オブジェクトを設定するための識別情報を指定します。これにより、未署名の証明書およびペアになった秘密鍵が生成され、指定した CA に対する証明書署名要求 (CSR) が作成されます。
- CA により署名付き証明書が発行されたら、それを内部 CA オブジェクトにアップロードして、未署名の証明書と置き換えます。

署名付き証明書が含まれている場合にのみ、SSL ルールで内部 CA オブジェクトを参照できません。

## 未署名の CA 証明書と CSR の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ 2** [PKI] ノードを展開し、[内部 CA (Internal CAs)] を選択します。

**ステップ 3** [CA の生成 (Generate CA)] をクリックします。

**ステップ 4** 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

**ステップ 5** ID 属性を入力します。

**ステップ 6** [CSR の作成 (Generate CSR)] をクリックします。

**ステップ 7** CA に送信するために CSR をコピーします。

ステップ 8 [OK] をクリックします。

#### 次のタスク

- CA によって発行される署名済み証明書をアップロードする必要があります。次のページを参照してください。 [CSR への応答として発行された署名付き証明書のアップロード \(492 ページ\)](#)

## CSR への応答として発行された署名付き証明書のアップロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

一度アップロードすると、署名付き証明書は SSL ルールで参照できます。

#### 手順

- ステップ 1 [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ 2 [PKI] ノードを展開し、[内部 CA (Internal CAs)] を選択します。
- ステップ 3 CSR を待機している未署名の証明書を含む CA オブジェクトの横の編集アイコン (✎) をクリックします。
- ステップ 4 [証明書のインストール (Install Certificate)] をクリックします。
- ステップ 5 [参照 (Browse)] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。
- ステップ 6 アップロードファイルがパスワード保護されている場合は、[暗号化済み、パスワード: (Encrypted, and the password is:)] チェックボックスをオンにして、パスワードを入力します。
- ステップ 7 [保存 (Save)] をクリックして、CA オブジェクトに署名付き証明書をアップロードします。

#### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## CA 証明書および秘密キーのダウンロード

証明書および鍵の情報を含むファイルを内部 CA オブジェクトからダウンロードすることにより、CA 証明書およびペアになった秘密鍵をバックアップまたは転送できます。



**注意** ダウンロードされた鍵情報は必ず安全な場所に保存してください。

システムは、内部 CA オブジェクトに保存されている秘密鍵をディスクに保存する前に、ランダムに生成された鍵を使って暗号化します。証明書および秘密鍵を内部 CA オブジェクトからダウンロードすると、システムはまず情報を復号してから、証明書および秘密鍵の情報を含むファイルを作成します。その後、ダウンロードファイルを暗号化するためにシステムで使われるパスワードを提供する必要があります。



**注意** システムバックアップの一部としてダウンロードされる秘密鍵は、復号されてから、非暗号化バックアップファイルに保存されます。

## CA 証明書と秘密キーのダウンロード

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPsv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

現在のドメインおよび先祖ドメインの両方の CA 証明書をダウンロードできます。

### 手順

- ステップ 1 [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ 2 [PKI] ノードを展開し、[内部 CA (Internal CAs)] を選択します。
- ステップ 3 証明書および秘密キーをダウンロードする対象となる内部 CA オブジェクトの横の編集アイコン (🔧) をクリックします。

マルチドメイン導入では、表示アイコン (🔍) をクリックして、先祖ドメインのオブジェクトの証明書および秘密キーをダウンロードします。

- ステップ 4 [ダウンロード (Download)] をクリックします。

**ステップ 5** [パスワード (Password) ]および[パスワードの確認 (Confirm Password) ]フィールドに、暗号化パスワードを入力します。

**ステップ 6** [OK] をクリックします。

## 信頼できる認証局オブジェクト

設定した信頼できる認証局 (CA) オブジェクトは、それぞれ信頼できる CA に属する CA 公開鍵証明書を表します。このオブジェクトは、オブジェクト名と CA 公開鍵証明書からなります。次のものに設定された外部 CA オブジェクトとグループを使用できます。

- 信頼できる CA、または信頼チェーン内のいずれかの CA によって署名された証明書で暗号化されたトラフィックを制御するための SSL ポリシー。
- LDAP または AD サーバへのセキュアな接続を確立するためのレルムの設定。
- ISE 接続。[pxGrid サーバ CA (pxGrid Server CA) ]フィールドと [MNT サーバ CA (MNT Server CA) ]フィールドで信頼できる認証局オブジェクトを選択します。

信頼できる CA オブジェクトを作成した後で、その名前を変更したり、証明書失効リスト (CRL) を追加したりすることはできますが、他のオブジェクトプロパティを変更することはできません。オブジェクトに追加できる CRL の数には制限がありません。オブジェクトにアップロード済みの CRL を変更するには、オブジェクトをいったん削除して再作成する必要があります。



(注) オブジェクトに CRL を追加しても、ISE の統合設定でオブジェクトを使用する際に影響はありません。

使用中の信頼できる CA オブジェクトを削除することはできません。また、使用中の信頼できる CA オブジェクトを編集すると、関連付けられているアクセス コントロール ポリシーが最新ではなくなります。変更を反映させるには、アクセス コントロール ポリシーを再度展開する必要があります。

## 信頼できる CA オブジェクト

外部 CA オブジェクトは、X.509 v3 CA 証明書をアップロードすることによって設定できます。次のサポートされている形式のいずれかでエンコードしたファイルをアップロードできます。

- 識別符号化規則 (DER)
- プライバシー強化電子メール (PEM)

ファイルがパスワードで保護されている場合は、復号パスワードを提供する必要があります。証明書が PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

ファイルに適切な証明書情報が含まれる場合にのみ、CA 証明書をアップロードできます。システムはオブジェクトを保存する前に証明書を検証します。

## 信頼できる CA オブジェクトの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ 2** [PKI] ノードを展開し、[信頼できる CA (Trusted CAs)] を選択します。

**ステップ 3** [信頼できる CA の追加 (Add Trusted CAs)] をクリックします。

**ステップ 4** 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

**ステップ 5** [参照 (Browse)] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

**ステップ 6** ファイルがパスワード保護されている場合は、[暗号化、パスワード: (Encrypted, and the password is:)] チェックボックスをオンにして、パスワードを入力します。

**ステップ 7** [保存 (Save)] をクリックします。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## 信頼できる CA オブジェクトの証明書失効リスト

信頼できる CA オブジェクトに CRL をアップロードできます。信頼できる CA オブジェクトを SSL ポリシーの中で参照すると、セッションの暗号化証明書を発行した CA がその後で証明書を取り消したかどうかに基づいて、暗号化されたトラフィックを制御できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則 (DER)
- プライバシー強化電子メール (PEM)

CRLを追加した後、失効した証明書のリストを表示することができます。オブジェクトにアップロード済みのCRLを変更するには、オブジェクトをいったん削除して再作成する必要があります。

適切なCRLを含んでいるファイルのみをアップロードできます。信頼できるCAオブジェクトに追加できるCRLの数には制限がありません。ただし、CRLをアップロードした場合、別のCRLを追加する前に、オブジェクトをその都度保存する必要があります。



(注) オブジェクトにCRLを追加しても、ISEの統合設定でオブジェクトを使用する際に影響はありません。

## 信頼できる CA オブジェクトへの証明書失効リストの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSvを除く)	任意 (Any)	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。



(注) オブジェクトにCRLを追加しても、ISEの統合設定でオブジェクトを使用する際に影響はありません。

### 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ 2** [PKI] ノードを展開し、[信頼できる CA (Trusted CAs)] を選択します。

**ステップ 3** 信頼できる CA オブジェクトの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 4** [CRL の追加 (Add CRL)] をクリックして、DER または PEM でエンコードされた CRL ファイルをアップロードします。

**ステップ 5** [OK] をクリックします。

### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## 外部証明書オブジェクト

設定済みのそれぞれの外部証明書オブジェクトは、組織に属さないサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名と証明書からなります。SSLルールで外部証明書オブジェクトとグループを使用すると、サーバ証明書で暗号化されたトラフィックを制御できます。たとえば、信頼できる自己署名サーバ証明書をアップロードできますが、信頼できるCA証明書を使って検証することはできません。

X.509 v3 サーバ証明書をアップロードすることによって、外部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則 (DER)
- プライバシー強化電子メール (PEM)

適切なサーバ証明書情報を含んでいるファイルだけをアップロードできます。システムはオブジェクトを保存する前にファイルを検証します。証明書が PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

### 外部証明書オブジェクトの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

#### 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ 2** [PKI] ノードを展開し、[外部証明書 (External Certs)] を選択します。

**ステップ 3** [外部証明書の追加 (Add External Cert)] をクリックします。

**ステップ 4** 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

**ステップ 5** [証明書データ (Certificate Data)] フィールドの上部にある [参照 (Browse)] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバ証明書ファイルをアップロードします。

ステップ6 [保存 (Save) ]をクリックします。

#### 次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します ([設定変更の導入 \(350 ページ\)](#) を参照)。

## 内部証明書オブジェクト

設定済みのそれぞれの内部証明書オブジェクトは、組織に属するサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名、公開鍵証明書、およびペアになった秘密鍵からなります。内部証明書オブジェクトとグループは、以下で使用することができます。

- SSL ルール。既知の秘密キーを使用する組織のサーバの1つに着信するトラフィックを復号します。
- ISE 接続。[MC サーバ証明書 (MC Server Certificate) ]フィールド用の内部証明書オブジェクトを選択します。
- キャプティブ ポータル設定。ユーザの Web ブラウザに接続する際にキャプティブ ポータルデバイスのアイデンティティを認証するように設定します。[サーバ証明書 (Server Certificate) ]フィールド用の内部証明書オブジェクトを選択します。

X.509v3RSA ベースまたは楕円曲線ベースのサーバ証明書およびペアの秘密キーをアップロードすることにより、内部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則 (DER)
- プライバシー強化電子メール (PEM)

ファイルがパスワード保護されている場合は、復号パスワードを提供する必要があります。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書またはキーの情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

内部証明書オブジェクトを作成した後、その名前を変更することはできますが、他のオブジェクトプロパティを変更することはできません。

使用中の内部証明書オブジェクトは削除できません。さらに、使用中の内部証明書オブジェクトを編集すると、関連するアクセスコントロールポリシーが失効します。変更を反映させるには、アクセスコントロールポリシーを再度展開する必要があります。



## 内部証明書オブジェクトの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ 2** [PKI] ノードを展開し、[内部証明書 (Internal Certs)] を選択します。

**ステップ 3** [内部証明書の追加 (Add Internal Cert)] をクリックします。

**ステップ 4** 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

**ステップ 5** [証明書データ (Certificate Data)] フィールドの上部にある [参照 (Browse)] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバ証明書ファイルをアップロードします。

**ステップ 6** [キー (Key)] フィールドの上部にある [参照 (Browse)] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

**ステップ 7** アップロードする秘密キー ファイルがパスワード保護されている場合は、[暗号化済み、パスワード: (Encrypted, and the password is:)] チェックボックスをオンにして、パスワードを入力します。

**ステップ 8** [保存 (Save)] をクリックします。

## SLA モニタ オブジェクト

各 SLA モニタでは、モニタリング対象のアドレスへの接続ポリシーを定義し、そのアドレスへのルートの可用性をトラッキングします。ルートの可用性は、ICMP エコー要求を送信し、応答を待機することによって、定期的にチェックされます。要求がタイムアウトすると、そのルートはルーティングテーブルから削除され、バックアップルートに置き換えられます。SLA モニタリング ジョブは、デバイス設定から SLA モニタを削除していない限り、展開後すぐに開始して実行し続けます (つまり、ジョブはエージングアウトしません)。SLA モニタ オブジェクトは、IPv4 スタティック ルート ポリシーの [ルート トラッキング (Route Tracking)] フィールドで使用されます。IPv6 ルートでは、ルート トラッキングによって SLA モニタを使用することはできません。

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

## 手順

- ステップ 1** [オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択し、コンテンツテーブルから [SLA モニタ (SLA Monitor) ] を選択します。
- ステップ 2** [SLA モニタの追加 (Add SLA Monitor) ] をクリックします。
- ステップ 3** [名前 (Name) ] フィールドにオブジェクトの名前を入力します。
- ステップ 4** (オプション) [説明 (Description) ] フィールドにオブジェクトの説明を入力します。
- ステップ 5** [頻度 (Frequency) ] フィールドに、ICMP エコー要求送信の頻度 (秒単位) を入力します。有効な値の範囲は、1 ~ 604800 秒 (7 日) です。デフォルトは 60 秒です。
- (注) 頻度はタイムアウト値未満にできません。これらの値を比較するには、頻度をミリ秒に換算する必要があります。
- ステップ 6** [SLA モニタ ID (SLA Monitor ID) ] フィールドに SLA 操作の ID 番号を入力します。値の範囲は 1 ~ 2147483647 です。1 つのデバイスには最大で 2000 個の SLA 操作を作成できます。各 ID 番号はポリシーとデバイス設定に対して一意である必要があります。
- ステップ 7** [しきい値 (Threshold) ] フィールドに、上昇しきい値が宣言されるまでに、ICMP エコー要求の後に経過する必要がある時間 (ミリ秒単位) を入力します。有効な値の範囲は、0 ~ 2147483647 ミリ秒です。デフォルトは 5000 ミリ秒です。しきい値は、定義された値を超過したイベントを示すためだけに使用されます。これらのイベントは、タイムアウト値が適切であるかどうかを評価するために使用できます。このイベントは、モニタリング対象のアドレスへの到達可能性を直接的に示すものではありません。
- (注) しきい値はタイムアウト値を超過しないようにします。
- ステップ 8** [タイムアウト (Timeout) ] フィールドに、SLA 操作が ICMP エコー要求への応答を待機する時間 (ミリ秒単位) を入力します。値の範囲は 0 ~ 604800000 ミリ秒 (7 日) です。デフォルトは 5000 ミリ秒です。モニタリング対象のアドレスからの応答がこのフィールドに定義された時間内に受信されない場合、スタティック ルートがルーティング テーブルから削除され、バックアップ ルートに置き換えられます。
- (注) タイムアウト値は頻度値を超過できません。2 つの数値を比較するには、頻度値をミリ秒に換算してください。
- ステップ 9** [データ サイズ (Data Size) ] フィールドに、ICMP 要求パケット ペイロードのサイズ (バイト単位) を入力します。値の範囲は 0 ~ 16384 バイトです。デフォルトは 28 バイトです。この場合、全体の ICMP パケットは 64 バイトとなります。この値には、プロトコルまたは Path Maximum Transmission Unit (PMTU) で許可される最大値を超える値を設定しないでください。場合によっては、到達可能性を確保するために、デフォルトのデータ サイズを大きくして、

ソースとターゲットの間での PMTU の違いを検出できるようにすることが必要となります。PMTU が小さいと、セッションのパフォーマンスに影響を及ぼすことがあります。セッションのパフォーマンスへの影響が検出されると、セカンダリパスが使用されます。

- ステップ 10** [ToS] フィールドに、ICMP 要求パケットの IP ヘッダーで定義されたタイプオブサービス (ToS) の値を入力します。値の範囲は 0 ~ 255 です。デフォルトは 0 です。このフィールドには、遅延、優先順位、信頼性などの情報が含まれます。この情報は、ポリシールーティングのためにネットワーク上の他のデバイスが使用する場合もあれば、専用アクセスレートなどの機能によって使用される場合もあります。
- ステップ 11** [パケット数 (Number of Packets)] フィールドに、送信されるパケットの数を入力します。値の範囲は 1 ~ 100 です。デフォルトは 1 パケットです。
- (注) パケット損失によって、Firepower Threat Defense デバイスがモニタリング対象のアドレスに到達できないと誤って認識することが懸念される場合は、デフォルトのパケット数を大きくしてください。
- ステップ 12** [モニタリング対象アドレス (Monitored Address)] フィールドに、SLA 操作によって可用性がモニタされている IP アドレスを入力します。
- ステップ 13** [ゾーン/インターフェイス (Zones/Interfaces)] リストで、デバイスが管理ステーションと通信するインターフェイスを含むゾーンを追加します。ゾーン内にはないインターフェイスの場合は、[選択したゾーン/インターフェイス (Selected Zone/Interface)] リストの下のフィールドにインターフェイス名を入力し、[追加 (Add)] をクリックします。デバイスに選択したインターフェイスまたはゾーンが含まれている場合のみ、デバイスでホストが設定されます。
- ステップ 14** [保存 (Save)] をクリックします。

## プレフィックスリスト

ルートマップ、ポリシーマップ、OSPF フィルタリング、BGP ネイバー フィルタリングを設定する際に使用する、IPv4 および IPv6 用のプレフィックスリストオブジェクトを作成できます。

### IPv6 プレフィックスリストの設定

IPv6 プレフィックスリストの設定ページを使用して、プレフィックスリストオブジェクトを作成、コピー、編集します。ルートマップ、ポリシーマップ、OSPF フィルタリングまたは BGP ネイバー フィルタリングを設定するときに使用する、プレフィックスリストオブジェクトを作成できます。

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

## 手順

- 
- ステップ 1 [オブジェクト (Objects) ]>[オブジェクト管理 (Object Management) ]を選択し、目次で[プレフィックス リスト (Prefix Lists) ]>[IPv6 プレフィックス リスト (IPv6 Prefix List) ]を選択します。
- ステップ 2 [プレフィックス リストの追加 (Add Prefix List) ]をクリックします。
- ステップ 3 [新しいプレフィックス リスト オブジェクト (New Prefix List Object) ]ウィンドウの[名前 (Name) ]フィールドで、プレフィックス リスト オブジェクトの名前を入力します。
- ステップ 4 [新しいプレフィックス リスト オブジェクト (New Prefix List Object) ]ウィンドウで、[追加 (Add) ]をクリックします。
- ステップ 5 [アクション (Action) ]ドロップダウンリストから適切なアクション、[許可 (Allow) ]または[ブロック (Block) ]を選択して、再配布アクセスを指定します。
- ステップ 6 このオブジェクトですでに設定されているプレフィックス リスト エントリのリストにおける、新しいプレフィックス リスト エントリの位置を示す固有の数字を、[シーケンス番号 (Sequence No.) ]フィールドに入力します。空白にしておく、現在使用されている最大シーケンス番号より 5 大きいシーケンス番号がデフォルトになります。
- ステップ 7 [IP アドレス (IP address) ]フィールドの IP アドレス/マスク長形式で、IPv6 アドレスを指定します。マスク長は 1 ~ 128 の有効な値でなければなりません。
- ステップ 8 [最小プレフィックス長 (Minimum Prefix Length) ]フィールドで最小プレフィックス長を入力します。値は、最大プレフィックス長の値が指定されている場合に、マスク長以上、最大プレフィックス長以下でなければなりません。
- ステップ 9 [最大プレフィックス長 (Maximum Prefix Length) ]フィールドで最大プレフィックス長を入力します。値は、最小プレフィックス長の値が指定されている場合に、最小プレフィックス長以上、最小プレフィックス長の値が指定されていない場合に、マスク長以上でなければなりません。
- ステップ 10 [追加 (Add) ]をクリックします。
- ステップ 11 このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可 (Allow Overrides) ]チェックボックスをオンにします (オブジェクトのオーバーライドの許可 (431 ページ) を参照)。
- ステップ 12 [保存 (Save) ]をクリックします。
- 

## IPv4 プレフィックス リストの設定

IPv4 プレフィックス リストの設定ページを使用して、プレフィックス リスト オブジェクトを作成、コピー、編集します。ルート マップ、ポリシー マップ、OSPF フィルタリングまたは BGP ネイバー フィルタリングを設定するときに使用する、プレフィックス リスト オブジェクトを作成できます。

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

## 手順

- 
- ステップ 1** [オブジェクト (Objects) ]>[オブジェクト管理 (Object Management) ]を選択し、目次で[プレフィックスリスト (Prefix Lists) ]>[IPv4 プレフィックスリスト (IPv4 Prefix List) ]を選択します。 >>
- ステップ 2** [プレフィックスリストの追加 (Add Prefix List) ]をクリックします。
- ステップ 3** [新しいプレフィックスリストオブジェクト (New Prefix List Object) ]ウィンドウの[名前 (Name) ]フィールドで、プレフィックスリストオブジェクトの名前を入力します。
- ステップ 4** [追加 (Add) ]をクリックします。
- ステップ 5** [アクション (Action) ]ドロップダウンリストから適切なアクション、[許可 (Allow) ]または[ブロック (Block) ]を選択して、再配布アクセスを指定します。
- ステップ 6** このオブジェクトですでに設定されているプレフィックスリストエントリのリストにおける、新しいプレフィックスリストエントリの位置を示す固有の数字を、[シーケンス番号 (Sequence No.) ]フィールドに入力します。空白にしておく、現在使用されている最大シーケンス番号より 5 大きいシーケンス番号がデフォルトになります。
- ステップ 7** [IP アドレス (IP address) ]フィールドの IP アドレス/マスク長形式で、IPv4 アドレスを指定します。マスク長は 1 ~ 32 の有効な値でなければなりません。
- ステップ 8** [最小プレフィックス長 (Minimum Prefix Length) ]フィールドで最小プレフィックス長を入力します。値は、最大プレフィックス長の値が指定されている場合に、マスク長以上、最大プレフィックス長以下でなければなりません。
- ステップ 9** [最大プレフィックス長 (Maximum Prefix Length) ]フィールドで最大プレフィックス長を入力します。値は、最小プレフィックス長の値が指定されている場合に、最小プレフィックス長以上、最小プレフィックス長の値が指定されていない場合に、マスク長以上でなければなりません。
- ステップ 10** [追加 (Add) ]をクリックします。
- ステップ 11** このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可 (Allow Overrides) ]チェックボックスをオンにします ([オブジェクトのオーバーライドの許可 \(431 ページ\)](#) を参照)。
- ステップ 12** [保存 (Save) ]をクリックします。
-

## ルートマップ

ルートマップは、ルートルーティングプロセスに再配布するときに使用できます。また、デフォルトルートルーティングプロセスに生成するときにも使用します。ルートマップは、指定されたルーティングプロトコルのどのルートを対象ルーティングプロセスに再配布できるのかを定義します。ルートマップを設定して、ルートマップオブジェクトの新しいルートマップエントリを作成したり、既存のルートマップエントリを編集したりします。

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

### 始める前に

ルートマップは、これらのオブジェクトの1つまたは複数を使用することができます。これらのオブジェクトをすべて追加する必要はありません。これらのオブジェクトを必要に応じて作成および使用して、ルートマップを設定します。

- ACL の追加
- プレフィックス リストの追加
- AS パスの追加
- コミュニティ リストの追加
- ポリシー リストの追加

### 手順

- ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、コンテンツテーブルから [ルートマップ (Route Map)] を選択します。
- ステップ 2** [ルートマップの追加 (Add Route Map)] をクリックします。
- ステップ 3** [新しいルートマップオブジェクト (New Route Map Object)] ウィンドウで [追加 (Add)] をクリックします。
- ステップ 4** [シーケンス番号 (Sequence No.)] フィールドで、このルートマップオブジェクトにすでに設定されているルートマップエントリのリストでの新しいルートマップエントリの位置を示す、0 ~ 65535 の番号を入力します。

(注) 将来的に句を挿入する必要性が生じたときの番号の間隔を確保するために、少なくとも 10 単位で句に番号を指定することをお勧めします。

**ステップ 5** [再配布 (Redistribution)] ドロップダウンリストから、再配布アクセスを示す適切なアクション ([許可 (Allow)] または [ブロック (Block)]) を選択します。

**ステップ 6** [句の照合 (Match Clauses)] タブをクリックして、コンテンツテーブルで選択する次の条件に基づいて照合します (ルート/トラフィック)。

- [セキュリティゾーン (Security Zones)] : (I/O) インターフェイスに基づいてトラフィックを照合します。ゾーンを選択して追加するか、インターフェイス名を入力して追加します。
- [IPv4] : 次の条件に基づいて IPv4 (ルート/トラフィック) を照合します。条件を定義するタブを選択します。
  1. ルートアドレスに基づいてルートを照合するには、[アドレス (Address)] タブをクリックします。IPv4 アドレスに対して、照合にアクセスリストまたはプレフィックスリストを使用するかどうかをドロップダウンリストから選択し、照合に使用する ACL オブジェクトまたはプレフィックスリストを入力または選択します。
  2. ルートのネクストホップアドレスに基づいてルートを照合するには、[ネクストホップ (Next Hop)] タブをクリックします。IPv4 アドレスに対して、照合にアクセスリストまたはプレフィックスリストを使用するかどうかをドロップダウンリストから選択し、照合に使用する ACL オブジェクトまたはプレフィックスリストを入力または選択します。
  3. ルートのアドバタイズ送信元アドレスに基づいてルートを照合するには、[ルート送信元 (Route Source)] タブをクリックします。IPv4 アドレスに対して、照合にアクセスリストまたはプレフィックスリストを使用するかどうかをドロップダウンリストから選択し、照合に使用する ACL オブジェクトまたはプレフィックスリストを入力または選択します。
- [IPv6] : ルート : ルートのルートアドレス、ネクストホップアドレス、またはアドバタイズ送信元アドレスに基づいて IPv6 (ルート/トラフィック) を照合します。
- [BGP] : 次の条件に基づいて BGP (ルート/トラフィック) を照合します。条件を定義するタブを選択します。
  1. BGP 自律システムパスアクセスリストと指定されたパスアクセスリストの照合を有効にするには、[AS パス (AS Path)] タブをクリックします。複数のパスアクセスリストを指定した場合、ルートはいずれかのパスアクセスリストと一致します。
  2. BGP コミュニティと指定されたコミュニティの照合を有効にするには、[コミュニティリスト (Community List)] タブをクリックします。複数のコミュニティを指定した場合、ルートはいずれかのコミュニティと一致します。少なくとも 1 つの Match コミュニティと一致しないルートは、アウトバウンドルートマップにアドバタイズされません。
  3. BGP ポリシーを評価および処理するためのルートマップを設定するには、[ポリシーリスト (Policy List)] タブをクリックします。1 つのルートマップエントリ内で複数のポリシーリストが照合を行う場合、ポリシーリストすべては受信属性だけで照合を行います。

- [その他 (Others) ] : 次の条件に基づいてルートまたはトラフィックを照合します。
  1. ルートのメトリックの照合を有効にするには、[メトリック ルート値 (Metric Route Value) ] フィールドに、照合に使用するメトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ~ 4294967295 の範囲で指定します。
  2. [タグ値 (Tag Values) ] フィールドに、照合に使用するタグ値を入力します。複数の値をカンマで区切って入力することもできます。指定したセキュリティ グループ タグを持つ任意のルートを照合できます。タグ値は、0 ~ 4294967295 の範囲で指定します。
  3. ルート タイプの照合を有効にするには、適切な **ルート タイプ** オプションをオンにします。有効なルートタイプは、External1、External2、Internal、Local、NSSA-External1、NSSA-External2 です。複数のルート タイプをリストから選択することができます。

**ステップ 7** [句の設定 (Set Clauses) ] タブをクリックして、コンテンツ テーブルで選択する次の条件に基づいてルート/トラフィックを設定します。

- [メトリック値 (Metric Values) ] : [帯域幅 (Bandwidth) ]、すべての値、または値なしを設定します。
  1. [帯域幅 (Bandwidth) ] フィールドに、メトリック値または帯域幅 (キロビット/秒) を入力します。有効な値は、0 ~ 4294967295 の範囲の整数値です。
  2. [メトリック タイプ (Metric Type) ] ドロップダウン リストから、宛先ルーティング プロトコルのメトリックのタイプを選択して指定します。有効な値は、internal、type-1、または type-2 です。
  3. [遅延 (Delay) ] フィールドに、EIGRP ルートの遅延を 10 マイクロ秒単位で入力します。有効な値の範囲は、1 ~ 4294967295 です。
  4. [信頼性 (Reliability) ] フィールドに、EIGRP のパケット伝送の成功率を入力します。有効な値の範囲は 0 ~ 255 です。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを意味します。
  5. [有効 (Effective) ] フィールドに、EIGRP の有効な帯域幅を入力します。有効な値の範囲は 1 ~ 255 です。値 255 は、100% のロードを意味します。
  6. [MTU] フィールドに、EIGRP のルートの最小 MTU サイズをバイト単位で入力します。有効な値の範囲は 1 ~ 4294967295 です。
- [BGP 句 (BGP Clauses) ] : 次の条件に基づいて BGP ルートを設定します。条件を定義するタブを選択します。
  1. BGP ルートの自律システム パスを変更するには、[AS パス (AS Path) ] タブをクリックします。
    1. 任意の自律システム パス文字列を BGP ルートの前に付加するには、[AS パスを前に付加 (Prepend AS Path) ] タブをクリックします。通常、ローカルな AS 番号が



複数回追加され、自律システムパス長が増します。複数の AS パス番号を指定した場合、ルートはいずれかの AS 番号を付加できます。

2. 最後の AS 番号を AS パスの前に付加するには、[最後の AS を AS パスの前に付加 (Prepend Last AS to AS Path)] フィールドに AS パス番号を入力します。AS 番号の値を 1 ~ 10 の範囲で入力します。
  3. ルートのタグを自律システムパスに変換するには、[ルートタグを AS パスに変換する (Convert route tag into AS path)] チェックボックスをオンにします。
2. コミュニティ属性を設定するには、[コミュニティリスト (Community List)] タブをクリックします。
    1. ルートマップをパスするプレフィックスからコミュニティ属性を除去するには、[なし (None)] ラジオ ボタンをクリックします。
    2. コミュニティ番号を入力するには、[コミュニティの指定 (Specify Community)] ラジオ ボタンをクリックします (必要な場合)。有効な値は 1 ~ 4294967295 です。
    3. 既存のコミュニティにコミュニティを追加するには、[既存のコミュニティに追加する (Add to existing communities)] チェックボックスをオンにします。
    4. 既知のコミュニティのいずれかを使用するには、[インターネット (Internet)]、[アドバタイズなし (No-Advertise)]、または [エクスポートなし (No-Export)] チェックボックスをオンにします。
  3. 追加属性を設定するには、[その他 (Others)] タブをクリックします。
    1. タグ値を自動的に計算するには、[自動タグを設定する (Set Automatic Tag)] チェックボックスをオンにします。
    2. [ローカル優先度の設定 (Set Local Preference)] フィールドに自律システムパスの優先度値を入力します。0 から 4294967295 までの値を入力してください。
    3. [重み付けの設定 (Set Weight)] フィールドにルーティング テーブルの BGP ウェイトを入力します。0 から 65535 までの値を入力してください。
    4. BGP の発信元コードを選択して指定します。有効な値は [ローカル IGP (Local IGP)] および [未完了 (Incomplete)] です。
    5. [IPv4 設定 (IPv4 Settings)] セクションで、パケットが出力されるネクストホップのネクストホップ IPv4 アドレスを指定します。隣接ルータである必要はありません。複数の IPv4 アドレスを指定した場合、いずれかの IP アドレスでパケットを出力できます。

[プレフィックスリスト (Prefix List)] ドロップダウンリストから IPv4 プレフィックスリストを選択して指定します。
    6. [IPv6 設定 (IPv6 Settings)] セクションで、パケットが出力されるネクストホップのネクストホップ IPv6 アドレスを指定します。隣接ルータである必要はありません。

ん。複数の IPv6 アドレスを指定した場合、いずれかの IP アドレスでパケットを出力できます。

[プレフィックスリスト (Prefix List)] ドロップダウンリストから IPv6 プレフィックスを選択して指定します。

**ステップ 8** [追加 (Add)] をクリックします。

**ステップ 9** このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可 (Allow Overrides)] チェックボックスをオンにします ([オブジェクトのオーバーライドの許可 \(431 ページ\)](#) を参照)。

**ステップ 10** [保存 (Save)] をクリックします。

## アクセスリスト

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

アクセスリスト オブジェクトは、アクセス コントロール リスト (ACL) と呼ばれ、トラフィックに適用されるサービスを選択します。アクセスリスト オブジェクトを使って、ルートマップなどの機能を設定します。ACL で許可されたトラフィックはサービスを利用できますが、「ブロックされた」トラフィックはサービスから除外されます。サービスから除外されたトラフィックが必ずしも完全にドロップされるわけではありません。

次のタイプの ACL を設定できます。

- **拡張**：送信元と宛先アドレスおよびポートに基づいてトラフィックを識別します。IPv4 および IPv6 アドレスをサポートしており、任意のルールで混在させることができます。
- **標準**：宛先アドレスのみに基づいてトラフィックを識別します。IPv4 のみサポートしています。

ACL は 1 つまたは複数のアクセス コントロール エントリ (ACE) またはルールで構成されます。ACE の順番は重要です。パケットを「許可」ACE と照合して ACL を評価する際、ACL に登録されている ACE の順番どおりに照合します。一致が見つかると、それ以降の ACE とは照合しません。たとえば、10.100.10.1 を「許可」して、10.100.10.0/24 の残りはすべて「ブロック」する場合、許可エントリがブロックエントリより前に登録されている必要があります。通常、具体性の高いルールを ACL の上部に置きます。

「許可」エントリに一致しないパケットはブロックされたと見なします。

次に、ACL オブジェクトの設定方法について説明します。

## 拡張 ACL オブジェクトの設定

送信元および宛先アドレス、プロトコル、およびポートに基づいて、あるいはトラフィックが IPv6 の場合にトラフィックを照合するには、拡張 ACL オブジェクトを使用します。

### 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、コンテンツテーブルから [アクセスコントロールリスト (Access Control Lists)] > [拡張 (Extended)] を選択します。

**ステップ 2** 次のいずれかを実行します。

- [拡張 ACL の追加 (Add Extended ACL)] をクリックして、新しいオブジェクトを作成します。
- 編集アイコン (✎) をクリックして、既存のオブジェクトを編集します。

**ステップ 3** [拡張 ACL オブジェクト (Extended ACL Object)] ダイアログボックスで、オブジェクトの名前を入力し (スペースは使用不可)、アクセスコントロールエントリを設定します。

a) 次のいずれかを実行します。

- [追加 (Add)] をクリックして、新しいエントリを作成します。
- 編集アイコン (✎) をクリックして、既存のエントリを編集します。

右クリックメニューからも、エントリの切り取り、コピー、貼り付け、または削除を行うことができます。

b) トラフィック基準を許可 (一致) するか、またはブロック (一致しない) するかの **アクション** を選択します。

(注) [ログ (Logging)]、[ログレベル (Log Level)]、および[ログインターバル (Log Interval)] オプションはアクセスルールに対してのみ使用されます (インターフェイスに接続されているか、グローバルで適用される ACL)。ACL オブジェクトがアクセスルールで使用されていないため、これらの値にはデフォルトを使用します。

c) 次のテクニックのいずれかを使用して、[ネットワーク (Network)] タブで送信元および宛先アドレスを設定します。

- [利用可能 (Available)] リストから目的のネットワーク オブジェクトまたはグループを選択し、[送信元に追加 (Add to Source)] または [宛先に追加 (Add to Destination)] をクリックします。リストの上の [+] ボタンをクリックすると、新しいオブジェクトを作成できます。IPv4 アドレスと IPv6 アドレスを組み合わせることができます。
- 送信元または宛先リストの下の編集ボックスにアドレスを入力し、[追加 (Add)] をクリックします。1つのホストアドレス (10.100.10.5、2001:DB8::0DB8:800:200C:417A

など) またはサブネット (10.100.10.0/24 または 10.100.10.0 255.255.255.0 の形式。IPv6 の場合は 2001:DB8:0:CD30::/60) を指定できます。

d) [ポート (Port)] タブをクリックし、次のテクニックのいずれかを使用してサービスを設定します。

- [利用可能 (Available)] リストから目的のポート オブジェクトまたはグループを選択し、[送信元に追加 (Add to Source)] または [宛先に追加 (Add to Destination)] をクリックします。リストの上の [+ ] ボタンをクリックすると、新しいオブジェクトを作成できます。オブジェクトによって TCP/UDP ポート、ICMP/ICMPv6 メッセージタイプ、その他のプロトコルを指定できます (「任意」を含む)。ただし、通常は空にしておく送信元ポートは TCP/UDP のみを受け入れます。
- 送信元または宛先リストの下の編集ボックスでポートまたはプロトコルを入力または選択し、[追加 (Add)] をクリックします。

(注) すべての IP トラフィックに適用するエントリを取得するには、「すべて」のプロトコルを指定する宛先ポート オブジェクトを選択します。

- e) [追加 (Add)] をクリックして、エントリをオブジェクトに追加します。
- f) 必要に応じて、エントリをクリックおよびドラッグして、ルール順序で目的の場所まで上下に移動します。

このプロセスを繰り返して、オブジェクトに追加エントリを作成または編集します。

**ステップ 4** このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可 (Allow Overrides)] チェックボックスをオンにします ([オブジェクトのオーバーライドの許可 \(431 ページ\)](#) を参照)。

**ステップ 5** [保存 (Save)] をクリックします。

## 標準 ACL オブジェクトの設定

宛先 IPv4 アドレスのみに基づいてトラフィックを照合する場合は、標準 ACL オブジェクトを使用します。それ以外の場合は、拡張 ACL を使用します。

### 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、コンテンツテーブルから [アクセスコントロールリスト (Access Control Lists)] > [標準 (Standard)] を選択します。

**ステップ 2** 次のいずれかを実行します。

- [標準 ACL の追加 (Add Standard ACL)] をクリックして、新しいオブジェクトを作成します。

- 編集アイコン (✎) をクリックして、既存のオブジェクトを編集します。

**ステップ 3** [標準 ACL オブジェクト (Standard ACL Object)] ダイアログボックスで、オブジェクトの名前を入力し (スペースは使用できません)、アクセス コントロール エントリを設定します。

a) 次のいずれかを実行します。

- [追加 (Add)] をクリックして、新しいエントリを作成します。
- 編集アイコン (✎) をクリックして、既存のエントリを編集します。

右クリックメニューからも、エントリの切り取り、コピー、貼り付け、または削除を行うことができます。

b) アクセス コントロール エントリごとに、次のプロパティを設定します。

- [アクション (Action)]: トラフィック基準を許可 (一致) またはブロック (不一致) するかどうか。
- [ネットワーク (Network)]: IPv4 ネットワーク オブジェクトまたはトラフィックの宛先を特定するグループを追加します。

c) [追加 (Add)] をクリックして、エントリをオブジェクトに追加します。

d) 必要に応じて、エントリをクリックおよびドラッグして、ルール順序で目的の場所まで上下に移動します。

このプロセスを繰り返して、オブジェクトに追加エントリを作成または編集します。

**ステップ 4** このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可 (Allow Overrides)] チェックボックスをオンにします ([オブジェクトのオーバーライドの許可 \(431 ページ\)](#) を参照)。

**ステップ 5** [保存 (Save)] をクリックします。

## AS パスのオブジェクト

AS パスは BGP のセットアップの必須属性です。これは、ネットワークのアクセスを可能にする AS 番号のシーケンスです。AS パスは、移動パケットの最短ルートになる送信元と宛先のルータ間の中間 AS 番号のシーケンスです。異なる AS プレフィックスにリーチする方法に関するメッセージを交換、更新するのに、ネイバー自律システム (ASes) で BGP が使用されます。各ルータで宛先までの最適ルートに関する新たなローカル判断が行われた後、用意されている距離メトリックおよびパス属性とともに、ルートまたはパスの情報がそれぞれのピアに送信されます。この情報がネットワークを移動すると、パスに沿った各ルータは、固有の AS 番号を BGP メッセージの ASes リストの前に付加します。このリストは、ルートの AS パスです。AS パスは AS プレフィックスとともに、ネットワークを介した一方向の中継ルートの特定のハンドルになります。AS パスページの設定を使用して、自律システム (AS) のパスのポリシー オブジェクトを作成、コピー、編集します。ルートマップ、ポリシー マップ、または

BGP ネイバーフィルタリングを設定するときに使用する、ASパスオブジェクトを作成できます。ASパスのフィルタにより、正規表現でルーティングアップデートメッセージをフィルタ処理できます。

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

## 手順

- 
- ステップ 1** [オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択して、目次で [AS パス (AS Path) ] を選択します。 >
- ステップ 2** [AS パスの追加 (Add AS Path) ] をクリックします。
- ステップ 3** [名前 (Name) ] フィールドに AS パス オブジェクトの名前を入力します。有効な値は、1 ~ 500 です。
- ステップ 4** [新しい AS パス オブジェクト (New AS Path Object) ] ウィンドウで、[追加 (Add) ] をクリックします。
- [アクション (Action) ] ドロップダウンリストから [許可 (Allow) ] または [ブロック (Block) ] オプションを選択して、再配布アクセスを指定します。
  - [正規表現 (Regular Expression) ] フィールドで AS パスのフィルタ処理を定義する正規表現を指定します。
  - [追加 (Add) ] をクリックします。
- ステップ 5** このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可 (Allow Overrides) ] チェックボックスをオンにします ([オブジェクトのオーバーライドの許可 \(431 ページ\)](#) を参照)。
- ステップ 6** [保存 (Save) ] をクリックします。
- 

## コミュニティリスト

コミュニティは、遷移的 BGP 属性のオプションです。コミュニティは、共通するいくつかの属性を共有する宛先のグループです。これはルート タギングに使用されます。BGP のコミュニティ属性は、特定のプレフィックスに割り当てられ、他のネイバーにアドバタイズされる数値です。コミュニティは、一般的な属性を共有する一連のプレフィックスのマーキングに使用できます。アップストリームプロバイダーは、これらのマーカーを使用して、特定のローカル設定のフィルタリングまたは割り当て、あるいは他の属性の変更などの一般的なルーティングポリシーを適用します。コミュニティリストの設定ページを使用して、コミュニティリストポリシー オブジェクトを作成、コピー、編集します。ルート マップまたはポリシー マップを

設定するときに使用する、コミュニティリストポリシーオブジェクトを作成できます。コミュニティリストを使用すると、ルートマップの match 句で使用されるコミュニティグループを作成できます。コミュニティリストは、一致ステートメントの番号付きリストです。接続先は、一致が見つかるまでルールに反する一致をします。

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

## 手順

**ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択して、目次で [コミュニティリスト (Community List)] を選択します。 >

**ステップ 2** [コミュニティリストの追加 (Add Community List)] をクリックします。

**ステップ 3** [名前 (Name)] フィールドに、コミュニティリスト オブジェクトの名前を指定します。

**ステップ 4** [新しいコミュニティリスト オブジェクト (New Community List Object)] ウィンドウで、[追加 (Add)] をクリックします。

**ステップ 5** [標準 (Standard)] オプションボタンを選択して、コミュニティルールの種類を表示します。

標準コミュニティリストは、ウェルノウン コミュニティやコミュニティ番号の指定に使用されます。

(注) 標準を使用したエントリ、コミュニティルールの拡張種類を使用したエントリを、同じコミュニティリスト オブジェクトに含めることはできません。

- [アクション (Action)] ドロップダウンリストから [許可 (Allow)] または [ブロック (Block)] オプションを選択して、再配布アクセスを指定します。
- [コミュニティ (Communities)] フィールドで、コミュニティ番号を指定します。有効な値は 1 ~ 4294967295 または 0:1 ~ 65534:65535 です。
- 適切な [ルートタイプ (Route Type)] を選択します。
  - [インターネット (Internet)] : インターネットのウェルノウン コミュニティを指定するために選択します。このコミュニティのルートは、すべてのピア (内部および外部) にアドバタイズされます。
  - [非アドバタイズ (No Advertise)] : 非アドバタイズのウェルノウン コミュニティを指定するために選択します。このコミュニティのあるルートはピア (内部または外部) にはアドバタイズされません。
  - [非エクスポート (No Export)] : 非エクスポートのウェルノウン コミュニティを指定するために選択します。このコミュニティのあるルートは、同じ自律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。

**ステップ 6** [拡張 (Expanded)] オプションボタンを選択して、コミュニティルールの種類を表示します。

拡張コミュニティ リストは正規表現によるフィルタ コミュニティに使用されます。正規表現は、コミュニティ属性の照合パターンの指定に使用されます。

- a) [アクション (Action) ] ドロップダウンリストから [許可 (Allow) ] または [ブロック (Block) ] オプションを選択して、再配布アクセスを指定します。
- b) [表現 (Expressions) ] フィールドで、正規表現を指定します。

**ステップ7** [追加 (Add) ] をクリックします。

**ステップ8** このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可 (Allow Overrides) ] チェックボックスをオンにします ([オブジェクトのオーバーライドの許可 \(431 ページ\)](#) を参照)。

**ステップ9** [保存 (Save) ] をクリックします。

## ポリシーリスト

ポリシーリストのポリシーオブジェクトを作成、コピー、編集するには、[ポリシーリストの設定 (Configure Policy List) ] ページを使用します。ルート マップを設定するときに使用するポリシー リストオブジェクトを作成できます。ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の `match` 文すべてが評価され、処理されます。1つのルート マップに2つ以上のポリシー リストを設定できます。ポリシー リストは、同じルート マップ内にあるがポリシー リストの外で設定されている他の既存の `match` および `set` 文とも共存できます。1つのルート マップ エントリ内で複数のポリシー リストが照合を行う場合、ポリシー リストすべては受信属性だけで照合を行います。

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

### 手順

- ステップ1** [オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択し、コンテンツ テーブルから [ポリシー リスト (Policy List) ] を選択します。
- ステップ2** [ポリシー リストの追加 (Add Policy List) ] をクリックします。
- ステップ3** [名前 (Name) ] フィールドにポリシー リスト オブジェクトの名前を入力します。オブジェクト名では、大文字と小文字が区別されません。
- ステップ4** [アクション (Action) ] ドロップダウンリストから、一致する条件へのアクセスを許可するかブロックするかを選択します。
- ステップ5** [インターフェイス (Interface) ] タブをクリックして、指定したいいずれかのインターフェイスの外部にネクスト ホップを持つルートを配布します。



[ゾーン/インターフェイス (Zones/Interfaces) ]リストで、デバイスが管理ステーションと通信するインターフェイスを含むゾーンを追加します。ゾーン内がないインターフェイスの場合は、[選択したゾーン/インターフェイス (Selected Zone/Interface) ]リストの下のフィールドにインターフェイス名を入力し、[追加 (Add) ]をクリックします。デバイスに選択したインターフェイスまたはゾーンが含まれている場合のみ、デバイスでホストが設定されます。

**ステップ 6** [アドレス (Address) ]タブをクリックして、標準アクセスリストまたはプレフィックスリストで許可された宛先アドレスを持つルートを再配布します。

照合に[アクセスリスト (Access List) ]または[プレフィックスリスト (Prefix List) ]のどちらを使用するかを選択し、照合に使用する標準アクセスリストオブジェクトまたはプレフィックスリストオブジェクトを入力するか選択します。

**ステップ 7** [ネクスト ホップ (Next Hop) ]タブをクリックして、指定したアクセスリストまたはプレフィックスリストの1つから渡されたネクスト ホップルータアドレスを持つルートを再配布します。

照合に[アクセスリスト (Access List) ]または[プレフィックスリスト (Prefix List) ]のどちらを使用するかを選択し、照合に使用する標準アクセスリストオブジェクトまたはプレフィックスリストオブジェクトを入力するか選択します。

**ステップ 8** [ルート送信元 (Route Source) ]タブをクリックして、アクセスリストまたはプレフィックスリストで指定されたアドレスのルータおよびアクセスサーバによってアドバタイズされたルートを再配布します。

照合に[アクセスリスト (Access List) ]または[プレフィックスリスト (Prefix List) ]のどちらを使用するかを選択し、照合に使用する標準アクセスリストオブジェクトまたはプレフィックスリストオブジェクトを入力するか選択します。

**ステップ 9** [AS パス (AS Path) ]タブをクリックして、BGP 自律システムパスを一致させます。複数のASパスを指定した場合、ルートはいずれかのASパスと一致します。

**ステップ 10** [コミュニティルール (Community Rule) ]タブをクリックすると、BGP コミュニティと指定されたコミュニティの照合が有効になります。複数のコミュニティを指定した場合、ルートはいずれかのコミュニティと一致します。BGP コミュニティと指定したコミュニティの完全一致を有効にするには、[指定したコミュニティと完全に一致 (Match the specified community exactly) ]チェックボックスをオンにします。

**ステップ 11** [メトリックとタグ (Metric & tag) ]タブをクリックして、メトリックとルートのセキュリティグループタグを照合します。

- a) [Metric (メトリック) ]フィールドに、照合に使用するメトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ~ 4294967295 の範囲で指定します。
- b) [タグ (Tag) ]フィールドに照合に使用するタグ値を入力します。複数の値をカンマで区切って入力することもできます。指定したセキュリティグループタグを持つ任意のルートを照合できます。タグ値は、0 ~ 4294967295 の範囲で指定します。

**ステップ 12** このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可 (Allow Overrides) ]チェックボックスをオンにします ([オブジェクトのオーバーライドの許可 \(431 ページ\)](#) を参照)。

ステップ 13 [保存 (Save) ] をクリックします。

## VPN オブジェクト

### Firepower Threat Defense IKE ポリシー

Internet Key Exchange (IKE; インターネットキーエクスチェンジ) は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association (SA; セキュリティアソシエーション) の自動的な確立に使用されるキー管理プロトコルです。IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティアソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKE プロポーザルは、2 つのピア間のネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通 (共有) IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。

IKEv1 では、IKE プロポーザルには、単一のアルゴリズムセットと係数グループが含まれています。複数のポリシーをプライオリティ付きで作成して、少なくとも 1 つのポリシーがリモートピアのポリシーに一致するようにできます。IKEv1 とは異なり、IKEv2 プロポーザルでは、1 つのポリシーで複数のアルゴリズムとモジュラスグループを選択できます。フェーズ 1 のネゴシエーションでピアを選択するため、作成する IKE プロポーザルの数を 1 つにすることは可能ですが、複数の異なる IKE プロポーザルを作成して、最も望ましいオプションを高い優先順位に設定することも検討してください。IKEv2 では、ポリシーオブジェクトは認証の指定は行わず、他のポリシーで認証の要件を定義する必要があります。

サイト間 IPsec VPN を設定する際は、IKE ポリシーが必要です。詳細については、[Firepower Threat Defense の VPN \(883 ページ\)](#) を参照してください。

### IKEv1 ポリシー オブジェクトの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
エクスポート コンプライアンス	該当なし	Firepower Threat Defense	リーフのみ	Admin

IKEv1 ポリシー ページを使用して、IKEv1 ポリシー オブジェクトを作成、削除、または編集します。これらのポリシーオブジェクトには、IKEv1 ポリシーに必要なパラメータが含まれています。

## 手順

- ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、目次で [VPN] > [IKEv1 ポリシー (IKEv1 Policy)] を選択します。
- 前に設定したポリシーは、システムによって定義されるデフォルトにリストされています。アクセスレベルによっては、プロポーザルを編集 (✎)、表示 (🔍)、または削除 (🗑️) することもできます。
- ステップ 2** (任意)  [IKEv1 ポリシーの追加 (Add IKEv1 Policy)] を選択して、新しいポリシー オブジェクトを作成します。
- ステップ 3** このポリシーの [名前 (Name)] を入力します。最大 128 文字を使用できます。
- ステップ 4** (任意) このプロポーザルの [説明 (Description)] を入力します。最大 1,024 文字を使用できます。
- ステップ 5** IKE ポリシーの [プライオリティ (Priority)] 値を入力します。
- このプライオリティ値によって、共通のセキュリティ アソシエーション (SA) の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティで定義されているパラメータの使用を試行します。有効な値の範囲は 1 ~ 65,535 です。値が小さいほど、プライオリティが高くなります。このフィールドを空白のままにすると、管理センターによって、まだ割り当てられていない最も小さい値が割り当てられます。値は 1 から始まり、次は 5 となり、その後は 5 ずつ増加します。
- ステップ 6** [暗号化 (Encryption)] 方法を選択します。
- IKEv1 ポリシーで使用する暗号化およびハッシュ アルゴリズムを決定する場合、ピア デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラ ネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。IKEv1 では、いずれかのオプションを選択します。オプションの説明の詳細については、[使用する暗号化アルゴリズムの決定 \(890 ページ\)](#) を参照してください。
- ステップ 7** [ハッシュ (Hash)] アルゴリズムを選択して、メッセージの整合性の確保に使用されるメッセージ ダイジェストを作成します。
- IKEv1 プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、管理対象 デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラ ネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。オプションの説明の詳細については、[使用するハッシュ アルゴリズムの決定 \(891 ページ\)](#) を参照してください。
- ステップ 8** [DH グループ (DH Group)] を設定します。
- 暗号化に使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。

ます。VPNで許可するグループを選択します。オプションの説明の詳細については、[使用する Diffie-Hellman 係数グループの決定 \(892 ページ\)](#) を参照してください。

**ステップ 9** セキュリティアソシエーション (SA) の [ライフタイム (Lifetime) ] (秒数) を設定します。120 ~ 2,147,483,647 秒の値を指定できます。デフォルトは 86400 です。

このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティアソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。

**ステップ 10** 2 つのピア間で使用する [認証方法 (Authentication Method) ] を設定します。

事前共有キーを選択します。これは唯一サポートされるメソッドで、証明書認証はこの時点でサポートされていません。事前共有キーは、秘密キーを2つのピア間で共有したり、認証フェーズ中にIKEで使用したりすることができます。参加ピアの1つに同じ事前共有キーが設定されていない場合は、IKE SA を確立できません。

(注) IKEv1 をサポートする VPN トポロジでは、選択した IKEv1 ポリシー オブジェクトで指定した [認証方式 (Authentication Method) ] が、IKEv1 の [認証タイプ (Authentication Type) ] 設定のデフォルトになります。これらの値は一致する必要があります。一致しないと設定がエラーになります。

**ステップ 11** [Save] をクリックします。  
新しい IKEv1 ポリシーがリストに追加されます。

## IKEv2 ポリシー オブジェクトの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
エクスポート コンプライアンス	該当なし	Firepower Threat Defense	リーフのみ	Admin

IKEv2 ポリシー ダイアログボックスを使用して、IKEv2 ポリシーオブジェクトを作成、削除、編集します。これらのポリシーオブジェクトには、IKEv2 ポリシーに必要なパラメータが含まれています。

### 手順

**ステップ 1** [オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択し、目次で [VPN] > [IKEv2 ポリシー (IKEv2 Policy) ] を選択します。

前に設定したポリシーは、システムによって定義されるデフォルトにリストされています。アクセスレベルによっては、ポリシーを編集 (✎)、表示 (🔍)、または削除 (🗑️) することもできます。

- ステップ 2** [IKEv2 ポリシーの追加 (Add IKEv2 Policy)] を選択して、新しいポリシーを作成します。 
- ステップ 3** このポリシーの [名前 (Name)] を入力します。  
ポリシー オブジェクトの名前。最大 128 文字を使用できます。
- ステップ 4** このポリシーの [説明 (Description)] を入力します。  
ポリシー オブジェクトの説明。最大 1024 文字を使用できます。
- ステップ 5** [プライオリティ (Priority)] を入力します。  
IKE プロポーザルのプライオリティ値。このプライオリティ値によって、共通のセキュリティ アソシエーション (SA) の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE プロポーザルの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティ ポリシーで定義されているパラメータの使用を試行します。有効な値の範囲は 1 ~ 65535 です。値が小さいほど、プライオリティが高くなります。このフィールドをブランクのままにすると、管理センターによって、まだ割り当てられていない最も小さい値が割り当てられます。値は 1 から始まり、次は 5 となり、その後は 5 ずつ増加します。
- ステップ 6** セキュリティ アソシエーション (SA) の [ライフタイム (Lifetime)] (秒数) を設定します。120 ~ 2,147,483,647 秒の値を指定できます。デフォルトは 86400 です。  
このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。
- ステップ 7** IKE ポリシーで使用するハッシュ アルゴリズムの [整合性アルゴリズム (Integrity Algorithms)] 部分を選択します。このハッシュ アルゴリズムによって、メッセージの整合性の確保に使用されるメッセージ ダイジェストが作成されます。  
IKEv2 プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、管理対象デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。VPN で許可するアルゴリズムすべてを選択します。オプションの説明の詳細については、[使用するハッシュ アルゴリズムの決定 \(891 ページ\)](#) を参照してください。
- ステップ 8** フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA の確立に使用される [暗号化アルゴリズム (Encryption Algorithm)] を選択します。  
IKEv2 プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、管理対象デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。VPN で許可するアルゴリズムすべてを選択します。オプションの説明の詳細については、[使用する暗号化アルゴリズムの決定 \(890 ページ\)](#) を参照してください。
- ステップ 9** [PRF アルゴリズム (PRF Algorithm)] を選択します。

IKE ポリシーで使用するハッシュ アルゴリズムの疑似乱数関数部分。IKEv1 では、整合性と PRF アルゴリズムは別ですが、IKEv2 では、これらの要素に異なるアルゴリズムを指定できません。VPN で許可するアルゴリズムすべてを選択します。オプションの説明の詳細については、[使用するハッシュ アルゴリズムの決定 \(891 ページ\)](#) を参照してください。

**ステップ 10** [DH グループ (DH Group) ] を選択し、[追加 (Add) ] します。

暗号化に使用される Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。VPN で許可するグループを選択します。オプションの説明の詳細については、[使用する Diffie-Hellman 係数グループの決定 \(892 ページ\)](#) を参照してください。

**ステップ 11** [Save] をクリックします。

任意の有効な組み合わせが選択された場合、新しい IKEv2 ポリシーがリストに追加されます。選択されなかった場合、エラーが表示され、このポリシーを正常に保存するために、変更する必要があります。

## Firepower Threat Defense IPsec プロポーザル

IPsec プロポーザル (またはトランスフォームセット) は VPN トポロジを設定するときに使用されます。ピアは、ISAKMP との IPsec セキュリティ アソシエーションのネゴシエーション中に、特定のデータフローを保護する特定のプロポーザルの使用に同意します。プロポーザルは、両方のピアで同じである必要があります。

IKE バージョン (IKEv1 または IKEv2) に基づいて、別個の IPsec プロポーザル オブジェクトがあります。

- IKEv1 IPsec プロポーザル (またはトランスフォームセット) オブジェクトを作成する場合、IPsec が動作するモードを選択し、必要な暗号化タイプおよび認証タイプを定義します。アルゴリズムには単一のオプションを選択できます。VPN で複数の組み合わせをサポートするには、複数の IKEv1 IPsec プロポーザル オブジェクトを作成します。
- IKEv2 IPsec プロポーザル オブジェクトを作成する際に、VPN で許可するすべての暗号化アルゴリズムとハッシュアルゴリズムを選択できます。IKEv2 ネゴシエーション中に、ピアは、それぞれでサポートされる最適なオプションを選択します。

カプセル化セキュリティ プロトコル (ESP) は、IKEv1 と IKEv2 の両方の IPsec プロポーザルに使用されます。これは認証、暗号化、およびアンチリプレイ サービスを提供します。ESP は、IP プロトコル タイプ 50 です。




(注) IPsec トンネルで暗号化と認証の両方を使用することを推奨します。

## IKEv1 IPsec プロポーザル オブジェクトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
エクスポート コンプライアンス	該当なし	Firepower Threat Defense	リーフのみ	Admin


### 手順

- ステップ 1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、目次で [VPN] > [IPsec IKEv1 プロポーザル (IPsec IKEv1 Proposal)] を選択します。
- 前に設定したプロポーザルは、システムによって定義されるデフォルトにリストされています。アクセスレベルによっては、プロポーザルを編集 (✎)、表示 (🔍)、または削除 (🗑️) することもできます。
- ステップ 2**  [IPsec IKEv1 プロポーザルの追加 (Add IPsec IKEv1 Proposal)] を選択して、新しいプロポーザルを作成します。
- ステップ 3** このプロポーザルの [名前 (Name)] を入力します。
- ポリシー オブジェクトの名前。最大 128 文字を使用できます。
- ステップ 4** このプロポーザルの [説明 (Description)] を入力します。
- ポリシー オブジェクトの説明。最大 1024 文字を使用できます。
- ステップ 5** [ESP 暗号化 (ESP Encryption)] 方法を選択します。このプロポーザルのカプセル化セキュリティ プロトコル (ESP) 暗号化アルゴリズム。
- IKEv1 では、いずれかのオプションを選択します。IPsec プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、VPN 内のデバイスによってサポートされているアルゴリズムだけを選択できます。オプションの説明の詳細については、[使用する暗号化アルゴリズムの決定 \(890 ページ\)](#) を参照してください。
- ステップ 6** [ESP ハッシュ (ESP Hash)] のオプションを選択します。
- オプションの説明の詳細については、[使用するハッシュアルゴリズムの決定 \(891 ページ\)](#) を参照してください。
- ステップ 7** [Save] をクリックします。
- 新しいプロポーザルがリストに追加されます。

## IKEv2 IPsec プロポーザル オブジェクトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
エクスポート コンプライアンス	該当なし	Firepower Threat Defense	リーフのみ	Admin

### 手順

- ステップ 1** [オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択し、目次で [VPN] > [IKEv2 IPsec プロポーザル (IKEv2 IPsec Proposal) ] を選択します。
- 前に設定したプロポーザルは、システムによって定義されるデフォルトにリストされています。アクセスレベルによっては、プロポーザルを編集 (✎)、表示 (🔍)、または削除 (🗑️) することもできます。
- ステップ 2** [  IKEv2 IPsec プロポーザルの追加 (Add IKEv2 IPsec Proposal) ] を選択して、新しいプロポーザルを作成します。
- ステップ 3** このプロポーザルの [名前 (Name) ] を入力します。
- ポリシー オブジェクトの名前。最大 128 文字を使用できます。
- ステップ 4** このプロポーザルの [説明 (Description) ] を入力します。
- ポリシー オブジェクトの説明。最大 1024 文字を使用できます。
- ステップ 5** [ESP ハッシュ (ESP Hash) ] 方法を選択して、ハッシュまたは整合性アルゴリズムを認証用プロポーザルに使用します。
- IKEv2 では、[ESP ハッシュ (ESP Hash) ] をサポートするオプションすべてを選択します。オプションの説明の詳細については、[使用するハッシュアルゴリズムの決定 \(891 ページ\)](#) を参照してください。
- ステップ 6** [ESP 暗号化 (ESP Encryption) ] 方法を選択します。このプロポーザルのカプセル化セキュリティ プロトコル (ESP) 暗号化アルゴリズム。
- IKEv2 では、[選択 (Select) ] をクリックして、サポートするすべてのオプションを選択できるダイアログボックスを開きます。IPsec プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、VPN 内のデバイスによってサポートされているアルゴリズムだけを選択できます。オプションの説明の詳細については、[使用する暗号化アルゴリズムの決定 \(890 ページ\)](#) を参照してください。
- ステップ 7** [Save] をクリックします。
- 新しいプロポーザルがリストに追加されます。





## 第 **V** 部

# アプライアンス管理の基本

- [Firepower Management Center の基礎 \(525 ページ\)](#)
- [Firepower Management Center ハイ アベイラビリティ \(529 ページ\)](#)
- [デバイスの管理の基本 \(547 ページ\)](#)





## 第 19 章

# Firepower Management Center の基礎

以下のトピックでは、Firepower Management Center の基礎について説明します。

- [Firepower Management Center](#) (525 ページ)
- [デバイス管理](#) (525 ページ)
- [NAT 環境](#) (527 ページ)

## Firepower Management Center

Firepower Management Center を使用して、Firepower システムを構成するすべてのデバイスを管理できます。デバイスを管理するには、Firepower Management Center とデバイス間に、双方向の SSL 暗号化通信チャンネルをセットアップします。Firepower Management Center はこのチャンネルを使用して、そのデバイスへのネットワークトラフィックの分析および管理の方法に関する情報をそのデバイスに送信します。そのデバイスはトラフィックを評価すると、イベントを生成し、同じチャンネルを使用してそれらのイベントを Firepower Management Center に送信します。

## デバイス管理

Firepower Management Center は、Firepower システムのキー コンポーネントです。Firepower システムを構成するあらゆるデバイスを管理したり、ネットワーク上で検出された脅威を集約し、分析して対処するために、Firepower Management Center を使用できます。

Firepower Management Center を使用してデバイスを管理すると、以下の利点があります。

- すべてのデバイスのポリシーを単一の場所から設定できるため、設定の変更が容易になります。
- さまざまなタイプのソフトウェア アップデートをデバイスにインストールできます。
- 正常性ポリシーを管理対象デバイスに適用して、Firepower Management Center からデバイスのヘルス ステータスをモニタできます。

Firepower Management Center は、侵入イベント、ネットワーク検出情報、およびデバイスのパフォーマンスデータを集約して相互に関連付けます。そのため、ユーザはデバイスが相互の関連でレポートする情報をモニタして、ネットワーク上で行われている全体的なアクティビティを評価することができます。

Firepower Management Center を使用することで、デバイス動作のほぼすべての側面を管理できます。



(注) Firepower Management Center は、<http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html> で使用可能な互換性マトリックスで指定されている特定の以前のリリースを実行しているデバイスを管理できますが、これらの以前のリリースのデバイスでは新しい機能は利用できません。

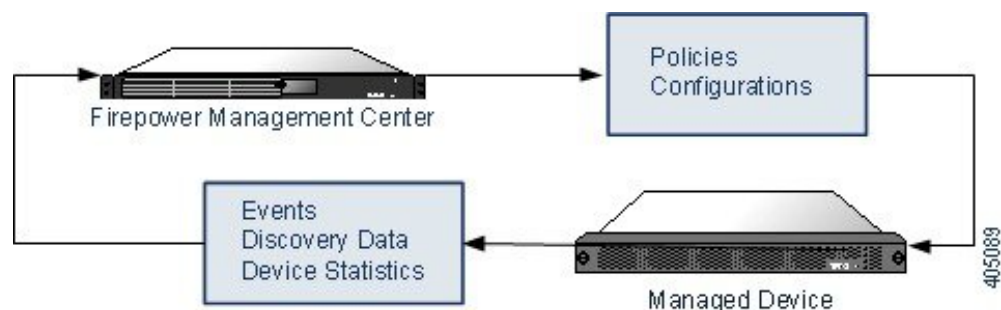
## Firepower Management Center で管理できるデバイス

Firepower Management Center を Firepower システムの展開環境における中央の管理ポイントとして使用して、次の各デバイスを管理することができます。

- 7000 および 8000 シリーズ デバイス
- ASA FirePOWER モジュール
- NGIPSv デバイス
- Firepower Threat Defense および Firepower Threat Defense Virtual

デバイスを管理する際の情報は、SSL で暗号化されたセキュアな TCP トンネルを介して、Firepower Management Center とデバイスの間で送信されます。

次の図に、Firepower Management Center と管理対象デバイスの間で送信される情報をリストします。アプライアンス間で送信されるイベントとポリシーのタイプは、デバイスタイプに基づくことに注意してください。



## ポリシーとイベント以外の機能

Firepower Management Center では、ポリシーをデバイスに展開したり、デバイスからイベントを受信するだけでなく、以下のデバイス関連のタスクも実行できます。

### デバイスのバックアップ

NGIPSv デバイスや ASA FirePOWER モジュールのバックアップ ファイルを作成、復元することはできません。

物理的な管理対象デバイス自体からそのバックアップを実行する場合は、デバイス設定のみをバックアップできます。設定データと統合ファイル（任意）をバックアップするには、管理 Firepower Management Center を使用してデバイスのバックアップを実行します。

イベントデータをバックアップするには、管理 Firepower Management Center のバックアップを実行します。

### デバイスの更新

シスコは適宜、Firepower システムの更新プログラムをリリースしています。これらのアップデートには以下が含まれます。

- 侵入ルールの更新（新しいルールや更新された侵入ルールが含まれる場合があります）
- 脆弱性データベースの更新
- 地理位置情報の更新
- ソフトウェア パッチおよびアップデート

Firepower Management Center を使用して、管理対象デバイスに更新プログラムをインストールできます。

### 関連トピック

[バックアップ ファイル](#)（199 ページ）

## NAT 環境

ネットワーク アドレス変換（NAT）とは、ルータを介したネットワーク トラフィックの送受信方式であり、送信元または宛先 IP アドレスの再割り当てが行われます。NAT の最も一般的な用途は、プライベートネットワークがインターネットと通信できるようにすることです。スタティック NAT は 1:1 変換を実行し、デバイスとの Firepower Management Center 通信に支障はありませんが、ポートアドレス変換（PAT）がより一般的です。PAT では、単一のパブリック IP アドレスと一意のポートを使用してパブリック ネットワークにアクセスできます。これらのポートは必要に応じて動的に割り当てられるため、PAT ルータの背後にあるデバイスへの接続は開始できません。

通常は、ルーティングと認証の両方の目的で両方の IP アドレス（登録キー付き）が必要です。Firepower Management Center がデバイスの IP アドレスを指定し、デバイスが Firepower

Management Center の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要があります。Firepower Management Center およびデバイスでは、初期登録の認証と承認を行うために、登録キーおよび NAT ID（IP アドレスではなく）を使用します。

たとえば、デバイスを Firepower Management Center に追加したときにデバイスの IP アドレスがわからない場合（たとえばデバイスが PAT ルータの背後にある場合）は、NAT ID と登録キーのみを指定します。デバイス上で、Firepower Management Center の IP アドレス、同じ NAT ID、および同じ登録キーを指定します。デバイスが Firepower Management Center の IP アドレスに登録されます。この時点で、Firepower Management Center は IP アドレスの代わりに NAT ID を使用してデバイスを認証します。

NAT 環境では NAT ID を使用するのが最も一般的ですが、NAT ID を使用することで、多数のデバイスを簡単に Firepower Management Center に追加することができます。Firepower Management Center で、追加するデバイスごとに一意の NAT ID を指定し、次に各デバイスで、Firepower Management Center の IP アドレスと NAT ID の両方を指定します。注：NAT ID はデバイスごとに一意でなければなりません。



## 第 20 章

# Firepower Management Center ハイアベイラビリティ

以下のトピックでは、Cisco Firepower Management Center のアクティブ/スタンバイ ハイアベイラビリティを設定する方法を示します。

- [Firepower Management Center のハイアベイラビリティについて \(529 ページ\)](#)
- [Firepower Management Center の高可用性の設定 \(536 ページ\)](#)
- [Firepower Management Center ハイアベイラビリティ ステータスの表示 \(538 ページ\)](#)
- [Firepower Management Center ハイアベイラビリティ ペアで同期される設定 \(539 ページ\)](#)
- [Firepower Management Center のハイアベイラビリティにおけるデバイス登録を解決するための CLI の使用 \(540 ページ\)](#)
- [Firepower Management Center ハイアベイラビリティ ペアにおけるピアの切り替え \(540 ページ\)](#)
- [Firepower Management Center ペア間の通信の一時停止 \(541 ページ\)](#)
- [Firepower Management Center ペア間の通信の再開 \(542 ページ\)](#)
- [高可用性ペアの Firepower Management Center の IP アドレスの変更 \(542 ページ\)](#)
- [ハイアベイラビリティ ペアでの Firepower Management Center のアップグレード \(543 ページ\)](#)
- [Firepower Management Center ハイアベイラビリティの無効化 \(544 ページ\)](#)

## Firepower Management Center のハイアベイラビリティについて

運用の継続性を確保するために、ハイアベイラビリティ機能を使用して、冗長 Firepower Management Center でデバイスを管理するように指定することができます。Firepower Management Center では、1つのアプライアンスがアクティブユニットであり、デバイスを管理する、アクティブ/スタンバイハイアベイラビリティがサポートされます。スタンバイユニットは、アクティブにデバイスを管理しません。アクティブユニットは、データストアに設定データを書き込み、両方のユニットのデータを複製し、必要な場合は同期を使用してスタンバイユニットと一部の情報を共有します。

アクティブ/スタンバイ ハイ アベイラビリティでは、プライマリ Firepower Management Center に障害が発生した場合、セカンダリ Firepower Management Center を設定して、プライマリの機能を引き継ぐことができます。プライマリ Firepower Management Center に障害が発生した場合は、セカンダリ Firepower Management Center をプロモートしてアクティブユニットにする必要があります。

イベント データは、管理対象デバイスからハイ アベイラビリティ ペアの両方の Firepower Management Center に配信されます。一方の Firepower Management Center で障害が発生した場合、他方の Firepower Management Center の使用を中断せずにネットワークをモニタすることができます。

ハイ アベイラビリティ ペアとして設定する 2 つの Firepower Management Center は、信頼された同じ管理ネットワーク上に存在する必要も、同じ地理的ロケーションに存在する必要もありません。



**注意** システムでは一部の機能をアクティブ Firepower Management Center に制限しているため、そのアプライアンスで障害が発生した場合は、スタンバイ Firepower Management Center をアクティブにプロモートする必要があります。

## Firepower Management Center のシステム要件

この項では、ハイアベイラビリティ設定にある Firepower Management Center のハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。

### ハードウェア要件

- 2 つの Firepower Management Center の間にハイ アベイラビリティ構成を設定するには、それらの間に少なくとも 5 MBPS のネットワーク帯域幅が必要です。
- ハイアベイラビリティ設定の 2 台の Firepower Management Center は、モデルが同じである必要があります。
- プライマリ Firepower Management Center バックアップをセカンダリ Firepower Management Center に復元することはできません。

### ソフトウェア要件

ハイアベイラビリティ設定の 2 台の Firepower Management Center には、同じメジャー（最初の番号）、マイナー（2 番めの番号）、メンテナンス（3 番めの番号）バージョンのソフトウェアがインストールされている必要があります。

### ライセンス要件

ハイアベイラビリティ構成の Firepower Management Center で管理されるデバイスには、単一の Firepower Management Center で管理されるデバイスと同じ数の機能ライセンスと関連するサブスクリプションが必要です。



たとえば、Firepower Management Center ペアで管理されている 2 つの デバイスに対して高度なマルウェア防御を有効にしたい場合は、2 つのマルウェア ライセンスと 2 つの TAM サブスクリプションを購入し、それらのライセンスを Firepower Management Center に追加してから、ライセンスをアクティブ Firepower Management Center 上の 2 つの デバイスに割り当てます。システムは、すべての機能ライセンスをアクティブからスタンバイ Firepower Management Center に自動的に複製するため、ライセンスをフェールオーバー時に使用できます。

また、Firepower Management Center ペアで管理されている 2 つの Firepower Threat Defense デバイスに対して高度なマルウェア防御を有効にしたい場合は、2 つのマルウェア ライセンスと 2 つの TM サブスクリプションを購入し、アクティブ Firepower Management Center を Cisco Smart Software Manager に登録してから、ライセンスをアクティブ Firepower Management Center 上の 2 つの Firepower Threat Defense デバイスに割り当てます。フェールオーバーが行われると、システムは Smart Software Manager と通信して、スマートライセンスの権利をアクティブ Firepower Management Center から解放し、スタンバイ Firepower Management Center に割り当てます。

## 高可用性 Firepower Management Center での役割とステータス

### プライマリ/セカンダリの役割

Firepower Management Center を高可用性ペアの形でセットアップする際は、一方の Firepower Management Center をプライマリとして設定し、もう一方をセカンダリとして設定します。設定中に、プライマリ ユニットのポリシーは、セカンダリ ユニットの同期されます。この同期が完了すると、プライマリ Firepower Management Center がアクティブ ピアになり、セカンダリ Firepower Management Center がスタンバイ ピアになって、2 つのユニットが管理対象デバイスおよびポリシー設定に対して単一のアプライアンスとして機能します。

### アクティブ/スタンバイ ステータス

高可用性ペアを構成する 2 つの Firepower Management Center の間の主な違いは、どちらがアクティブ ピアで、どちらがスタンバイ ピアであるかという点です。アクティブ Firepower Management Center は、完全に機能する状態に維持され、デバイスとポリシーを管理するために使用できます。スタンバイ Firepower Management Center では機能が非表示になるため、設定の変更を行うことはできません。

## Firepower Management Center ハイ アベイラビリティ ペアのデバイス登録

高可用性を確立する前に、すべての管理対象デバイスを目的のアクティブ Firepower Management Center に登録する必要があります。これには、目的のセカンダリからデバイスを削除し、それらを目的のプライマリに登録することが含まれます。

また、高可用性を確立する前に、目的のセカンダリでポリシーをエクスポートする必要があります。セカンダリとして使用するアプライアンスがどれであっても、デバイス登録とポリシー設定のすべてが失われます。

高可用性が確立されると、アクティブ Firepower Management Center に登録されたデバイスが自動的にスタンバイ Firepower Management Center に登録されます。

登録済みのデバイスに NAT IP アドレスが割り当てられている場合、デバイスの自動登録は失敗し、セカンダリ Firepower Management Center の [ハイ アベイラビリティ (High Availability) ] ページには、そのデバイスがローカルで保留中であると表示されます。次に、スタンバイ Firepower Management Center の [ハイ アベイラビリティ (High Availability) ] ページで、異なる NAT IP アドレスをデバイスに割り当てることができます。

自動登録がスタンバイ Firepower Management Center で失敗しても、デバイスがアクティブな Firepower Management Center に登録されているように見える場合は、[Firepower Management Center のハイ アベイラビリティにおけるデバイス登録を解決するための CLI の使用 \(540 ページ\)](#) を参照してください。

## Firepower Management Center のハイ アベイラビリティ ペアでのイベント処理

ハイ アベイラビリティ ペアの両方の Firepower Management Center が管理対象デバイスからイベントを受信するため、アプライアンスの管理 IP アドレスは共有されません。これは Firepower Management Center で障害が発生した場合に、継続的な処理を確保するために介入する必要がないことを意味します。

### AMP クラウド接続とマルウェア情報

ハイ アベイラビリティ ペアを構成する Firepower Management Center は、ファイル ポリシーおよび関連する設定は共有しますが、シスコ AMP クラウド接続およびマルウェア処理は共有しません。運用の継続性を確保し、検出されたファイルのマルウェア処理が両方の Firepower Management Center で同じであるようにするためには、プライマリとセカンダリ両方の Firepower Management Center が AMP クラウドにアクセスできる必要があります。

### URL フィルタリングとセキュリティ インテリジェンス

URL フィルタリングとセキュリティ インテリジェンスの設定および情報は、ハイ アベイラビリティ展開の Firepower Management Center の間で同期されます。ただし、プライマリ Firepower Management Center だけが、セキュリティ インテリジェンス フィードの更新用の URL カテゴリおよびレピュテーション データをダウンロードします。

プライマリ Firepower Management Center に障害が発生した場合は、セカンダリ Firepower Management Center がインターネットにアクセスして脅威インテリジェンスを更新できることを確認する必要があるだけでなく、セカンダリ Firepower Management Center の Web インターフェイスを使用してセカンダリをアクティブにプロモートする必要もあります。

## Firepower Management Center のフェールオーバー中のユーザ データの処理

プライマリ Firepower Management Center で障害が発生した場合、ユーザ エージェント、ISE、TS エージェント、またはキャプティブ ポータル デバイスから報告されるすべてのログインは、それらのユーザが前に確認されて Firepower Management Center にダウンロードされていた場合でも、フェールオーバーのダウンタイム中に識別することはできません。識別されていないユーザは、Firepower Management Center で [不明 (Unknown)] のユーザとして記録されます。

ダウンタイム後、不明のユーザはアイデンティティ ポリシーのルールに従って再確認され、処理されます。

## Firepower Management Center ハイ アベイラビリティ ペアの構成管理

ハイアベイラビリティ展開では、アクティブな Firepower Management Center のみがデバイスを管理し、ポリシーを適用できます。両方の Firepower Management Center は継続的な同期状態を保ちます。

アクティブ状態の Firepower Management Center に障害が発生すると、ハイアベイラビリティペアは縮退状態となります。縮退状態は、スタンバイ状態のアプライアンスを手動でアクティブ状態に上げるまで続きます。スタンバイ状態のアプライアンスをアクティブ状態に上げると、両アプライアンスのメンテナンス モードが終了します。

## バックアップ中の Firepower Management Center の高可用性動作

Firepower Management Center 高可用性ペアでバックアップを実行する場合、バックアップ動作によってピア間の同期が一時停止します。この動作中は、引き続きアクティブな Firepower Management Center を使用できますが、スタンバイピアを使用することはできません。

バックアップが完了すると、同期が再開され、少しの間、アクティブピアでのプロセスが無効になります。この一時停止中、[高可用性 (High Availability)] ページには、すべてのプロセスが再開されるまでは一時的に保留ページが表示されます。

## Firepower Management Center ハイアベイラビリティのスプリットブレイン

高可用性ペアのアクティブな Firepower Management Center が（電源の問題、ネットワークや接続の問題で）ダウンした場合は、スタンバイ Firepower Management Center をアクティブ状態に昇格させることができます。元のアクティブなピアが起動すると、両方のピアがアクティブであるとみなされる場合があります。この状態は「スプリットブレイン」と定義されます。このような状況が発生すると、システムによってアクティブなアプライアンスを選択するように要求されます。それによって、もう一方のアプライアンスはスタンバイ状態に降格します。

アクティブな Firepower Management Center がダウンした（またはネットワーク障害により切断された）場合は、高可用性を中断するか、またはロールを切り替えることができます。スタンバイ Firepower Management Center は縮退状態になります。



- (注) セカンダリとして使用するアプライアンスがどれであっても、スプリットブレインの解決時にデバイス登録とポリシー設定のすべてが失われます。たとえば、セカンダリに存在し、プライマリには存在しなかったポリシーへの変更は失われます。Firepower Management Center が両方のアプライアンスがアクティブな高可用スプリットブレインシナリオである場合に、スプリットブレインを解決する前に管理対象デバイスを登録してポリシーを展開する場合は、ハイアベイラビリティを再確立する前に、ポリシーをエクスポートして、管理対象デバイスを対象のスタンバイ Firepower Management Center から登録解除する必要があります。その後、管理対象デバイスを登録し、目的のアクティブ Firepower Management Center にポリシーをインポートすることができます。

## ハイアベイラビリティペアでの Firepower Management Center のアップグレード

Cisco は、各種の更新プログラムを電子形式で定期的に配信します。更新プログラムには、システムソフトウェアのメジャーおよびマイナーアップグレードが含まれます。ハイアベイラビリティセットアップでは、これらの更新を両方の Firepower Management Center にインストールする必要が生じることがあります。



- 警告** アップグレード中には、少なくとも 1 つの Firepower Management Center を動作状態に維持してください。

### 始める前に

アップグレードに付属しているリリースノートまたはアドバイザリテキストを読んでください。リリースノートでは、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストールおよびアンインストールの手順など重要なデータが提供されます。

### 手順

- ステップ 1** アクティブ Firepower Management Center の Web インターフェイスにアクセスし、データを同期を一時停止します（[Firepower Management Center ペア間の通信の一時停止（541 ページ）](#)を参照）。
- ステップ 2** スタンバイ Firepower Management Center をアップグレードします（[Firepower Management Center でのソフトウェアの更新（169 ページ）](#)を参照）。
- アップグレードが完了すると、スタンバイユニットがアクティブになります。両方のピアがアクティブになると、ハイアベイラビリティペアが劣化状態（スプリットブレイン）になります。

**ステップ 3** もう一方の Firepower Management Center をアップグレードします。

**ステップ 4** どちらの Firepower Management Center をセカンダリとして使用するかを決定します。そのデバイスを登録解除し、維持する必要がある設定をエクスポートします。

新しいアクティブ Firepower Management Center を選択すると、セカンダリとして指定される Firepower Management Center のデバイス登録と展開済みポリシー設定がすべて失われます。たとえば、同期を一時停止した後に行ったポリシーの変更内容はすべて失われます。

**ステップ 5** 新しいアクティブ Firepower Management Center を選択してスプリットブレインを解決します。

## Firepower Management Center のハイアベイラビリティのトラブルシューティング

この項では、Firepower Management Center のハイアベイラビリティ操作のいくつかの一般的なエラーに関するトラブルシューティング情報を示します。

エラー (Error)	説明	ソリューション
500 内部 (500 Internal)	ピア ロールの切り替えや同期の一時停止と再開などのクリティカルな Firepower Management Center のハイアベイラビリティ操作を実行しているときに Web インターフェイスにアクセスしようとする则表示されることがあります。	Web インターフェイスを使用する前に、操作が完了するまでお待ちください。

エラー (Error)	説明	ソリューション
<p>システム プロセスが起動していません、お待ちください (System processes are starting, please wait)</p> <p>また、Web インターフェイスは応答しません。 (Also, the web interface does not respond.)</p>	<p>ハイアベイラビリティまたはデータ同期操作中に Firepower Management Center が再起動 (手動でまたは電源切断からの回復中に) する場合に表示されることがあります。</p>	<ol style="list-style-type: none"> <li>1. Firepower Management Center シェルにアクセスし、<code>manage_hadc.pl</code> コマンドを使用して Firepower Management Center のハイアベイラビリティ構成ユーティリティにアクセスします。  (注) <code>sudo</code> を使用して、ルート ユーザとしてユーティリティを実行します。</li> <li>2. オプション 5 を使用してミラーリング操作を一時停止します。  Firepower Management Center Web インターフェイスをリロードします。</li> <li>3. Web インターフェイスを使用して同期を再開します。[システム (System)] &gt; [統合 (Integration)] の順に選択し、[ハイアベイラビリティ (High Availability)] タブをクリックして、[同期の再開 (Resume Synchronization)] を選択します。</li> </ol>

## Firepower Management Center の高可用性の設定

スマート ライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、 MC2000、 MC3500、MC4000	グローバル	Admin

高可用性を確立するには、ピア間の帯域幅とポリシーの数に応じてかなりの時間がかかり、数時間かかることもあります。また、スタンバイ状態の Firepower Management Center と同期される必要のある、アクティブ Firepower Management Center に登録されたデバイスの数によっても

異なります。[ハイ アベイラビリティ (High Availability) ] ページを表示すると、ハイ アベイラビリティ ピアのステータスを確認できます。

#### 始める前に

- 両方の Firepower Management Center が同じモデルで、同じソフトウェアバージョンを実行していることを確認します。
- セカンダリの Firepower Management Center に登録されているすべてのデバイスの登録を解除します。

#### 手順

- 
- ステップ 1** セカンダリとして指定する Firepower Management Center にログインします。
- ステップ 2** [システム (System) ] > [統合 (Integration) ] を選択します。
- ステップ 3** [高可用性 (High Availability) ] を選択します。
- ステップ 4** この Firepower Management Center の権限で、[セカンダリ (Secondary) ] を選択します。
- ステップ 5** [プライマリ Firepower Management Center ホスト (Primary Firepower Management Center Host) ] テキストボックスに、プライマリ Firepower Management Center のホスト名または IP アドレスを入力します。
- ルーティング可能なアドレスがプライマリ Firepower Management Center に設定されていない場合は、空白のままにしても構いません。この場合は、[登録キー (Registration Key) ] と [一意の NAT ID (Unique NAT ID) ] の両方のフィールドを使用します。プライマリ ユニットでセカンダリ IP アドレスを指定する必要もあります。少なくとも 1 つのユニットの IP アドレスを指定する必要があります。
- ステップ 6** [登録キー (Registration Key) ] テキストボックスに、1 回限り使用する登録キーを入力します。登録キーは、ユーザ定義の最大 37 文字の英数字値です。
- ステップ 7** プライマリ IP アドレスを指定しなかった場合、またはプライマリ Firepower Management Center でセカンダリ IP アドレスを指定しない場合は、[一意の NAT ID (Unique NAT ID) ] フィールドに一意の英数字 ID を入力します。詳細については、[NAT 環境 \(527 ページ\)](#) を参照してください。
- ステップ 8** [登録 (Register) ] をクリックします。
- ステップ 9** 管理者アクセス権限を持つアカウントを使用して、プライマリとして指定する Firepower Management Center にログインします。
- ステップ 10** [システム (System) ] > [統合 (Integration) ] を選択します。
- ステップ 11** [高可用性 (High Availability) ] を選択します。
- ステップ 12** この Firepower Management Center の権限で、[プライマリ (Primary) ] を選択します。
- ステップ 13** [セカンダリ Firepower Management Center ホスト (Secondary Firepower Management Center Host) ] テキストボックスに、セカンダリ Firepower Management Center のホスト名または IP アドレスを入力します。

ルーティング可能なアドレスがセカンダリ Firepower Management Center に設定されていない場合は、空白のままにしても構いません。この場合は、[登録キー (Registration Key)] と [一意の NAT ID (Unique NAT ID)] の両方のフィールドを使用します。セカンダリ ユニットでプライマリ IP アドレスを指定する必要もあります。少なくとも 1 つのユニットの IP アドレスを指定する必要があります。

- ステップ 14 [登録キー (Registration Key)] テキストボックスに、ステップ 6 で入力した 1 回限り使用する登録キーと同じものを入力します。
- ステップ 15 必要に応じて、[一意の NAT ID (Unique NAT ID)] テキストボックスに手順 7 で使用したのと同じ NAT ID を入力します。
- ステップ 16 [登録 (Register)] をクリックします。

## Firepower Management Center ハイ アベイラビリティ ステータスの表示

スマートライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、MC2000、MC3500、MC4000	グローバル	Admin

アクティブおよびスタンバイ Firepower Management Center を識別した後、ローカル Firepower Management Center とそのピアに関する情報を表示できます。



- (注) このコンテキストでは、ローカル ピアは、システム ステータスを表示するアプライアンスを参照します。リモートピアは、アクティブステータスかスタンバイステータスかに関係なく、その他のアプライアンスを参照します。

### 手順

- ステップ 1 高可用性を使用してペアにした Firepower Management Center のいずれかにログインします。
  - ステップ 2 [システム (System)] > [統合 (Integration)] を選択します。
  - ステップ 3 [ハイ アベイラビリティ (High Availability)] を選択します。
- 次の情報を表示できます。



### サマリー情報

- ハイ アベイラビリティ ペアのヘルス ステータス
- ハイ アベイラビリティ ペアの現在の同期ステータス
- アクティブ ピアの IP アドレスと最後に同期された時間
- スタンバイ ピアの IP アドレスと最後に同期された時間

### システム ステータス

- 両方のピアの IP アドレス
- 両方のピアのオペレーティング システム
- 両方のピアのソフトウェア バージョン
- 両方のピアのアプライアンス モデル

## Firepower Management Center ハイ アベイラビリティ ペア で同期される設定

この項では、ハイ アベイラビリティが確立されたときに2つの Firepower Management Center 間で同期される特定の設定データについて説明します。

- アクセス コントロール ポリシー
- 侵入ルール
- マルウェアおよびファイル ポリシー
- DNS ポリシー
- アイデンティティ ポリシー
- SSL ポリシー
- プレフィルタ ポリシー
- ネットワーク検出ルール
- アプリケーション ディテクタ
- 関連ポリシー ルール
- アラート (Alerts)
- スキャナ (Scanners)
- 応答グループ

- 修復設定。ただし、両方の Firepower Management Center にカスタム モジュールをインストールする必要があります。修復設定の詳細については、[修復モジュールの管理 \(2299ページ\)](#) を参照してください。

## Firepower Management Center のハイ アベイラビリティにおけるデバイス登録を解決するための CLI の使用

スマート ライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、MC2000、MC3500、MC4000	グローバル	Admin

自動デバイス登録がスタンバイ Firepower Management Center で失敗したものの、アクティブ Firepower Management Center に登録されたと表示される場合、次の手順を実行します。

### 手順

**ステップ 1** アクティブ Firepower Management Center からデバイスの登録を解除します。

**ステップ 2** 影響を受けるデバイスの CLI にログインします。

**ステップ 3** CLI コマンド `configure manager delete` を実行します。

**ステップ 4** CLI コマンド `configure manager add` を実行します。

アクティブ Firepower Management Center のリモート管理を設定します。

**ステップ 5** アクティブ Firepower Management Center にログインし、デバイスを登録します。

## Firepower Management Center ハイ アベイラビリティ ペアにおけるピアの切り替え

スマート ライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、MC2000、MC3500、MC4000	グローバル	Admin

システムでは一部の機能をアクティブ Firepower Management Center に制限しているため、そのアプライアンスで障害が発生した場合は、スタンバイ Firepower Management Center をアクティブ ステータスにプロモートする必要があります。

手順

- ステップ 1 ハイアベイラビリティを使用してペアリングした Firepower Management Center のいずれか一方にログインします。
- ステップ 2 [システム (System)] > [統合 (Integration)] を選択します。
- ステップ 3 [ハイアベイラビリティ (High Availability)] を選択します。
- ステップ 4 [ピア ロールの切り替え (Switch Peer Roles)] を選択して、ローカル ロールをアクティブからスタンバイ、またはスタンバイからアクティブに変更します。プライマリまたはセカンダリの指定は変更されずに、2つのピア間でロールが切り替わります。

## Firepower Management Center ペア間の通信の一時停止

スマート ライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、 MC2000、 MC3500、MC4000	グローバル	Admin

一時的に高可用性を無効にする場合は、Firepower Management Center 間の通信チャンネルを無効にすることができます。アクティブ ピアの同期を一時停止した場合は、スタンバイ ピアまたはアクティブ ピアのいずれでも同期を再開できます。ただし、スタンバイ ピアで同期を一時停止した場合、同期の再開はスタンバイ ピアでのみ可能になります。

手順

- ステップ 1 高可用性を使用してペアにした Firepower Management Center のいずれかにログインします。
- ステップ 2 [システム (System)] > [統合 (Integration)] を選択します。
- ステップ 3 [高可用性 (High Availability)] を選択します。
- ステップ 4 [同期の一時停止 (Pause Synchronization)] を選択します。

## Firepower Management Center ペア間の通信の再開

スマートライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、 MC2000、 MC3500、MC4000	グローバル	Admin

一時的に高可用性を無効にしている場合は、Firepower Management Center 間の通信チャンネルを有効にすることで、高可用性を再開することができます。アクティブユニットで同期を一時停止した場合、スタンバイユニットまたはアクティブユニットのいずれでも同期を再開できます。ただし、スタンバイユニットで同期を一時停止した場合、同期の再開はスタンバイユニットでのみ可能になります。

### 手順

- ステップ 1 高可用性を使用してペアにした Firepower Management Center のいずれかにログインします。
- ステップ 2 [システム (System)] > [統合 (Integration)] を選択します。
- ステップ 3 [高可用性 (High Availability)] を選択します。
- ステップ 4 [同期の再開 (Resume Synchronization)] を選択します。

## 高可用性ペアの Firepower Management Center の IP アドレスの変更

スマートライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、 MC2000、 MC3500、MC4000	グローバル	Admin



- (注) 7000 および 8000 シリーズ 管理対象デバイスのリモート管理を編集しているときに、このトピックにたどり着いた場合は、[管理対象デバイスでのリモート管理の編集 \(575ページ\)](#) を参照してください。

高可用性ピアのいずれかの IP アドレスを変更すると、高可用性が低下した状態になります。高可用性を回復するには、手動で IP アドレスを変更する必要があります。

#### 手順

- 
- ステップ 1 高可用性を使用してペアにした Firepower Management Center のいずれかにログインします。
  - ステップ 2 [システム (System)] > [統合 (Integration)] を選択します。
  - ステップ 3 [高可用性 (High Availability)] を選択します。
  - ステップ 4 [ピア マネージャ (Peer Manager)] を選択します。
  - ステップ 5 編集アイコン (✎) を選択します。
  - ステップ 6 アプライアンスの表示名を入力します。この表示名は、Firepower システムのコンテキストでのみ使用されます。  
別の表示名を入力しても、アプライアンスのホスト名は変更されません。
  - ステップ 7 完全修飾ドメイン名を入力するか、ローカル DNS で有効な IP アドレス (ホスト名) に解決される名前、またはホストの IP アドレスを入力します。
  - ステップ 8 [保存 (Save)] を選択します。
- 

## ハイアベイラビリティペアでの Firepower Management Center のアップグレード

Cisco は、各種の更新プログラムを電子形式で定期的に配信します。更新プログラムには、システム ソフトウェアのメジャーおよびマイナー アップグレードが含まれます。ハイアベイラビリティセットアップでは、これらの更新を両方の Firepower Management Center にインストールする必要が生じることがあります。



**警告** アップグレード中には、少なくとも 1 つの Firepower Management Center を動作状態に維持してください。

---

#### 始める前に

アップグレードに付属しているリリースノートまたはアドバイザリテキストを読んでください。リリースノートでは、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストールおよびアンインストールの手順など重要なデータが提供されます。

手順

- 
- ステップ1 アクティブ Firepower Management Center の Web インターフェイスにアクセスし、データ同期を一時停止します（[Firepower Management Center ペア間の通信の一時停止（541 ページ）](#) を参照）。
  - ステップ2 スタンバイ Firepower Management Center をアップグレードします（[Firepower Management Center でのソフトウェアの更新（169 ページ）](#) を参照）。アップグレードが完了すると、スタンバイユニットがアクティブになります。両方のピアがアクティブになると、ハイアベイラビリティペアが劣化状態(スプリットブレイン)になります。
  - ステップ3 もう一方の Firepower Management Center をアップグレードします。
  - ステップ4 どちらの Firepower Management Center をセカンダリとして使用するかを決定します。そのデバイスを登録解除し、維持する必要がある設定をエクスポートします。  
新しいアクティブ Firepower Management Center を選択すると、セカンダリとして指定される Firepower Management Center のデバイス登録と展開済みポリシー設定がすべて失われます。たとえば、同期を一時停止した後に行ったポリシーの変更内容はすべて失われます。
  - ステップ5 新しいアクティブ Firepower Management Center を選択してスプリットブレインを解決します。
- 

## Firepower Management Center ハイ アベイラビリティの無効化

スマートライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、MC2000、MC3500、MC4000	グローバル	Admin

手順

- 
- ステップ1 ハイアベイラビリティペアのいずれか一方の Firepower Management Center にログインします。
  - ステップ2 [システム (System) ] > [統合 (Integration) ] を選択します。
  - ステップ3 [ハイアベイラビリティ (High Availability) ] を選択します。
  - ステップ4 [ハイアベイラビリティの解消 (Break High Availability) ] を選択します。
  - ステップ5 管理対象デバイスを処理するための以下のいずれかのオプションを選択します。

- この Firepower Management Center を使用してすべての管理対象デバイスを制御する場合には、[このコンソールから登録済みデバイスを管理 (Manage registered devices from this console) ] を選択します。すべてのデバイスがピアから登録解除されます。
- 他の Firepower Management Center を使用してすべての管理対象デバイスを制御する場合には、[ピアコンソールから登録済みデバイスを管理 (Manage registered devices from peer console) ] を選択します。すべてのデバイスがこの Firepower Management Center から登録解除されます。
- デバイスの管理をまとめて停止する場合には、[両方のコンソールからの登録済みデバイスの管理を停止 (Stop managing registered devices from both consoles) ] を選択します。すべてのデバイスが両方の Firepower Management Center から登録解除されます。

**ステップ 6** [OK] をクリックします。

---







## 第 21 章

# デバイスの管理の基本

次のトピックでは、Firepower システムでデバイスを管理する方法について説明します。

- [\[デバイス管理 \(Device Management\) \] ページ \(547 ページ\)](#)
- [リモート管理の設定 \(549 ページ\)](#)
- [Firepower Management Center へのデバイスの追加 \(550 ページ\)](#)
- [Firepower Management Center からのデバイスの削除 \(552 ページ\)](#)
- [デバイス コンフィギュレーションの設定 \(553 ページ\)](#)
- [インターフェイス テーブル ビュー \(564 ページ\)](#)
- [デバイス グループ管理 \(568 ページ\)](#)

## [デバイス管理 (Device Management) ] ページ

[デバイス管理 (Device Management) ] ページには、登録されたデバイス、7000 および 8000 シリーズデバイスのハイ アベイラビリティ ペア、およびデバイス グループを管理するために使用できる、一連の情報とオプションが表示されます。このページには、現在 Firepower Management Center に登録されているすべてのデバイスの一覧が表示されます。

[ソート基準 (sort-by) ] ドロップダウン リストを使用すると、グループ、ライセンス、モデル、またはアクセス コントロール ポリシーのいずれかのカテゴリでデバイス一覧をソートできます。マルチドメイン導入では、ドメイン (その導入のデフォルトの表示カテゴリ) を基準にソートすることもできます。デバイスはリーフ ドメインに属している必要があります。

デバイス カテゴリに属するデバイスの一覧は、展開または縮小表示できます。デフォルトでは、デバイス一覧が展開されます。

デバイス一覧の詳細については、以下の表を参照してください。

表 49: [デバイス一覧 (Device List)] のフィールド

フィールド	説明
[名前 (Name)]	Firepower Management Center でデバイスに使用されている表示名。名前の左側にあるステータスアイコンは、その名前の現在のヘルスステータスを示します。
グループ	管理対象デバイスを割り当てたグループ。
モデル	管理対象デバイスのモデル。
ライセンスのタイプ (License Type)	管理対象デバイスで有効なライセンス。
アクセスコントロールポリシー (Access Control Policy)	現在導入されているアクセスコントロールポリシーへのリンク。システムがアクセスコントロールポリシーを古いものとして識別すると、そのリンクの横に警告アイコン (ⓘ) が表示されます。

関連トピック

- [Firepower の機能ライセンスについて \(137 ページ\)](#)
- [ヘルス モニタリングについて \(275 ページ\)](#)
- [アクセスコントロールポリシーの管理 \(1328 ページ\)](#)

## 管理対象デバイスのフィルタリング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Network Admin

Firepower Management Center が大量のデバイスを管理する場合、[デバイス管理 (Device Management)] ページの結果を絞り込むことで特定のデバイスを見つけやすくなります。

手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 デバイスのリストを絞り込むには、[デバイス名 (Device Name)] [デバイス/ホスト名 (Device/Host Name)] フィールドにデバイス名の全体または一部を入力します。
- ステップ 3 フィルタをクリアするには：
  - [デバイス名 (Device Name)] [デバイス/ホスト名 (Device/Host Name)] フィールドをクリアします。

- [一部のデバイスがリストされていません。 (Not all devices are listed.) すべてのデバイスを一覧表示するには、ここをクリックしてください。 (Click here to list all devices) ] リンクを選択してください。

#### 関連トピック

[Firepower の機能ライセンスについて \(137 ページ\)](#)

[ヘルス モニタリングについて \(275 ページ\)](#)

[アクセスコントロールポリシーの管理 \(1328 ページ\)](#)

## リモート管理の設定

Firepower System デバイスを管理できるようにするには、デバイスと Firepower Management Center との間に双方向の SSL 暗号化通信チャネルをセットアップする必要があります。このチャネルを使用して、両方のアプライアンスが設定とイベント情報を共有します。ハイアベイラビリティピアも、このチャネルを使用します。このチャネルは、デフォルトではポート 8305/tcp に位置します。



(注) この章では、FMCにデバイスを登録する前にローカル Web インターフェイスを使用して、7000 または 8000 シリーズ デバイスのリモート管理の設定方法について説明します。他のモデルのリモート管理の設定の詳細については、適切なクイックスタートガイドを参照してください。

2つのアプライアンス間の通信を可能にするためには、アプライアンスが互いを認識する手段を提供しなければなりません。Firepower System では3つの基準を使用して、通信を許可します。

- 通信を確立する対象のアプライアンスのホスト名または IP アドレス。  
NAT 環境では、ルーティング可能なアドレスがもう一方のアプライアンスにないとしても、リモート管理を設定する際、または管理対象アプライアンスを追加する際には、ホスト名または IP アドレスのいずれかを指定する必要があります。
- 接続を識別するために自己生成される、最大 37 文字の英数字による登録キー。
- Firepower System が NAT 環境で通信を確立するために利用できるオプションの一意の英数字による NAT ID。

NAT ID は、管理対象アプライアンスを登録するために使用されているすべての NAT ID の間で一意でなければなりません。

## Firepower Management Center へのデバイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Network Admin

Firepower Management Center に 1 つのデバイスを追加するには、ここに示す手順を実行します。冗長性やパフォーマンスのためにデバイスをリンクする場合、次の点を念頭に置いて、この手順を実行する必要があります。

- 8000 シリーズ スタック：この手順を使用して各デバイスを Firepower Management Center に追加した後、スタックを確立します ([デバイススタックの確立 \(628 ページ\)](#) を参照)。
- 7000 および 8000 シリーズ ハイ アベイラビリティ：この手順を使用して各デバイスを Firepower Management Center に追加した後、高可用性を確立します ([デバイスのハイ アベイラビリティの確立 \(609 ページ\)](#) を参照)。ハイアベイラビリティスタックの場合、デバイスをスタックしてから、スタック間のハイアベイラビリティを確立します。
- Firepower Threat Defense ハイアベイラビリティ：この手順を使用して各デバイスを Firepower Management Center に追加した後、高可用性を確立します ([Firepower Threat Defense ハイアベイラビリティ ペアの追加 \(745 ページ\)](#) を参照)。
- Firepower Threat Defense クラスタ：クラスタユニットが FXOS に正常に形成されたクラスタであることを確認し、次の手順を使用して各ユニットを別個の管理対象デバイスとして Firepower Management Center に追加します。最後に、Firepower Management Center でユニットをクラスタ化します。詳細については、[Management Center へのクラスタの追加 \(771 ページ\)](#) を参照してください。



- (注) Firepower Management Center ハイアベイラビリティを確立したか、または確立する予定がある場合、デバイスをアクティブな (またはアクティブにする予定の) Firepower Management Center にのみ追加します。ハイアベイラビリティを確立すると、アクティブ Firepower Management Center に登録されたデバイスが自動的にスタンバイに登録されます。

### 始める前に

- デバイスを Firepower Management Center の管理対象として設定します。7000 および 8000 シリーズデバイスについては、[管理対象デバイス上のリモート管理の設定 \(574 ページ\)](#) を参照してください。他のモデルのリモート管理設定の詳細については、該当するクイックスタートガイドを参照してください。
- IPv4 を使用して登録した Firepower Management Center とデバイスを IPv6 に変換する場合は、デバイスをいったん削除してから再登録する必要があります。

## 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2** [追加 (Add) ] ドロップダウンメニューから、[デバイスの追加 (Add Device) ] を選択します。
- ステップ 3** [ホスト (Host) ] フィールドに、追加するデバイスの IP アドレスまたはホスト名を入力します。
- デバイスのホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。
- NAT 環境では、Firepower Management Center の管理対象としてデバイスを設定するときに Firepower Management Center の IP アドレスまたはホスト名をすでに指定した場合、デバイスの IP アドレスまたはホスト名を指定する必要がない場合があります。詳細については、[NAT 環境 \(527 ページ\)](#) を参照してください。
- ステップ 4** [表示名 (Display Name) ] フィールドに、Firepower Management Center でのデバイスの表示名を入力します。
- ステップ 5** [登録キー (Registration Key) ] フィールドに、Firepower Management Center の管理対象としてデバイスを設定したときに使用したのと同じ登録キーを入力します。登録キーは、1 回限り使用可能な共有シークレットです。
- ステップ 6** マルチドメイン展開では、現在のドメインに関係なく、デバイスをリーフドメインに割り当てます。
- 現在のドメインがリーフドメインである場合、デバイスは自動的に現在のドメインに追加されます。現在のドメインがリーフドメインでない場合、登録後、デバイスを設定するために、リーフドメインに切り替える必要があります。
- ステップ 7** 必要に応じて、デバイスをデバイスグループに追加します。
- ステップ 8** 登録後すぐに、デバイスに展開する最初の [アクセスコントロールポリシー (Access Control Policy) ] を選択するか、新しいポリシーを作成します。
- デバイスが選択したポリシーに適合しない場合、展開は失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。この障害の原因を解決した後、デバイスに手作業で設定を行います。
- ステップ 9** デバイ스에適用するライセンスを選択します。
- 従来型のデバイスでは、次の点に注意してください。
- コントロール、マルウェア、URL フィルタリングライセンスには、保護ライセンスが必要です。
  - VPN ライセンスでは、7000 または 8000 シリーズ デバイスを必要とします。

- コントロール ライセンスは、NGIPSv と ASA FirePOWER デバイスでサポートされていますが、8000 シリーズ Fastpath ルール、スイッチング、ルーティング、スタック、デバイスのハイ アベイラビリティを設定することはできません。

**ステップ 10** デバイスの設定時に、NAT ID を使用した場合、[詳細 (Advanced)] セクションを展開し、[一意の NAT ID (Unique NAT ID)] フィールドに同じ NAT ID を入力します。

**ステップ 11** [パケットの転送 (Transfer Packets)] チェックボックスをオンにし、デバイスで Firepower Management Center にパケットを転送することを許可します。

このオプションは、デフォルトで有効です。無効にすると、Firepower Management Center へのパケット転送が完全に禁止されます。

**ステップ 12** [登録 (Register)] をクリックします。

Firepower Management Center がデバイスのハートビートを確認して通信を確立するまでに、最大 2 分かかる場合があります。

#### 関連トピック

[基本的なアクセス コントロール ポリシーの作成](#) (1329 ページ)

## Firepower Management Center からのデバイスの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Network Admin

デバイスを管理する必要がなくなった場合、Firepower Management Center からそのデバイスを削除できます。デバイスを削除すると、以下のようになります。


- Firepower Management Center とそのデバイスとの間のすべての通信が切断されます。
- [デバイス管理 (Device Management)] ページからデバイスが削除されます。
- プラットフォーム設定ポリシーで、NTP を介して Firepower Management Center から時間を受信するようにデバイスが設定されている場合は、デバイスがローカル時間管理に戻されます。

デバイスを後者で管理するには、デバイスを Firepower Management Center に再度追加します。



(注) デバイスを削除し、再び追加すると、Firepower Management Center Web インターフェイスによって、アクセス コントロール ポリシーを再適用するよう求められます。ただし、登録時に NAT と VPN ポリシーを再適用するオプションはありません。以前に適用された NAT または VPN 設定はすべて登録時に削除されるため、登録が完了した後に再適用する必要があります。

手順

- ステップ1 [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ2 削除するデバイスの横にある削除アイコン (  ) をクリックします。
- ステップ3 デバイスを削除することを確認します。

## デバイス コンフィギュレーションの設定

アプライアンスエディタの[デバイス (Device) ] ページには、詳細なデバイス設定および情報が表示されます。また、デバイス設定の一部 (ライセンスの有効化と無効化、デバイスのシャットダウンと再起動、管理の変更、詳細オプションの設定など) を変更することもできます。

### 一般的なデバイスの設定

[デバイス (Device) ] タブの[全般 (General) ] セクションには、以下の表に記載された設定を表示します。

表 50: [全般 (General) ] セクション テーブルのフィールド

フィールド	説明
[名前 (Name) ]	Firepower Management Center でのデバイスの表示名。
パケット転送 (Transfer Packets)	管理対象デバイスがイベントを含むパケットデータを Firepower Management Center に送信するかどうか。
[モード (Mode) ]	デバイスの管理インターフェイスのモード: [ルーテッド (routed) ] または [トランスパレント (transparent) ]。
展開を強制 (Force Deploy)	デバイスのすべてのポリシーおよびデバイス設定の更新を強制的に展開します。

### デバイス ライセンスの設定

[デバイス (Device) ] タブの[ライセンス (License) ] セクションでは、そのデバイスに対して有効になっているライセンスが表示されます。

関連トピック

[Firepower の機能ライセンスについて](#) (137 ページ)

## デバイス システムの設定

[デバイス (Device) ] タブの [システム (System) ] セクションには、次の表に示すように、システム情報の読み取り専用テーブルが表示されます。

表 51: [システム (System) ] セクション テーブルのフィールド

フィールド	説明
モデル	管理対象デバイスのモデル名と番号。
シリアル (Serial)	管理対象デバイスのシャーシのシリアル番号。
時刻 (Time)	デバイスの現在のシステム時刻。
バージョン (Version)	管理対象デバイスに現在インストールされているソフトウェアのバージョン。
ポリシー	管理対象デバイスに現在展開されているプラットフォーム設定ポリシーへのリンク。

デバイスをシャットダウンまたは再起動することもできます。

## デバイス ヘルスの設定

[デバイス (Device) ] タブの [ヘルス (Health) ] セクションには、以下の表に記載された情報を表示します。

表 52: [ヘルス (Health) ] セクション テーブルのフィールド

フィールド	説明
Status	デバイスの現在のヘルス ステータスを表すアイコン。アイコンをクリックすると、アプライアンスのヘルス モニタが表示されます。
ポリシー	現在デバイスで展開されている、読み取り専用バージョンの正常性ポリシーへのリンク。
ブラックリスト	[ヘルス ブラックリスト (Health Blacklist) ] ページへのリンク。このページでは、ヘルス ブラックリスト モジュールを有効または無効に設定できます。

### 関連トピック

[アプライアンス ヘルス モニタの表示 \(297 ページ\)](#)

[正常性ポリシーの編集 \(287 ページ\)](#)

[正常性ポリシー モジュールのブラックリスト登録 \(291 ページ\)](#)



## デバイス管理設定

[デバイス (Device) ] タブの [管理 (Management) ] セクションには、以下の表に記載されたフィールドを表示します。

表 53: [管理 (Management) ] セクション テーブルのフィールド

フィールド	説明
ホスト	デバイスの IP アドレスまたはホスト名。ホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前（つまり、ホスト名）です。
ステータス	Firepower Management Center と管理対象デバイス間の通信チャンネルのステータスを示すアイコン。ステータス アイコンにポインタを置くと、Firepower Management Center が最後にデバイスにアクセスした時間を表示することができます。

## デバイスの詳細設定

[デバイス (Device) ] タブの [詳細設定 (Advanced) ] セクションには、以下で説明する詳細設定のテーブルが表示されます。上記の設定は、いずれも [詳細設定 (Advanced) ] セクションを使用して編集できます。

表 54: [詳細設定 (Advanced) ] セクションのテーブルのフィールド

フィールド	説明	サポートされるデバイス
アプリケーション バイパス (Application Bypass)	デバイスでの自動アプリケーション バイパスの状態。	7000 & 8000 シリーズ、NGIPSv、ASA FirePOWER
バイパスしきい値 (Bypass Threshold)	自動アプリケーション バイパスのしきい値 (ミリ秒)。	7000 & 8000 シリーズ、NGIPSv、ASA FirePOWER
ローカル ルータ トラフィック を検査する (Inspect Local Router Traffic)	デバイスで、ルーテッド インターフェイスで受信した自己宛先とするトラフィック (ICMP、DHCP、および OSPF トラフィックなど) を検査するかどうかを示します。	7000 & 8000 シリーズ
高速パス ルール (Fast-Path Rules)	デバイスで作成されている 8000 シリーズ 高速パス ルールの数。	8000 シリーズ

## デバイス情報の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Network Admin

マルチドメイン展開では、先祖ドメインは、子孫ドメイン内のすべてのデバイスに関する情報を表示できます。デバイスを編集するリーフドメインに位置している必要があります。

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 表示するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、先祖ドメインに位置している場合、表示アイコン (🔍) をクリックすると、読み取り専用モードで子孫ドメインのデバイスを表示できます。

**ステップ 3** [デバイス (Device)] タブをクリックします。

**ステップ 4** 次の情報が表示されます。

- [全般 (General)] : デバイスの一般設定を表示します (一般的なデバイスの設定 (553 ページ) を参照)。
- [ライセンス (License)] : デバイスのライセンス情報を表示します (デバイスライセンスの設定 (553 ページ) を参照)。
- [システム (System)] : デバイスのシステム情報を表示します (デバイスシステムの設定 (554 ページ) を参照)。
- [ヘルス (Health)] : デバイスの現在のヘルスステータスに関する情報を表示します (デバイスヘルスの設定 (554 ページ) を参照)。
- [管理 (Management)] : Firepower Management Center とデバイス間の通信チャンネルに関する情報を表示します (デバイス管理設定 (555 ページ) を参照)。
- [詳細 (Advanced)] : 高度な機能設定に関する情報を表示します (デバイスの詳細設定 (555 ページ) を参照)。

## デバイス管理設定の編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Network Admin



(注) 場合によっては、(デバイスの LCD パネルまたは CLI などを使用して) 別の方法でデバイスのホスト名や IP アドレスを編集する場合は、次の手順を実行して、管理用の Firepower Management Center でホスト名や IP アドレスを手動で更新する必要があります。

#### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 管理オプションを変更するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [デバイス (Device)] タブをクリックします。

ヒント スタック構成のデバイスの場合、アプライアンス エディタの [デバイス (Devices)] ページで、個々のデバイスの管理オプションを変更します。

**ステップ 4** 次の操作を実行できます。

- リモート管理の無効化 : [管理 (Management)] セクションのスライダをクリックして、デバイスの管理を有効または無効にします。管理を無効化すると、Firepower Management Center とデバイス間の接続がブロックされますが、Firepower Management Center からデバイスは削除されません。デバイスを管理する必要がなくなった場合は、[Firepower Management Center からのデバイスの削除 \(552 ページ\)](#) を参照してください。
- 管理ホストの編集 : [管理 (Management)] セクションの編集アイコン (✎) をクリックし、[ホスト (Host)] フィールドで名前または IP アドレスを変更し、[保存 (Save)] をクリックします。この設定を使用して、管理ホスト名を指定したり、仮想 IP アドレスを再生成することができます。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 一般的なデバイス設定の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Network Admin

## 手順

**ステップ1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。

**ステップ2** 変更するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ3** [デバイス (Device) ] をクリックします。

**ステップ4** [一般 (General) ] セクションで、編集アイコン (✎) をクリックします。

**ステップ5** [名前 (Name) ] に、管理対象デバイスの名前を入力します。

**ヒント** スタック構成のデバイスの場合、アプライアンスエディタの[スタック (Stack) ] ページで、スタックでデバイスに割り当てられている名前を編集します。アプライアンスエディタの[デバイス (Devices) ] ページでは、個々のデバイスに割り当てられているデバイス名を編集できます。

**ステップ6** [パケットの転送 (Transfer Packets) ] 設定を変更します。

- パケットデータをイベントと一緒に Firepower Management Center に保存できるようにするには、[パケットの転送 (Transfer Packets) ] チェックボックスをオンにします。
- 管理対象デバイスがイベントと一緒にパケットデータを送信できないようにするには、このチェックボックスをオフにします。

**ステップ7** [強制展開 (Force Deploy) ] をクリックし、デバイスに現在のポリシーとデバイス設定の展開を強制します。

**ステップ8** [保存 (Save) ] をクリックします。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## デバイス ライセンスの有効化と無効化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Network Admin

Firepower Management Center で使用可能なライセンスがある場合、デバイスでそのライセンスを有効にすることができます。

## 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** ライセンスを有効または無効にするデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [デバイス (Device)] タブをクリックします。

**ヒント** スタック構成のデバイスの場合、アプライアンスエディタの[スタック (Stack)] ページで、スタックに対してライセンスを有効または無効にします。

**ステップ 4** [ライセンス (License)] セクションで、編集アイコン (✎) をクリックします。

**ステップ 5** 管理対象デバイスに対して有効または無効にするライセンスの横にあるチェックボックスをオンまたはオフにします。

**ステップ 6** [保存 (Save)] をクリックします。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 関連トピック

[Firepower の機能ライセンスについて \(137 ページ\)](#)

# 詳細なデバイス設定の編集

アプリケーションバイパス、ローカルルータトラフィックのインスペクション、および高速パスのルールを設定できます。

## 自動アプリケーションバイパスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ、 NGIPSv、ASA FirePOWER	リーフのみ	Admin Network Admin

自動アプリケーションバイパス (AAB) 機能は、インターフェイスでのパケット処理時間に制限を設け、この時間を超過した場合、パケットに検出のバイパスを許可します。この機能は任意の展開で使用できますが、インライン展開ではとりわけ価値があります。

パケット処理の遅延は、ネットワークで許容できるパケットレイテンシとバランスを取って調整します。Snort 内での不具合やデバイスの誤った設定が原因で、トラフィックの処理時間が指定のしきい値を超えると、AABにより、その障害発生から10分以内にSnortが再起動され、トラブルシューティングデータが生成されます。このデータを分析することで、過剰な処理時間の原因を調査できます。

一般に、遅延しきい値を超えた後は、高速パスパケットに対して侵入ポリシーの[ルール遅延しきい値 (Rule Latency Thresholding)]を使用します。[ルール遅延しきい値 (Rule Latency Thresholding)]により、エンジンがシャットダウンされたり、しきい値データが生成されることはありません。

検出がバイパスされると、デバイスがヘルス モニタリング アラートを生成します。



**注意** 単一パケットに過剰な処理時間がかかっている場合、AAB がアクティブになります。AAB のアクティブ化は、いくつかのパケットのインスペクションを一時的に中断する Snort プロセスを部分的に再起動します。インスペクションが中断されている間に、パケットがドロップされるかインスペクションを行わずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

## 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** 高度なデバイス設定を編集するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** [デバイス (Device)] タブ (またはスタック構成のデバイスの場合は [スタック (Stack)] タブ) をクリックし、[詳細 (Advanced)] セクションの編集アイコン (✎) をクリックします。
- ステップ 4** [自動アプリケーションバイパス (Automatic Application Bypass)] をオンにします。
- ステップ 5** [バイパスしきい値 (Bypass Threshold)] に 250 ~ 60,000 ミリ秒を入力します。デフォルト設定は 3000 ミリ秒 (ms) です。
- ステップ 6** [保存 (Save)] をクリックします。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ローカルルータ トラフィックの検査

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ローカル内トラフィックがレイヤ3展開のモニタールールと一致する場合、そのトラフィックは検査をバイパスすることがあります。トラフィックの検査を確認するには、[ローカルルータ トラフィックの検査 (Inspect Local Router Traffic)] を有効にします。

### 手順

- ステップ1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ2 高度なデバイス設定を編集するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ3 [デバイス (Devices)] タブ (スタック構成のデバイスの場合は [スタック (Stack)] タブ) をクリックして、[詳細 (Advanced)] セクションの編集アイコン (✎) をクリックします。
- ステップ4 7000 または 8000 シリーズ デバイスがルータとして展開されている場合は、[ローカルルータ トラフィックの検査] をオンにして、例外トラフィックを検査します。
- ステップ5 [保存 (Save)] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 高速パス ルールの設定 (8000 シリーズ)

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	8000 シリーズ	リーフのみ	Admin/Network Admin

トラフィック処理の初期形式として、8000 シリーズ高速パスルールでは、それ以上のインスペクションやロギングを行わずに 8000 シリーズ デバイスを介してトラフィックを直接送信できます。(パッシブ展開では、8000 シリーズ高速パスルールは単に分析を停止します)。各 8000 シリーズ高速パスルールは、特定のセキュリティゾーンまたはインラインインターフェイスセットに適用されます。8000 シリーズ高速パスルールはハードウェア レベルで機能するため、高速パス トラフィックには、次の単純な外部ヘッダーの基準のみを使用できます。

- 発信側および応答側の IP アドレスまたはアドレス ブロック
- プロトコル、および TCP と UDP の場合は、発信側および応答側のポート
- VLAN ID (Admin. VLAN ID)

デフォルトでは、8000 シリーズ高速パス ルールは指定した発信側から指定した応答側への接続に影響します。ルールの基準を満たすすべての接続を高速パス処理するには、どちらのホストが発信側か応答側かに関係なく、ルールを双方向にすることができます。



(注) 同様の機能を実行しますが、8000 シリーズ高速パス ルールはプレフィルタ ポリシーで設定する高速パス トンネルやプレフィルタ ルールに関連しません。

### 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2** ルールを設定する 8000 シリーズデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** [デバイス (Device) ] タブ (またはスタック構成のデバイスの場合は [スタック (Stack) ] タブ) をクリックし、[詳細 (Advanced) ] セクションの編集アイコン (✎) をクリックします。
- ステップ 4** [新しい IPv4 ルール (New IPv4 Rule) ] または [新しい IPv6 ルール (New IPv6 Rule) ] をクリックします。
- ステップ 5** [ドメイン (Domain) ] ドロップダウンリストから、インラインセットまたはパッシブセキュリティゾーンを選択します。
- ステップ 6** 高速パス処理するトラフィックを設定します。トラフィックは高速パス処理のためのすべての条件を満たしている必要があります。
  - [発信側 (Initiator) ] および [応答側 (Responder) ] (必須) : 発信側および応答側の IP アドレスまたはアドレス ブロックを入力します。
  - [プロトコル (Protocol) ] : プロトコルを選択するか、[すべて (All) ] を選択します。
  - [発信側ポート (Initiator Port) ] および [応答側ポート (Responder Port) ] : TCP および UDP トラフィックの場合は、発信側ポートと応答側ポートを入力します。フィールドを空白のままにするか、**Any** と入力して、すべての TCP または UDP トラフィックに一致するようにします。ポートのカンマ区切りリストを入力できますが、ポート範囲を入力することはできません。
  - [VLAN] : VLAN ID を入力します。フィールドを空白のままにするか、**Any** と入力して、VLAN タグに関係なくすべてのトラフィックに一致するようにします。
- ステップ 7** (任意) ルールを [双方向 (Bidirectional) ] にします。



**ステップ 8** [保存 (Save) ]をクリックしてから、もう一度 [保存 (Save) ]をクリックします。

次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## システム シャットダウンの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (ASA FirePOWER を除く)	リーフのみ	Admin/Network Admin



(注) Firepower システムのユーザインターフェイスでは、ASA FirePOWER のシャットダウンまたは再起動はできません。それぞれのデバイスをシャットダウンする方法の詳細については、ASA の資料を参照してください。

手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。

**ステップ 2** 再起動するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [デバイス (Device) ] タブをクリックします。

ヒント スタックに含まれるデバイスの場合、アプライアンスエディタの [デバイス (Devices) ] ページで、個々のデバイスをシャットダウンまたは再起動します。

**ステップ 4** デバイスをシャットダウンするには、[システム (System) ] セクションでデバイスのシャットダウンアイコン (🔴) をクリックします。

**ステップ 5** プロンプトが表示されたら、デバイスのシャットダウンを確認します。

**ステップ 6** デバイスを再起動するには、デバイスの再起動アイコン (🟢) をクリックします。

**ステップ 7** プロンプトが表示されたら、デバイスを再起動することを確認します。

## インターフェイス テーブル ビュー

ハードウェア ビューの下にあるインターフェイス テーブル ビューには、デバイスで使用可能なすべてのインターフェイスが一覧表示されます。テーブル内のナビゲーションツリーを展開すると、設定されているすべてのインターフェイスを表示できます。インターフェイスの横にある矢印アイコンをクリックして、インターフェイスを縮小または展開することで、サブコンポーネントの非表示/表示を切り替えることができます。このインターフェイステーブルビューには、各インターフェイスに関する以下の要約情報が表示されます。

### 従来のデバイスのインターフェイス

[MAC アドレス (MAC Address) ] 列と [IP アドレス (IP Address) ] 列が表示されるのは、8000 シリーズ デバイスのみです。詳細については、次の表を参照してください。

表 55:従来のデバイスのインターフェイス テーブル ビューのフィールド

フィールド	説明
[名前 (Name) ]	

フィールド	説明
	<p>各インターフェイスタイプは、タイプとリンクステート（該当する場合）を示す固有のアイコンによって表されます。名前またはアイコンの上にマウスポインタを移動すると、インターフェイスタイプ、速度、デュプレックスモード（該当する場合）がツールチップに表示されます。インターフェイスアイコンについては、<a href="#">インターフェイスアイコン（577ページ）</a>を参照してください。</p> <p>アイコンでは、インターフェイスの現在のリンク状態を示す表示方法が使用されています。次の3つの状態のいずれかが表示されます。</p> <ul style="list-style-type: none"> <li>• エラー </li> <li>• 障害 </li> <li>• 使用不可 </li> </ul> <p>論理インターフェイスのリンク状態は、親物理インターフェイスのリンク状態と同じです。ASA FirePOWER モジュールには、リンク状態は表示されません。無効化されたインターフェイスは、半透明のアイコンで表されます。</p> <p>アイコンの右側に表示されるインターフェイス名は自動生成されます。ただし、ハイブリッドインターフェイスと ASA FirePOWER インターフェイスの名前はユーザが定義します。ASA FirePOWER インターフェイスについては、名前が付けられており、リンクを持つ有効なインターフェイスのみが表示されることに注意してください。</p> <p>物理インターフェイスでは、物理インターフェイスの名前が表示されます。論理インターフェイスでは、物理インターフェイスの名前と、割り当てられている VLAN タグが表示されます。</p> <p>ASA FirePOWER インターフェイスでは、複数のセキュリティコンテキストがある場合は、セキュリティコンテキストの名前とインターフェイスの名前が表示されます。セキュリティコンテキストが1つしかない場合は、インター</p>

フィールド	説明
	フェイスの名前のみが表示されます。
セキュリティゾーン (Security Zone)	インターフェイスが割り当てられているセキュリティゾーン。セキュリティゾーンを追加または編集するには、編集アイコン (✎) をクリックします。
使用者 (Used by)	インターフェイスが割り当てられているインラインセット、仮想スイッチ、または仮想ルータ。ASA FirePOWER モジュールでは、[使用者 (Used by) ]列は表示されません。
MAC アドレス (MAC Address)	スイッチド機能およびルーテッド機能で有効にされているインターフェイスに対して表示される MAC アドレス。  NGIPSv デバイスの場合、表示された MAC アドレスにより、デバイス上に設定されたネットワーク アダプタと、[インターフェイス (Interfaces) ] ページに表示されるインターフェイスを対応させることができます。ASA FirePOWER モジュールでは、MAC アドレスは表示されません。
IP アドレス	インターフェイスに割り当てられた IP アドレス。マウスのポインタを IP アドレスの上に重ねると、その IP アドレスがアクティブであるか非アクティブであるかを確認できます。非アクティブな IP アドレスはグレー表示されません。ASA FirePOWER モジュールでは、IP アドレスは表示されません。

### Firepower Threat Defense のインターフェイス

表 56: Firepower Threat Defense のインターフェイス テーブル ビューのフィールド

フィールド	説明
インターフェイス (Interface)	インターフェイス ID。フェールオーバーリンクまたはクラスタ制御リンクのインターフェイスの場合、インターフェイス設定は表示専用です。
論理名 (Logical Name)	インターフェイスの構成名。

フィールド	説明
タイプ (Type)	インターフェイスのタイプ : [物理 (Physical) ]、[サブインターフェイス (SubInterface) ]、[EtherChannel]、[冗長 (Redundant) ]、または[ブリッジグループ (BridgeGroup) ] (トランスペアレント ファイアウォール モードのみ)。
インターフェイス オブジェクト (Interface Object)	インターフェイスが割り当てられているセキュリティゾーンまたはインターフェイスグループ。
MACアドレス (MAC Address) (アクティブ/スタンバイ)	インターフェイスの MAC アドレス。ハイ アベイラビリティの場合、アクティブなMACアドレスとスタンバイ状態のMACアドレスの両方が表示されます。
[IPアドレス (IP Address) ]	インターフェイスに割り当てられている IP アドレス。括弧で示されるアドレス割り当てのタイプ : [静的 (Static) ]、[DHCP]、または [PPPoE]。

## デバイス グループ管理

Firepower Management Center でデバイスをグループ化すると、複数のデバイスへのポリシーの展開やアップデートのインストールを簡単に行えます。グループに属するデバイスのリストは、展開または縮小表示できます。デフォルトでは、このリストは縮小表示されます。

マルチドメイン展開では、リーフドメイン内でのみデバイスグループを作成できます。Firepower Management Center をマルチテナンシー向けに設定すると既存のデバイスグループは削除されます。デバイスグループはリーフドメインレベルで再度追加できます。

## デバイス グループの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Network Admin

デバイスグループにより、複数デバイスへのポリシーの割り当てとインストール更新が簡単に行えます。

スタック内または高可用性ペア内のプライマリデバイスをグループに追加すると、両方のデバイスがグループに追加されます。デバイスのスタック構成を解除または高可用性ペアを分解しても、これらのデバイスは両方ともグループに属したままになります。

手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 [追加 (Add)] ドロップダウンメニューから、[グループの追加 (Add Group)] を選択します。
- ステップ 3 名前を入力します。
- ステップ 4 [使用可能なデバイス (Available Devices)] から、デバイスグループに追加するデバイスを 1 つ以上選択します。複数のデバイスを選択する場合は、Ctrl または Shift キーを押しながらかリックします。
- ステップ 5 [追加 (Add)] をクリックして、選択したデバイスをデバイスグループに追加します。
- ステップ 6 [OK] をクリックして、デバイスグループを追加します。

## デバイスグループの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Network Admin

任意のデバイスグループに含まれる一連のデバイスを変更できます。アプライアンスは、現行のグループから削除してからでないと、新しいグループに追加できません。

アプライアンスを新しいグループに移動しても、そのアプライアンスのポリシーが、新しいグループにすでに割り当てられているポリシーに変更される訳ではありません。グループのポリシーを新しいデバイスに割り当てする必要があります。

スタック内またはデバイスのハイアベイラビリティペア内のプライマリデバイスをグループに追加すると、両方のデバイスがグループに追加されます。デバイスのスタック構成を解除または高可用性ペアを分解しても、これらのデバイスは両方ともグループに属したままになります。

マルチドメイン展開では、デバイスグループは、それらが作成されたドメイン内でのみ編集できます。

手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 編集するデバイスグループの横にある編集アイコン (✎) をクリックします。

- ステップ3** 必要に応じて、[名前 (Name)] フィールドに、グループの新しい名前を入力します。
- ステップ4** [使用可能なデバイス (Available Devices)] から、デバイスグループに追加するデバイスを1つ以上選択します。複数のデバイスを選択する場合は、Ctrl または Shift キーを押しながらクリックします。
- ステップ5** [追加 (Add)] をクリックして、選択したデバイスをデバイスグループに追加します。
- ステップ6** 必要に応じて、デバイスグループからデバイスを削除するには、削除するデバイスの横にある削除アイコン (🗑️) をクリックします。
- ステップ7** [OK] をクリックして、デバイスグループに加えた変更を保存します。
-





## 第 **VI** 部

# クラシック デバイス設定の基本

- 従来型デバイスの管理の基本 (573 ページ)
- IPS デバイスの展開と設定 (587 ページ)





## 第 22 章

# 従来型デバイスの管理の基本

次のトピックでは、Firepower システムで従来型デバイス（7000 および 8000 シリーズ デバイス、ASA with FirePOWER サービス、NGIPSv）を管理する方法について説明します。

- [リモート管理の設定（573 ページ）](#)
- [インターフェイス構成時の設定（576 ページ）](#)

## リモート管理の設定

Firepower System デバイスを管理できるようにするには、デバイスと Firepower Management Center との間に双方向の SSL 暗号化通信チャンネルをセットアップする必要があります。このチャンネルを使用して、両方のアプライアンスが設定とイベント情報を共有します。ハイアベイラビリティピアも、このチャンネルを使用します。このチャンネルは、デフォルトではポート 8305/tcp に位置します。



(注) この章では、FMCにデバイスを登録する前にローカルWebインターフェイスを使用して、7000 または 8000 シリーズ デバイスのリモート管理の設定方法について説明します。他のモデルのリモート管理の設定の詳細については、適切なクイックスタートガイドを参照してください。

2つのアプライアンス間の通信を可能にするためには、アプライアンスが互いを認識する手段を提供しなければなりません。Firepower System では3つの基準を使用して、通信を許可します。

- 通信を確立する対象のアプライアンスのホスト名または IP アドレス。  
NAT 環境では、ルーティング可能なアドレスがもう一方のアプライアンスにないとしても、リモート管理を設定する際、または管理対象アプライアンスを追加する際には、ホスト名または IP アドレスのいずれかを指定する必要があります。
- 接続を識別するために自己生成される、最大 37 文字の英数字による登録キー。
- Firepower System が NAT 環境で通信を確立するために利用できるオプションの一意の英数字による NAT ID。

NAT ID は、管理対象アプライアンスを登録するために使用されているすべての NAT ID の間で一意でなければなりません。

## 管理対象デバイス上のリモート管理の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	該当なし	Admin/Network Admin

### 手順

**ステップ 1** 管理するデバイスの Web インターフェイスで、[設定 (Configuration)] > [ASA FirePOWER の設定 (ASA FirePOWER Configuration)] > [統合 (Integration)] > [リモート管理 (Remote Management)] を選択します。

**ステップ 2** [リモート管理 (Remote Management)] タブが表示されていない場合は、クリックします。

**ステップ 3** [マネージャの追加 (Add Manager)] をクリックします。

**ステップ 4** [管理ホスト (Management Host)] フィールドに、このアプライアンスを管理するために使用する Firepower Management Center について、次のいずれかを入力します。

- IP アドレス
- 完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前 (つまり、ホスト名)

**注意** ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

NAT 環境では、管理対象アプライアンスを追加する際に IP アドレスまたはホスト名を指定する予定の場合、ここで IP アドレスまたはホスト名を指定する必要はありません。その場合、Firepower システムは後で指定される NAT ID を使用して、管理対象アプライアンスの Web インターフェイス上のリモート マネージャを識別します。

**ステップ 5** [登録キー (Registration Key)] フィールドに、アプライアンス間の通信をセットアップするために使用する登録キーを入力します。

**ステップ 6** NAT 環境の場合は、[固有 NAT ID (Unique NAT ID)] フィールドに、アプライアンス間の通信をセットアップするために使用する、英数字による一意の NAT ID を入力します。

**ステップ 7** [保存 (Save)] をクリックします。

### 次のタスク

- アプライアンスが相互に通信できることを確認し、ステータスとして [登録保留 (Pending Registration)] が表示されるまで待ちます。

- このデバイスを Firepower Management Center に追加します。 [Firepower Management Center へのデバイスの追加 \(550 ページ\)](#) を参照してください。

## 管理対象デバイスでのリモート管理の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	該当なし	Admin/Network Admin

リモート マネージャを編集するには、次の点に注意してください。

- [ホスト (Host) ] フィールドでは、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前（つまり、ホスト名）を指定します。
- [名前 (Name) ] フィールドには、Firepower システムのコンテキストでのみ使用される、管理アプライアンスの表示名を指定します。別の表示名を入力しても、管理デバイスのホスト名は変更されません。

### 手順

**ステップ 1** デバイスの Web インターフェイスで、[システム (System) ] > [統合 (Integration) ] を選択します。

**ステップ 2** まだ表示されていない場合は、[リモート管理 (Remote Management) ] タブをクリックします。

**ステップ 3** 次の操作を実行できます。

- リモート管理の無効化：マネージャの横にあるスライダをクリックして、これを有効または無効にします。管理を無効化すると、Firepower Management Center とデバイス間の接続がブロックされますが、Firepower Management Center からデバイスは削除されません。デバイスを管理する必要がなくなった場合は、[Firepower Management Center からのデバイスの削除 \(552 ページ\)](#) を参照してください。
- マネージャ情報の編集：変更するマネージャの横にある編集アイコン (✎) をクリックして、[名前 (Name) ] および [ホスト (Host) ] フィールドをクリックし、[保存 (Save) ] をクリックします。

## 管理ポートの変更

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ Management Center	グローバルだけ	Admin/Network Admin

アプライアンスは、双方向の SSL 暗号化通信チャネルを使用して通信します。このチャネルは、デフォルトではポート 8305 に位置します。

設定をデフォルトのままにすることを強く奨励します。管理ポートがネットワークでの他の通信と競合する場合には、他のポートを選択できます。通常、管理ポートの変更は、Firepower System のインストール時に行います。



**注意** 管理ポートを変更する場合は、導入内の相互に通信する必要があるすべてのアプライアンスの管理ポートを変更する必要があります。

### 手順

- ステップ 1 [システム (System)] > [設定 (Configuration)] を選択します。
- ステップ 2 [管理インターフェイス (Management Interfaces)] をクリックします。
- ステップ 3 [共有設定 (Shared Settings)] セクションで、[リモート管理ポート (Remote Management Port)] フィールドに使用するポート番号を入力します。
- ステップ 4 [保存 (Save)] をクリックします。

### 次のタスク

- このアプライアンスと通信する必要がある、展開環境内のすべてのアプライアンスについて、この手順を繰り返します。

## インターフェイス構成時の設定

アプライアンスエディタの [インターフェイス (Interfaces)] ページには、詳細なインターフェイス設定情報が表示されます。このページは、物理ハードウェア ビューとインターフェイス テーブルビューで構成されており、構成の詳細情報にドリルダウンできます。このページからインターフェイスを追加したり編集したりできます。

## 物理的なハードウェア ビュー





[ インターフェイス (Interfaces) ] ページの一番上には、7000 または 8000 シリーズ デバイスの物理的なハードウェア ビューがグラフィカル表示されます。






物理的なハードウェア ビューは、次の目的で使用します。

- ネットワーク モジュールのタイプ、部品番号、およびシリアル番号を確認する
- インターフェイス テーブル ビューでインターフェイスを選択する
- インターフェイス エディタを開く
- インターフェイスの名前、タイプ、リンクの有無、速度設定、およびインターフェイスがバイパス モードになっているかを確認する
- エラーまたは警告の詳細を参照する

## インターフェイス アイコン

表 57: インターフェイス アイコンのタイプと説明

アイコン	インターフェイス タイプ	詳細
	物理的：未設定の物理インターフェイス。	物理スイッチドインターフェイスの設定 (1223 ページ) または物理ルーテッドインターフェイスの設定 (1235 ページ)
	パッシブ：パッシブ展開でトラフィックを分析するように設定されているセンシングインターフェイス。	パッシブ インターフェイスの設定 (588 ページ)
	インライン：インライン展開でトラフィックを処理するように設定されているセンシングインターフェイス。	インラインインターフェイスの設定 (592 ページ)
	スイッチド：レイヤ 2 展開でトラフィックを切り替えるように設定されているインターフェイス。	スイッチドインターフェイスの設定 (1222 ページ)
	ルーテッド：レイヤ 3 展開でトラフィックをルーティングするように設定されているインターフェイス。	ルーテッドインターフェイス (1234 ページ)

アイコン	インターフェイス タイプ	詳細
	集約：1つの論理リンクとして設定されている複数の物理インターフェイス。	<a href="#">集約インターフェイスについて (1273 ページ)</a>
	集約スイッチド：レイヤ2 展開で1つの論理リンクとして設定されている複数の物理インターフェイス。	<a href="#">集約スイッチドインターフェイスの追加 (1280 ページ)</a>
	集約ルーテッド：レイヤ3 展開で1つの論理リンクとして設定されている複数の物理インターフェイス。	<a href="#">集約ルーテッドインターフェイスの追加 (1283 ページ)</a>
	ハイブリッド：仮想ルータと仮想スイッチ間でトラフィックをブリッジするように設定されている論理インターフェイス。	<a href="#">論理ハイブリッドインターフェイス (1291 ページ)</a>
	ASA FirePOWER：ASA FirePOWER モジュールがインストールされた ASA デバイスに設定されているインターフェイス。	<a href="#">Cisco ASA FirePOWER インターフェイスの管理 (583 ページ)</a>

## 物理ハードウェアビューの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 管理するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** グラフィカルインターフェイスを使用して、以下を実行できます。



- **選択**：インターフェイスを選択する場合、インターフェイスアイコンをクリックします。システムは、インターフェイス テーブルの関連項目を強調表示します。
- **編集**：インターフェイスエディタを開く場合、インターフェイスアイコンをダブルクリックします。
- **エラーまたは警告情報の表示**：エラーまたは警告に関する詳細を表示するには、ネットワーク モジュール上の影響を受けるポートの上にカーソルを置きます。
- **インターフェイス情報の表示**：インターフェイスの名前、インターフェイスのタイプ、インターフェイスにリンク画が存在するかどうか、インターフェイスの速度設定、インターフェイスが現在バイパスモードであるかどうかについて表示するには、インターフェイス上にカーソルを置きます。
- **ネットワーク モジュール情報の表示**：ネットワーク モジュールのタイプ、製品番号、シリアル番号を表示するには、ネットワーク モジュールの左下隅にある黒い円の上にカーソルを置きます。

## センシング インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	従来型 (Classic)	リーフのみ	Admin/Network Admin

アプライアンス エディタの [インターフェイス (Interfaces) ] ページで、Firepower システムの展開に応じて、管理対象デバイスのセンシングインターフェイスを設定できます。管理対象デバイスには、合計 1024 個のインターフェイスを設定できることに注意してください。



(注) Firepower Management Center では、ASA FirePOWER が SPAN ポート モードで展開されている場合、ASA インターフェイスを表示しません。

### 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2** インターフェイスを設定するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** 設定するインターフェイスの横にある編集アイコン (✎) をクリックします。
- ステップ 4** インターフェイス エディタを使用して、センシング インターフェイスを設定します。

- [HA リンク (HALink) ]: デバイスのハイアベイラビリティペアの各メンバーに設定されたインターフェイスを、(ハイアベイラビリティリンクインターフェイスとも呼ばれる) デバイス間の冗長通信チャネルとして機能させるには、[HA リンク (HALink) ]をクリックし、[HA リンク インターフェイスの設定 \(580 ページ\)](#) の説明に従って続行します。
- [インライン (Inline) ]: 設定されたインターフェイスでインライン展開のトラフィックを処理するように設定するには、[インライン (Inline) ]をクリックし、[インラインインターフェイスの設定 \(592 ページ\)](#) の説明に従って続行します。
- [パッシブ (Passive) ]: 設定されたインターフェイスでパッシブ展開のトラフィックを分析するように設定するには、[パッシブ (Passive) ]をクリックし、[パッシブインターフェイスの設定 \(588 ページ\)](#) の説明に従って続行します。
- [ルーテッド (Routed) ]: 設定されたインターフェイスでレイヤ 3 展開のトラフィックをルーティングするように設定するには、[ルーテッド (Routed) ]をクリックし、[ルーテッドインターフェイス \(1234 ページ\)](#) の説明に従って続行します。
- [スイッチド (Switched) ]: 設定されたインターフェイスでレイヤ 2 展開のトラフィックをスイッチングするように設定するには、[スイッチド (Switched) ]をクリックし、[スイッチドインターフェイスの設定 \(1222 ページ\)](#) の説明に従って続行します。

ステップ 5 [保存 (Save) ]をクリックして構成を完了します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## HA リンク インターフェイスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

7000 または 8000 シリーズデバイスの高可用性ペアを確立した後、物理インターフェイスをハイアベイラビリティ (HA) リンク インターフェイスとして設定する必要があります。このリンクは、ペアリングされたデバイス間でヘルス情報を共有するために使用する、冗長通信チャネルとして機能します。1つのデバイスに HA リンク インターフェイスを設定すると、自動的に2番目のデバイスにインターフェイスが設定されます。同じブロードキャストドメインに、両方の HA リンクを設定する必要があります。

ダイナミック NAT は、他の IP アドレスとポートにマップする IP アドレスとポートの動的割り当てに依存します。HA リンクがなければ、これらのマッピングはフェールオーバーで失われます。その場合、変換されたすべての接続は高可用性ペアで新しくアクティブになったデバイスを介してルーティングされることになるため、それらの接続は失敗します。

同様に、高可用性状態共有、ダイナミック NAT、または VPN が設定された 7000 または 8000 シリーズ デバイスには、HA リンク インターフェイスが必要です。

## 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。

**ステップ 2** HA リンク インターフェイスを設定するピアの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** HA リンク インターフェイスとして設定するインターフェイスの横にある編集アイコン (✎) をクリックします。

**ステップ 4** [HA リンク (HA Link) ] をクリックします。

**ステップ 5** [有効 (Enabled) ] チェックボックスをオンにします。

(注) チェックボックスをオフにした場合、システムはインターフェイスを管理上停止し、無効にします。

**ステップ 6** [モード (Mode) ] ドロップダウン リストからリンク モードを指定するオプションを選択するか、[自動ネゴシエーション (Autonegotiation) ] を選択して、速度とデュプレックスの設定を自動ネゴシエートするようにインターフェイスを設定します。

**ステップ 7** [MDI/MDIX] ドロップダウンリストから、インターフェイスの設定対象として MDI (メディア依存型インターフェイス) 、MDIX (メディア依存型インターフェイスクロスオーバー) 、または自動 MDIX のいずれかを指定するオプションを選択します。

(注) 通常、[MDI/MDIX] は [自動 MDIX (Auto-MDIX) ] に設定します。これにより、MDI と MDIX の間の切り替えが自動的に処理され、リンクが確立されます。

**ステップ 8** [MTU] フィールドに最大伝送ユニット (MTU) を入力します。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。詳細については、[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 \(584 ページ\)](#) を参照してください。

**注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

ステップ9 [保存 (Save) ]をクリックします。

#### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[Snort® の再起動シナリオ \(354 ページ\)](#)

[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 \(584 ページ\)](#)

## インターフェイスの無効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ NGIPSv	リーフのみ	Admin/Network Admin

インターフェイス タイプを [なし (None) ] に設定することで、インターフェイスを無効にすることができます。無効にされたインターフェイスは、インターフェイスリストでグレー表示されます。

#### 手順

ステップ1 [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。

ステップ2 インターフェイスを無効にするデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ3 無効にするインターフェイスの横にある編集アイコン (✎) をクリックします。

ステップ4 [なし (None) ] をクリックします。

ステップ5 [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## Cisco ASA FirePOWER インターフェイスの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	ASA FirePOWER	リーフのみ	Admin/Network Admin

ASA FirePOWER インターフェイスを編集する際に、Firepower Management Center から設定できるのは、インターフェイスのセキュリティゾーンのみです。

ASA FirePOWER インターフェイスを完全に設定するには、ASA 専用ソフトウェアおよび CLI を使用します。ASA FirePOWER およびスイッチを編集して、マルチコンテキストモードからシングルコンテキストモード（またはその逆）に切り替えると、ASA FirePOWER はそのインターフェイスの名前をすべて変更します。ASA FirePOWER の更新されたインターフェイス名を使用するように、すべての Firepower System セキュリティゾーン、相関ルール、関連する設定を再設定する必要があります。ASA FirePOWER インターフェイスの設定の詳細については、ASA のマニュアルを参照してください。



- (注) ASA FirePOWER インターフェイスのタイプは変更できません。また、Firepower Management Center からインターフェイスを無効にすることもできません。

### 手順

- ステップ 1 [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2 インターフェイスを編集するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3 [インターフェイス (Interfaces) ] タブが表示されていない場合は、そのタブをクリックします。
- ステップ 4 編集するインターフェイスの横にある編集アイコン (✎) をクリックします。
- ステップ 5 [セキュリティゾーン (Security Zone) ] ドロップダウンリストから既存のセキュリティゾーンを選択するか、[新規 (New) ] を選択して新しいセキュリティゾーンを追加します。
- ステップ 6 [保存 (Save) ] をクリックして、セキュリティゾーンを設定します。

### 次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

## 7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲

デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。



(注) システムは、設定された MTU 値から 18 バイトを切り捨てます。594 より小さい IPv4 MTU または 1298 より小さい IPv6 MTU を設定しないでください。

従来のデバイス モデル	MTU 範囲
7000 & 8000 シリーズ	576 ~ 9234 (管理インターフェイス) 576 ~ 10172 (インライン セット、パッシブ インターフェイス) 576 ~ 9922 (その他)
NGIPSv	576 ~ 9018 (すべてのインターフェイス、インライン セット)

### 関連トピック

[MTU について \(684 ページ\)](#)

## セキュリティ ゾーンオブジェクトのリビジョンの同期

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	7000 & 8000 シリーズ NGIPSv	リーフのみ	Admin/Network Admin

セキュリティゾーンオブジェクトを更新すると、システムはそのオブジェクトの新しいリビジョンを保存します。その結果、同じセキュリティゾーン内の管理対象デバイスに、インターフェイスで設定されたセキュリティオブジェクトの異なるリビジョンがある場合、接続が重複しているようなログが記録される可能性があります。

接続の重複が報告されていることに気づいた場合、同じリビジョンのオブジェクトを使用するよう、すべての管理対象デバイスを更新できます。

## 手順

- 
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** セキュリティ ゾーンを選択を更新するデバイスの横にある編集アイコン (✎) をクリックします。
- マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** 重複する接続のイベントを記録しているインターフェイスのそれぞれについて、[セキュリティゾーン (Security Zone)] を別のゾーンに変更して [保存 (Save)] をクリックした後、目的のゾーンに再び設定し、もう一度 [保存 (Save)] をクリックします。
- ステップ 4** 重複イベントを記録しているデバイスごとに、ステップ 2 から 3 を繰り返します。続行する前に、すべてのデバイスを編集する必要があります。
- 

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。



---

**注意** 同期させるすべてのデバイスでインターフェイスのゾーン設定を編集するまでは、デバイスに設定変更を展開しないでください。すべての管理対象デバイスに同時に展開する必要があります。

---







## 第 23 章

# IPS デバイスの展開と設定

以下のトピックでは、IPS 展開でデバイスを設定する方法について説明します。

- [IPS デバイスの展開と設定の概要 \(587 ページ\)](#)
- [パッシブ IPS 展開 \(587 ページ\)](#)
- [インライン IPS 展開 \(590 ページ\)](#)

## IPS デバイスの展開と設定の概要

パッシブまたはインラインのいずれかの IPS 展開でデバイスを設定できます。パッシブ展開では、ネットワークトラフィックのフローからアウトオブバンドでシステムを展開します。インライン展開では、2つのポートを一緒にバインドすることで、ネットワークセグメント上でシステムを透過的に設定します。

## パッシブ IPS 展開

パッシブ（受動）IPS 展開では、Firepower システムはスイッチ SPAN またはミラー ポートを使用してネットワークを流れるトラフィックをモニタします。SPAN またはミラー ポートでは、スイッチ上の他のポートからトラフィックをコピーできます。これにより、ネットワークトラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション（トラフィックのブロッキングやシェーピングなど）を実行することができません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。



- (注) アウトバウンドトラフィックにはフロー制御パケットが含まれています。そのため、アプライアンスのパッシブインターフェイスにアウトバウンドトラフィックが表示されることがあり、設定によっては、イベントが生成されることもあります。これは正常な動作です。

## Firepower システムのパッシブインターフェイス

管理対象デバイス上の 1 つ以上の物理ポートをパッシブインターフェイスとして設定できません。

パッシブインターフェイスがトラフィックをモニタすることを可能にする場合、銅線インターフェイスでのみ使用可能なモードおよび MDI/MDIX 設定を指定します。8000 シリーズアプライアンスのインターフェイスは、半二重オプションをサポートしません。

パッシブインターフェイスを無効にする場合、ユーザはセキュリティのためにアクセスできなくなります。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイスタイプによって異なる場合があります。



**注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### 関連トピック

[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 \(584 ページ\)](#)

[Snort® の再起動シナリオ \(354 ページ\)](#)

## パッシブインターフェイスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** パッシブインターフェイスを設定するデバイスの横にある編集アイコン (✎) をクリックします。
- マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

- ステップ 3** パッシブ インターフェイスとして設定するインターフェイスの横にある編集アイコン (✎) をクリックします。
- ステップ 4** [パッシブ (Passive) ] をクリックします。
- ステップ 5** セキュリティ ゾーンにパッシブ インターフェイスを関連付けるには、次のいずれかを実行します。
- [セキュリティ ゾーン (Security Zone) ] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
  - [新規 (New) ] を選択して、新しいセキュリティ ゾーンを追加します。 [セキュリティゾーンおよびインターフェイスグループオブジェクトの作成 \(438 ページ\)](#) を参照してください。
- ステップ 6** [有効 (Enabled) ] チェックボックスをオンにします。
- このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。
- ステップ 7** 7000 & 8000 シリーズのみ : [モード (Mode) ] ドロップダウン リストからリンク モードを指定するか、または [自動ネゴシエーション (Auto Negotiation) ] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようにインターフェイスを設定します。
- モード設定は銅線インターフェイスにのみ使用できます。
- 8000 シリーズアプライアンスのインターフェイスは、半二重オプションをサポートしません。
- ステップ 8** 7000 & 8000 シリーズのみ : [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI (メディア依存型インターフェイス) 、 MDIX (メディア依存型インターフェイス クロスオーバー) 、または自動 MDIX のいずれかを指定します。
- [MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。
- デフォルトでは、[MDI/MDIX] は [自動 MDIX (Auto-MDIX) ] に設定され、MDI と MDIX の間の切り替えを自動的に処理してリンクを確立します。
- ステップ 9** [MTU] フィールドに最大伝送ユニット (MTU) を入力します。
- MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。
- 注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。
- ステップ 10** [保存 (Save) ] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## インライン IPS 展開

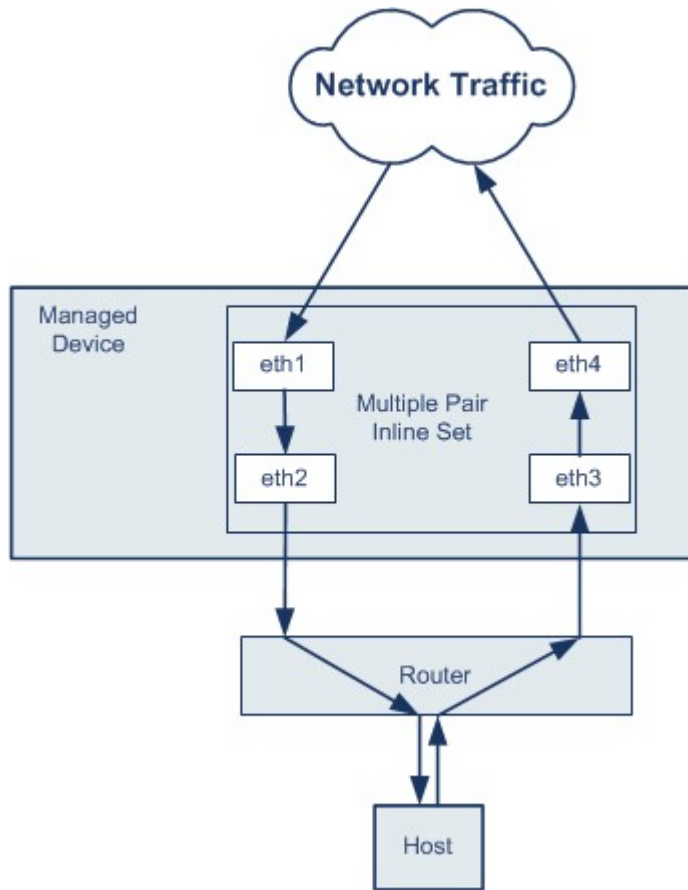
インライン IPS 展開では、2つのポートを一緒にバインドすることで、ネットワーク セグメント上で Firepower システムを透過的に設定します。これによって、隣接するネットワーク デバイスの設定がなくても、任意のネットワーク環境にシステムをインストールすることができます。インラインインターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インラインセットの外部に再送信されます。



(注) システムがトラフィックに影響を与えるためには、ルーテッド、スイッチド、トランスペアレント インターフェイスまたはインライン インターフェイスのペアを使用して関連する設定を管理対象デバイスに展開する必要があります。

デバイストラフィックがインバウンドであるかアウトバウンドであるかに応じて、異なるインライン インターフェイス ペアを介してネットワーク上のホストと外部ホスト間のトラフィックをルーティングするように、管理対象デバイスのインターフェイスを設定できます。これは非同期ルーティング設定です。非同期ルーティングを展開し、インラインセットに1つのインターフェイスペアしか含めないと、デバイスがトラフィックの半分しか認識しないため、ネットワークトラフィックが適切に分析されない可能性があります。同じインラインインターフェイスセットに複数のインライン インターフェイス ペアを追加すると、システムがインバウンドトラフィックとアウトバウンドトラフィックを同じトラフィック フローの一部として識別できるようになります。これは、同じセキュリティゾーンにインターフェイス ペアを含めることによっても実現できます。

非同期ルーティング構成を通過するトラフィックから接続イベントが生成された場合、そのイベントは同じインライン インターフェイス ペアの入力インターフェイスと出力インターフェイスを識別できます。たとえば、次の図の構成では、**eth3**を入力インターフェイス、**eth2**を出力インターフェイスとして識別する接続イベントが生成されます。これは、この構成の予期される動作です。



- (注) 単一のインライン インターフェイス セットに複数のインターフェイス ペアを割り当てたときに、重複トラフィックの問題が発生した場合は、システムがパケットを一意に識別できるように再設定します。たとえば、別のインラインセットにインターフェイス ペアを再度割り当てるか、セキュリティゾーンを変更することができます。

インラインセットを使用するデバイスでは、デバイス再起動後にパケットを転送するようソフトウェアブリッジが自動的にセットアップされます。デバイスが再起動しているときには、実行中のソフトウェアブリッジがありません。インラインセットでバイパスモードを有効にすると、デバイスの再起動中にハードウェアバイパスになります。その場合、システムが停止して再起動する際に、デバイスとのリンクの再ネゴシエーションが原因で数秒間のパケットが失われる可能性があります。ただし、Snort®の再起動中にシステムはトラフィックを通過させます。

#### 関連トピック

[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲](#) (584 ページ)

[Snort® の再起動シナリオ](#) (354 ページ)

## Firepower システムのインライン インターフェイス

管理対象デバイス上の1つ以上の物理ポートをインラインインターフェイスとして設定できます。インラインインターフェイスがインライン展開環境のトラフィックを処理するには、その前に、インラインインターフェイスのペアをインラインセットに割り当てる必要があります。

(注)

- インライン ペアのインターフェイスをそれぞれ異なる速度に設定した場合、またはインターフェイスが異なる速度にネゴシエートされる場合は、システムによって警告が出されます。
- インターフェイスをインラインインターフェイスとして設定すると、そのインターフェイスのNetMod上の隣接ポートも自動的にインラインインターフェイスとなり、インラインインターフェイスのペアが完成します。
- NGIPSv デバイスでインラインインターフェイスを設定するには、隣接するインターフェイスを使用してインラインペアを作成する必要があります。

## インライン インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** インターフェイスを設定するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** 設定するインターフェイスの横にある編集アイコン (✎) をクリックします。
- ステップ 4** [インライン (Inline)] をクリックします。
- ステップ 5** インライン インターフェイスをセキュリティゾーンと関連付ける場合は、次のいずれかを実行します。
  - [セキュリティゾーン (Security Zone)] ドロップダウン リストから既存のセキュリティゾーンを選択します。
  - [新規 (New)] を選択して、新しいセキュリティゾーンを追加します。[セキュリティゾーンおよびインターフェイスグループオブジェクトの作成 \(438 ページ\)](#) を参照してください。

- ステップ 6** [インラインセット (Inline Set) ] ドロップダウン リストから既存のインラインセットを選択するか、[新規 (New) ] を選択して新しいインラインセットを追加します。
- (注) 新しいインラインセットを追加する場合は、インライン インターフェイスを設定した後、設定する必要があります。 [インラインセットの追加 \(595 ページ\)](#) を参照してください。
- ステップ 7** [有効 (Enabled) ] チェックボックスをオンにします。
- このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。
- ステップ 8** 7000 & 8000 シリーズのみ : [モード (Mode) ] ドロップダウン リストからリンク モードを指定するか、または[自動ネゴシエーション (AutoNegotiation) ] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようにインターフェイスを設定します。
- モード設定は銅線インターフェイスにのみ使用できます。
- 8000 シリーズアプライアンスのインターフェイスは、半二重オプションをサポートしません。
- ステップ 9** 7000 & 8000 シリーズのみ : [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI (メディア依存型インターフェイス) 、 MDIX (メディア依存型インターフェイス クロスオーバー) 、または自動 MDIX のいずれかを指定します。
- [MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。
- デフォルトでは、[MDI/MDIX]は[自動 MDIX (Auto-MDIX) ]に設定され、MDI と MDIX の間の切り替えを自動的に処理してリンクを確立します。
- ステップ 10** [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## Firepower システムのインラインセット

インライン展開でインライン インターフェイスを使用するには、事前に、インラインセットを設定してインライン インターフェイス ペアをそれらに割り当てる必要があります。インラインセットは、デバイス上の 1 つ以上のインライン インターフェイス ペアからなるグループです。インライン インターフェイス ペアは、一度に 1 つのインラインセットにのみ属することができます。

[デバイス管理 (Device Management) ] ページの [インラインセット (Inline Sets) ] タブには、デバイスに設定されているすべてのインラインセットのリストが表示されます。

[デバイスの管理 (Device Management) ] ページの [インラインセット (Inline Sets) ] タブからインラインセットを追加できます。または、インライン インターフェイスを設定するときにインラインセットを追加できます。

インラインセットにはインライン インターフェイス ペアのみを割り当てることができます。管理対象デバイスでインライン インターフェイスを設定する前にインラインセットを作成する必要がある場合は、空のインラインセットを作成し、後からそれにインターフェイスを追加できます。インラインセットの名前を入力する場合は、英数字とスペースを使用できます。

### 【名前 (Name)】

インラインセットの名前。

### インターフェイス

インラインセットに割り当てられているすべてのインラインペアのリスト。[インターフェイス (Interfaces)] タブでペアのいずれかのインターフェイスを無効にした場合、そのペアは含まれません。

### MTU

インラインセットの最大伝送ユニット。MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。



**注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### フェールセーフ (Failsafe)

トラフィックに検出のバイパスと、デバイス経由の続行を許可します。管理対象デバイスは、内部トラフィックバッファをモニタし、それらのバッファが満杯である場合は検出をバイパスします。

### バイパス モード (Bypass Mode)

Firepower 7000 または 8000 シリーズのみ：インラインセットの設定済みバイパス モード。この設定により、インターフェイスに障害が発生した場合のインライン インターフェイスのリレーの応答方法が決まります。バイパスモードは、トラフィックがインターフェイスを通過し続けることを許可します。非バイパスモードは、トラフィックをブロックします。



**注意** バイパス モードでは、アプライアンスの再起動時に少数のパケットが失われることがあります。高可用性ペアの 7000 または 8000 シリーズ デバイスのインラインセット、NGIPSv デバイスのインラインセット、8000 シリーズ デバイスの非バイパス NetMod、Firepower 7115 または 7125 デバイスの SFP モジュールには、バイパス モードを設定できません。



## 関連トピック

[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲](#) (584 ページ)

[Snort® の再起動シナリオ](#) (354 ページ)

## インラインセットの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Network Admin

## 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** インラインセットを表示するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [インラインセット (Inline Sets)] タブをクリックします。

## インラインセットの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

## 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** インラインセットを追加するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [インラインセット (Inline Sets)] タブをクリックします。

**ステップ 4** [インラインセットの追加 (Add Inline Set)] をクリックします。

**ステップ 5** 名前を入力します。

**ステップ 6** [インターフェイス (Interfaces)] の横で、1つ以上のインラインインターフェイスペアを選択し、選択項目の追加アイコン (➡) をクリックします。すべてのインターフェイス ペアをインラインセットに追加するには、「すべてを追加」アイコン (➡) をクリックします。

**ヒント** インラインセットからインラインインターフェイスを削除するには、1つ以上のインライン インターフェイス ペアを選択して、選択項目の削除アイコン (←) をクリックします。インラインセットからすべてのインターフェイス ペアを削除するには、「すべてを削除」アイコン (←) をクリックします。また、[インターフェイス (Interfaces)] タブでペアのいずれかのインターフェイスを無効にすると、ペアが削除されます。

**ステップ 7** [MTU] フィールドに最大伝送ユニット (MTU) を入力します。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

**注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

**ステップ 8** に検出をバイパスさせ、デバイスにトラフィックを通すには、[フェールセーフ (Failsafe)] を選択します。

管理対象デバイスは、内部トラフィックバッファをモニタし、それらのバッファが満杯である場合は検出をバイパスします。

内部トラフィックバッファがいっぱいになったが、特定の状況下でデバイスがまだパケットをドロップする可能性がある場合は、インラインセットでデバイスの[フェールセーフ (Failsafe)] を有効にすると、ドロップされたパケットのリスクが大幅に軽減されます。最悪の場合は、デバイスで一時的にネットワークが停止することがあります。

**ステップ 9** 7000 および 8000 シリーズ の場合のみ、バイパス モードを指定します:

- トラフィックがインターフェイスを通過し続けることを許可するには、[バイパス (Bypass)] をクリックします。
- トラフィックをブロックするには、[バイパスしない (Non-Bypass)] をクリックします。

(注) 高可用性ペアの 7000 または 8000 シリーズ デバイスのインラインセット、NGIPSv デバイスのインラインセット、8000 シリーズ デバイスの非バイパス ネットワーク モジュール、Firepower 7115 または 7125 デバイスの SFP モジュールには、バイパス モードを設定できません。

- ステップ 10** 必要に応じて、詳細な設定を行います。 [インラインセットの詳細オプション \(597 ページ\)](#) を参照してください。
- ステップ 11** [OK] をクリックします。

#### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

- [7000 および 8000 シリーズ デバイスおよび NGIPsv の MTU 範囲 \(584 ページ\)](#)
- [Snort® の再起動シナリオ \(354 ページ\)](#)

## インラインセットの詳細オプション

インラインセットを設定する際に考慮できる詳細オプションがいくつかあります。

#### タップモード

7000 および 8000 シリーズ デバイスでは、インライン（またはフェールオープン可能なインライン） インターフェイス セットを作成するときにタップモードを使用できます。

タップモードの場合、デバイスはインラインで展開されますが、パケットがデバイスを通る代わりに各パケットのコピーがデバイスに送信され、ネットワークトラフィックフローは影響を受けません。パケット自体ではなくパケットのコピーを処理するので、パケットをドロップするように設定したルールおよび置換キーワードを使用するルールはパケットストリームに影響を及ぼしません。ただし、これらのタイプのルールでは、トリガーされた侵入イベントが生成され、侵入イベントのテーブルビューには、トリガーの原因となったパケットがインライン展開でドロップされたことが示されます。

インライン展開されたデバイスでタップモードを使用することには、利点があります。たとえば、デバイスがインラインであるかのようにデバイスとネットワークの間の配線をセットアップし、デバイスが生成するタイプの侵入イベントを分析することができます。その結果に基づいて、効率性に影響を与えることなく最適なネットワーク保護を提供するように、侵入ポリシーを変更して廃棄ルールを追加できます。デバイスをインラインで展開する準備ができたら、タップモードを無効にして、デバイスとネットワーク間の配線を再びセットアップせずに、不審なトラフィックのドロップを開始することができます。

ただし、同じインラインセットに対してこのオプションと厳格な TCP 強制を有効にすることはできません。

#### リンクステートの伝達 (Propagate Link State)

リンクステートの伝達は、インラインセットのペアの両方で状態を追跡できるようにするためにバイパスモードで設定されるインラインセットの機能です。リンクステートの伝達は、銅線と光ファイバの両方の設定可能なバイパスインターフェイスで使用できます。

リンクステートの伝達によって、インラインセットのインターフェイスの1つが停止した場合、インラインインターフェイスペアの2番目のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、2番目のインターフェイスも自動的に起動します。つまり、1つのインターフェイスのリンクステートが変化すると、アプライアンスはその変化を検知し、それに合わせて他のインターフェイスのリンクステートを更新します。ただし、アプライアンスがリンクステートの変更を伝達するのに最大4秒かかります。

リンクステートの伝達は、ルータが障害状態のネットワークデバイスを避け、トラフィックを自動的に再ルーティングするよう設定された、復元力の高いネットワーク環境では特に有効です。

リンクステートの伝達は7000および8000シリーズデバイスのみでサポートされていることに注意してください。

高可用性ペアの7000および8000シリーズデバイスで設定されたインラインセットのリンクステートの伝達を無効にすることはできません。

### トランスペアレントインラインモード (Transparent Inline Mode)

[トランスペアレントインラインモード (Transparent Inline Mode)] オプションを使用すると、デバイスを「Bump In The Wire」として機能させることができます。つまり、デバイスは、送信元と宛先に関係なく、認識するすべてのネットワークトラフィックを転送するという事です。7000および8000シリーズのデバイスではこのオプションを無効にできないことに注意してください。

### 厳格なTCP強制 (Strict TCP Enforcement)

最大限のTCPセキュリティを実現するため、厳格な強制を有効にすることができます。この機能は、3ウェイハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3ウェイハンドシェイクが完了していない接続の非SYN TCPパケット
- 応答側がSYN-ACKを送信する前にTCP接続の発信側から送信された非SYN/RSTパケット
- SYNの後、セッションの確立前にTCP接続のレスポンドから送信された非SYN-ACK/RSTパケット
- 発信側または応答側のどちらかから送信された、確立されたTCP接続のSYNパケット

なお、このオプションは、7000および8000シリーズデバイスでのみ使用できます。また、同じインラインセットに対してこのオプションとタップモードを有効にすることはできません。

## 高度なインラインセットオプションの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** インラインセットを編集するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [インラインセット (Inline Sets)] タブをクリックします。

**ステップ 4** 編集するインラインセットの横にある編集アイコン (✎) をクリックします。

**ステップ 5** [Advanced] タブをクリックします。

**ステップ 6** [インラインセットの詳細オプション \(597 ページ\)](#) の説明に従ってオプションを設定します。

**ステップ 7** [OK] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## インラインセットの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	リーフのみ	Admin/Network Admin

インラインセットを削除すると、そのセットに割り当てられたインライン インターフェイスを別のセットに含めることができますようになります。それらのインターフェイスは削除されません。

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

- ステップ2** インラインセットを削除するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ3** [インラインセット (Inline Sets) ] タブをクリックします。
- ステップ4** 削除するインラインセットの横にある削除アイコン (🗑) をクリックします。
- ステップ5** プロンプトが表示されたら、インラインセットを削除することを確認します。
- 

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。



## 第 **VII** 部

# クラシック デバイスのハイ アベイラビリティと拡張性

- [7000 および 8000 シリーズ デバイスのハイ アベイラビリティ \(603 ページ\)](#)
- [8000 シリーズ デバイスのスタック構成 \(625 ページ\)](#)







## 第 24 章

# 7000 および 8000 シリーズ デバイスのハイ アベイラビリティ

次の各トピックでは、Firepower システムにおける Firepower 7000 シリーズおよび 8000 シリーズ デバイスのハイ アベイラビリティの設定方法について説明します。

- [7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて \(603 ページ\)](#)
- [デバイスのハイ アベイラビリティの確立 \(609 ページ\)](#)
- [デバイスのハイ アベイラビリティの編集 \(610 ページ\)](#)
- [高可用性ペアの個々のデバイスの設定 \(611 ページ\)](#)
- [高可用性ペアの個々のデバイス スタックの設定 \(612 ページ\)](#)
- [高可用性ペアのデバイスでのインターフェイスの設定 \(613 ページ\)](#)
- [デバイスのハイ アベイラビリティペアにおけるアクティブピアの切り替え \(613 ページ\)](#)
- [高可用性ピアのメンテナンス モードへの切り替え \(614 ページ\)](#)
- [高可用性ペアのスタック内のデバイスの交換 \(615 ページ\)](#)
- [デバイスのハイ アベイラビリティ状態共有 \(616 ページ\)](#)
- [トラブルシューティングのためのデバイスのハイ アベイラビリティの状態共有統計情報 \(619 ページ\)](#)
- [デバイス高可用性ペアの分離 \(622 ページ\)](#)

## 7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて

7000 および 8000 シリーズ デバイス ハイ アベイラビリティを利用することで、2つのピア デバイス間または2つのピア デバイス スタック間のネットワークング機能と設定データの冗長性を確保できます。

2つのピア デバイスまたは2つのピア デバイス スタックを、ポリシーの展開、システムの更新、登録を行う単一の論理システムとして機能するハイ アベイラビリティ ペアとして構成することにより、構成の冗長性を実現できます。その他の設定データは、システムによって自動的に同期されます。



- (注) スタティック ルート、非 SFRP IP アドレス、およびルーティングの優先順位は、ピア デバイスまたはピア デバイス スタック間で同期されません。各ピア デバイスまたはピア デバイス スタックは、独自のルーティング インテリジェンスを維持します。

#### 関連トピック

##### SFRP

[仮想スイッチの詳細設定](#) (1229 ページ)

## デバイスのハイ アベイラビリティ要件

7000 および 8000 シリーズ デバイスのハイ アベイラビリティ ペアを構成するには、以下に従う必要があります。

- 単一デバイスと単一デバイスのペア、またはデバイス スタックとデバイス スタックのペアのみを構成できます。
- 両方のデバイスまたはデバイス スタックが正常なヘルス ステータスであり、同じソフトウェアを実行し、同じライセンスが有効になっている必要があります。詳細については、[ヘルス モニタの使用 \(295 ページ\)](#) を参照してください。特に、デバイスでのハードウェア障害は許容されません。ハードウェア障害が発生すると、デバイスがメンテナンスモードに入り、フェールオーバーがトリガーされます。



- (注) デバイスのペアを構成した後は、ペアを構成する個々のデバイスのライセンス オプションを変更することはできませんが、ハイ アベイラビリティ ペア全体のライセンスは変更できます。

- 各デバイスまたはスタック内の各プライマリ デバイスにインターフェイスを設定する必要があります。
- 両方のデバイスまたはデバイス スタックのプライマリ メンバーが同じモデルである必要があります。銅ケーブルまたは光ファイバの同じインターフェイスが必要です。
- デバイス スタックのハードウェア構成は同一でなければなりません。インストール済みのマルウェアストレージパックについてはその限りではありません。たとえば、Firepower 8290 と別の 8290 のペアを構成することができます。どちらかのスタック内でマルウェアストレージパックが、どのデバイスに存在しなくても、1つのデバイスにのみ、またはすべてのデバイスに存在しても構いません。



**注意** シスコから供給されたハードドライブ以外はデバイスに取り付け  
ないでください。サポートされていないハードドライブを取り付  
けると、デバイスが破損する可能性があります。マルウェアスト  
レージパック キットは、シスコからのみ購入でき、8000 シリー  
ズ デバイスでのみ使用できます。マルウェア ストレージ パック  
のサポートが必要な場合は、サポートにお問い合わせください。  
詳細については、*Firepower System Malware Storage Pack Guide*を参  
照してください。

- デバイスが NAT ポリシーのターゲットとなっている場合、両方のピアに同じ NAT ポリ  
シーを適用する必要があります。
- マルチドメイン展開では、7000 または 8000 シリーズ デバイスのハイ アベイラビリティま  
たはリーフ ドメイン内のデバイス スタックのみを確立できます。

#### 関連トピック

[SFRP](#)

[仮想スイッチの詳細設定](#) (1229 ページ)

## デバイスハイアベイラビリティフェールオーバーとメンテナンスモー ド

7000 および 8000 シリーズ デバイス ハイ アベイラビリティのフェールオーバーは、手動また  
は自動で行われます。手動でフェールオーバーをトリガーするには、ピアを構成するデバイス  
またはスタックのいずれかでメンテナンス モードを開始します。

自動フェールオーバーは、アクティブ デバイスまたはアクティブ スタックの正常性が損なわ  
れた場合、システム更新時、または管理者権限によりデバイスがシャットダウンされた場合に  
発生します。また、自動フェールオーバーは、アクティブ デバイスまたはデバイス スタック  
で NMSB 障害、NFE 障害、ハードウェア障害、ファームウェア障害、重大なプロセス障害、  
ディスク フルエラー、または 2 つのスタック構成のデバイス間のリンク障害が起きた場合にも  
発生します。スタンバイのデバイスまたはスタックの正常性がアクティブデバイス同様に損  
なわれている場合は、フェールオーバーは行われず、クラスタは縮退状態になります。また、  
いずれかのデバイスまたはデバイス スタックがメンテナンス モードになっている場合も、  
フェールオーバーは行われません。アクティブスタックからスタック ケーブルを切断すると、  
そのスタックはメンテナンス モードに入ることに注意してください。アクティブ スタックの  
セカンダリ デバイスをシャットダウンした場合も、スタックはメンテナンス モードに入ります。



(注) ハイ アベイラビリティ ペアのアクティブなメンバーがメンテナンス モードになり、アクティ  
ブロールが他のピアメンバーにフェールオーバーされた場合、元のアクティブピアのメンバー  
は、通常動作に復帰したときに自動的にアクティブ ロールを再要求しません。

## 関連トピック

[SFRP](#)[仮想スイッチの詳細設定 \(1229 ページ\)](#)

## デバイスの高可用性ペアでのポリシーの導入と更新

ポリシーを導入する際は、個々のデバイスやデバイススタックではなく、デバイスの高可用性ペアにポリシーを導入します。ポリシーの導入が失敗すると、システムはいずれのデバイスまたはスタックにもポリシーを導入しません。ポリシーは最初にアクティブ デバイスまたはスタックに導入されてから、スタンバイに導入されます。したがって、高可用性ペアでは常に、ピアのいずれかがネットワークトラフィックを処理します。ポリシーの導入が完了すると、デバイスは自動的にメンテナンス モードから削除されます。



## 注意

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。このインスペクション中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。Firepower 7010、7020、および 7030 の管理対象デバイスでは、設定変更の展開に最大 5 分かかる場合があります。利用できない時間を最小限にするために、導入は変更時間帯に実行します。[Snort® の再起動シナリオ \(354 ページ\)](#) および [展開またはアクティブ化された際に Snort プロセスを再起動する設定 \(357 ページ\)](#) を参照してください。

個々のデバイスまたはスタックが更新を受信するのではなく、高可用性ペアを構成するデバイスが単一のエンティティとして更新を受信します。更新が開始されると、システムは最初にスタンバイデバイスまたはスタックに更新を導入します。それによって、そのデバイスまたはスタックはメンテナンスモードに入ります。この状態は、必要なプロセスが再開してデバイスがトラフィックの処理を再び開始するまで維持されます。その後、システムはアクティブデバイスまたはスタックに更新を導入して、同じプロセスを行います。

## 関連トピック

[SFRP](#)[仮想スイッチの詳細設定 \(1229 ページ\)](#)

## 展開タイプとデバイス ハイ アベイラビリティ

7000 または 8000 シリーズ デバイスのハイ アベイラビリティ構成は、Firepower システム展開 (パッシブ、インライン、ルーテッド、またはスイッチド) に応じて決定します。同時に複数のロールを持たせてシステムを展開することもできます。4つの展開タイプのうち、ハイアベイラビリティを用いた冗長性をもたらすためにデバイスまたはスタックの構成が必要になるのは、パッシブ展開のみです。他の展開タイプでは、デバイス ハイ アベイラビリティを使用し

でも使用しなくてもネットワークの冗長性を確立できます。各展開タイプにおけるハイアベイラビリティの概要については、以降の各項を参照してください。



- (注) レイヤ3の冗長性については、デバイスハイアベイラビリティを使わずに、Cisco Redundancy Protocol (SFRP) により実現できます。SFRPでは、指定したIPアドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。ネットワークの冗長性では、2つのデバイスまたは2つのスタックが同一のネットワーク接続を提供するように設定することで、ネットワーク上の他のホストに対する接続を維持できます。

### パッシブ展開での冗長性

一般に、パッシブインターフェイスは中央スイッチのタップポートに接続されます。この場合、スイッチを通過するトラフィックのすべてを、パッシブインターフェイスで分析することが可能になります。複数のデバイスが同じタップフィードに接続されている場合、システムはそれぞれのデバイスからイベントを生成します。ハイアベイラビリティペアとして構成されているデバイスは、アクティブまたはスタンバイのいずれかとして機能するため、システムはシステム障害が発生したとしてもトラフィックを分析できると同時に、重複するイベントを防止できます。

### インライン展開での冗長性

インラインセットは、自身を通過するパケットのルーティングを制御できないため、展開環境で常にアクティブになっていなければなりません。したがって、冗長性を確立できるかどうかは、外部システムがトラフィックを適切にルーティングするかどうか依存します。冗長インラインセットは、7000または8000シリーズデバイスのハイアベイラビリティを使用しても使用しなくても設定できます。

冗長インラインセットを展開するには、循環ルーティングを防止する一方で、トラフィックがインラインセットのいずれか1つだけを通り過ぎるようにネットワークトポロジを設定します。インラインセットのいずれかで障害が発生すると、周辺ネットワークインフラストラクチャがゲートウェイアドレスへの接続が切断されたことを検出し、ルートを調整して冗長セット経由でトラフィックを送信します。

### ルーテッド展開での冗長性

IPネットワーク内のホストは、既知のゲートウェイアドレスを使用してトラフィックをさまざまなネットワークに送信する必要があります。ルーテッド展開で冗長性を確立するには、ルーテッドインターフェイスがゲートウェイアドレスを共有し、そのアドレスに対するトラフィックを常に1つのインターフェイスだけが処理するようにしなければなりません。そのためには、仮想ルータで同じ数のIPアドレスを維持する必要があります。1つのインターフェイスがアドレスをアドバタイズします。そのインターフェイスがダウンすると、スタンバイインターフェイスがアドレスのアドバタイズを開始します。

ハイアベイラビリティペアのメンバーではないデバイスでは、複数のルーティングされたインターフェイス間で共有するゲートウェイIPアドレスの設定し、SFRPによって冗長性を確保します。SFRPは、7000または8000シリーズデバイスのハイアベイラビリティを使用しても

使用しなくても設定できます。また、OSPF や RIP などのダイナミック ルーティングを使用して冗長性を確保することもできます。

### スイッチド展開での冗長性

スイッチド展開では、高度な仮想スイッチ設定の 1 つであるスパンニング ツリー プロトコル (STP) を使用して冗長性を確保します。STP はブリッジ型ネットワーク トポロジを管理するプロトコルです。このプロトコルは、スタンバイリンクを設定することなく、冗長リンクでスイッチドインターフェイスの自動スタンバイを行えるように設計されています。スイッチド展開でのデバイスは、STP に依存して、冗長インターフェイス間のトラフィックを管理します。同じブロードキャストネットワークに接続されている 2 つのデバイスは、STP によって計算されたトポロジに基づいてトラフィックを受信します。



(注) 7000 または 8000 シリーズデバイスのハイ アベイラビリティ ペアに展開する予定の仮想スイッチを設定する際には、STP を有効にするよう強く推奨します。

### 関連トピック

[SFRP](#)


[仮想スイッチの詳細設定](#) (1229 ページ)

## デバイスのハイ アベイラビリティ設定

7000 または 8000 シリーズデバイスのハイ アベイラビリティを確立する際には、デバイスまたはスタックのうち的一方をアクティブとして指定し、もう一方をスタンバイとして指定します。システムは、マージした設定を、ペアを構成するデバイスに適用します。競合が存在する場合、システムはアクティブとして指定されたデバイスまたはスタックの設定を適用します。

デバイスのペアを構成した後は、ペアを構成する個々のデバイスのライセンスオプションを変更することはできませんが、ハイ アベイラビリティ ペア全体のライセンスは変更できます。スイッチドインターフェイスまたはルーテッドインターフェイスで設定しなければならないインターフェイス属性がある場合、システムはハイ アベイラビリティ ペアを確立しますが、そのステータスを保留中に設定します。ユーザが必要な属性を設定した後、システムはハイ アベイラビリティ ペアを完成させて、正常なステータスに設定します。

ハイ アベイラビリティ ペアを確立した後、[デバイス管理 (Device Management)] ページでは、ピア デバイスまたはスタックが単一のデバイスとして扱われます。デバイスのハイ アベイラ

ビリティ ペアは、アプライアンスリストではハイ アイコン アイコン (  ) が表示されます。ユーザが行った設定変更は、いずれもペアを構成するデバイスの中で同期されます。[デバイス管理 (Device Management)] ページには、ハイ アベイラビリティ ペアのどのデバイスまたはスタックがアクティブであるかが表示されます。アクティブなデバイスまたはスタックは、手動または自動フェールオーバーが発生すると変更されます。

デバイスのハイ アベイラビリティ ペアの登録を Firepower Management Center から削除すると、その登録は両方のデバイスまたはスタックから削除されます。デバイスのハイ アベイラビ

ティペアを Firepower Management Center から削除する方法は、個々の管理対象デバイスを削除する場合の方法と同じです。

登録が削除されたハイ アベイラビリティ ペアは、別の Firepower Management Center に登録できます。ハイ アベイラビリティ ペアを構成する一方のデバイスを登録するには、ペアのうちアクティブ デバイスにリモート管理を追加してから、そのデバイスを Firepower Management Center に追加します。これにより、ペア全体が追加されます。ハイ アベイラビリティ ペアのうちスタック構成のデバイスを登録するには、どちらか一方のスタックのプライマリデバイスにリモート管理を追加してから、そのデバイスを Firepower Management Center に追加します。これにより、ペア全体が追加されます。

デバイスのハイ アベイラビリティ ペアを確立したら、ハイ アベイラビリティ リンク インターフェイスを設定する必要があります。



- (注) ハイ アベイラビリティ ペアのデバイスを使用してダイナミック NAT、HA 状態共有、または VPN を設定する場合は、ハイ アベイラビリティ リンク インターフェイスを構成する必要があります。詳細については、[HA リンク インターフェイスの設定 \(580 ページ\)](#) を参照してください。

#### 関連トピック

[SFRP](#)

[仮想スイッチの詳細設定 \(1229 ページ\)](#)

## デバイスのハイ アベイラビリティの確立

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin



- (注) この手順では、7000 & 8000 シリーズ デバイスのハイ アベイラビリティ ペアの確立について説明します。Firepower Threat Defense のハイ アベイラビリティの確立については、[Firepower Threat Defense ハイ アベイラビリティ ペアの追加 \(745 ページ\)](#) を参照してください。

7000 & 8000 シリーズ デバイスのハイ アベイラビリティ ペアを確立する際には、デバイスまたはスタックのうち一方をアクティブとして指定し、もう一方をスタンバイとして指定します。システムは、マージした設定を、ペア内のデバイスに適用します。競合が存在する場合、システムはアクティブとして指定されたデバイスまたはスタックの設定を適用します。

マルチドメイン展開では、ハイ アベイラビリティ ペアのデバイスは同じドメインに属している必要があります。

### 始める前に

- すべての要件が満たされていることを確認します。[デバイスのハイアベイラビリティ要件 \(604 ページ\)](#) を参照してください。

### 手順

- 
- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2** [追加 (Add) ] ドロップダウンメニューから、[ハイ アベイラビリティの追加 (Add High Availability) ] を選択します。
- ステップ 3** 名前を入力します。
- ステップ 4** [デバイス タイプ (Device Type) ] で [Firepower] を選択します。
- ステップ 5** デバイスまたはスタックにロールを割り当てます。
- [アクティブ ピア (Active Peer) ] のデバイスまたはスタックをハイ アベイラビリティ ペア用に選択します。
  - [スタンバイ ピア (Standby Peer) ] のデバイスまたはスタックをハイ アベイラビリティ ペア用に選択します。
- ステップ 6** [追加 (Add) ] をクリックします。このプロセスではデータの同期が行われるため、プロセスが完了するまでに数分かかります。
- 

### 次のタスク

HA 状態共有、ダイナミック NAT、または VPN をデバイスに設定する予定の場合は、高可用性ペアの各デバイスで HA リンク インターフェイスを作成します。HA リンク インターフェイスの詳細については、[HA リンク インターフェイスの設定 \(580 ページ\)](#) を参照してください。

## デバイスのハイ アベイラビリティの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアを確立した後は、デバイス設定を変更すると、通常はハイ アベイラビリティ ペア全体の設定も変更されます。

[一般 (General) ] セクションのステータス アイコンにマウスのポインタを合わせると、ハイ アベイラビリティ ペアのステータスが表示されます。また、ペア内のデバイスまたはスタックのどれがアクティブ ピアで、どれがスタンバイ ピアであるかも確認できます。



## 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** 設定を編集するデバイスのハイアベイラビリティペアの横にある編集アイコン (✎) をクリックします。
- マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** [ハイアベイラビリティ (High Availability)] ページのセクションを使用して、単一のデバイス設定を変更する場合と同じように、ハイアベイラビリティペアの設定を変更します。

## 高可用性ペアの個々のデバイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

7000 または 8000 シリーズ デバイスの高可用性ペアを確立した後でも、ペア内の個々のデバイスに対して設定できる属性がいくつかあります。ペアリングされたデバイスに変更を加える方法は、単一のデバイスに変更を加える場合の方法と同じです。

## 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** 設定を編集するデバイスの高可用性ペアの横にある編集アイコン (✎) をクリックします。
- マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** [デバイス] タブをクリックします。
- ステップ 4** [選択されたデバイス (Selected Device)] ドロップダウン リストから、変更するデバイスを選択します。
- ステップ 5** [デバイス (Devices)] ページのセクションを使用して、単一のデバイスに対して変更を加える場合と同じように、ペアリングされた個々のデバイスに変更を加えます。

## 高可用性ペアの個々のデバイス スタックの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	Firepower 8140、 Firepower 8200 ファミリー、 Firepower 8300 ファミリー	リーフのみ	Admin/Network Admin

高可用性ペアにスタック構成の 8000 シリーズ デバイスを設定すると、編集可能なスタック属性が制限されます。ペアリングされたスタックの名前は編集できます。また、[高可用性ペアのデバイスでのインターフェイスの設定 \(613 ページ\)](#) で説明している手順に従って、スタックのネットワーク設定を編集できます。

### 手順

- 
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** 設定を編集するデバイスの高可用性ペアの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** [スタック (Stacks)] タブをクリックします。
- ステップ 4** [選択されたデバイス (Selected Device)] ドロップダウン リストから、変更するスタックを選択します。
- ステップ 5** [一般 (General)] セクションの横にある編集アイコン (✎) をクリックします。
- ステップ 6** 名前を入力します。
- ステップ 7** [保存 (Save)] をクリックします。
- 

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 高可用性ペアのデバイスでのインターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

7000 または 8000 シリーズ デバイスの高可用性ペアの個々のデバイスに、インターフェイスを設定できます。ただし、その場合には、ペアのピアデバイスにも同等のインターフェイスを設定する必要があります。ペアリングされたスタックの場合は、スタックのプライマリデバイスのそれぞれに、同じインターフェイスを設定する必要があります。仮想ルータを設定するとき、その仮想ルータを設定するスタックを選択します。

### 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。

**ステップ 2** インターフェイスを設定するデバイスの高可用性ペアの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [インターフェイス (Interfaces) ] タブをクリックします。

**ステップ 4** [選択されたデバイス (Selected Device) ] ドロップダウン リストから、変更するデバイスを選択します。

**ステップ 5** 個々のデバイスに設定する場合と同じようにインターフェイスを設定します。

### 関連トピック

[仮想ルータ設定](#) (1244 ページ)

## デバイスのハイアベイラビリティペアにおけるアクティブペアの切り替え

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアを確立した後、アクティブ なピア デバイスまたはスタックをスタンバイに手動で切り替えることができます。

### 手順

- 
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** アクティブ ピアを変更するデバイスのハイ アベイラビリティ ペアの横にあるアクティブ ピア 切り替えアイコン (🔁) をクリックします。
- ステップ 3** 次の操作を実行できます。
- ハイ アベイラビリティ ペアでスタンバイ ピアをアクティブ ピアにすぐに切り替える場合は、[はい (Yes)] をクリックします。
  - キャンセルして[デバイス管理 (Device Management)] ページに戻る場合は、[いいえ (No)] をクリックします。
- 

## 高可用性ピアのメンテナンス モードへの切り替え

スマート ライセ ンス	従来のライセンス	サポートされるデ バイス	サポートされるド メイン	アクセス (Access)
該当なし	Control	7000 & 8000 シ リーズ	任意 (Any)	Admin/Network Admin

7000 または 8000 シリーズデバイス高可用性ペアを設定した後で、デバイスのメンテナンスを実行するために、いずれかのピアをメンテナンスモードに切り替えることで、手動でフェールオーバーをトリガーできます。メンテナンスモードでは、システムが管理目的で管理インターフェイスを除くすべてのインターフェイスをダウンさせます。メンテナンスの完了後、ピアを再度有効にして、通常の動作を再開できます。




- (注) 高可用性ペアの両方のピアを同時にメンテナンスモードにしないでください。これを行うと、そのペアではトラフィックを検査できなくなります。
- 

### 手順

- 
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** メンテナンス モードを開始するピアの横にあるメンテナンス モード切り替えアイコン (🔧) をクリックします。

**ステップ3** [はい (Yes) ] をクリックして、メンテナンス モードを確定します。

#### 次のタスク

- メンテナンスが完了したら、メンテナンス モード切り替えアイコン (  ) を再度クリックして、ピアのメンテナンス モードを終了します。


## 高可用性ペアのスタック内のデバイスの交換

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	Firepower 8140、 8200 ファミリ、 8300 ファミリ	任意 (Any)	Admin/Network Admin


高可用性ペアのメンバーになっているスタックをメンテナンス モードに切り替えた後で、スタック内のセカンダリ デバイスを別のデバイスと交換できます。選択できるデバイスは、現在スタックのメンバーにも、ペアにもなっていないデバイスのみです。新しいデバイスは、デバイス スタックを確立する場合と同じガイドラインに従っている必要があります。

#### 手順

**ステップ1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。


**ステップ2** メンテナンス モードを開始するスタック メンバーの横にあるメンテナンス モード切り替えアイコン (  ) をクリックします。

**ステップ3** [はい (Yes) ] をクリックして、メンテナンス モードを確定します。

**ステップ4** デバイス交換アイコン (  ) をクリックします。

**ステップ5** ドロップダウンリストから [交換デバイス (Replacement Device) ] を選択します。

**ステップ6** [交換 (Replace) ] をクリックして、デバイスを交換します。

**ステップ7** メンテナンス モード切り替えアイコン (  ) を再度クリックすると、スタックのメンテナンス モードが即時に終了します。

(注) デバイス設定を再展開する必要はありません。

## デバイスのハイ アベイラビリティ状態共有

デバイスのハイ アベイラビリティ状態共有を使用すると、ハイ アベイラビリティ ペアのデバイスまたはスタックで、可能な限り状態を同期できます。したがって、いずれか一方のデバイスまたはスタックで障害が発生しても、もう一方のピアがトラフィックフローを中断せずに引き継ぐことができます。状態共有を使用しない場合、以下の機能が適切にフェールオーバーしない可能性があります。

- 厳格な TCP 強制
- 単方向アクセス コントロール ルール
- ブロッキングの永続性

ただし、状態共有を有効にすると、システムパフォーマンスが低下することに注意してください。

ハイ アベイラビリティ状態共有を設定するには、あらかじめハイ アベイラビリティ ペアの両方のデバイスまたはスタック構成のプライマリ デバイスで HA リンク インターフェイスを設定し、有効にする必要があります。Firepower 82xx ファミリーおよび 83xx ファミリーには 10 G の HA リンクが必要ですが、他のモデルのデバイスには 1 G の HA リンクで十分です。

HA リンク インターフェイスを変更する前に、状態共有を無効にする必要があります。



(注) ペアを構成するデバイスでフェールオーバーが発生した場合は、アクティブデバイス上の既存の SSL 暗号化セッションがすべて終了されます。ハイ アベイラビリティ状態共有を設定しているとしても、これらのセッションをスタンバイデバイスで再ネゴシエートする必要があります。SSL セッションを確立しているサーバがセッションの再利用をサポートしている場合でも、スタンバイデバイスに SSL セッション ID がないと、セッションを再ネゴシエートできません。

### 厳格な TCP 強制

ドメインに対して厳密な TCP 適用を有効にすると、システムは TCP セッションで正常ではないパケットをすべてドロップします。たとえば、未確立の接続で受信した SYN 以外のパケットはドロップされます。状態共有が有効な場合、厳密な TCP 適用が有効にされているとしても、ハイ アベイラビリティ ペアのデバイスは、フェールオーバー後に接続を再び確立することなく TCP セッションを続行できます。厳密な TCP 適用は、インラインセット、仮想ルータ、および仮想スイッチで有効にすることができます。

### 単方向アクセス コントロール ルール

単方向アクセス コントロール ルールを設定している場合、システムがフェールオーバーの後に接続ミッドストリームを再評価する際に、ネットワークトラフィックが意図されたものとは

異なるアクセス コントロール ルールに一致する可能性があります。たとえば、ポリシーに以下の2つのアクセス コントロール ルールが含まれているとします。

```
Rule 1: Allow from 192.168.1.0/24 to 192.168.2.0/24
Rule 2: Block all
```

状態共有が有効でない場合、フェールオーバーの後に 192.168.1.1 ~ 192.168.2.1 からの許可される接続がまだアクティブになっているために、次のパケットが応答パケットとしてみなされると、システムは接続を拒否します。状態共有が有効であれば、ミッドストリームピックアップが既存の接続に一致することになり、接続が引き続き許可されます。

### ブロッキングの永続性

アクセス コントロール ルールやその他の要素に基づいて、最初のパケットで多数の接続がブロックされるとしても、システムが接続のブロッキングを決定する前に、いくつかのパケットを許可する場合があります。状態共有が有効な場合、システムはピアデバイスまたはスタックでも即時に接続をブロックします。

ハイ アベイラビリティ ペアの状態共有を確立するときに、次のオプションを設定できます。

#### [有効 (Enabled) ]

状態共有を有効にするには、このチェックボックスをクリックします。チェックボックスをクリアすると、状態共有が無効になります。

#### 最短フロー寿命 (Minimum Flow Lifetime)

最小セッション時間 (ミリ秒) を指定します。この時間を経過すると、システムがセッションの同期メッセージを送信します。0 ~ 65535 の整数を使用できます。この最小フロー有効期間に達しないセッションは、いずれも同期されず、接続のパケットを受信した時点でのみ、同期が行われます。

#### 最短同期間隔インターバル (Interval)

セッションの更新メッセージ最短間隔 (ミリ秒) を指定します。0 ~ 65535 の整数を使用できます。最短同期間隔を設定することで、特定の接続が最短有効期間に達した後、その接続に対して、設定された値より頻繁に同期メッセージが送信されないようにします。

#### HTTP URL の最大文字数 (Maximum HTTP URL Length)

ペアを構成するデバイス間で同期する、URL の最大文字数を指定します。0 ~ 225 の整数を使用できます。

#### 関連トピック

[HA リンク インターフェイスの設定 \(580 ページ\)](#)

## デバイスのハイ アベイラビリティ状態共有の確立

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

デバイスのハイ アベイラビリティ状態共有を使用すると、ハイ アベイラビリティ ペア内の 7000 または 8000 シリーズ デバイスまたはスタック間で、可能な限り状態を同期できます。したがって、いずれか一方のデバイスまたはスタックで障害が発生しても、もう一方のピアがトラフィック フローを中断せずに引き継ぐことができます。



**注意** 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ状態共有オプションを変更すると、プライマリ デバイスとセカンダリ デバイスの Snort プロセスが再起動され、両方のデバイスのトラフィック インспекションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### 手順

- ステップ 1** デバイスのハイ アベイラビリティ ペアのデバイスごとに HA リンク インターフェイスを設定します。[HA リンク インターフェイスの設定 \(580 ページ\)](#) を参照してください。
- ステップ 2** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 3** 編集するデバイスハイアベイラビリティ ペアの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 4** [状態共有 (State Sharing)] セクションの横にある編集アイコン (✎) をクリックします。
- ステップ 5** 状態共有の値を下げてペア内のピアの準備状況を改善するか、値を上げてパフォーマンスを向上できるようにします。  
(注) シスコでは、展開で値を変更する正当な理由がない限り、デフォルト値を使用することを推奨しています。
- ステップ 6** [OK] をクリックして変更を保存します。



## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 関連トピック

[HA リンク インターフェイスの設定 \(580 ページ\)](#)

[Snort® の再起動シナリオ \(354 ページ\)](#)

# トラブルシューティングのためのデバイスのハイアベイラビリティの状態共有統計情報

以下の項では、デバイスごとに表示可能な統計情報と、7000 および 8000 シリーズ デバイスのハイ アベイラビリティ ペアの状態共有設定をトラブルシューティングするためにどのように利用できるかを説明します。

## 受信メッセージ (ユニキャスト) (Messages Received (Unicast))

ペアを構成するピアから受信した、ハイ アベイラビリティ同期メッセージの数です。

値は、ピアが送信したメッセージ数と同等になっているはずですが、アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずですが。トラフィックが停止すると、値は安定し、受信したメッセージ数が送信されたメッセージ数と一致します。

トラブルシューティングを行う場合は、受信したメッセージ数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同等であることを確認します。各ピアでの送信数の値は、対応するピアでの受信数の値とほぼ同じ率で増えていなければなりません。

受信したメッセージの数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

## 受信パケット数 (Packets received)

システムはオーバーヘッドを低減させるために、複数のメッセージを単一のパケットにまとめます。[受信パケット数 (Packets Received) ]カウンタは、デバイスが受信したこれらのデータパケットとその他の制御パケットの数を表示します。

値は、ピアデバイスが送信したパケット数と同等になっているはずですが。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずですが。受信メッセージの数は、ピアが送信したメッセージ数と同等で、同じ率で増加していなければなりません。したがって、受信したパケットの数も同じ動作となるはずですが。

トラブルシューティングを行う場合は、受信したパケットと送信されたメッセージの両方を確認して増加率を比較し、値が同じ率で増加していることを確認します。ペアを構成するピアでの送信の値が増えている場合、デバイスでの受信の値も同じ率で増えているはずですが。

受信したパケットの数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

### 合計受信バイト数 (Total Bytes Received)

ピアで受信されたパケットの合計バイト数です。

値は、もう一方のピアが送信したバイト数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信した合計バイト数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同じ率で増えていることを確認します。ピアを構成するピアでの送信の値が増えている場合、デバイスでの受信の値も同じ率で増えているはずです。

受信バイト数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

### 受信プロトコルバイト数 (Protocol Bytes Received)

受信したプロトコルオーバーヘッドのバイト数です。この数には、セッション状態同期メッセージのペイロードを除くすべてが含まれます。

値は、ピアが送信したバイト数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信した合計バイト数を確認してプロトコルデータと比較し、実際の状態データがどれだけ共有されているのかを調べます。プロトコルデータが送信されるデータの大部分を占めている場合は、最小同期間隔を調整できます。

受信したプロトコルバイト数が、受信した合計バイト数と同等の割合で増えている場合は、サポートに連絡してください。受信したプロトコルバイト数が受信した合計バイト数に占める割合は、最小限でなければなりません。

### 送信メッセージ (Messages Sent)

ピアを構成するピアに送信した、ハイ アベイラビリティ同期メッセージの数です。

このデータは、受信メッセージ数との比較で役立ちます。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信したメッセージ数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同等であることを確認します。

送信したメッセージ数が、受信した合計バイト数と同等の割合で増えている場合は、サポートに連絡してください。

### 送信バイト数 (Bytes Sent)

ピアに送信したハイ アベイラビリティ同期メッセージの合計送信バイト数です。

このデータは、受信メッセージ数との比較で役立ちます。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。ピアで受信されたバイト数は、この値と同等であり、それより大きい値にはなっていません。

受信した合計バイト数が、送信されたバイト数と同じような比率で増えていない場合は、サポートに連絡してください。

### Tx Errors

システムがペアを構成するピアに送信するメッセージ用にスペースを割り当てるときに、メモリ割り当てに失敗した回数です。

この値は両方のピアで常にゼロでなければなりません。この数がゼロでない場合、あるいは着実に増加している場合（これは、システムにメモリ割り当てが不可能なエラーが発生していることを示します）は、サポートに連絡してください。

### Tx オーバーラン (Tx Overruns)

システムがメッセージをトランジット キューに入れようとして失敗した回数です。

この値は両方のピアで常にゼロでなければなりません。値がゼロでない場合、あるいは着実に増加している場合、これは、システムが HA リンクの間で過剰なデータを共有していて、データの送信に時間がかかりすぎていることを示します。

HA リンク MTU がデフォルト値 (9918 または 9922) 未満に設定されている場合は、値を増やす必要があります。最小フロー有効期間と最小同期間隔の設定を変更することで、HA リンク間で共有されるデータ量を減らし、この数の増加を防ぐことができます。

この値がゼロにならない場合、または増加し続けている場合は、サポートに連絡してください。

### 最近のログ (Recent Logs)

システムログには、最新のハイアベイラビリティ同期メッセージが表示されます。ログには、ERROR または WARN メッセージが示されてはなりません。ログの内容は、常にピア間で同等でなければなりません（接続ソケットの数が同じであるなど）。

ただし、場合によっては、対照的なデータが表示されることもあります。たとえば、一方のピアがもう一方のピアから接続を受信したことをレポートしている場合、それぞれのログで参照される IP アドレスは異なります。このログから、ハイアベイラビリティ状態共有接続を包括的に理解し、接続で発生したすべてのエラーを確認できます。

ログに、ERROR または WARN メッセージ、あるいは単なる通知目的ではないようなメッセージが示されている場合は、サポートに連絡してください。

## デバイス ハイ アベイラビリティの状態共有統計情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

状態共有を確立した後は、[ハイ アベイラビリティ (High Availability)] ページの [状態共有 (State Sharing)] セクションで、設定に関する以下の情報を確認できます。

- 使用されている HA リンク インターフェイスおよび現在のリンク状態
- 問題のトラブルシューティングに使用できる、同期に関する詳細な統計情報

状態共有の統計情報は、主に、送受信されたハイアベイラビリティ同期トラフィックのさまざまな側面に関するカウンタで、その他のエラー カウンタも含まれます。さらに、ハイアベイラビリティ ペアのデバイスごとの最新システム ログも表示できます。

## 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 編集するデバイスハイアベイラビリティ ペアの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [状態共有 (State Sharing)] セクションで、統計情報表示アイコン (📊) をクリックします。

**ステップ 4** ハイアベイラビリティ ペアがデバイス スタックで構成されている場合、表示する [デバイス (Device)] を選択します。

**ステップ 5** 次の操作を実行できます。

- [更新 (Refresh)] をクリックして統計情報を更新します。
- [表示 (View)] をクリックして、ハイアベイラビリティ ペアのデバイスごとの最新システム ログを表示します。

## デバイス高可用性ペアの分離

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

7000 または 8000 シリーズ デバイス高可用性ペアを分離 (分断) すると、次のようになります。

- アクティブなピア (デバイスまたはスタック) は、完全な展開機能を維持します

- スタンバイピア（デバイスまたはスタック）はインターフェイス設定を失って、アクティブピアにフェールオーバーします。ただし、インターフェイス設定をアクティブのままにすることを選択すると、スタンバイピアは通常の動作を再開します。
- スタンバイピアは、常にパッシブ インターフェイスの設定を失います。
- メンテナンス モードのピアは、通常の動作を再開します。

## 手順

---

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 分断する高可用性ペアの横にある HA の分断アイコン (🔌) をクリックします。

**ステップ 3** 必要に応じて、スタンバイピアのインターフェイス設定を削除するためのチェックボックスをオンにします。

この手順により、管理インターフェイス以外のすべてのインターフェイスを管理のためにダウンさせます。

**ステップ 4** [Yes] をクリックします。

---





## 第 25 章

# 8000 シリーズ デバイスのスタック構成

次のトピックでは、Firepower システムにおける Firepower 8000 シリーズ デバイス スタックの使用方法について説明します。

- [デバイス スタックについて \(625 ページ\)](#)
- [デバイス スタック設定 \(627 ページ\)](#)
- [デバイス スタックの確立 \(628 ページ\)](#)
- [デバイス スタックの編集 \(630 ページ\)](#)
- [スタック内のデバイスの交換 \(630 ページ\)](#)
- [高可用性ペアのスタック内のデバイスの交換 \(631 ページ\)](#)
- [スタックに含まれる個々のデバイスの設定 \(632 ページ\)](#)
- [スタック構成のデバイスでのインターフェイスの設定 \(633 ページ\)](#)
- [スタック構成のデバイスの分離 \(634 ページ\)](#)
- [スタック内のデバイスの交換 \(635 ページ\)](#)

## デバイス スタックについて

スタック構成に含まれるデバイスを使用して、ネットワークセグメントで検査されるトラフィックの量を増やすことができます。それぞれのスタック構成では、スタックに含まれるすべてのデバイスが同じハードウェアを使用していなければなりません。ただし、マルウェアストレージパックが一部またはすべてのデバイスにインストールされていたり、どのデバイスにもインストールされていなかったりする場合があります。また、以下のスタック構成に従って、同じデバイス ファミリのデバイスを使用する必要があります。

スタック構成は Firepower 8140、Firepower 8200 ファミリ、Firepower 8300 ファミリのデバイスでサポートされます。

### 81xx ファミリの場合：

- 2 台の Firepower 8140

**82xx ファミリの場合 :**

- 最大 4 台の Firepower 8250
- 1 台の Firepower 8260 (プライマリ デバイスおよびセカンダリ デバイス)
- 1 台の Firepower 8270 (容量 40 G のプライマリ デバイスと 2 つのセカンダリ デバイス)
- 1 台の Firepower 8290 (容量 40 G のプライマリ デバイスと 3 つのセカンダリ デバイス)

**83xx ファミリの場合 :**

- 最大 4 台の Firepower 8350
- 最大 4 つの AMP8350
- 1 台の Firepower 8360 (容量 40 G のプライマリ デバイスと 1 つのセカンダリ デバイス)
- 1 つの AMP8360 (容量 40 G のプライマリ デバイスとセカンダリ デバイス)
- 1 台の Firepower 8370 (容量 40 G のプライマリ デバイスと 2 つのセカンダリ デバイス)
- 1 つの AMP8370 (容量 40 G のプライマリ デバイスと 2 つのセカンダリ デバイス)
- 1 台の Firepower 8390 (容量 40 G のプライマリ デバイスと 3 つのセカンダリ デバイス)
- 1 つの AMP8390 (容量 40 G のプライマリ デバイスと 3 つのセカンダリ デバイス)

スタック構成の詳細については、*Cisco Firepower 8000 Series Getting Started Guide*を参照してください。マルウェア ストレージ パックの詳細については、*Firepower System Malware Storage Pack Guide*を参照してください。



**注意** シスコから供給されたハードドライブ以外はデバイスに取り付けしないでください。サポートされていないハードドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、シスコからのみ購入でき、8000 シリーズ デバイスでのみ使用できます。マルウェア ストレージ パックのサポートが必要な場合は、サポートにお問い合わせください。詳細については、*Firepower System Malware Storage Pack Guide*を参照してください。

スタック構成を確立するときに、各スタック構成デバイスのリソースを1つの共有構成に統合します。

1つのデバイスをプライマリ デバイスとして指定し、そのデバイスにスタック全体のインターフェイスを設定します。その他のデバイスはセカンダリ デバイスとして指定します。セカンダリ デバイスは、現在トラフィックを検知していないデバイスで、かつインターフェイス上にリンクがないデバイスでなければなりません。

単一のデバイスを設定する場合と同じように、プライマリ デバイスを分析対象のネットワーク セグメントに接続します。*Cisco Firepower 8000 Series Getting Started Guide*で説明されているス



タック構成のデバイスの配線手順に従って、セカンダリ デバイスをプライマリ デバイ스에接続します。

スタック構成に含まれるすべてのデバイスは、同じハードウェアを使用し、同じソフトウェアバージョンを実行し、同じライセンスが適用されている必要があります。デバイスが NAT ポリシーのターゲットとなっている場合は、プライマリ デバイスとセカンダリ デバイスの両方に同じ NAT ポリシーを適用する必要があります。更新は、Firepower Management Center からスタック全体に対して展開する必要があります。スタック構成の1つ以上のデバイスで更新に失敗した場合、スタックはバージョンが混在した状態になります。バージョンが混在するスタックには、ポリシーを展開することも、更新を展開することもできません。この状態を修正するには、スタックを解除するか、バージョンが異なる個々のデバイスを削除し、それらのデバイスを個別に更新してからスタック構成を再確立します。デバイスをスタックに入れた後は、ライセンスの変更は、スタック全体に対してのみ行うことができます。

スタック構成を確立した後は、スタック構成に含まれるすべてのデバイスが単一の共有構成のように機能します。プライマリ デバイスで障害が発生した場合、トラフィックはセカンダリ デバイスに渡されません。この場合、セカンダリ デバイスでスタック ハートビートが失敗したことを通知する、ヘルス アラートが生成されます。

スタック内のセカンダリ デバイスで障害が発生すると、設定可能なバイパスが有効になっているインラインセットがプライマリ デバイス上でバイパス モードになります。それ以外のすべての設定では、システムは、失敗したセカンダリ デバイスへ継続してトラフィックをロード バランスします。いずれの場合も、リンクが失われたことを示すためのヘルスアラートが生成されます。

デバイススタックは展開内で単一のデバイスと同じように使用できますが、いくつかの例外があります。ハイ アベイラビリティ ペアに 7000 または 8000 シリーズ デバイスがある場合は、デバイスのハイ アベイラビリティ ペアまたはハイ アベイラビリティ ペアのデバイスをスタックできません。また、デバイススタックに NAT を設定することもできません。



- (注) スタック構成のデバイスからのイベント データを、eStreamer を使用して外部クライアントアプリケーションに配信する場合は、各デバイスからデータを収集して、各デバイスが同じように設定されていることを確認します。eStreamer 設定は、スタック構成のデバイス間で自動的に同期されません。

マルチドメイン展開では、同じドメインに属しているデバイスのみをスタックできます。

#### 関連トピック

[ヘルス モニタリングについて](#) (275 ページ)

## デバイス スタック設定

2 台の Firepower 8140 デバイス、最大 4 台の Firepower 8250、1 台の Firepower 8260、1 台の Firepower 8270、1 台の Firepower 8290、最大 4 台の Firepower 8350、1 台の Firepower 8360、1 台の Firepower 8370、または 1 台の Firepower 8390 をスタック構成し、それらを組み合わせた

リソースを単一の共有設定で使用するによって、ネットワークセグメントで検査されるトラフィック量を増やすことができます。ハイアベイラビリティペアに7000または8000シリーズデバイスがある場合、デバイスのハイアベイラビリティペア、またはハイアベイラビリティペアの一方のデバイスのスタックは構成できません。ただし、2つのデバイススタックのハイアベイラビリティペアを構成できます。

デバイススタックを確立すると、これらのデバイスは、[デバイス管理 (Device Management)] ページで単一のデバイスとして扱われます。デバイススタックには、アプライアンスのリストでスタックアイコン (📦) が表示されます。

デバイススタックの登録を Firepower Management Center から削除すると、その登録は両方のデバイスから削除されます。スタックに含まれるデバイスを Firepower Management Center から削除する方法は、単一の管理対象デバイスを削除する場合と同じです。削除したスタックは、別の Firepower Management Center に登録できます。新しい Firepower Management Center に、スタックに含まれるデバイスのいずれか1つを登録するだけで、スタック全体が表示されるようになります。

デバイススタックを確立した後は、スタックを解除して再確立しない限り、デバイスのプライマリまたはセカンダリとしての役割を変更することはできません。ただし、次の作業を実行できます。

- 最大4台の Firepower 8250 を1つのスタックの限度として、2台または3台の Firepower 8250、1台の Firepower 8260、または1台の Firepower 8270 からなる既存のスタックにセカンダリ デバイスを追加できます。
- 最大4台の Firepower 8350 を1つのスタックの限度として、2台または3台の Firepower 8350、1台の Firepower 8360、または1台の Firepower 8370 からなる既存のスタックにセカンダリ デバイスを追加できます。

デバイスを追加する場合、スタックのプライマリデバイスに、追加のデバイスを配線するために必要なスタック NetMods がなければなりません。たとえば、プライマリに単一のスタック NetMod しかない Firepower 8260 を使用している場合、このスタックに別のセカンダリ デバイスを追加することはできません。セカンダリ デバイスを既存のスタックに追加する方法は、最初にスタックに含まれるデバイスの設定を確立したときの方法と同じです。

## デバイス スタックの確立

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Firepower 8140、 8200 ファミリ、 8300 ファミリ	任意 (Any)	Admin/Network Admin

スタック内のすべてのデバイスが同じハードウェアモデル (たとえば、Firepower 8140 と別の 8140) である必要があります。8200 ファミリおよび 8300 ファミリでは、合計4つのデバイス (1つのプライマリデバイスと最大3つのセカンダリデバイス) でスタックを構成できます。

マルチドメイン展開では、スタック内のすべてのデバイスが同じドメインに属している必要があります。

### 始める前に

- プライマリ デバイスとして指定するユニットを決定します。
- プライマリとセカンダリの間関係を指定する前に、ユニット間の配線が適切に行われていることを確認します。ケーブルについては、*Cisco Firepower 8000 Series Getting Started Guide* を参照してください。

### 手順

- 
- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2** [追加 (Add) ] ドロップダウンメニューから、[スタックの追加 (Add Stack) ] を選択します。
- ステップ 3** [プライマリ (Primary) ] ドロップダウンリストから、プライマリ デバイスとして運用するために配線したデバイスを選択します。
- (注) プライマリ デバイスとして配線されていないデバイスを選択すると、以降の手順を実行できなくなります。
- ステップ 4** 名前を入力します。
- ステップ 5** [追加 (Add) ] をクリックし、スタックに含めるデバイスを選択します。
- ステップ 6** [プライマリ デバイスのスロット (Slot on Primary Device) ] ドロップダウンリストから、プライマリ デバイスをセカンダリ デバイスに接続するスタック構成ネットワーク モジュールを選択します。
- ステップ 7** [セカンダリ デバイス (Secondary Device) ] ドロップダウンリストから、セカンダリ デバイスとして運用するために配線したデバイスを選択します。
- ステップ 8** [セカンダリ デバイスのスロット (Slot on Secondary Device) ] ドロップダウンリストから、セカンダリ デバイスをプライマリ デバイスに接続するスタック構成ネットワーク モジュールを選択します。
- ステップ 9** [追加 (Add) ] をクリックします。
- ステップ 10** 複数の Firepower 8250、1つの Firepower 8260、1つの Firepower 8270 の既存のスタック、複数の Firepower 8350、1つの Firepower 8360 または 1つの Firepower 8370 の既存のスタックにセカンダリ デバイスを追加する場合は、手順 5 ~ 9 を繰り返します。
- ステップ 11** [スタック (Stack) ] をクリックし、デバイス スタックを確立するか、セカンダリ デバイスを追加します。このプロセスではシステムデータの同期が行われるため、プロセスが完了するまでに数分かかることに注意してください。

---

### 関連トピック

- [7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて \(603 ページ\)](#)
- [Firepower Management Center からのデバイスの削除 \(552 ページ\)](#)

Firepower Management Center へのデバイスの追加 (550 ページ)

## デバイス スタックの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Firepower 8140、 Firepower 8200 ファミリ、 Firepower 8300 ファミリ	リーフのみ	Admin/Network Admin

デバイス スタックを確立した後は、デバイス設定を変更すると、通常はスタック全体の設定も変更されます。単一のデバイスの[デバイス (Device)] ページで設定を変更する場合と同じように、アプライアンス エディタの[スタック (Stack)] ページで、スタック設定に変更を加えることができます。

スタックの表示名を変更したり、ライセンスを有効または無効にしたり、システムポリシーや正常性ポリシーを表示したり、詳細設定を構成したりすることができます。

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 設定を編集する、スタックに含まれるデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [スタック (Stack)] ページのセクションを使用して、単一のデバイス設定を変更する場合と同じように、スタック構成の設定を変更します。

## スタック内のデバイスの交換

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	FirePOWER 8140、8200 ファ ミリ、8300 ファ ミリ	任意 (Any)	Admin/Network Admin

Firepower Management Center がデバイスと通信できない場合に、スタックを分離してデバイスの登録を解除するには、デバイスに接続してCLIコマンドを使用する必要があります。詳細については、関連する章「[コンフィギュレーションコマンド \(2830 ページ\)](#)」の **stacking disable** CLI コマンドおよび **delete** CLI コマンドを参照してください。

スタック内のデバイスを交換するには、以下を行います。

#### 手順

- 
- ステップ 1 デバイスを含むスタックを選択し、そのスタックを交換して解除します。詳細については、[スタック構成のデバイスの分離 \(634 ページ\)](#) を参照してください。
  - ステップ 2 Firepower Management Center からデバイスを登録解除します。詳細については、[Firepower Management Center からのデバイスの削除 \(552 ページ\)](#) を参照してください。
  - ステップ 3 交換デバイスを Firepower Management Center に登録します。詳細については、[Firepower Management Center へのデバイスの追加 \(550 ページ\)](#) を参照してください。
  - ステップ 4 交換デバイスを含むデバイス スタックを作成します。詳細については、[デバイス スタックの確立 \(628 ページ\)](#) を参照してください。
- 

## 高可用性ペアのスタック内のデバイスの交換

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	Firepower 8140、 8200 ファミリ、 8300 ファミリ	任意 (Any)	Admin/Network Admin

高可用性ペアのメンバーになっているスタックをメンテナンス モードに切り替えた後で、スタック内のセカンダリ デバイスを別のデバイスと交換できます。選択できるデバイスは、現在スタックのメンバーにも、ペアにもなっていないデバイスのみです。新しいデバイスは、デバイス スタックを確立する場合と同じガイドラインに従っている必要があります。

#### 手順

- 
- ステップ 1 **[デバイス (Devices)] > [デバイス管理 (Device Management)]** を選択します。
  - ステップ 2 メンテナンス モードを開始するスタック メンバーの横にあるメンテナンス モード切り替えアイコン (🔧) をクリックします。
  - ステップ 3 **[はい (Yes)]** をクリックして、メンテナンス モードを確定します。
  - ステップ 4 デバイス交換アイコン (🔄) をクリックします。
  - ステップ 5 ドロップダウンリストから **[交換デバイス (Replacement Device)]** を選択します。

**ステップ6** [交換 (Replace)] をクリックして、デバイスを交換します。

**ステップ7** メンテナンス モード切り替えアイコン (🔧) を再度クリックすると、スタックのメンテナンス モードが即時に終了します。

(注) デバイス設定を再展開する必要はありません。

## スタックに含まれる個々のデバイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Firepower 8140、 Firepower 8200 ファミリ、 Firepower 8300 ファミリ	リーフのみ	Admin/Network Admin

デバイススタックを確立した後でも、スタック内の個々のデバイスに対して設定できる属性がいくつかあります。スタックに設定されたデバイスに変更を加える方法は、単一のデバイスに変更を加える場合の方法と同じです。このページでは、デバイスの表示名の変更、システム設定の表示、デバイスのシャットダウンまたは再起動、ヘルス情報の表示、およびデバイス管理設定の編集を行うことができます。

### 手順

**ステップ1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ2** 設定を編集する、スタックに含まれるデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ3** [デバイス (Device)] タブをクリックします。

**ステップ4** [選択されたデバイス (Selected Device)] ドロップダウン リストから、変更するデバイスを選択します。

**ステップ5** [デバイス (Devices)] ページのセクションを使用して、単一のデバイスに対して変更を加える場合と同じように、スタックに含まれる個々のデバイスに変更を加えます。

## スタック構成のデバイスでのインターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Firepower 8140、 Firepower 8200 ファミリ、 Firepower 8300 ファミリ	リーフのみ	Admin/Network Admin

管理インターフェイスを除き、スタック構成のデバイスにインターフェイスを設定するには、スタックのプライマリ デバイスの [インターフェイス (Interfaces)] ページを使用します。管理インターフェイスを設定する場合は、スタックに含まれる任意のデバイスを選択できます。

Firepower スタック構成デバイスの [インターフェイス (Interfaces)] ページに、個々のデバイスのハードウェアおよびインターフェイスのビューがあります。

### 手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 プライマリ スタック構成デバイスの横で、編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3 [インターフェイス (Interfaces)] タブをクリックします。
- ステップ 4 [選択されたデバイス (Selected Device)] ドロップダウン リストから、変更するデバイスを選択します。
- ステップ 5 個々のデバイスに設定する場合と同じようにインターフェイスを設定します。[センシングインターフェイスの設定 \(579 ページ\)](#) を参照してください。

### 関連トピック

[管理インターフェイス \(931 ページ\)](#)

## スタック構成のデバイスの分離

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	FirePOWER 8140、8200 ファ ミリ、8300 ファ ミリ	任意 (Any)	Admin/Network Admin

デバイスのスタック構成を使用する必要がなくなった場合、スタックを解除してデバイスを分離できます。



- (注) スタック構成のデバイスに障害が発生した場合や、スタックのメンバーデバイス間の通信に障害が発生した場合は、Firepower Management Center Web インターフェイスを使用してスタック構成のデバイスを分離することはできません。この場合は、補助 CLI コマンド `configure stacking disable` を使用して、それぞれのデバイスから個別にスタック設定を削除します。

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 分断するデバイス スタックの横にあるスタックの分断アイコン (🔪) をクリックします。

**ヒント** スタックを分断することなく、3 台以上の Firepower 8250 デバイスのスタックからセカンダリ デバイスを削除するには、スタックからの削除アイコン (🗑️) をクリックします。セカンダリ デバイスを削除すると、システムがそのデバイス抜きで動作するスタックを再設定する間、トラフィック検査、トラフィックフロー、またはリンク状態が短時間中断されます。

**ステップ 3** [はい (Yes)] をクリックして、デバイス スタックを分離します。



## スタック内のデバイスの交換

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	FirePOWER 8140、8200 ファミリ、8300 ファミリ	任意 (Any)	Admin/Network Admin

Firepower Management Center がデバイスと通信できない場合に、スタックを分離してデバイスの登録を解除するには、デバイスに接続して CLI コマンドを使用する必要があります。詳細については、関連する章「[コンフィギュレーションコマンド \(2830 ページ\)](#)」の **stacking disable** CLI コマンドおよび **delete** CLI コマンドを参照してください。

スタック内のデバイスを交換するには、以下を行います。

### 手順

- 
- ステップ 1** デバイスを含むスタックを選択し、そのスタックを交換して解除します。詳細については、[スタック構成のデバイスの分離 \(634 ページ\)](#) を参照してください。
  - ステップ 2** Firepower Management Center からデバイスを登録解除します。詳細については、[Firepower Management Center からのデバイスの削除 \(552 ページ\)](#) を参照してください。
  - ステップ 3** 交換デバイスを Firepower Management Center に登録します。詳細については、[Firepower Management Center へのデバイスの追加 \(550 ページ\)](#) を参照してください。
  - ステップ 4** 交換デバイスを含むデバイス スタックを作成します。詳細については、[デバイス スタックの確立 \(628 ページ\)](#) を参照してください。
-





## 第 **VIII** 部

### **Firepower Threat Defense の設定の基本**

- [Firepower Threat Defense 用のトランスペアレントまたはルーテッドファイアウォールモード \(639 ページ\)](#)
- [Firepower Threat Defense のインターフェイス \(649 ページ\)](#)
- [Threat Defense 用の DHCP および DDNS サービス \(705 ページ\)](#)
- [Firepower Threat Defense 用の Quality of Service \(QoS\) \(717 ページ\)](#)





## 第 26 章

# Firepower Threat Defense 用のトランスペアレントまたはルーテッド ファイアウォールモード

この章では、ファイアウォールモードをルーテッドまたはトランスペアレントに設定する方法と、各ファイアウォールモードでファイアウォールがどのように機能するかについて説明します。



(注) ファイアウォールモードは通常のファイアウォールインターフェイスにのみ影響を与えます。インラインセットやパッシブインターフェイスなどの IPS 専用インターフェイスには影響を与えません。IPS 専用インターフェイスは両方のファイアウォールモードで使用可能です。IPS 専用インターフェイスの詳細については、[IPS のみ対応のインターフェイスの設定 \(694 ページ\)](#) を参照してください。インラインセットは「トランスペアレントインラインセット」と呼ばれることもありますが、インラインインターフェイスタイプはこの章で説明するトランスペアレント ファイアウォールモードおよびファイアウォールタイプのインターフェイスとは無関係です。

- [ファイアウォールモードについて \(639 ページ\)](#)
- [デフォルト設定 \(646 ページ\)](#)
- [ファイアウォールモードのガイドライン \(646 ページ\)](#)
- [ファイアウォールモードの設定 \(647 ページ\)](#)

## ファイアウォールモードについて

Firepower Threat Defense デバイスは、通常のファイアウォールインターフェイスでルーテッドファイアウォールモードとトランスペアレントファイアウォールモードの2つのファイアウォールモードをサポートします。

## ルータード ファイアウォール モードについて

ルータードモードでは、Firepower Threat Defense デバイスはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。

## トランスペアレント ファイアウォール モードについて

従来、ファイアウォールはルータードホップであり、保護されたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように機能するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。ただし、他のファイアウォールのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のすべてのチェックが実施されます。

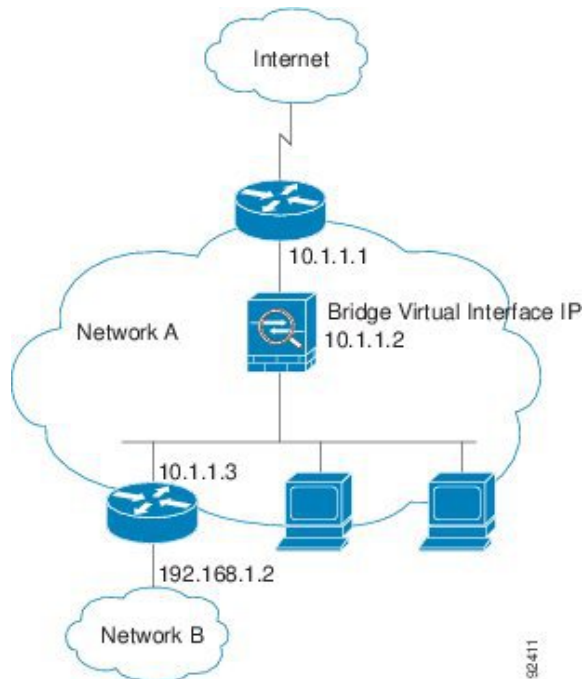
レイヤ2の接続は、ネットワーク上の内部、外部のインターフェイスをまとめた「ブリッジグループ」を使用して達成されます。また、Firepower Threat Defense デバイスはブリッジング技術を使用してインターフェイス間のトラフィックを通します。各ブリッジグループには、ネットワーク上でIPアドレスが割り当てられるブリッジ仮想インターフェイス (BVI) が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレントモードでは、これらのブリッジグループは相互通信できません。

## ネットワークでのトランスペアレント ファイアウォールの使用

Firepower Threat Defense デバイスは、自身のインターフェイス間を同じネットワークで接続します。トランスペアレント ファイアウォールはルータードホップではないので、既存のネットワークに簡単に導入できます。

次の図に、外部デバイスが内部デバイスと同じサブネット上にある一般的なトランスペアレント ファイアウォール ネットワークを示します。内部ルータと各ホストは、外部ルータに直接接続されているように見えます。

図 1: トランスペアレント ファイアウォール ネットワーク



## ブリッジグループについて

ブリッジグループは、Firepower Threat Defense デバイスがルーティングではなくブリッジするインターフェイスのグループです。ブリッジグループはトランスペアレントファイアウォールモードでのみサポートされています。他のファイアウォールインターフェイスのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のチェックがすべて実施されます。

### ブリッジ仮想インターフェイス (BVI)

各ブリッジグループには、ブリッジ仮想インターフェイス (BVI) が含まれます。Firepower Threat Defense デバイスは、ブリッジグループから発信されるパケットの発信元アドレスとしてこの BVI IP アドレスを使用します。BVI IP アドレスはブリッジグループメンバーインターフェイスと同じサブネット上になければなりません。BVI では、セカンダリネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

インターフェイスベースの各機能はブリッジグループのメンバーインターフェイスだけを指定でき、これらについてのみ使用できます。

### トランスペアレントファイアウォールモードのブリッジグループ

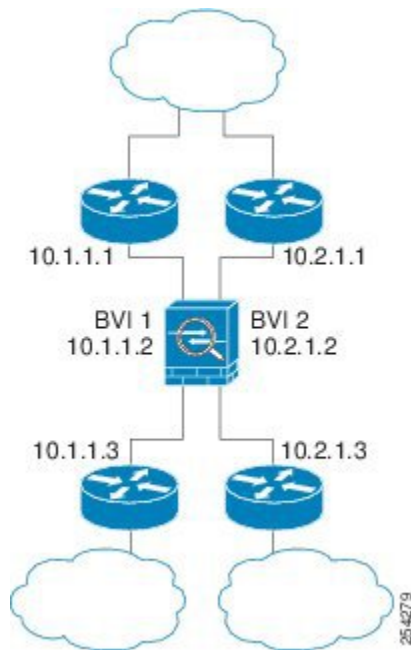
ブリッジグループのトラフィックは他のブリッジグループから隔離され、トラフィックは Firepower Threat Defense デバイス内の他のブリッジグループにはルーティングされません。また、トラフィックは外部ルータから Firepower Threat Defense デバイス内の別のブリッジグループにルーティングされる前に、Firepower Threat Defense デバイスから出る必要があります。ブ

リッジング機能はブリッジグループごとに分かれています。その他の多くの機能はすべてのブリッジグループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、すべてのブリッジグループで共有されます。

1つのブリッジグループにつき複数のインターフェイスを入れることができます。サポートされるブリッジグループとインターフェイスの正確な数については、[ファイアウォールモードのガイドライン \(646ページ\)](#) を参照してください。ブリッジグループごとに2つ以上のインターフェイスを使用する場合は、内部、外部への通信だけでなく、同一ネットワーク上の複数のセグメント間の通信を制御できます。たとえば、相互通信を希望しない内部セグメントが3つある場合、インターフェイスを別々のセグメントに置き、外部インターフェイスとのみ通信させることができます。または、インターフェイス間のアクセスルールをカスタマイズし、希望通りのアクセスを設定できます。

次の図に、2つのブリッジグループを持つ、Firepower Threat Defense デバイスに接続されている2つのネットワークを示します。

図 2: 2つのブリッジグループを持つトランスペアレントファイアウォールネットワーク



## 診断インターフェイス

各ブリッジ仮想インターフェイス (BVI) IP アドレスのほかに、別の診断スロットポートインターフェイスを追加できます。このインターフェイスはどのブリッジグループにも属さず、Firepower Threat Defense デバイス への管理トラフィックのみを許可します。

## レイヤ3 トラフィックの許可

- ユニキャストの IPv4 および IPv6 トラフィックがブリッジグループを通過するにはアクセスルールが必要です。



- ARP は、アクセスルールなしで両方向にブリッジグループを通過できます。ARP トラフィックは、ARP インスペクションによって制御できます。
- IPv6 ネイバー探索およびルータ送信要求パケットは、アクセスルールを使用して通過させることができます。
- ブロードキャストおよびマルチキャストトラフィックは、アクセスルールを使用して通過させることができます。

## 許可される MAC アドレス

アクセスポリシーで許可されている場合、以下の宛先 MAC アドレスをブリッジグループで使用できます ([レイヤ 3 トラフィックの許可 \(642 ページ\)](#) を参照)。このリストにない MAC アドレスはドロップされます。

- FFFF.FFFF.FFFF の TRUE ブロードキャスト宛先 MAC アドレス
- 0100.5E00.0000 ~ 0100.5EFE.FFFF までの IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ~ 3333.FFFF.FFFF までの IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD の BPDU マルチキャストアドレス

## BPDU 処理

スパニング ツリー プロトコルの使用によるループを回避するため、BPDU はデフォルトで通過します。

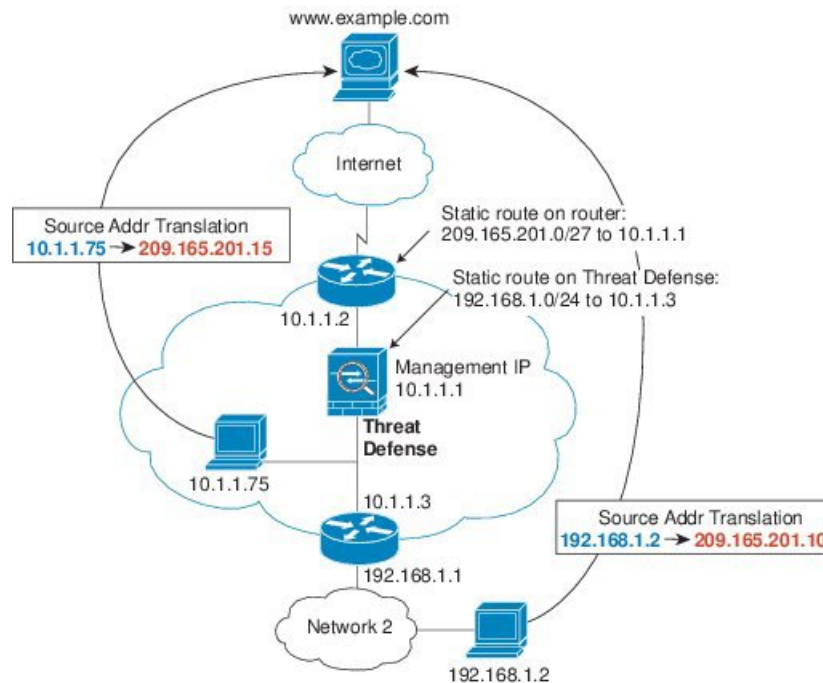
## MAC アドレスとルート ルックアップ

ブリッジグループ内のトラフィックでは、パケットの発信インターフェイスは、ルートルックアップではなく宛先 MAC アドレス ルックアップを実行することによって決定されます。

ただし、次のトラフィック タイプにはルート ルックアップが必要です。

- Firepower Threat Defense デバイス で発信されたトラフィック：たとえば、syslog サーバがリモートネットワークにある場合は、Firepower Threat Defense デバイス がそのサブネットに到達できるようにデフォルト/スタティック ルートを使用する必要があります。
- Firepower Threat Defense デバイス から少なくとも 1 ホップ離れており、Firepower Threat Defense デバイス が NAT を実行するトラフィック：Firepower Threat Defense デバイス がブリッジグループ インターフェイスに入ったパケットに対して NAT を実行し、そのパケットがリモートネットワークからのものだった場合、そのネットワークの Firepower Threat Defense デバイスのスタティック ルートを設定する必要があります。

図 3: NAT の例 : ブリッジグループ内の NAT



1. 内部ホスト 10.1.1.75 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.1.75 はマッピングアドレス 209.165.201.15 に変更されます。
  2. サーバが応答すると、マッピングアドレス 209.165.201.15 に応答を送信し、Firepower Threat Defense デバイスがそのパケットを受信します。これは、アップストリームルータには、Firepower Threat Defense デバイスの管理 IP アドレスに転送されるスタティックルートがこのマッピングネットワークが含まれるためです。
  3. その後、Firepower Threat Defense デバイスはマッピングアドレス 209.165.201.15 を変換して実際のアドレス 10.1.1.75 に戻します。実際のアドレスは直接接続されているため、Firepower Threat Defense デバイスはそのアドレスを直接ホストに送信します。
  4. ホスト 192.168.1.2 の場合も、リターントラフィックを除き、同じプロセスが発生します。Firepower Threat Defense デバイスはルーティングテーブルでルートを検索し、192.168.1.0/24 の Firepower Threat Defense デバイススタティックルートに基づいてパケットを 10.1.1.3 にあるダウンストリームルータに送信します。
- エンドポイントが Firepower Threat Defense デバイス から少なくとも 1 ホップ離れている Voice over IP (VoIP) と DNS トラフィック : たとえば、あるブリッジグループメンバーインターフェイスに CCM があり、別のブリッジグループメンバーインターフェイスにルータと H.323 ゲートウェイがある場合、H.323 ゲートウェイであるルータの正常なコール完了のために、Firepower Threat Defense デバイスにスタティックルートを追加する必要があります。検査されるトラフィックに対して NAT を有効化すると、スタティックルートは、パケットに埋め込まれている本当のホストアドレスの出力インターフェイスを決定する必要があります。影響を受けるアプリケーションは次のとおりです。

- DNS
- H.323
- RTSP
- SIP
- Skinny (SCCP)
- SunRPC
- TFTP

### トランスペアレントモードのブリッジグループのサポートされていない機能

次の表に、トランスペアレントモードのブリッジグループでサポートされない機能を示します。

表 58: トランスペアレントモードでサポートされない機能

機能	説明
ダイナミック DNS	-
DHCP リレー	トランスペアレント ファイアウォールは DHCPv4 サーバとして機能することができますが、DHCP リレーはサポートしません。2つのアクセスルール（1つは内部インターフェイスから外部インターフェイスへの DHCP 要求を許可し、もう1つはサーバからの応答を逆方向に許可します。）を使用して DHCP トラフィックを通過させることができるので、DHCP リレーは必要ありません。
ダイナミック ルーティング プロトコル	ただし、ブリッジグループメンバーインターフェイスの場合、Firepower Threat Defense デバイスで発信されたトラフィックにスタティックルートを追加できます。アクセスルールを使用して、ダイナミックルーティングプロトコルが Firepower Threat Defense デバイスを通過できるようにすることもできます。
マルチキャスト IP ルーティング	アクセスルールで許可することによって、マルチキャストトラフィックが Firepower Threat Defense デバイスを通過できるようにすることができます。
QoS	□

機能	説明
通過トラフィック用の VPN 終端	トランスペアレントファイアウォールは、ブリッジグループメンバーインターフェイスでのみ、管理接続用のサイト間VPNトンネルをサポートします。これは、Firepower Threat Defense デバイスを通過するトラフィックに対してVPN接続を終端しません。アクセスルールを使用してVPNトラフィックにASAを通過させることはできますが、非管理接続は終端されません。

## ルーテッドモード機能のためのトラフィックの通過

トランスペアレントファイアウォールで直接サポートされていない機能の場合は、アップストリームルータとダウンストリームルータが機能をサポートできるようにトラフィックの通過を許可することができます。たとえば、アクセスルールを使用することによって、（サポートされていないDHCPリレー機能の代わりに）DHCPトラフィックを許可したり、IP/TVで作成されるようなマルチキャストトラフィックを許可したりできます。また、トランスペアレントファイアウォールを通過するルーティングプロトコル隣接関係を確立することもできます。つまり、OSPF、RIP、EIGRP、またはBGPトラフィックをアクセスルールに基づいて許可できます。同様に、HSRPやVRRPなどのプロトコルはFirepower Threat Defense デバイスを通過できます。

## デフォルト設定

### ブリッジグループのデフォルト

デフォルトでは、すべてのARPパケットはブリッジグループ内で渡されます。

## ファイアウォールモードのガイドライン

### モデルのガイドライン

- ブリッジされたixgbevifインターフェイスを持つVMware上のFirepower Threat Defense Virtualでは、トランスペアレントファイアウォールモードのブリッジグループはサポートされません。

### ブリッジグループのガイドライン（トランスペアレントモード）

- 4のインターフェイスをもつブリッジグループを250まで作成できます。
- 直接接続された各ネットワークは同じサブネット上に置かれている必要があります。

- Firepower Threat Defense デバイス では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- IPv4 の場合は、管理トラフィックと、Firepower Threat Defense デバイス を通過するトラフィックの両方の各ブリッジグループに対し、BVI の IP アドレスが必要です。IPv6 アドレスは BVI でサポートされますが必須ではありません。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホストサブネット (255.255.255.255) を設定することはできません。
- 管理インターフェイスはブリッジグループのメンバーとしてサポートされません。
- トランスペアレントモードでは、少なくとも1つのブリッジグループを使用し、データインターフェイスがブリッジグループに属している必要があります。
- トランスペアレントモードでは、接続されたデバイス用のデフォルトゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは Firepower Threat Defense デバイスの反対側にあるルータをデフォルトゲートウェイとして指定する必要があります。
- トランスペアレントモードでは、管理トラフィックの戻りパスを指定するために必要なデフォルトルートは、1つのブリッジグループネットワークからの管理トラフィックにだけ適用されます。これは、デフォルトルートはブリッジグループのインターフェイスとブリッジグループネットワークのルータ IP アドレスを指定しますが、ユーザは1つのデフォルトルートしか定義できないためです。複数のブリッジグループネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティックルートを指定する必要があります。
- トランスペアレントモードでは、PPPoE は 診断インターフェイスとしてサポートされません。

## ファイアウォール モードの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ファイアウォールモードは、最初のシステムセットアップの実行時に CLI で設定できます。セットアップ時にファイアウォールモードを設定することをお勧めします。これは、ファイアウォールモードを変更すると、非適合の設定が発生しないように設定が消去されるためです。ファイアウォールモードの変更が後で必要になった場合は、CLI から変更する必要があります。

## 手順

**ステップ 1** Management Center から Firepower Threat Defense デバイスの登録を解除します。

モードの変更は、デバイスの登録を解除するまで実行できません。

- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- b) 管理対象デバイスのリストから、デバイスを選択します。
- c) デバイスを削除 (ゴミ箱アイコンをクリック) して、確認してから、システムがデバイスを削除するまで待機します。

**ステップ 2** Firepower Threat Defense デバイスの CLI にアクセスします。可能ならばコンソールポートからアクセスします。

診断インターフェイスへの SSH を使用している場合、モードを変更すると、インターフェイスの設定が消去され、切断されます。代わりに、管理インターフェイスに接続する必要があります。

**ステップ 3** ファイアウォール モードを変更します。

**configure firewall [routed | transparent]**

例 :

```
> configure firewall transparent
This will destroy the current interface configurations, are you sure that you want to
proceed? [y/N] y
The firewall mode was changed successfully.
```

**ステップ 4** Management Center に再登録します。

**configure manager add {hostname | ip\_address | DONTRESOLVE} reg\_key [nat\_id]**

引数の説明

- {hostname | ip\_address | DONTRESOLVE } は、Management Center の完全修飾ホスト名または IP アドレスのいずれかを指定します。Management Center を直接アドレス指定できない場合は、DONTRESOLVE を使用します。
- reg\_key は、デバイスを Management Center に登録するために必要な一意の英数字による登録キーです。
- nat\_id は、Management Center とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。これは、ホスト名が DONTRESOLVE に設定されている場合に必要です。



## 第 27 章

# Firepower Threat Defense のインターフェイス

この章では、Firepower Threat Defense のインターフェイス設定（イーサネット設定、EtherChannel、VLAN サブインターフェイス、IP アドレス指定など）について説明します。

- [Firepower Threat Defense インターフェイスについて](#) (649 ページ)
- [通常の（ファイアウォール）モードインターフェイスの設定](#) (654 ページ)
- [IPS のみ対応のインターフェイスの設定](#) (694 ページ)
- [インターフェイスと Firepower Management Center の同期](#) (702 ページ)

## Firepower Threat Defense インターフェイスについて

Firepower Threat Defense デバイスには、種々のモードで設定できるデータインターフェイス、および管理/診断インターフェイスが組み込まれています。

### 管理/診断インターフェイスとネットワーク配置

物理的な管理インターフェイスは、診断論理インターフェイスと管理論理インターフェイスの間で共有できます。

### 管理インターフェイス

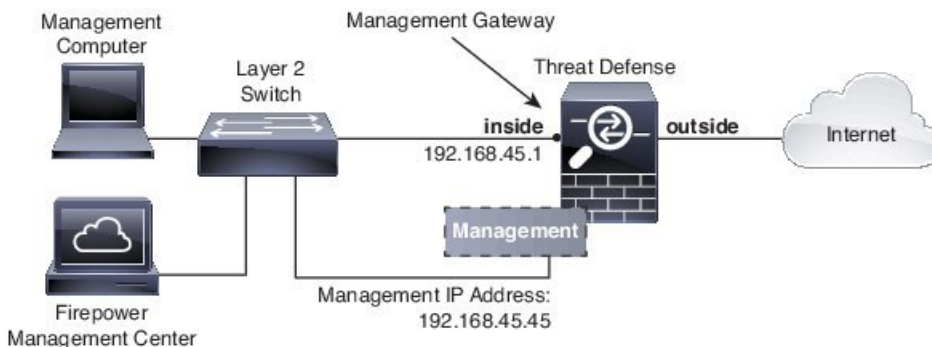
管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。Firepower Management Center にデバイスを設定し、登録するために使用されます。また、固有の IP アドレスとスタティック ルーティングを使用します。管理インターフェイスの設定を構成するには、CLI で `configure network` コマンドを使用します。管理インターフェイスを Firepower Management Center に追加した後にその IP アドレスを CLI で変更した場合、Firepower Management Center での IP アドレスを [デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Devices)] > [管理 (Management)] 領域で一致させることができます。

## 診断インターフェイス

診断論理インターフェイスは残りのデータインターフェイスとともに、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [インターフェイス (Interfaces)] 画面で設定できます。診断インターフェイスの使用はオプションです（シナリオについては、ルーテッドモードおよびトランスペアレントモードの展開を参照）。診断インターフェイスは管理トラフィックのみを許可し、トラフィックのスルーは許可しません。これはSSHをサポートしません。データインターフェイスまたは管理インターフェイスのみにSSHを使用できます。診断インターフェイスは、SNMP や syslog のモニタリングに役立ちます。

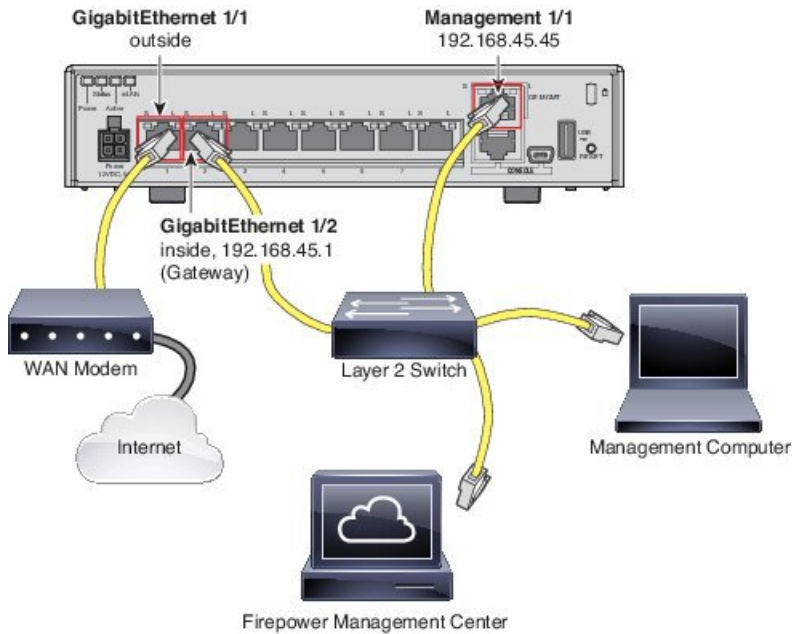
## ルーテッドモードの導入

内部ルータがない場合は診断インターフェイスのIPアドレスを設定しないことをお勧めします。診断インターフェイスのIPアドレスを設定しなければ、他のデータインターフェイスと同じネットワーク上に管理インターフェイスを配置できます。診断インターフェイスを設定すると、一般的にそのIPアドレスは管理IPアドレスと同じネットワークになり、他のデータインターフェイスと同じネットワーク上に存在できない標準インターフェイスと見なされます。管理インターフェイスは更新のためにインターネットにアクセスする必要があるため、管理インターフェイスを内部インターフェイスと同じネットワーク上に置くと、内部にスイッチのみを持つ Firepower Threat Defense デバイスを導入して、そのゲートウェイとして内部インターフェイスを指定することができます。内部スイッチを使用する次の導入を参照してください。

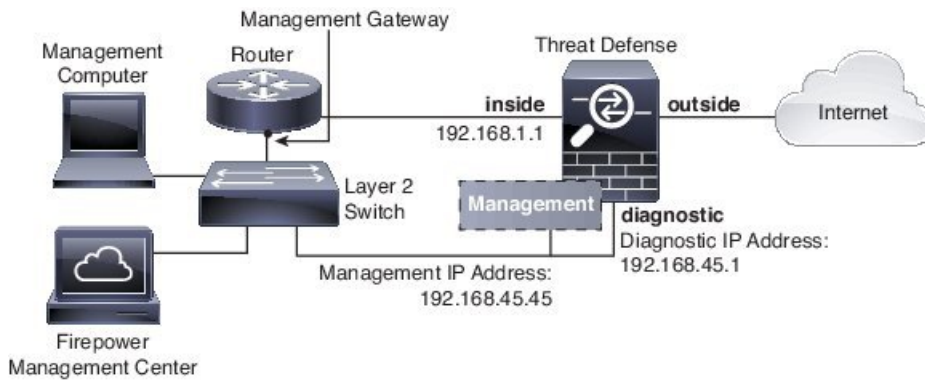


ASA 5506-X、ASA 5508-X、または ASA 5516-X で上記のシナリオをケーブル接続するには、次を参照してください。



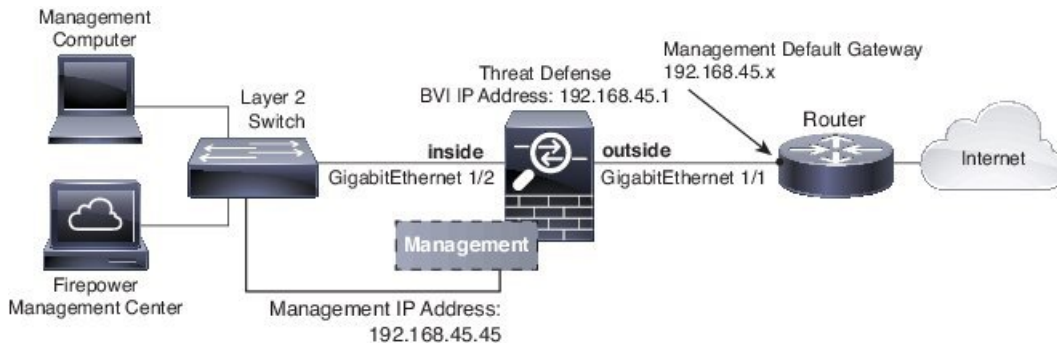


診断 IP アドレスを設定する場合は、内部ルータが必要です。

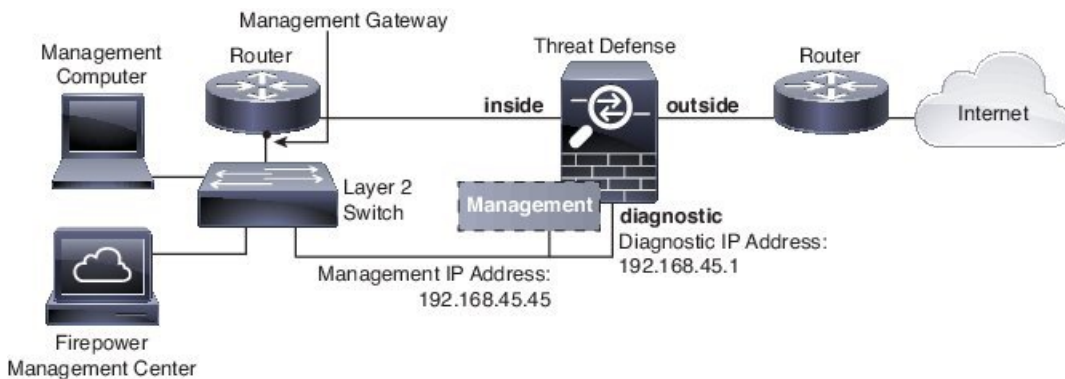


## トランスペアレントモードの展開

ルーテッドモードの展開と同様、内部スイッチを使用したデバイスの展開を選択できます。この場合、診断インターフェイスを IP アドレスなしで維持する必要があります。



また、内部ルータを使用して展開することもできます。この場合、追加の管理アクセスのために、IP アドレスを持つ診断インターフェイスを使用できます。



## インターフェイスモードとタイプ

通常のファイアウォールモードと IPS 専用モードの 2 つのモードで Firepower Threat Defense インターフェイスを展開できます。同じデバイスにファイアウォールインターフェイスと IPS 専用インターフェイスの両方を含めることができます。

### 通常のファイアウォールモード

ファイアウォールモードのインターフェイスでは、トラフィックが、フローの維持、IP レイヤおよび TCP レイヤの両方でのフロー状態の追跡、IP 最適化、TCP の正規化などのファイアウォール機能の対象となります。オプションで、セキュリティポリシーに従ってこのトラフィックに IPS 機能を設定することもできます。

設定できるファイアウォールインターフェイスのタイプは、ルーテッドモードとトランスペアレントモードのどちらのファイアウォールモードがそのデバイスに設定されているかによって異なります。詳細については、[Firepower Threat Defense 用のトランスペアレントまたはルーテッドファイアウォールモード \(639 ページ\)](#) を参照してください。

- ルーテッドモードインターフェイス（ルーテッドファイアウォールモードのみ）：ルーティングを行う各インターフェイスは異なるサブネット上にあります。
- ブリッジグループインターフェイス（トランスペアレントファイアウォールモードのみ）：複数のインターフェイスをネットワーク上でグループ化することができ、Firepower Threat Defense デバイスはブリッジング技術を使用してインターフェイス間のトラフィックを通過させることができます。各ブリッジグループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。各ブリッジグループは分離されていて、相互通信できません。

### IPS 専用モード

IPS 専用モードのインターフェイスは、多数のファイアウォールのチェックをバイパスし、IPS セキュリティポリシーのみをサポートします。別のファイアウォールがこれらのインターフェ

イスを保護していて、ファイアウォール機能のオーバーヘッドを避けたい場合、IPS 専用のインターフェイスを実装することがあります。



- (注) ファイアウォールモードは通常のファイアウォールインターフェイスのみに影響し、インラインセットやパッシブインターフェイスなどのIPS専用インターフェイスには影響しません。IPS専用インターフェイスはどちらのファイアウォールモードでも使用できます。

IPS専用インターフェイスは以下のタイプとして展開できます。

- **インラインセット、タップモードのオプションあり**：インラインセットは「Bump In The Wire」のように動作し、2つのインターフェイスを一緒にバインドし、既存のネットワークに組み込みます。この機能によって、隣接するネットワークデバイスの設定がなくても、任意のネットワーク環境にシステムをインストールすることができます。インラインインターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インラインセットの外部に再送信されます。

タップモードの場合、デバイスはインラインで展開されますが、パケットがデバイスを通過する代わりに各パケットのコピーがデバイスに送信され、ネットワークトラフィックフローは影響を受けません。ただし、これらのタイプのルールでは、トリガーされた侵入イベントが生成され、侵入イベントのテーブルビューには、トリガーの原因となったパケットがインライン展開でドロップされたことが示されます。インライン展開されたデバイスでタップモードを使用することには、利点があります。たとえば、デバイスがインラインであるかのようにデバイスとネットワークの間の配線をセットアップし、デバイスが生成するタイプの侵入イベントを分析することができます。その結果に基づいて、効率性に影響を与えることなく最適なネットワーク保護を提供するように、侵入ポリシーを変更して廃棄ルールを追加できます。デバイスをインラインで展開する準備ができたなら、タップモードを無効にして、デバイスとネットワークの間の配線を再びセットアップすることなく、不審なトラフィックをドロップし始めることができます。



- (注) 「透過インラインセット」としてインラインセットに馴染みがある人もいますが、インラインインターフェイスのタイプはトランスペアレントファイアウォールモードやファイアウォールタイプのインターフェイスとは無関係です。

- **パッシブまたは ERSPAN パッシブ**：パッシブインターフェイスは、スイッチ SPAN またはミラーポートを使用してネットワークを流れるトラフィックをモニタします。SPAN またはミラーポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワークトラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション（トラフィックのブロッキングやシェーピングなど）を実行することができません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。Encapsulated Remote Switched

Port Analyzer (ERSPAN) インターフェイスは、複数のスイッチに分散された送信元ポートからのトラフィックをモニタし、GRE を使用してトラフィックをカプセル化します。ERSPAN インターフェイスは、デバイスがルーテッドファイアウォールモードになっている場合にのみ許可されます。

## セキュリティゾーンとインターフェイスグループ

各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てる必要があります。その上で、ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。また、たとえば、トラフィックが内部から外部に移動できるようにアクセスコントロールポリシーを設定することはできますが、外部から内部に向けては設定できません。ポリシーによっては、セキュリティゾーンだけをサポートする場合も、ゾーンとグループの両方をサポートする場合もあります。詳細については、[インターフェイスオブジェクト：インターフェイスグループとセキュリティゾーン \(437 ページ\)](#) を参照してください。セキュリティゾーンおよびインターフェイスグループは、[オブジェクト (Objects)] ページで作成できます。また、インターフェイスを設定する際にゾーンを追加することもできます。インターフェイスは、そのインターフェイスに適切なタイプのゾーン (パッシブ、インライン、ルーテッド、スイッチドゾーンタイプ) にのみ追加できます。

診断/管理インターフェイスは、ゾーンまたはインターフェイスグループには属しません。

## Auto-MDI/MDIX 機能

RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーションフェーズでストレートケーブルを検出すると、内部クロスオーバーを実行することでクロスケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。ギガビットイーサネットの速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常にイネーブルになり、ディセーブルにできません。

## 通常の (ファイアウォール) モードインターフェイスの設定

通常のインターフェイスでは、物理インターフェイスを設定し、冗長インターフェイス、EtherChannel インターフェイス、および VLAN サブインターフェイスを作成することもできます。ルーテッドインターフェイスまたはブリッジインターフェイスを設定できます。

## 手順

**ステップ 1** Firepower Threat Defense アプライアンスの場合は、次のタスクを実行します。FXOS シャーシ上の Firepower Threat Defense の場合は、Firepower 4100/9300 シャーシスーパーバイザで基本のインターフェイス設定を構成します。詳細については、『[Firepower 9300 configuration guide](#)』を参照してください。

- a) [物理インターフェイスの有効化およびイーサネット設定の構成 \(655 ページ\)](#)
- b) (任意) (オプション) [冗長インターフェイスの設定 \(662 ページ\)](#)

冗長インターフェイスを設定して Firepower Threat Defense の信頼性を高めることができます。

- c) (任意) (オプション) [EtherChannel の設定 \(664 ページ\)](#)

EtherChannel により複数のインターフェイスを組み合わせることができるため、単一ネットワークに帯域幅を増大し、インターフェイス冗長性を提供することもできます。

**ステップ 2** (任意) [VLAN サブインターフェイスと 802.1Q トランキングの設定 \(666 ページ\)](#) .

VLAN サブインターフェイスを使用すると、1 つの物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。

**ステップ 3** [ルーテッドモードのインターフェイスの設定 \(672 ページ\)](#) または [トランスペアレントモードのブリッジグループインターフェイスの設定 \(674 ページ\)](#) ファイアウォールモードに応じて。

**ステップ 4** (任意) [IPv6 アドレッシングの設定 \(678 ページ\)](#)

**ステップ 5** (任意) [インターフェイスの詳細設定 \(683 ページ\)](#) を実行します。

インターフェイスの MAC アドレス、MTU、およびその他の設定を手動で設定できます。

## 物理インターフェイスの有効化およびイーサネット設定の構成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ここでは、次の方法について説明します。

- 物理インターフェイスを有効にします。デフォルトでは、物理インターフェイスは無効になっています (診断 インターフェイスを除く)。

- 特定の速度と二重通信を設定します。デフォルトでは、速度とデュプレックスは [自動 (Auto) ] に設定されます。

この手順は、インターフェイス設定のごく一部にすぎません。この時点では、他のパラメータを設定しないようにします。たとえば、EtherChannel または冗長インターフェイスの一部として使用するインターフェイスには名前を付けることはできません。



- (注) FXOS シャーシ上の Firepower Threat Defense の場合は、Firepower 4100/9300 シャーシ で基本のインターフェイス設定を構成します。詳細については、『[Firepower 9300 configuration guide](#)』を参照してください。

### 始める前に

Management Center に追加した後、デバイスの物理インターフェイスを変更した場合、[インターフェイス (Interfaces) ] タブの左上にある [デバイスからのインターフェイスの同期 (Sync Interfaces from device) ] ボタンをクリックしてそのインターフェイスリストを更新する必要があります。

### 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (✎) をクリックします。デフォルトで [インターフェイス (Interfaces) ] タブが選択されています。
- ステップ 2** 編集するインターフェイスの編集アイコン (✎) をクリックします。
- ステップ 3** [モード (Mode) ] ドロップダウンリストで、[なし (None) ] を選択します。
- 通常のファイアウォールインターフェイスのモードは [なし (None) ] に設定されています。他のモードは IPS 専用インターフェイスタイプ向けです。
- ステップ 4** [有効 (Enabled) ] チェック ボックスをオンにして、インターフェイスを有効化します。
- ステップ 5** (任意) [説明 (Description) ] フィールドに説明を追加します。
- 説明は 200 文字以内で、改行を入れずに 1 行で入力します。
- ステップ 6** (任意) [ハードウェア構成 (Hardware Configuration) ] タブをクリックして、デュプレックスと速度を設定します。
- [デュプレックス (Duplex) ] : [全 (Full) ]、[半 (Half) ]、または [自動 (Auto) ] を選択します。[自動 (Auto) ] は、インターフェイスによってサポートされる場合のみデフォルトとなります。
  - [速度 (Speed) ] : [10]、[100]、[1000]、または [自動 (Auto) ] を選択します。デフォルトは [自動 (Auto) ] です。インターフェイスのタイプによって、選択可能なオプションが制限されます。

ステップ7 [OK] をクリックします。

ステップ8 [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## EtherChannel インターフェイスと冗長インターフェイス

このセクションでは、EtherChannel インターフェイスと冗長インターフェイスを設定する方法について説明します。

### EtherChannel インターフェイスと冗長インターフェイスについて

ここでは、EtherChannel インターフェイスと冗長インターフェイスについて説明します。

#### 冗長インターフェイス

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブインターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイインターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定して Firepower Threat Defense デバイスの信頼性を高めることができます。

最大 8 個の冗長インターフェイス ペアを設定できます。

#### 冗長インターフェイスの MAC アドレス

冗長インターフェイスでは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバー インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに手動で MAC アドレスを割り当てることができます。これはメンバー インターフェイスの MAC アドレスに関係なく使用されます。アクティブ インターフェイスがスタンバイインターフェイスにフェールオーバーすると、トラフィックが中断しないように同じ MAC アドレスが維持されます。

#### EtherChannel

802.3ad EtherChannel は、単一のネットワークの帯域幅を増やすことができるように、個別のイーサネット リンク（チャンネルグループ）のバンドルで構成される論理インターフェイスです（ポートチャンネルインターフェイスと呼びます）。ポートチャンネルインターフェイスは、インターフェイス関連の機能を設定するときに、物理インターフェイスと同じように使用します。

最大 48 個の EtherChannel を設定できます。

## チャンネルグループインターフェイス

各チャンネルグループは、最大 16 個のアクティブ インターフェイスを設定できます。8 個のアクティブインターフェイスだけをサポートするスイッチの場合、1つのチャンネルグループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイリンクとして動作できます。16 個のアクティブ インターフェイスの場合、スイッチがこの機能をサポートしている必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。

チャンネルグループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャンネルグループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。RJ-45 または SFP コネクタを使用するように設定できるインターフェイスの場合、同一の EtherChannel に RJ-45 インターフェイスと SFP インターフェイスの両方を含めることができることに注意してください。

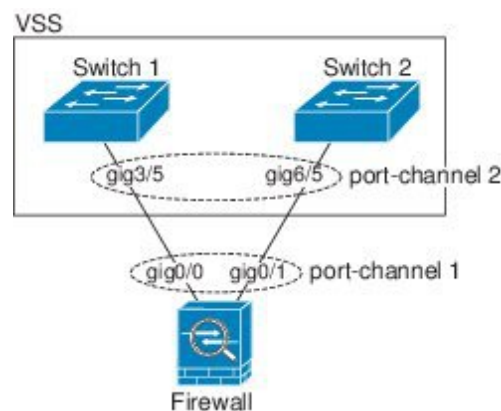
EtherChannel によって、チャンネル内の使用可能なすべてのアクティブインターフェイスのトラフィックが集約されます。インターフェイスは、送信元または宛先 MAC アドレス、IP アドレス、TCP および UDP ポート番号、および VLAN 番号に基づいて、独自のハッシュアルゴリズムを使用して選択されます。

別のデバイスの *EtherChannel* への接続

Firepower Threat Defense デバイス EtherChannel の接続先のデバイスも 802.3ad EtherChannel をサポートしている必要があります。たとえば、Catalyst 6500 スイッチまたは Cisco Nexus 7000 に接続できます。

スイッチが仮想スイッチングシステム (VSS) または仮想ポートチャンネル (vPC) の一部である場合、同じ EtherChannel 内の Firepower Threat Defense デバイス インターフェイスを VSS/vPC 内の個別のスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャンネルインターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。

図 4: VSS/vPC への接続

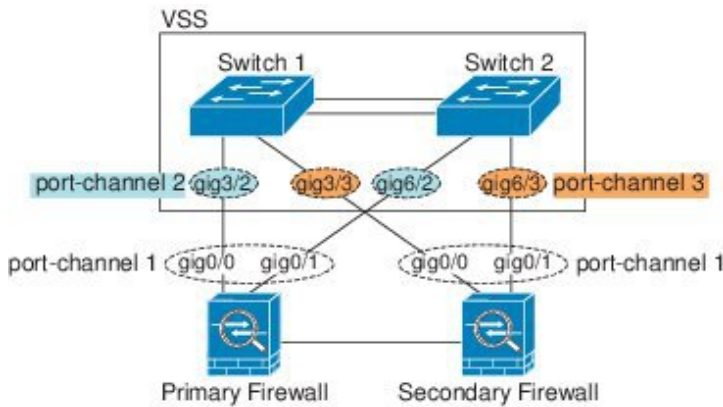


Firepower Threat Defense デバイス をアクティブ/スタンバイ フェールオーバー配置で使用する場合、Firepower Threat Defense デバイスごとに 1 つ、VSS/vPC 内のスイッチで個別の EtherChannel



を作成する必要があります。各 Firepower Threat Defense デバイスで、1つの EtherChannel が両方のスイッチに接続します。すべてのスイッチ インターフェイスを両方の Firepower Threat Defense デバイスに接続する単一の EtherChannel にグループ化できる場合でも（この場合、個別の Firepower Threat Defense デバイス システム ID のため、EtherChannel は確立されません）、単一の EtherChannel は望ましくありません。これは、トラフィックをスタンバイ Firepower Threat Defense デバイスに送信しないようにするためです。

図 5: アクティブ/スタンバイ フェールオーバーと VSS/vPC



## リンク集約制御プロトコル

リンク集約制御プロトコル（LACP）では、2つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理インターフェイスを次のように設定できます。

- **アクティブ**：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- **パッシブ**：LACP アップデートを受信します。パッシブ EtherChannel は、アクティブ EtherChannel のみと接続を確立できます。
- **オン**：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバ インターフェイスの両端が正しいチャンネルグループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャンネルグループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

## ロード バランシング

Firepower Threat Defense デバイスは、パケットの送信元および宛先 IP アドレスをハッシュすることによって、パケットを EtherChannel 内のインターフェイスに分散します（この基準は設

定可能です)。生成されたハッシュ値をアクティブなリンクの数で割り、そのモジュロ演算で求められた余りの値によってフローの割り当て先のインターフェイスが決まります。

$hash\_value \bmod active\_links$  の結果が 0 となるすべてのパケットは、EtherChannel 内の最初のインターフェイスへ送信され、以降は結果が 1 となるものは 2 番目のインターフェイスへ、結果が 2 となるものは 3 番目のインターフェイスへ、というように送信されます。たとえば、15 個のアクティブリンクがある場合、モジュロ演算では 0～14 の値が得られます。6 個のアクティブリンクの場合、値は 0～5 となり、以降も同様になります。

アクティブインターフェイスがダウンし、スタンバイインターフェイスに置き換えられない場合、トラフィックは残りのリンク間で再バランスされます。失敗はレイヤ 2 のスパンニングツリーとレイヤ 3 のルーティングテーブルの両方からマスクされるため、他のネットワークデバイスへのスイッチオーバーはトランスペアレントです。

### EtherChannel MAC アドレス

1 つのチャンネルグループに含まれるすべてのインターフェイスは、同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワークアプリケーションとユーザに対してトランスペアレントになります。ネットワークアプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。

ポートチャンネルインターフェイスは、最も小さいチャンネルグループインターフェイスの MAC アドレスをポートチャンネル MAC アドレスとして使用します。または、ポートチャンネルインターフェイスの MAC アドレスを手動で設定することもできます。グループチャンネルインターフェイスのメンバーシップを変更する場合は、固有の MAC アドレスを手動で設定するか、設定することを推奨します。ポートチャンネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャンネル MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。

## EtherChannel インターフェイスと冗長インターフェイスのガイドライン

### ハイアベイラビリティ

- 冗長インターフェイスまたは EtherChannel インターフェイスをハイアベイラビリティリンクとして使用する場合、ハイアベイラビリティペアの両装置内で事前設定が必要です。プライマリ装置で設定し、その設定がセカンダリ装置に複製されることはありません。これは、ハイアベイラビリティリンク自体が複製に必要であるためです。
- 冗長インターフェイスまたは EtherChannel インターフェイスをスタートリンクに対して使用する場合、特別なコンフィギュレーションは必要ありません。コンフィギュレーションは通常どおりプライマリ装置から複製されます。
- 冗長インターフェイスまたは EtherChannel インターフェイスから、ハイアベイラビリティをモニタできます。アクティブなメンバーインターフェイスがスタンバイインターフェイスにフェールオーバーした場合、デバイスレベルのハイアベイラビリティをモニタ中、このアクティビティが冗長インターフェイスまたは EtherChannel インターフェイスの障害発生の原因のように見えません。すべての物理インターフェイスで障害が発生した場合にのみ、冗長インターフェイスまたは EtherChannel インターフェイスで障害が発生して

いるように見えます (EtherChannel インターフェイスでは、障害の発生が許容されるメンバーインターフェイスの数を設定できます)。

- EtherChannel インターフェイスをハイ アベイラビリティ またはステート リンクに使用する場合、out-of-order パケット (順番の乱れたパケット) を防ぐために、EtherChannel のインターフェイスを1つだけ使用します。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。ハイアベイラビリティリンクとして使用中の EtherChannel の設定は変更できません。設定を変更するには、変更時に EtherChannel をシャットダウンするか、ハイアベイラビリティを一時的にディセーブルにする必要があります。どちらの操作でも、その間はハイアベイラビリティは行われません。

### モデルのサポート

- EtherChannel は、Firepower Threat Defense デバイス アプライアンスでのみサポートされています。ではサポートされません Firepower Threat Defense Virtual。
- Firepower 9300 シャーシでは、Firepower Threat Defense デバイス OS ではなく、FXOS で EtherChannel を構成します。
- Firepower 9300 シャーシでは、冗長インターフェイスはサポートされません。

### 冗長インターフェイス

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- すべての Firepower Threat Defense デバイス コンフィギュレーションは、メンバー物理インターフェイスではなく論理冗長インターフェイスを参照します。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを Firepower Threat Defense デバイス 上で設定できます。
- アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。
- 冗長インターフェイスは、診断 *slot/port* インターフェイスをメンバーとしてサポートしません。ただし、診断以外のインターフェイスで構成される冗長インターフェイスを、管理専用として設定することができます。

### EtherChannel

- EtherChannel は、Firepower Threat Defense デバイス アプライアンスでのみサポートされています。ではサポートされません Firepower Threat Defense Virtual。
- 最大 48 個の EtherChannel を設定できます。

- 各チャンネルグループは、最大 16 個のアクティブ インターフェイスを設定できます。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャンネルグループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。
- チャンネルグループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャンネルグループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。RJ-45 または SFP コネクタを使用するように設定できるインターフェイスの場合、同一の EtherChannel に RJ-45 インターフェイスと SFP インターフェイスの両方を含めることができることに注意してください。
- Firepower Threat Defense デバイス EtherChannel の接続先のデバイスも 802.3ad EtherChannel をサポートしている必要があります。たとえば、Catalyst 6500 スイッチまたは Cisco Nexus 7000 スイッチに接続できます。
- Firepower Threat Defense デバイスは、VLAN タグ付きの LACPDU をサポートしていません。Cisco IOS `vlan dot1Q tag native` コマンドを使用して、隣接スイッチのネイティブ VLAN タギングをイネーブルにすると Firepower Threat Defense デバイスはタグ付きの LACPDU をドロップします。隣接スイッチのネイティブ VLAN タギングは、必ずディセーブルにしてください。
- 15.1(1)S2 以前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンを実行する Firepower Threat Defense デバイスでは、スイッチ スタックに EtherChannel を接続することをサポートしていませんでした。デフォルトのスイッチ設定では、Firepower Threat Defense デバイス EtherChannel がクロス スタックに接続されている場合、マスター スイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、`stack-mac persistent timer` コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0（無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- すべての Firepower Threat Defense デバイス コンフィギュレーションは、メンバ物理インターフェイスではなく論理 EtherChannel インターフェイスを参照します。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを Firepower Threat Defense デバイス 上で設定できます。

## 冗長インターフェイスの設定

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブインターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定して Firepower Threat Defense の信頼性を高めることができます。デフォルトでは、冗長インターフェイスは有効になっています。



(注) FXOS シャーシ上の Firepower Threat Defense では、冗長インターフェイスはサポートされません。

#### 始める前に

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- 両方のメンバーインターフェイスが同じ物理タイプである必要があります。たとえば、両方ともギガビットイーサネットにする必要があります。
- 名前が設定されている場合は、物理インターフェイスを冗長インターフェイスに追加できません。最初に名前を削除する必要があります。

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin



**注意** コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

#### 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (🔧) をクリックします。デフォルトで [インターフェイス (Interfaces) ] タブが選択されています。
- ステップ 2** [物理インターフェイスの有効化およびイーサネット設定の構成 \(655 ページ\)](#) に従って、メンバー インターフェイスを有効にします。
- ステップ 3** [インターフェイスの追加 (Add Interfaces) ] > [冗長インターフェイス (Redundant Interface) ] をクリックします。
- ステップ 4** [一般 (General) ] タブで、次のパラメータを設定します。
  - [冗長 ID (Redundant ID) ] : 1 ~ 8 の整数を設定します。
  - [プライマリ インターフェイス (Primary Interface) ] : ドロップダウン リストからインターフェイスを選択します。インターフェイスを追加すると、インターフェイスのコンフィギュレーション (IP アドレスなど) はすべて削除されます。
  - [セカンダリ インターフェイス (Secondary Interface) ] : 2 番目のインターフェイスは、最初のインターフェイスと同じ物理的なタイプである必要があります。

**ステップ 5** [OK] をクリックします。

**ステップ 6** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

**ステップ 7** (任意) VLAN サブインターフェイスを追加します。 [VLAN サブインターフェイスと 802.1Q トランキングの設定 \(666 ページ\)](#) を参照してください。

**ステップ 8** ルーテッドまたはトランスペアレント モード インターフェイスのパラメータを設定します。 [ルーテッドモードのインターフェイスの設定 \(672 ページ\)](#) または [トランスペアレントモードのブリッジグループ インターフェイスの設定 \(674 ページ\)](#) を参照してください。

## EtherChannel の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ここでは、EtherChannel ポートチャンネル インターフェイスの作成、インターフェイスの EtherChannel への割り当て、EtherChannel のカスタマイズ方法について説明します。



(注) FXOS シャーシ上の Firepower Threat Defense の場合は、Firepower 4100/9300 シャーシスーパーバイザで EtherChannel を設定します。詳細については、『[Firepower 9300 configuration guide](#)』を参照してください。

### 始める前に

- 最大 48 個の EtherChannel を設定できます。
- 各チャンネルグループは、最大 16 個のアクティブ インターフェイスを設定できます。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャンネルグループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。
- チャンネルグループのすべてのインターフェイスは、同じタイプ、速度、および二重通信である必要があります。半二重はサポートされません。
- 名前が設定されている場合は、物理インターフェイスをチャンネルグループに追加できません。最初に名前を削除する必要があります。



- (注) コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

#### 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (  ) をクリックします。デフォルトで [インターフェイス (Interfaces) ] タブが選択されています。
- ステップ 2** [物理インターフェイスの有効化およびイーサネット設定の構成 \(655 ページ\)](#) に従って、メンバー インターフェイスを有効にします。
- ステップ 3** [インターフェイスの追加 (Add Interfaces) ] > [Ether Channel インターフェイス (Ether Channel Interface) ] をクリックします。
- ステップ 4** [一般 (General) ] タブで、[Ether Channel ID (Ether Channel ID) ] を 1 ~ 48 の数値に設定します。
- ステップ 5** [使用可能なインターフェイス (Available Interfaces) ] 領域でインターフェイスをクリックし、[追加 (Add) ] をクリックして [選択したインターフェイス (Selected Interface) ] 領域にそのインターフェイスを移動します。メンバーを作成するすべてのインターフェイスに対してを繰り返します。
- すべてのインターフェイスが同じタイプと速度であるようにします。最初に追加するインターフェイスによって、EtherChannel のタイプと速度が決まります。一致しないインターフェイスを追加すると、そのインターフェイスは停止状態になります。Management Center では、一致しないインターフェイスの追加は防止されません。
- ステップ 6** (任意) [詳細 (Advanced) ] タブをクリックして EtherChannel をカスタマイズします。[情報 (Information) ] サブタブで次のパラメータを設定します。
- [ロードバランシング (Load Balance) ] : パケットをグループチャネルインターフェイス間でロードバランスするために使用する基準を選択します。デフォルトでは、Firepower Threat Defense デバイスはパケットの送信元および宛先 IP アドレスに従って、インターフェイスでのパケットのロードをバランスします。パケットが分類される基準になるプロパティを変更する場合は、別の基準のセットを選択します。たとえば、トラフィックが同じ送信元および宛先 IP アドレスに大きく偏っている場合、EtherChannel 内のインターフェイスに対するトラフィックの割り当てがアンバランスになります。別のアルゴリズムに変更すると、トラフィックはより均等に分散される場合があります。ロードバランシングの詳細については、[ロードバランシング \(659 ページ\)](#) を参照してください。
  - [LACP モード (LACP Mode) ] : [アクティブ (Active) ]、[パッシブ (Passive) ]、または [オン (On) ] を選択します。[アクティブ (Active) ] モード (デフォルト) を使用することを推奨します。

- [アクティブな物理インターフェイス：範囲 (Active Physical Interface: Range)] : 左側のドロップダウンリストから、EtherChannel をアクティブにするために必要なアクティブインターフェイスの最小数を 1～16 の範囲で選択します。デフォルトは 1 です。右側のドロップダウンリストから、EtherChannel で許可されるアクティブインターフェイスの最大数を 1～16 の範囲で選択します。デフォルトは 8 です。スイッチが 16 個のアクティブインターフェイスをサポートしていない場合、このコマンドは必ず 8 以下に設定する必要があります。
- [アクティブな MAC アドレス (Active Mac Address)] : 必要に応じて手動 MAC アドレスを設定します。mac\_address は、H.H.H 形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。

**ステップ 7** (任意) [ハードウェア構成 (Hardware Configuration)] タブをクリックしてデュプレックスと速度を設定し、すべてのメンバーインターフェイスでこれらの設定を上書きします。これらのパラメータはチャンネルグループのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。

**ステップ 8** [OK] をクリックします。

**ステップ 9** [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

**ステップ 10** (任意) VLAN サブインターフェイスを追加します。VLAN サブインターフェイスと 802.1Q トランキングの設定 (666 ページ) を参照してください。

**ステップ 11** ルーテッドまたはトランスペアレント モード インターフェイスのパラメータを設定します。ルーテッドモードのインターフェイスの設定 (672 ページ) またはトランスペアレントモードのブリッジグループ インターフェイスの設定 (674 ページ) を参照してください。

## VLAN サブインターフェイスと 802.1Q トランキングの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

VLAN サブインターフェイスを使用すると、1つの物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたはデバイスを追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。



## 始める前に

物理インターフェイス上のタグなしパケットの禁止：サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。この特性は、冗長インターフェイスペアのアクティブな物理インターフェイスと EtherChannel リンクにも当てはまります。サブインターフェイスでトラフィックを通過させるには物理、冗長、または EtherChannel インターフェイスを有効にする必要があるため、インターフェイスに名前を付けないことでトラフィックを通過させないようにします。物理、冗長、または EtherChannel インターフェイスにタグの付いていないパケットを通過させる場合には、通常のようにインターフェイスに名前を付けることができます。

## 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (✎) をクリックします。デフォルトで [インターフェイス (Interfaces)] タブが選択されています。
- ステップ 2** [インターフェイスの追加 (Add Interfaces)] > [サブインターフェイス (Sub Interface)] をクリックします。
- ステップ 3** [一般 (General)] タブで、次のパラメータを設定します。
  - a) [インターフェイス (Interface)] : サブインターフェイスを追加する物理、冗長、またはポートチャネルインターフェイスを選択します。
  - b) [サブインターフェイス ID (Sub-Interface ID)] : サブインターフェイス ID を 1 ~ 4294967295 の範囲の整数で入力します。許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。
  - c) [VLAN ID] : VLAN ID を 1 ~ 4094 の範囲で入力します。これは、このサブインターフェイス上のパケットにタグを付けるために使用されます。
- ステップ 4** [OK] をクリックします。
- ステップ 5** [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。
- ステップ 6** ルーテッドまたはトランスペアレント モード インターフェイスのパラメータを設定します。[ルーテッドモードのインターフェイスの設定 \(672 ページ\)](#) または [トランスペアレントモードのブリッジグループ インターフェイスの設定 \(674 ページ\)](#) を参照してください。

## ルーテッドモードインターフェイスおよびトランスペアレントモードインターフェイス

この項では、ルーテッドファイアウォールモードおよびトランスペアレントファイアウォールモードで、すべてのモデルに対応する標準のインターフェイス設定を完了するためのタスクについて説明します。

### ルーテッドモードインターフェイスとトランスペアレントモードインターフェイスについて

Firepower Threat Defense デバイスは、ルーテッドおよびブリッジという2つのタイプのインターフェイスをサポートします。各レイヤ3ルーテッドインターフェイスに、固有のサブネット上のIPアドレスが必要です。ブリッジされたインターフェイスはブリッジグループに属し、すべてのインターフェイスが同じネットワーク上にあります。ブリッジグループはブリッジネットワークにIPアドレスを持つブリッジ仮想インターフェイス (BVI) によって表されます。ルーテッドモードはルーテッドインターフェイスのみをサポートします。トランスペアレントファイアウォールモードでは、ブリッジグループとBVIインターフェイスのみがサポートされます。

#### トランスペアレントモードのブリッジグループ

ブリッジグループは、Firepower Threat Defense デバイスがルーティングではなくブリッジするインターフェイスのグループです。ブリッジグループはトランスペアレントファイアウォールモードでのみサポートされています。ブリッジグループの詳細については、[ブリッジグループについて \(641 ページ\)](#) を参照してください。

#### デュアルIPスタック (IPv4 および IPv6)

Firepower Threat Defense デバイスは、インターフェイス上でIPv6アドレスとIPv4アドレスの両方をサポートしています。IPv4とIPv6の両方で、デフォルトルートを設定してください。

#### IPv6

ここでは、IPv6の設定方法について説明します。

##### IPv6アドレス指定

次の2種類のIPv6のユニキャストアドレスを設定できます。

- **グローバル**：グローバルアドレスは、パブリックネットワークで使用可能なパブリックアドレスです。ブリッジグループの場合、このアドレスは各メンバーインターフェイスごとに設定するのではなく、BVI用に設定する必要があります。また、トランスペアレントモードで管理インターフェイスのグローバルなIPv6アドレスを設定することもできます。
- **リンクローカル**：リンクローカルアドレスは、直接接続されたネットワークだけで使用できるプライベートアドレスです。ルータは、リンクローカルアドレスを使用してパケットを転送するのではなく、特定の物理ネットワークセグメント上で通信だけを行います。

ルータは、アドレス設定またはアドレス解決などのネイバー探索機能に使用できます。ブリッジグループでは、メンバーインターフェイスのみがリンクローカルアドレスを所有しています。BVI にはリンクローカルアドレスはありません。

最低限、IPv6 が動作するようにリンクローカルアドレスを設定する必要があります。グローバルアドレスを設定すると、リンクローカルアドレスがインターフェイスに自動的に設定されるため、リンクローカルアドレスを個別に設定する必要はありません。ブリッジグループインターフェイスでは、BVI でグローバルアドレスを設定した場合、Firepower Threat Defense デバイスが自動的にメンバーインターフェイスのリンクローカルアドレスを生成します。グローバルアドレスを設定しない場合は、リンクローカルアドレスを自動的にするか、手動で設定する必要があります。

### Modified EUI-64 インターフェイス ID

RFC 3513 「Internet Protocol Version 6 (IPv6) Addressing Architecture」（インターネットプロトコルバージョン6アドレッシングアーキテクチャ）では、バイナリ値000で始まるものを除き、すべてのユニキャスト IPv6 アドレスのインターフェイス識別子部分は長さが 64 ビットで、Modified EUI-64 形式で組み立てることが要求されています。Firepower Threat Defense デバイスでは、ローカルリンクに接続されたホストにこの要件を適用できます。

この機能がインターフェイスで有効化されていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカルリンク上のホストに対してのみ実行できます。

### IPv6 ネイバー探索

IPv6 ネイバー探索プロセスは、ICMPv6 メッセージおよび要請ノードマルチキャストアドレスを使用して、同じネットワーク（ローカルリンク）上のネイバーのリンク層アドレスを特定し、ネイバーの読み出し可能性を確認し、隣接ルータを追跡します。

ノード（ホスト）はネイバー探索を使用して、接続リンク上に存在することがわかっているネイバーのリンク層アドレスの特定や、無効になったキャッシュ値の迅速なページを行います。また、ホストはネイバー探索を使用して、ホストに代わってパケットを転送しようとしている隣接ルータを検出します。さらに、ノードはこのプロトコルを使用して、どのネイバーが到達可能でどのネイバーがそうでないかをアクティブに追跡するとともに、変更されたリンク層アドレスを検出します。ルータまたはルータへのパスが失われると、ホストは機能している代替ルータまたは代替パスをアクティブに検索します。

## ネイバー送信要求メッセージ

ローカルリンク上にある他のノードのリンクレイヤアドレスを検出するため、ノードからネイバー送信要求メッセージ (ICMPv6 Type 135) がローカルリンクに送信されます。ネイバー送信要求メッセージを受信すると、宛先ノードは、ネイバーアドバタイズメントメッセージ (ICMPv6 Type 136) をローカルリンク上に送信して応答します。

送信元ノードがネイバーアドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ノードがあるネイバーの到達可能性を検証する場合、ネイバー送信要求メッセージ内の宛先アドレスとして、そのネイバーのユニキャストアドレスを使用します。

ネイバーアドバタイズメントメッセージは、ローカルリンク上のノードのリンク層アドレスが変更されたときにも送信されます。

## ネイバー到達可能時間

ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

## 重複アドレス検出

ステータス自動設定プロセス中に、重複アドレス検出は、アドレスがインターフェイスに割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を確認します。

重複アドレスが検出されると、そのアドレスの状態は **DUPLICATE** に設定され、アドレスは使用対象外となり、次のエラーメッセージが生成されます。

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

重複アドレスがインターフェイスのリンクローカルアドレスであれば、インターフェイス上で IPv6 パケットの処理は無効になります。重複アドレスがグローバルアドレスであれば、そのアドレスは使用されません。

Firepower Threat Defense デバイスは、ネイバー要請メッセージを使用して、重複アドレス検出を実行します。デフォルトでは、インターフェイスが重複アドレス検出を行う回数は 1 回です。

## ルータアドバタイズメントメッセージ

ネイバーデバイスがデフォルトのルータアドレスをダイナミックに把握できるように、Firepower Threat Defense デバイスはルータアドバタイズメントに参加できます。ルータアドバタイズメントメッセージ (ICMPv6 Type 134) は、Firepower Threat Defense デバイスの IPv6 が設定された各インターフェイスから定期的に送信されます。

ルータアドバタイズメントもルータ要請メッセージ (ICMPv6 Type 133) に応答して送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、

次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。

### スタティック IPv6 ネイバー

ネイバーを手動で IPv6 ネイバー キャッシュに定義できます。IPv6 ネイバー探索プロセスによる学習を通して、指定された IPv6 アドレスのエントリがネイバー探索キャッシュにすでに存在する場合、エントリは自動的にスタティック エントリに変換されます。IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。

## ルーテッド モードおよびトランスペアレント モードのインターフェイスのガイドライン

### ハイ アベイラビリティ

- この章の手順で ハイ アベイラビリティ リンク インターフェイスを設定しないでください。詳細については、「ハイ アベイラビリティ」の章を参照してください。
- ハイ アベイラビリティ を使用する場合、データ インターフェイスの IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。

### IPv6

- IPv6 はすべてのインターフェイスでサポートされます。
- トランスペアレント モードでは、IPv6 アドレスは手動でのみ設定できます。
- Firepower Threat Defense デバイスは、IPv6 エニーキャストアドレスはサポートしません。

### トランスペアレント モードとブリッジグループのガイドライン

- 4 のインターフェイスをもつブリッジグループを 250 まで作成できます。
- 直接接続された各ネットワークは同じサブネット上に置かれている必要があります。
- Firepower Threat Defense デバイス では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- IPv4 の場合は、管理トラフィックと、Firepower Threat Defense デバイス を通過するトラフィックの両方の各ブリッジグループに対し、BVI の IP アドレスが必要です。IPv6 アドレスは BVI でサポートされますが必須ではありません。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット (255.255.255.255) を設定することはできません。

- 管理インターフェイスはブリッジグループのメンバーとしてサポートされません。
- トランスペアレントモードでは、少なくとも1つのブリッジグループを使用し、データインターフェイスがブリッジグループに属している必要があります。
- トランスペアレントモードでは、接続されたデバイス用のデフォルトゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは Firepower Threat Defense デバイスの反対側にあるルータをデフォルトゲートウェイとして指定する必要があります。
- トランスペアレントモードでは、管理トラフィックの戻りパスを指定するために必要なデフォルトルートは、1つのブリッジグループネットワークからの管理トラフィックにだけ適用されます。これは、デフォルトルートはブリッジグループのインターフェイスとブリッジグループネットワークのルータ IP アドレスを指定しますが、ユーザは1つのデフォルトルートしか定義できないためです。複数のブリッジグループネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティックルートを指定する必要があります。
- トランスペアレントモードでは、PPPoE は診断インターフェイスとしてサポートされません。

## ルーテッドモードのインターフェイスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

この手順では、名前、セキュリティゾーン、および IPv4 アドレスを設定する方法について説明します。

### 始める前に

- [物理インターフェイスの有効化およびイーサネット設定の構成 \(655 ページ\)](#)
- 特別なインターフェイスを設定します。
  - [VLAN サブインターフェイスと 802.1Q トランキングの設定 \(666 ページ\)](#)
  - [冗長インターフェイスの設定 \(662 ページ\)](#)
  - [EtherChannel の設定 \(664 ページ\)](#)

## 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (✎) をクリックします。デフォルトで [インターフェイス (Interfaces) ] タブが選択されています。

**ステップ 2** 編集するインターフェイスの編集アイコン (✎) をクリックします。

**ステップ 3** [名前 (Name) ] フィールドに、48 文字以内で名前を入力します。

**ステップ 4** [セキュリティゾーン (Security Zone) ] ドロップダウンリストからセキュリティゾーンを選択するか、[新規 (New) ] をクリックして、新しいセキュリティゾーンを追加します。

ルーテッドインターフェイスは、ルーテッドタイプインターフェイスであり、ルーテッドタイプのゾーンにのみ属することができます。

**ステップ 5** [IPv4] タブをクリックします。IP アドレスを設定するには、[IP タイプ (IP Type) ] ドロップダウンリストにある次のオプションのいずれかを使用します。

- [静的 IP を使用する (Use Static IP) ] : IP アドレスおよびサブネットマスクを入力します。
- [DHCP の使用 (Use DHCP) ] : 次のオプションのパラメータを設定します。
  - [DHCP を使用してデフォルトルートを取得 (Obtain default route using DHCP) ] : DHCP サーバからデフォルト ルートを取得します。
  - [DHCP ルートメトリック (DHCP route metric) ] : アドミニストレーティブ ディスタンスを学習したルートに割り当てます (1 ~ 255)。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。
- [PPPoE を使用 (Use PPPoE) ] : インターフェイスが DSL、ケーブル モデム、またはその他の手段で ISP に接続されていて、ISP が PPPoE を使用して IP アドレスを割り当てる場合は、次のパラメータを設定します。
  - [VPDN グループ名 (VPDN Group Name) ] : この接続を表すために選択するグループ名を指定します。
  - [PPPoE ユーザ名 (PPPoE User Name) ] : ISP によって提供されたユーザ名を指定します。
  - [PPPoE パスワード/パスワードの確認 (PPPoE Password/Confirm Password) ] : ISP によって提供されたパスワードを指定し、確認します。
  - [PPP 認証 (PPP Authentication) ] : [PAP]、[CHAP]、または [MSCHAP] を選択します。

PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリアテキストパスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。

- [PPPoE ルートメトリック (PPPoE route metric) ] : アドミニストレーティブディスタンスを学習したルートに割り当てます。有効な値は 1 ~ 255 です。デフォルトでは、学習したルートのアドミニストレーティブディスタンスは 1 です。
- [ルート設定の有効化 (Enable Route Settings) ] : 手動で PPPoE の IP アドレスを設定するには、このチェックボックスをオンにして、[IP アドレス (IP Address) ] を入力します。
- [フラッシュにユーザ名とパスワードを保存 (Store Username and Password in Flash) ] : フラッシュメモリにユーザ名とパスワードを保存します。

Firepower Threat Defense は、NVRAM の特定の場所にユーザ名とパスワードを保存します。

**ステップ 6** (任意) IPv6 アドレッシングの設定については、[IPv6 アドレッシングの設定 \(678 ページ\)](#) を参照してください。

**ステップ 7** [OK] をクリックします。

**ステップ 8** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## トランスペアレントモードのブリッジグループインターフェイスの設定

ブリッジグループと関連インターフェイスを設定するには、次の手順を実行します。

### ブリッジグループメンバーの一般的なインターフェイスパラメータの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

この手順は、ブリッジグループメンバーインターフェイスの名前とセキュリティゾーンを設定する方法について説明します。

### 始める前に

- [物理インターフェイスの有効化およびイーサネット設定の構成 \(655 ページ\)](#) .
- 同じブリッジグループで、さまざまな種類のインターフェイス (物理インターフェイス、VLAN サブインターフェイス、EtherChannel、冗長インターフェイス) を含めることができます。診断インターフェイスはサポートされていません。
- 特別なインターフェイスを設定します。



- [VLAN サブインターフェイスと 802.1Q トランッキングの設定 \(666 ページ\)](#)
- [冗長インターフェイスの設定 \(662 ページ\)](#)
- [EtherChannel の設定 \(664 ページ\)](#)

## 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (✎) をクリックします。デフォルトで [インターフェイス (Interfaces) ] タブが選択されています。

**ステップ 2** 編集するインターフェイスの編集アイコン (✎) をクリックします。

**ステップ 3** [名前 (Name) ] フィールドに、48 文字以内で名前を入力します。

**ステップ 4** [セキュリティゾーン (Security Zone) ] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規 (New) ] をクリックして、新しいセキュリティ ゾーンを追加します。

ブリッジグループ メンバー インターフェイスは、スイッチドタイプ インターフェイスであり、スイッチドタイプのゾーンにのみ属することができます。このインターフェイスに対して IP アドレス設定は行わないでください。ブリッジ仮想インターフェイス (BVI) に対してのみ IP アドレスを設定します。BVI はゾーンに属しておらず、BVI にはアクセス コントロール ポリシーを適用できないことに注意してください。

**ステップ 5** [OK] をクリックします。

**ステップ 6** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## ブリッジ仮想インターフェイス (BVI) の設定

ブリッジグループごとに、IP アドレスを設定する BVI が必要です。Firepower Threat Defense はブリッジグループが発信元になるパケットの送信元アドレスとして、この IP アドレスを使用します。BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、BVI IP アドレスが必要です。IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカルアドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。



(注) 個別の診断 インターフェイスでは、設定できないブリッジグループ (ID 301) は、設定に自動的に追加されます。このブリッジグループはブリッジグループの制限に含まれません。

### 始める前に

セキュリティゾーンに BVI を追加することはできません。そのため、BVI にアクセス コントロールポリシーを適用することはできません。ゾーンに基づいてブリッジグループのメンバーインターフェイスにポリシーを適用する必要があります。

### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (✎) をクリックします。デフォルトで [インターフェイス (Interfaces)] タブが選択されています。
- ステップ 2** [インターフェイスの追加 (Add Interfaces)] > [ブリッジグループインターフェイス (Bridge Group Interface)] を選択します。
- ステップ 3** [ブリッジグループ ID (Bridge Group ID)] フィールドに、1 ~ 250 の間のブリッジグループ ID を入力します。
- ステップ 4** (オプション) [説明 (Description)] フィールドに、このブリッジグループの説明を入力します。
- ステップ 5** [インターフェイス (Interfaces)] タブでインターフェイスをクリックし、[追加 (Add)] をクリックして [選択したインターフェイス (Selected Interfaces)] 領域にそのインターフェイスを移動します。ブリッジグループのメンバーにするすべてのインターフェイスに対して繰り返します。
- ステップ 6** [IPv4] タブをクリックします。[IP アドレス (IP Address)] フィールドに IPv4 アドレスおよびサブネット マスクを入力します。  
  
BVI にはホストアドレス (/32 または 255.255.255.255) を割り当てないでください。また、/30 サブネットなど (255.255.255.252)、ホストアドレスが 3 つ未満 (アップストリームルータ、ダウンストリームルータ、トランスペアレント ファイアウォールにそれぞれ 1 つずつ) の他のサブネットを使用しないでください。Firepower Threat Defense デバイスは、サブネットの先頭アドレスと最終アドレスで送受信されるすべての ARP パケットをドロップします。たとえば、/30 サブネットを使用し、そのサブネットからアップストリームルータへの予約済みアドレスを割り当てた場合、Firepower Threat Defense デバイスはダウンストリームルータからアップストリームルータへの ARP 要求をドロップします。
- ステップ 7** (任意) IPv6 アドレッシングの設定については、[IPv6 アドレッシングの設定 \(678 ページ\)](#) を参照してください。
- ステップ 8** [OK] をクリックします。
- ステップ 9** [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## トランスペアレントモードの診断（管理）インターフェイスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

トランスペアレントファイアウォールモードでは、すべてのインターフェイスがブリッジグループに属している必要があります。唯一の例外は診断 *slot/port* インターフェイスです。Firepower 4100/9300 シャーシでは、診断インターフェイス ID は Firepower Threat Defense 論理デバイスに割り当てた *mgmt-type* インターフェイスに基づいています。他のインターフェイスタイプは診断インターフェイスとして使用できません。シングルモードまたはコンテキストごとに 1 つの診断インターフェイスを設定できます。

## 始める前に

このインターフェイスをブリッジグループに割り当てないでください。設定できないブリッジグループ (ID 301) は、コンフィギュレーションに自動的に追加されます。このブリッジグループはブリッジグループの制限に含まれません。

## 手順

- 
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (🔧) をクリックします。デフォルトで [インターフェイス (Interfaces)] タブが選択されています。
- ステップ 2** 診断インターフェイスの編集アイコン (🔧) をクリックします。
- ステップ 3** [名前 (Name)] フィールドに、48 文字以内で名前を入力します。
- ステップ 4** [IPv4] タブをクリックします。IP アドレスを設定するには、[IP タイプ (IP Type)] ドロップダウンリストにある次のオプションのいずれかを使用します。
- [静的 IP を使用する (Use Static IP)] : IP アドレスおよびサブネットマスクを入力します。
  - [DHCP の使用 (Use DHCP)] : 次のオプションのパラメータを設定します。
    - [DHCP を使用してデフォルトルートを取得 (Obtain default route using DHCP)] : DHCP サーバからデフォルトルートを取得します。
    - [DHCP ルートメトリック (DHCP route metric)] : アドミニストレーティブディスタンスを学習したルートに割り当てます (1 ~ 255)。学習したルートのデフォルトのアドミニストレーティブディスタンスは 1 です。
  - [PPPoE の使用 (Use PPPoE)] : 次のパラメータを設定します。
    - [VPDN グループ名 (VPDN Group Name)] : グループ名を指定します。

- [PPPoE ユーザ名 (PPPoE User Name) ] : ISP によって提供されたユーザ名を指定します。
- [PPPoE パスワード/パスワードの確認 (PPPoE Password/Confirm Password) ] : ISP によって提供されたパスワードを指定し、確認します。
- [PPP 認証 (PPP Authentication) ] : [PAP]、[CHAP]、または [MSCHAP] を選択します。

PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリアテキストパスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。

- [PPPoE ルートメトリック (PPPoE route metric) ] : アドミニストレーティブディスタンスを学習したルートに割り当てます。有効な値は 1 ~ 255 です。デフォルトでは、学習したルートのアドミニストレーティブディスタンスは 1 です。
- [ルート設定の有効化 (Enable Route Settings) ] : 手動で PPPoE の IP アドレスを設定するには、このチェックボックスをオンにして、[IP アドレス (IP Address) ] を入力します。
- [フラッシュにユーザ名とパスワードを保存 (Store Username and Password in Flash) ] : フラッシュメモリにユーザ名とパスワードを保存します。

Firepower Threat Defense は、NVRAM の特定の場所にユーザ名とパスワードを保存します。

**ステップ 5** (任意) IPv6 アドレッシングの設定については、[IPv6 アドレッシングの設定 \(678 ページ\)](#) を参照してください。

**ステップ 6** [OK] をクリックします。

**ステップ 7** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

---

## IPv6 アドレッシングの設定

ここでは、ルーテッドモードおよびトランスペアレントモードで IPv6 アドレッシングを設定する方法について説明します。

## グローバル IPv6 アドレスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ルーテッドモードの任意のインターフェイスとトランスペアレントモードの BVI に対してグローバル IPv6 アドレスを設定するには、次の手順を実行します。



- (注) グローバルアドレスを設定すると、リンクローカルアドレスは自動的に設定されるため、別々に設定する必要はありません。ブリッジグループについて、BVI でグローバルアドレスを設定すると、すべてのメンバー インターフェイスのリンクローカルアドレスが自動的に設定されます。

## 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (✎) をクリックします。デフォルトで [インターフェイス (Interfaces) ] タブが選択されています。

**ステップ 2** 編集するインターフェイスの編集アイコン (✎) をクリックします。

**ステップ 3** [IPv6] タブをクリックします。

ルーテッドモードでは、[基本 (Basic) ] タブがデフォルトで選択されています。トランスペアレントモードでは、[アドレス (Address) ] タブがデフォルトで選択されています。

**ステップ 4** グローバル IPv6 アドレスを次のいずれかの方法で設定します。

- (ルーテッドインターフェイス) ステートレス自動設定 : [自動設定 (Autoconfiguration) ] チェックボックスをオンにします。

インターフェイス上でステートレス自動設定を有効にすると、受信したルータアドバタイズメントメッセージのプレフィックスに基づいて IPv6 アドレスを設定します。ステートレスな自動設定が有効になっている場合、インターフェイスのリンクローカルアドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

RFC 4862 では、ステートレス自動設定用に設定されたホストはルータアドバタイズメントメッセージを送信しないと規定されていますが、この場合は、Firepower Threat Defense デバイスがルータアドバタイズメントメッセージを送信します。[IPv6] > [設定

(Settings) ] > [RA の有効化 (Enable RA) ] チェックボックスをオフにして、メッセージを抑制します。

- 手動設定 : グローバル IPv6 アドレスを手動で設定するには、次の手順を実行します。

1. [アドレス (Address)] タブをクリックして、[アドレスの追加 (Add Address)] をクリックします。  
[アドレスの追加 (Add Address)] ダイアログボックスが表示されます。
2. [アドレス (Address)] フィールドに、インターフェイス ID を含む完全なグローバル IPv6 アドレス、または IPv6 プレフィックス長と IPv6 プレフィックスのいずれかを入力します。(ルーテッドモード) プレフィックスだけを入力した場合は、必ず[EUI-64 を適用 (Enforce EUI 64)] チェックボックスをオンにして、Modified EUI-64 形式を使用してインターフェイス ID を生成するようにしてください。たとえば、2001:0DB8::BA98:0:3210/48 (完全なアドレス) または 2001:0DB8::/48 (プレフィックス、[EUI 64] はオン)。

**ステップ 5** ルーテッドインターフェイスの場合は、オプションで [基本 (Basic)] タブで次の値を設定できます。

- グローバルアドレスを設定しない場合に自動的にリンクローカルアドレスを設定するには、[IPv6 の有効化 (Enable IPv6)] チェックボックスをオンにします。  
グローバルアドレスを設定する必要がなく、リンクローカルアドレスだけを設定する必要がある場合は、リンクローカルアドレスをインターフェイスの MAC アドレスに基づいて作成することもできます (Modified EUI-64 形式。MAC アドレスで使用するビット数は 48 ビットであるため、インターフェイス ID に必要な 64 ビットを埋めるために追加ビットを挿入する必要があります)。
- ローカルリンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[EUI-64 を適用 (Enforce EUI-64)] チェックボックスをオンにします。
- リンクローカルアドレスを手動で設定するには、[リンクローカルアドレス (Link-Local address)] フィールドにアドレスを入力します。  
リンクローカルアドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。例、fe80::20d:88ff:feec:6a82。グローバルアドレスを設定する必要がなく、リンクローカルアドレスだけを設定する必要がある場合は、リンクローカルアドレスを手動で定義できます。Modified EUI-64 形式に基づくリンクローカルアドレスを自動的に割り当てることを推奨します。たとえば、その他のデバイスで Modified EUI-64 形式の使用が強制される場合、手動で割り当てたリンクローカルアドレスによりパケットがドロップされることがあります。
- [アドレス設定の DHCP を有効化 (Enable DHCP for address config)] チェックボックスをオンにして、IPv6 ルータ アドバタイズメント パケットの Managed Address Config フラグを設定します。  
IPv6 ルータ アドバタイズメント内のこのフラグは、取得されるステートレス自動設定のアドレス以外のアドレスの取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。
- [アドレス設定の DHCP を有効化 (Enable DHCP for address config)] チェックボックスをオンにして、IPv6 ルータ アドバタイズメント パケットの Other Address Config フラグを設定します。

IPv6 ルータ アドバタイズメント内のこのフラグは、DHCPv6 から DNS サーバアドレスなどの追加情報の取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。

**ステップ 6** ルーテッドインターフェイスの場合は、[プレフィックス (Prefixes)] タブと [設定 (Settings)] タブでの設定について [IPv6 ネイバー探索の設定（ルーテッドモードのみ）（681 ページ）](#) を参照してください。BVI インターフェイスの場合は、[設定 (Settings)] タブの以下のパラメータを参照してください。

- [DAD 試行 (DAD attempts)] : DAD 試行の最大数 (1 ~ 600)。重複アドレス検出 (DAD) プロセスを無効にするには、この値を 0 に設定します。この設定では、DAD が IPv6 アドレスで実行されている間に、インターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定します。デフォルトでは 1 になっています。
- [NS 間隔 (NS Interval)] : インターフェイスでの IPv6 ネイバー要請再送信の間隔 (1000 ~ 3600000 ms)。デフォルト値は 1000 ミリ秒です。
- [到達可能時間 (Reachable Time)] : 到達可能性確認イベントが発生した後でリモートの IPv6 ノードを到達可能とみなす時間 (0 ~ 3600000 ms)。デフォルト値は 0 ミリ秒です。value に 0 を使用すると、到達可能時間が判定不能として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

**ステップ 7** [OK] をクリックします。

**ステップ 8** [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## IPv6 ネイバー探索の設定（ルーテッドモードのみ）

IPv6 ネイバー探索プロセスは、ICMPv6 メッセージおよび送信要求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカルリンク）上のネイバーのリンク層アドレスを決定し、ネイバーの読み出し可能性を確認し、隣接ルータを追跡します。

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (🔧) をクリックします。デフォルトで [インターフェイス (Interfaces)] タブが選択されています。

**ステップ 2** 編集するインターフェイスの編集アイコン (🔧) をクリックします。

- ステップ 3** [IPv6] タブをクリックして、[プレフィックス (Prefixes)] タブをクリックします。
- ステップ 4** (任意) IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定するには、次の手順を実行します。
- [プレフィックスの追加 (Add Prefix)] をクリックします。
  - [アドレス (Address)] フィールドに、プレフィックス長の IPv6 アドレスを入力するか、または [デフォルト (Default)] チェックボックスをオンにして、デフォルトのプレフィックスを使用します。
  - (任意) IPv6 プレフィックスをアドバタイズしない場合は、[アドバタイズメント (Advertisement)] チェックボックスをオフにします。
  - [オフリンク (Off Link)] チェックボックスをオンにして、指定したプレフィックスがリンクに割り当てられたことを示します。指定したプレフィックスを含むアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。このプレフィックスは、オンラインの判別には使用しないでください。
  - 指定されているプレフィックスを自動設定に使用する場合、[自動設定 (Autoconfiguration)] チェックボックスをオンにします。
  - [プレフィックス ライフタイム (Prefix Lifetime)] で、[期間 (Duration)] または [失効日 (Expiration Date)] をクリックします。
    - [期間 (Duration)] : プレフィックスの [優先ライフタイム (Preferred Lifetime)] を秒単位で入力します。この設定は、指定の IPv6 プレフィックスが有効なものとしてアドバタイズする時間です。最大値は無量大です。有効な値は 0 ~ 4294967295 です。デフォルトは 2592000 (30 日間) です。プレフィックスの [有効ライフタイム (Valid Lifetime)] を秒単位で入力します。この設定は、指定の IPv6 プレフィックスが優先であるとしてアドバタイズする時間です。最大値は無量大です。有効な値は 0 ~ 4294967295 です。デフォルト設定は、604800 (7 日) です。または、[無量大 (Infinite)] チェックボックスをオンにして、時間無制限を設定します。
    - [失効日 (Expiration Date)] : [有効 (Valid)]、[優先 (Preferred)] 日時を選択します。
  - [OK] をクリックします。
- ステップ 5** [設定 (Settings)] タブをクリックします。
- ステップ 6** (任意) [DAD 試行 (DAD attempts)] の最大数、1 ~ 600 を設定します。デフォルトでは 1 になっています。重複アドレス検出 (DAD) プロセスをディセーブルにするには、この値を 0 に設定します。
- この設定では、DAD が IPv6 アドレスで実行されている間に、インターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定します。
- ステップ 7** (任意) [NS インターバル (NS Interval)] フィールドで、IPv6 ネイバー勧誘再送信の時間の間隔を、1000 ~ 3600000ms で設定します。
- デフォルト値は 1000 ミリ秒です。
- ステップ 8** (任意) 到達可能性確認イベントが発生した後でリモート IPv6 ノードが到達可能であると見なされる時間を、[到達可能時間 (Reachable Time)] フィールドにて、0 ~ 3600000ms で設定します。



デフォルト値は 0 ミリ秒です。value に 0 を使用すると、到達可能時間が判定不能として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。

ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

**ステップ 9** (任意) ルータ アドバタイズメントの伝送を抑制にするには、[RA を有効にする (Enable RA)] チェックボックスをオフにします。ルータアドバタイズメントの伝送を有効にすると、RA ライフタイムと時間間隔を設定できます。

ルータ アドバタイズメント メッセージは、ルータ送信要求メッセージへの応答として自動的に送信されます。Firepower Threat Defense デバイスで IPv6 プレフィックスを提供する必要がないインターフェイス (外部インターフェイスなど) では、これらのメッセージを無効にすることができます。

- [RA ライフタイム (RA Lifetime)] : IPv6 ルータ アドバタイズメントのルータのライフタイム値を、0 ~ 9000 秒で設定します。

デフォルトは 1800 秒です。

- [RA インターバル (RA Interval)] : IPv6 ルータ アドバタイズメントの伝送の間の時間間隔を、3 ~ 1800 秒で設定します。

デフォルトは 200 秒です。

**ステップ 10** [OK] をクリックします。

**ステップ 11** [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

---

## インターフェイスの詳細設定

ここでは、インターフェイスの MAC アドレスの設定方法、最大伝送ユニット (MTU) の設定方法、その他の詳細パラメータの設定方法について説明します。

### インターフェイスの詳細設定について

ここでは、インターフェイスの詳細設定について説明します。

#### MAC アドレスについて

手動で MAC アドレスを割り当ててデフォルトをオーバーライドできます。の一意の MAC アドレスを自動的に生成することもできます。

## デフォルトの MAC アドレス

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは **Burned-In MAC Address** を使用します。
- 冗長インターフェイス：冗長インターフェイスでは、最初に追加された物理インターフェイスの MAC アドレスが使用されます。構成でメンバーインターフェイスの順序を変更すると、MAC アドレスがリストの先頭にあるインターフェイスの MAC アドレスと一致するように変更されます。冗長インターフェイスに MAC アドレスを割り当てると、メンバーインターフェイスの MAC アドレスに関係なく、割り当てた MAC アドレスが使用されます。
- EtherChannel：EtherChannel の場合は、そのチャンネルグループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワークアプリケーションとユーザに対してトランスペアレントになります。ネットワークアプリケーションやユーザから見えるのは1つの論理接続のみであり、個々のリンクのことは認識しないからです。ポートチャンネルインターフェイスは、最も小さいチャンネルグループインターフェイスの MAC アドレスをポートチャンネル MAC アドレスとして使用します。または、ポートチャンネルインターフェイスの MAC アドレスを設定することもできます。グループチャンネルインターフェイスメンバーシップが変更された場合に備えて、一意の MAC アドレスを構成することを推奨します。ポートチャンネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャンネル MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。
- サブインターフェイス：物理インターフェイスのすべてのサブインターフェイスが同じ **Burned-In MAC Address** を使用します。サブインターフェイスに固有の MAC アドレスを割り当てることが必要になる場合があります。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで IPv6 リンクローカルアドレスも一意にできます。

## フェールオーバー MAC アドレス

ハイアベイラビリティで使用できるように、Firepower Threat Defense デバイスはインターフェイスごとにアクティブとスタンバイの両方の MAC アドレスを生成します。アクティブユニットがフェールオーバーしてスタンバイユニットがアクティブになると、その新規アクティブユニットがアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。

## MTU について

MTU は、Firepower Threat Defense デバイスが特定のイーサネットインターフェイスで送信する最大フレームペイロードサイズを指定します。MTU の値は、イーサネットヘッダー、VLAN タギング、またはその他のオーバーヘッドを含まないフレームサイズです。たとえば MTU を 1500 に設定した場合、想定されるフレームサイズはヘッダーを含めて 1518 バイト、VLAN を使用する場合は 1522 バイトです。これらのヘッダーに対応するために MTU 値を高く設定しないでください。

## パス MTU ディスカバリ

Firepower Threat Defense デバイスは、Path MTU Discovery (RFC 1191 の定義に従う) をサポートします。つまり、2 台のホスト間のネットワーク パス内のすべてのデバイスで MTU を調整できます。したがってパスの最小 MTU の標準化が可能です。

## デフォルト MTU

Firepower Threat Defense デバイスのデフォルト MTU は、1500 バイトです。この値には、イーサネット ヘッダー、VLAN タギングや他のオーバーヘッド分の 18~22 バイトは含まれません。

## MTU およびフラグメンテーション

IPv4 では、出力 IP パケットが指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは宛先（場合によっては中間ホップ）で組み立て直されますが、フラグメント化はパフォーマンス低下の原因となります。IPv6 では、通常、パケットをフラグメント化することはできません。したがって、フラグメント化を避けるために、IP パケットを MTU サイズ以内に収める必要があります。

UDP または ICMP の場合、アプリケーションではフラグメント化を避けるために MTU を考慮する必要があります。



---

(注) Firepower Threat Defense デバイスはメモリに空きがある限り、設定された MTU よりも大きいフレームを受信します。

---

## MTU とジャンボ フレーム

MTU が大きいほど、大きいパケットを送信できます。パケットが大きいほど、ネットワークの効率が良くなる可能性があります。次のガイドラインを参照してください。

- **トラフィック パスの MTU の一致**：すべての Firepower Threat Defense デバイス インターフェイスとトラフィック パス内のその他のデバイスのインターフェイスでは、MTU が同じになるように設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- **ジャンボ フレームへの対応**：MTU は最大で 9198 バイトに設定できます。最大値は、Firepower 9300 シャーシの Firepower Threat Defense Virtual で 9000、Firepower Threat Defense で 9184 です。

## ブリッジグループ トラフィックの ARP インспекション

デフォルトでは、ブリッジグループのメンバーの間ですべての ARP パケットが許可されます。ARP パケットのフローを制御するには、ARP インспекションを有効にします。

ARP インспекションによって、悪意のあるユーザが他のホストやルータになります (ARP スプーフィングと呼ばれる) のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイル

## ブリッジグループの MAC アドレス テーブル

タに送信すると、ゲートウェイルータはゲートウェイルータの MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホストトラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

ARP インスペクションをイネーブルにすると、Firepower Threat Defense デバイスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、Firepower Threat Defense デバイスはパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするように Firepower Threat Defense デバイスを設定できます。



(注) 専用の診断インターフェイスは、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

## ブリッジグループの MAC アドレス テーブル

Firepower Threat Defense デバイスは、通常のブリッジまたはスイッチと同様に、MAC アドレスを学習して MAC アドレス テーブルを作成します。デバイスがブリッジグループ経由でパケットを送信すると、Firepower Threat Defense デバイスが MAC アドレスをアドレス テーブルに追加します。このテーブルでは MAC アドレスと送信元インターフェイスが関連付けられているため、Firepower Threat Defense デバイスはデバイスのアドレスが指定されたパケットを正しいインターフェイスに送信できます。

Firepower Threat Defense デバイスはファイアウォールなので、パケットの宛先 MAC アドレスがテーブルにない場合、Firepower Threat Defense デバイスは通常のブリッジとは異なり、元のパケットをすべてのインターフェイスにフラッドすることはありません。代わりに、直接接続されたデバイスまたはリモートデバイスに対して次のパケットを生成します。

- 直接接続されたデバイスへのパケット：Firepower Threat Defense デバイスは宛先 IP アドレスに対して ARP 要求を生成し、ARP 応答を受信したインターフェイスを学習します。
- リモートデバイスへのパケット：Firepower Threat Defense デバイスは宛先 IP アドレスへの ping を生成し、ping 応答を受信したインターフェイスを学習します。

元のパケットはドロップされます。

## デフォルト設定

- ARP インспекションを有効にした場合、デフォルト設定では、一致しないパケットはフラグディングします。
- ダイナミック MAC アドレス テーブル エントリのデフォルトのタイムアウト値は 5 分です。
- デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、Firepower Threat Defense デバイスは対応するエントリを MAC アドレス テーブルに追加します。

## ARP インспекションと MAC アドレス テーブルのガイドライン

- ARP インспекションは、ブリッジ グループでのみサポートされます。
- MAC アドレス テーブル構成は、ブリッジ グループでのみサポートされます。
- ブリッジ グループは、トランスペアレント ファイアウォール モードでのみサポートされます。

## MTU の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

たとえば、ジャンボ フレームを許可するようにインターフェイスの MTU をカスタマイズします。



### 注意

デバイス上で非管理/診断インターフェイスの最大 MTU 値を変更し、設定の変更を展開すると、Snort プロセスが再起動され、一時的にトラフィックのインспекションが中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理/診断インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### 始める前に

- MTU を 1500 バイトより大きい値に変更すると、自動的にジャンボフレームが有効になります。ジャンボ フレームを使用するには、システムをリロードする必要があります。

- インラインセットでインターフェイスを使用する場合、MTU 設定は使用されません。ただし、ジャンボフレームの設定はインラインセットに関連します。ジャンボフレームによりインラインインターフェイスは最大 9000 バイトの packets を受信できます。ジャンボフレームを有効にするには、すべてのインターフェイスの MTU を 1500 バイトより大きい値に設定する必要があります。

#### 手順

- 
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (✎) をクリックします。デフォルトで [インターフェイス (Interfaces)] タブが選択されています。
- ステップ 2** 編集するインターフェイスの編集アイコン (✎) をクリックします。
- ステップ 3** [一般 (General)] タブで、[MTU] を 64 ~ 9198 バイトに設定します。最大値は Firepower Threat Defense Virtual では 9000、Firepower 9300 シャーシ上の Firepower Threat Defense では 9184 です。  
デフォルト値は 1500 バイトです。
- ステップ 4** [OK] をクリックします。
- ステップ 5** [保存 (Save)] をクリックします。  
これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。
- ステップ 6** MTU を 1500 バイトを超える値に設定する場合は、システムをリロードしてジャンボフレームを有効にします。
- 

## MAC アドレスの設定

MAC アドレスを手動で割り当てる必要がある場合があります。

#### 手順

- 
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (✎) をクリックします。デフォルトで [インターフェイス (Interfaces)] タブが選択されています。
- ステップ 2** 編集するインターフェイスの編集アイコン (✎) をクリックします。
- ステップ 3** [Advanced] タブをクリックします。  
[情報 (Information)] タブが選択されています。
- ステップ 4** [アクティブな MAC アドレス (Active MAC Address)] フィールドに、MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数です。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。

(注) [スタンバイ MAC アドレス (Standby MAC Address)] および [DNS ルックアップ (DNS Lookup)] は現時点では使用されません。

**ステップ 5** [OK] をクリックします。

**ステップ 6** [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## スタティック ARP エントリの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

デフォルトでは、ブリッジグループのメンバーの間ですべての ARP パケットが許可されます。ARP パケットのフローを制御するには、ARP インспекションを有効にします ([ARP インспекションの設定 \(1033 ページ\)](#) 参照)。ARP インспекションは、ARP パケットを ARP テーブルのスタティック ARP エントリと比較します。



ルーテッドインターフェイスの場合、スタティック ARP エントリを入力できますが、通常はダイナミック エントリで十分です。ルーテッドインターフェイスの場合、直接接続されたホストにパケットを配送するために ARP テーブルが使用されます。送信者は IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARP テーブルは、ARP 応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合 (たとえば、所定の IP アドレスの MAC アドレスが変更された場合など)、新しい情報で更新される前にこのエントリがタイムアウトする必要があります。

トランスペアレントモードの場合、管理トラフィックなどの Firepower Threat Defense デバイスとの間のトラフィックに、Firepower Threat Defense は ARP テーブルのダイナミック ARP エントリのみを使用します。

### 始める前に

この画面は、名前付きインターフェイスについてのみ使用できます。

## 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (  ) をクリックします。デフォルトで [インターフェイス (Interfaces) ] タブが選択されています。
- ステップ 2** 編集するインターフェイスの編集アイコン (  ) をクリックします。
- ステップ 3** [詳細 (Advanced) ] タブをクリックして、[ARP] タブをクリックします (トランスペアレントモードでは、[ARP と MAC (ARP and MAC) ] ) 。
- ステップ 4** [ARP 設定を追加 (Add ARP Config) ] をクリックします。  
[ARP 設定を追加 (Add ARP Config) ] ダイアログボックスが表示されます。
- ステップ 5** [IP アドレス (IP Address) ] フィールドに、ホストの IP アドレスを入力します。
- ステップ 6** [MAC アドレス (MAC Address) ] フィールドに、ホストの MAC アドレスを入力します。たとえば、「00e0.1e4e.3d8b」のように入力します。
- ステップ 7** このアドレスでプロキシ ARP を実行するには、[エイリアスを有効にする (Enable Alias) ] チェックボックスをオンにします。
- Firepower Threat Defense デバイスは、指定された IP アドレスの ARP 要求を受信すると、指定された MAC アドレスで応答します。
- ステップ 8** [OK] をクリックし、次にもう一度 [OK] をクリックして、[詳細設定 (Advanced settings) ] を閉じます。
- ステップ 9** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## 静的 MAC アドレスの追加とトランスペアレントモードのブリッジグループの MAC 学習の無効化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

通常、MAC アドレスは、特定の MAC アドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。MAC アドレス ラーニングを無効にすることができます。ただし、MAC アドレスをスタティックにテーブルに追加しないかぎり、トラフィックは Firepower Threat Defense デバイスを通過できません。スタティック MAC アドレスは、MAC アドレス テーブルに追加することもできます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エン





トリと同じMACアドレスを持つクライアントが、そのスタティック エントリに一致しないインターフェイスにトラフィックを送信しようとした場合、Firepower Threat Defense デバイスはトラフィックをドロップし、システム メッセージを生成します。スタティック ARP エントリを追加するときに（[スタティック ARP エントリの追加（689 ページ）](#) を参照）、スタティック MAC アドレス エントリはMAC アドレス テーブルに自動的に追加されます。

### 始める前に

この画面は、名前付きインターフェイスについてのみ使用できます。

### 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (  ) をクリックします。デフォルトで [インターフェイス (Interfaces) ] タブが選択されています。
- ステップ 2** 編集するインターフェイスの編集アイコン (  ) をクリックします。
- ステップ 3** [詳細 (Advanced) ] タブをクリックして、[ARP と MAC (ARP and MAC) ] タブをクリックします。
- ステップ 4** (任意) [MAC ラーニングを有効にする (Enable MAC Learning) ] チェックボックスをオフにして MAC ラーニングを無効にします。
- ステップ 5** スタティック MAC アドレスを追加するには、[MAC 設定を追加 (Add MAC Config) ] をクリックします。  
[MAC 設定を追加 (Add MAC Config) ] ダイアログボックスが表示されます。
- ステップ 6** [MAC アドレス (MAC Address) ] フィールドに、ホストの MAC アドレスを入力します。たとえば、「00e0.1e4e.3d8b」のように入力します。[OK] をクリックします。
- ステップ 7** [OK] をクリックして詳細設定を終了します。
- ステップ 8** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## セキュリティの設定パラメータの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

この項では、IP スプーフィングの防止方法、完全フラグメントリアセンブルの許可方法、および [プラットフォーム設定 (Platform Settings)] でデバイス レベルで設定されるデフォルトのフラグメント設定のオーバーライド方法について説明します。

### アンチスプーフィング

この項では、インターフェイスでユニキャストリバースパスフォワーディング (ユニキャスト RPF) を有効にします。ユニキャスト RPF は、ルーティングテーブルに従って、すべてのパケットが正しい送信元インターフェイスと一致する送信元 IP アドレスを持っていることを確認して、IP スプーフィング (パケットが不正な送信元 IP アドレスを使用し、実際の送信元を隠蔽すること) から保護します。

通常、Firepower Threat Defense デバイスは、パケットの転送先を判定するときに宛先アドレスだけを調べます。ユニキャスト RPF は、送信元アドレスも調べるようにデバイスに指示します。そのため、リバースパスフォワーディング (Reverse Path Forwarding) と呼ばれます。Firepower Threat Defense デバイスの通過を許可するすべてのトラフィックについて、送信元アドレスに戻るルートがデバイスのルーティングテーブルに含まれる必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックの場合、Firepower Threat Defense デバイスはデフォルトルートを使用してユニキャスト RPF 保護の条件を満たすことができます。トラフィックが外部インターフェイスから入り、送信元アドレスがルーティングテーブルにない場合、デバイスはデフォルトルートを使用して、外部インターフェイスを送信元インターフェイスとして正しく識別します。

ルーティングテーブルにあるアドレスから外部インターフェイスにトラフィックが入り、このアドレスが内部インターフェイスに関連付けられている場合、Firepower Threat Defense デバイスはパケットをドロップします。同様に、未知の送信元アドレスから内部インターフェイスにトラフィックが入った場合は、一致するルート (デフォルトルート) が外部インターフェイスを示しているため、デバイスはパケットをドロップします。

ユニキャスト RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP と TCP にはセッションがあるため、最初のパケットは逆ルートルックアップが必要です。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

### パケットあたりのフラグメント

デフォルトでは、Firepower Threat Defense デバイスは 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。NFS over UDP など、アプリケーションが日常的にパケットをフラグメント化する場合は、ネットワークでフラグメント化を許可する必要があります。ただし、トラフィックをフラグメント化するアプリケーションがない場合は、フラグメントが Firepower Threat Defense デバイスを通過できないようにすることをお勧めします。フラグメント化されたパケットは、DoS 攻撃によく使われます。

### フラグメントのリアセンブル

Firepower Threat Defense デバイスは、次に示すフラグメントリアセンブルプロセスを実行します。

- IP フラグメントは、フラグメントセットが作成されるまで、またはタイムアウト間隔が経過するまで収集されます。
- フラグメントセットが作成されると、セットに対して整合性チェックが実行されます。これらのチェックには、重複、テール オーバーフロー、チェーン オーバーフローはいずれも含まれません。
- Firepower Threat Defense デバイスで終端する IP フラグメントは、常に完全にリアセンブルされます。
- [完全フラグメントリアセンブル (Full Fragment Reassembly)] が無効化されている場合 (デフォルト)、フラグメントセットは、さらに処理するためにトランスポート層に転送されます。
- [完全フラグメントリアセンブル (Full Fragment Reassembly)] が有効化されている場合、フラグメントセットは、最初に単一の IP パケットに結合されます。この単一の IP パケットは、さらに処理するためにトランスポート層に転送されます。

### 始める前に

この画面は、名前付きインターフェイスでのみ使用できます。

### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (🔧) をクリックします。デフォルトで [インターフェイス (Interfaces)] タブが選択されています。
- ステップ 2** 編集するインターフェイスの編集アイコン (🔧) をクリックします。
- ステップ 3** [詳細 (Advanced)] タブをクリックして、[セキュリティ設定 (Security Configuration)] タブをクリックします。
- ステップ 4** ユニキャスト リバース パス フォワーディングを有効にするには、[アンチ スプーフィング (Anti-Spoofing)] チェックボックスをオンにします。
- ステップ 5** 完全フラグメントリアセンブルを有効化するには、[完全フラグメントリアセンブル (Full Fragment Reassembly)] チェックボックスをオンにします。
- ステップ 6** パケットごとに許容するフラグメント数を変更するには、[デフォルトフラグメント設定のオーバーライド (Override Default Fragment Setting)] チェックボックスをオンにして、次に示す値を設定します。
  - サイズ (Size) : リアセンブルを待機する IP リアセンブル データベースに格納可能なパケットの最大数を設定します。デフォルトは 200 です。この値を 1 に設定すると、フラグメントが無効化されます。

- チェーン (Chain) : 1 つの完全な IP パケットにフラグメント化できる最大パケット数を指定します。デフォルトは 24 パケットです。
- タイムアウト (Timeout) : フラグメント化されたパケット全体が到着するまで待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントの到着後に開始されます。指定した秒数までに到着しなかったパケットフラグメントがある場合、到着済みのすべてのパケットフラグメントが廃棄されます。デフォルトは 5 秒です。

ステップ 7 [OK] をクリックします。

ステップ 8 [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## IPS のみ対応のインターフェイスの設定

IPS のみ対応のインターフェイスでは、パッシブ インターフェイス、パッシブ ERSPAN インターフェイス、インラインセットを設定できます。

### インラインセットのハードウェア バイパスについて

Firepower 9300 および 4100 シリーズの特定のインターフェイス モジュール ([インラインセットの前提条件 \(695 ページ\)](#)) を参照) では、ハードウェア バイパス機能を有効にできます。ハードウェア バイパスは、停電時にトラフィックがインラインインターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。

### ハードウェア バイパス トリガー

ハードウェア バイパス は次のシナリオでトリガーされることがあります。

- Firepower Threat Defense アプリケーションのクラッシュ
- セキュリティ モジュールの再起動
- Firepower 4100/9300 シャーシ のクラッシュ
- Firepower 4100/9300 シャーシ の再起動またはアップグレード
- 手動トリガー
- Firepower 4100/9300 シャーシ の電力損失
- セキュリティ モジュールの電力損失

## ハードウェアバイパスのスイッチオーバー

通常の運用からハードウェアバイパスに切り替えたとき、またはハードウェアバイパスから通常の運用に戻したときに、トラフィックが数秒間中断する可能性があります。中断時間の長さに影響を与える可能性があるいくつかの要因があります。たとえば、銅線ポートの自動ネゴシエーション、リンクエラーやデバウンスのタイミングをどのように処理するかなどのオプティカルリンクパートナーの動作、スパニングツリープロトコルのコンバージェンス、ダイナミックルーティングプロトコルのコンバージェンスなどです。この間は、接続が落ちることがあります。

また、通常の操作に戻った後で接続のミッドストリームを分析するときに、アプリケーションの識別エラーが原因で接続が切断されることがあります。

## フェールセーフとハードウェアバイパス

インラインセットには、「フェールセーフ」と呼ばれるソフトウェア障害設定が含まれます。IPSにソフトウェア障害がある場合は、サブシステムによってインラインセットのトラフィックの通過が回避され、フェールセーフオプションによってトラフィックが流れ続けます。フェールセーフは、[ハードウェアバイパス (Hardware Bypass)]機能でサポートされるインターフェイスペアのみでなく、タップモードのものを除くすべてのインターフェイスペアでサポートされます。ハードウェアバイパス

[ハードウェアバイパス (Hardware Bypass)]機能を使用すると、停電時や特定の限定されたソフトウェア障害などのハードウェア障害時にトラフィックが流れます。フェールセーフをトリガーするソフトウェアの障害は、[ハードウェアバイパス (Hardware Bypass)]機能をトリガーしません。

## ハードウェアバイパスのステータス

システムの電源が入っている場合、バイパスLEDはハードウェアバイパスのステータスを表示します。LEDの説明については、Firepower 4100/9300 シャーシのドキュメントを参照してください。

## インラインセットの前提条件

### ハードウェアバイパスのサポート

Firepower Threat Defense は、以下のモデルの特定のネットワークモジュールのインターフェイスペアでハードウェアバイパスをサポートします。

- Firepower 9300
- Firepower 4100 シリーズ

これらのモデルでサポートされているハードウェアバイパスネットワークモジュールは以下のとおりです。

- Firepower 6 ポート 1G SX FTW ネットワークモジュール シングルワイド (FPR-NM-6X1SX-F)

- Firepower 6 ポート 10G SR FTW ネットワーク モジュール シングルワイド (FPR-NM-6X10SR-F)
- Firepower 6 ポート 10G LR FTW ネットワーク モジュール シングルワイド (FPR-NM-6X10LR-F)
- Firepower 2 ポート 40G SR FTW ネットワーク モジュール シングルワイド (FPR-NM-2X40G-F)

ハードウェア バイパス では以下のポート ペアのみ使用できます。

- 1 および 2
- 3 および 4
- 5 および 6

## IPS 専用インターフェイスのガイドライン

### 一般的なガイドライン

- IPS 専用インターフェイスは物理インターフェイスだけをサポートし、EtherChannel、冗長インターフェイス、VLAN などにはできません。
- IPS 専用インターフェイスは、シャーシ間およびシャーシ内クラスタリングでサポートされます。

### ハードウェア バイパスのガイドライン

- ハードウェア バイパス ポートは、インラインセットでのみサポートされます。
- ハードウェア バイパス ポートを EtherChannel の一部にはできません。
- シャーシ内クラスタリングでサポートされます。シャーシ内の最後のユニットに障害が発生すると、ポートはハードウェア バイパス モードになります。
- クラスタ内のすべてのユニットに障害が発生すると、最終ユニットでハードウェア バイパスがトリガーされ、トラフィックは引き続き通過します。ユニットが復帰すると、ハードウェア バイパスはスタンバイモードに戻ります。ただし、アプリケーショントラフィックと一致するルールを使用すると、それらの接続が切断され、再確立する必要がある場合があります。状態情報がクラスタユニットに保持されず、ユニットがトラフィックを許可されたアプリケーションに属するものとして識別できないため、接続は切断されます。トラフィックのドロップを回避するには、アプリケーションベースのルールの代わりにポートベースのルールを使用します（展開に適している場合）。
- 高可用性モードでは、ハードウェア バイパスはサポートされていません。

## パッシブ IPS 専用インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ここでは、次の方法について説明します。

- インターフェイスを有効にします。デフォルトでは、インターフェイスは無効です。
- インターフェイスモードをパッシブまたはERSPANに設定します。ERSPANインターフェイスの場合は、ERSPAN パラメータと IP アドレスを設定します。
- MTU を交換してください。デフォルトでは、MTU は 1500 バイトに設定されます。MTU の詳細については、[MTU について \(684 ページ\)](#) を参照してください。
- 特定の速度と二重通信（使用できる場合）を設定する。デフォルトでは、速度とデュプレックスは [自動 (Auto)] に設定されます。



(注) FXOS シャーシ上の Firepower Threat Defense の場合は、Firepower 4100/9300 シャーシ で基本のインターフェイス設定を構成します。詳細については、『[Firepower 9300 configuration guide](#)』を参照してください。

### 始める前に

- ERSPAN インターフェイスは、デバイスがルーテッドファイアウォールモードになっているときにのみ使用できます。
- Management Center に追加した後、デバイスの物理インターフェイスを変更した場合、[インターフェイス (Interfaces)] タブの左上にある [デバイスからのインターフェイスの同期 (Sync Interfaces from device)] ボタンをクリックしてそのインターフェイスリストを更新する必要があります。

### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (✎) をクリックします。デフォルトで [インターフェイス (Interfaces)] タブが選択されています。
- ステップ 2** 編集するインターフェイスの編集アイコン (✎) をクリックします。
- ステップ 3** [モード (Mode)] ドロップダウンリストで、[パッシブ (Passive)] または [Erspan] を選択します。

- ステップ 4** [有効 (Enabled) ] チェック ボックスをオンにして、インターフェイスを有効化します。
- ステップ 5** [名前 (Name) ] フィールドに、48 文字以内で名前を入力します。
- ステップ 6** [セキュリティ ゾーン (Security Zone) ] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規 (New) ] をクリックして、新しいセキュリティ ゾーンを追加します。
- ステップ 7** (任意) [説明 (Description) ] フィールドに説明を追加します。  
説明は 200 文字以内で、改行を入れずに 1 行で入力します。
- ステップ 8** (任意) [一般 (General) ] タブで、[MTU] を 64 ~ 9198 バイトの間で設定します。Firepower Threat Defense Virtual および FXOS シャーシ上の Firepower Threat Defense の場合、最大値は 9000 バイトです。  
デフォルト値は 1500 バイトです。
- ステップ 9** ERSPAN インターフェイスの場合は、次のパラメータを設定します:
- [フロー ID (Flow Id) ] : ERSPAN トラフィックを特定するために送信元と宛先セッションによって使用される ID を、1 ~ 1023 の間で設定します。この ID は、ERSPAN 宛先セッション設定でも入力する必要があります。
  - [ソース IP (Source IP) ] : ERSPAN トラフィックの送信元として使用される IP アドレスを設定します。
- ステップ 10** ERSPAN インターフェイスの場合は、[IPv4] タブで IPv4 アドレスとマスクを設定します。
- ステップ 11** (任意) [ハードウェア構成 (Hardware Configuration) ] タブをクリックして、デュプレックスと速度を設定します。  
正確な速度とデュプレックス オプションはハードウェアによって異なります。
- [デュプレックス (Duplex) ] : [全 (Full) ]、[半 (Half) ]、または [自動 (Auto) ] を選択します。デフォルトは [自動 (Auto) ] です。
  - [速度 (Speed) ] : [10]、[100]、[1000]、または [自動 (Auto) ] を選択します。デフォルトは [自動 (Auto) ] です。
- ステップ 12** [OK] をクリックします。
- ステップ 13** [保存 (Save) ] をクリックします。  
これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。
-



## IPS 専用インターフェイスのインラインセットの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ここでは、インラインセットに追加できる2つの物理インターフェイスを有効にして名前を付けます。また、状況に応じて、サポートされるインターフェイス ペアに対してハードウェアバイパスを有効にすることができます。



- (注) FXOS シャーシ上の Firepower Threat Defense の場合は、Firepower 4100/9300 シャーシで基本のインターフェイス設定を構成します。詳細については、『[Firepower 9300 configuration guide](#)』を参照してください。

### 始める前に

- Firepower Threat Defense インライン ペア インターフェイスに接続する STP 対応スイッチに対して STP PortFast を設定することをお勧めします。この設定は、ハードウェアバイパスの設定に特に有効でバイパス時間を短縮できます。
- Management Center に追加した後、デバイスの物理インターフェイスを変更した場合、[インターフェイス (Interfaces)] タブの左上にある [デバイスからのインターフェイスの同期 (Sync Interfaces from device)] ボタンをクリックしてそのインターフェイス リストを更新する必要があります。

### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (✎) をクリックします。デフォルトで [インターフェイス (Interfaces)] タブが選択されています。
- ステップ 2** 編集するインターフェイスの編集アイコン (✎) をクリックします。
- ステップ 3** [モード (Mode)] ドロップダウンリストで、[なし (None)] を選択します。  
このインターフェイスをインラインセットに追加すると、このフィールドにモードのインラインが表示されます。
- ステップ 4** [有効 (Enabled)] チェック ボックスをオンにして、インターフェイスを有効化します。
- ステップ 5** [名前 (Name)] フィールドに、48 文字以内で名前を入力します。
- ステップ 6** [セキュリティゾーン (Security Zone)] ドロップダウンリストで、セキュリティゾーンを選択するか、[新規 (New)] をクリックして新しいセキュリティゾーンを追加します。

- ステップ 7** (任意) [説明 (Description)] フィールドに説明を追加します。  
説明は 200 文字以内で、改行を入れずに 1 行で入力します。
- ステップ 8** (任意) [ハードウェア構成 (Hardware Configuration)] タブをクリックして、デュプレックスと速度を設定します。  
正確な速度とデュプレックス オプションはハードウェアによって異なります。
- [デュプレックス (Duplex)] : [全 (Full)]、[半 (Half)]、または [自動 (Auto)] を選択します。デフォルトは [自動 (Auto)] です。
  - [速度 (Speed)] : [10]、[100]、[1000]、または [自動 (Auto)] を選択します。デフォルトは [自動 (Auto)] です。
- ステップ 9** [OK] をクリックします。  
このインターフェイスに対して他の設定は行わないでください。
- ステップ 10** インラインセットに追加する 2 番目のインターフェイスの編集アイコン (✎) をクリックします。
- ステップ 11** 最初のインターフェイスに関する設定を行います。
- ステップ 12** [インラインセット (Inline Sets)] タブをクリックします。
- ステップ 13** [インラインセットの追加 (Add Inline Set)] をクリックします。  
[インラインセットの追加 (Add Inline Set)] ダイアログボックスが、[一般 (General)] タブが選択された状態で表示されます。
- ステップ 14** [名前 (Name)] フィールドに、セットの名前を入力します。
- ステップ 15** (任意) [MTU] を 64 ~ 9198 バイトの間で変更します。Firepower Threat Defense Virtual および FXOS シャーシ上の Firepower Threat Defense の場合、最大値は 9000 バイトです。  
デフォルト値は 1500 バイトです。
- ステップ 16** (任意) センサー障害発生時に、トラフィックが検出をバイパスして、デバイスを通過できるように指定するには、[フェールセーフ (Failsafe)] チェックボックスをオンにします。  
管理対象デバイスは、内部トラフィックバッファをモニタし、それらのバッファが満杯である場合は検出をバイパスします。
- ステップ 17** (任意) [バイパス (Bypass)] モードの場合、次のいずれかのオプションを選択します。
- [無効 (Disabled)] : ハードウェア バイパス がサポートされているインターフェイスの場合はハードウェアバイパスを無効に設定するか、またはハードウェアバイパスがサポートされていないインターフェイスを使用します。
  - [スタンバイ (Standby)] : サポートされているインターフェイスのハードウェアバイパスをスタンバイ状態に設定します。ハードウェアバイパスインターフェイスのペアのみ表示されます。スタンバイ状態の場合、トリガーイベントが発生するまで、インターフェイスは通常動作を保ちます。

- [バイパス強制 (Bypass-Force)] : インターフェイス ペアを手動で強制的にバイパス状態にします。[インラインセット (Inline Sets)] タブでは、[バイパス強制 (Bypass-Force)] モードになっているインターフェイス ペアに対して [はい (Yes)] が表示されます。

**ステップ 18** [使用可能なインターフェイス ペア (Available Interfaces Pairs)] 領域でペアをクリックし、[追加 (Add)] をクリックして [選択済みインターフェイス ペア (Selected Interface Pair)] 領域にそのペアを移動します。

この領域には、モードが [なし (None)] に設定されている名前付きインターフェイスと有効なインターフェイス間で可能なすべてのペアが表示されます。

**ステップ 19** (任意) [詳細 (Advanced)] タブをクリックして、次のオプションパラメータを設定します。

- [タップ モード (Tap Mode)] : インライン タップ モードに設定します。  
同じインラインセットでこのオプションと厳密な TCP 強制を有効にすることはできないことに注意してください。
- [リンク ステートの伝達 (Propagate Link State)] : リンク ステートの伝達を設定します。  
リンク ステートの伝達によって、インラインセットのインターフェイスの 1 つが停止した場合、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、2 番目のインターフェイスも自動的に起動します。つまり、1 つのインターフェイスのリンク ステートが変化すると、デバイスはその変化を検知し、その変化に合わせて他のインターフェイスのリンク ステートを更新します。ただし、デバイスからリンク ステートの変更が伝達されるまで最大 4 秒かかります。障害状態のネットワーク デバイスを自動的に避けてトラフィックを再ルーティングするようにルータが設定されている復元力の高いネットワーク環境では、リンク ステートの伝達が特に有効です。
- [厳密な TCP 強制 (Strict TCP Enforcement)] : TCP のセキュリティを最大限に生かすために、厳密な強制を有効にできます。この機能は 3 ウェイハンドシェイクが完了していない接続をブロックします。

厳密な適用では次のパケットもブロックされます。

- 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
- レスポンダが SYN-ACK を送信する前に TCP 接続のイニシエータから送信された非 SYN/RST パケット
- SYN の後、セッションの確立前に TCP 接続のレスポンダから送信された非 SYN-ACK/RST パケット
- イニシエータまたはレスポンダから確立された TCP 接続の SYN パケット

**ステップ 20** [インターフェイス (Interfaces)] タブをクリックします。

**ステップ 21** いずれかのメンバー インターフェイスの編集 (✎) アイコンをクリックします。

**ステップ 22** [セキュリティ ゾーン (Security Zone)] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規 (New)] をクリックして、新しいセキュリティ ゾーンを追加します。

ゾーンは、インラインセットにインターフェイスを追加した後にのみ設定できます。インラインセットにインターフェイスを追加することで、インラインのモードが設定され、インラインタイプのセキュリティゾーンを選択できます。

**ステップ 23** [OK] をクリックします。

**ステップ 24** 2 番目のインターフェイスのセキュリティゾーンを設定します。

**ステップ 25** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## インターフェイスと Firepower Management Center の同期

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

デバイスでインターフェイスを追加または変更した場合は、Firepower Management Center でインターフェイスを手動で更新する必要があります。たとえば、Firepower 9300 デバイス上に EtherChannel、Firepower Threat Defense Virtual の上に追加のインターフェイス、またはネットワーク インターフェイス カードを追加する場合は、この手順を実行する必要があります。

### 手順

	コマンドまたはアクション	目的
<b>ステップ 1</b>	[デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、使用する Firepower Threat Defense デバイスの編集アイコン (✎) をクリックします。デフォルトで [インターフェイス (Interfaces) ] タブが選択されています。	
<b>ステップ 2</b>	[インターフェイス (Interfaces) ] タブの左上にある [デバイスからインターフェイスを同期 (Sync Interfaces from device) ] ボタンをクリックします。	
<b>ステップ 3</b>	[保存 (Save) ] をクリックします。	これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展

	コマンドまたはアクション	目的
		開できます。変更は、実際に展開するまで有効化されません。

例

次のタスク

-





## 第 28 章

# Threat Defense 用の DHCP および DDNS サービス

次のトピックでは、DHCP サービスと DDNS サービスについて、および Threat Defense デバイスでこれらを設定する方法について説明します。

- [DHCP サービスと DDNS サービスについて \(705 ページ\)](#)
- [DHCP サービスと DDNS サービスのガイドライン \(708 ページ\)](#)
- [DHCP サーバの設定 \(709 ページ\)](#)
- [DHCP リレー エージェントの設定 \(711 ページ\)](#)
- [DDNS の設定 \(713 ページ\)](#)

## DHCP サービスと DDNS サービスについて

次の項では、DHCP サーバ、DHCP リレー エージェント、および DDNS 更新について説明します。

### DHCPv4 サーバについて

DHCP は、IP アドレスなどのネットワーク構成パラメータを DHCP クライアントに提供します。Firepower Threat Defense デバイスは、Firepower Threat Defense デバイス インターフェイスに接続されている DHCP クライアントに、DHCP サーバを提供します。DHCP サーバは、ネットワーク構成パラメータを DHCP クライアントに直接提供します。

IPv4 DHCP クライアントは、サーバに到達するために、マルチキャストアドレスよりもブロードキャストを使用します。DHCP クライアントは UDP ポート 68 でメッセージを待ちます。DHCP サーバは UDP ポート 67 でメッセージを待ちます。

IPv6 の DHCP サーバはサポートされていません。ただし、IPv6 トラフィックの DHCP リレーを有効にできます。

## DHCP オプション

DHCP は、TCP/IP ネットワーク上のホストに設定情報を渡すフレームワークを提供します。設定パラメータは DHCP メッセージの Options フィールドにストアされているタグ付けされたアイテムにより送信され、このデータはオプションとも呼ばれます。ベンダー情報も Options に保存され、ベンダー拡張情報はすべて DHCP オプションとして使用できます。

たとえば、Cisco IP Phone が TFTP サーバから設定をダウンロードする場合を考えます。Cisco IP Phone の起動時に、IP アドレスと TFTP サーバの IP アドレスの両方が事前に設定されていない場合、Cisco IP Phone ではオプション 150 または 66 を伴う要求を DHCP サーバに送信して、この情報を取得します。

- DHCP オプション 150 では、TFTP サーバのリストの IP アドレスが提供されます。
- DHCP オプション 66 では、1 つの TFTP サーバの IP アドレスまたはホスト名が与えられます。
- DHCP オプション 3 では、デフォルト ルートが設定されます。

1 つの要求にオプション 150 と 66 の両方が含まれている場合があります。この場合、両者が ASA ですでに設定されていると、ASA の DHCP サーバは、その応答で両方のオプションに対する値を提供します。

高度な DHCP オプションにより、DNS、WINS、ドメイン名のパラメータを DHCP クライアントに提供できます。DNS ドメインサフィックスには DHCP オプション 15 が使用されます。これらの値は DHCP 自動構成設定を使用して取得するか、または手動で定義できます。この情報の定義に 2 つ以上の方法を使用すると、次の優先順位で情報が DHCP クライアントに渡されます。

1. 手動で行われた設定
2. 高度な DHCP オプションの設定
3. DHCP 自動構成設定

たとえば、DHCP クライアントが受け取るドメイン名を手動で定義し、次に DHCP 自動構成を有効にできます。DHCP 自動構成によって、DNS サーバおよび WINS サーバとともにドメインが検出されても、手動で定義したドメイン名が、検出された DNS サーバ名および WINS サーバ名とともに DHCP クライアントに渡されます。これは、DHCP 自動構成プロセスで検出されたドメイン名よりも、手動で定義されたドメイン名の方が優先されるためです。

## DHCP リレー エージェントについて

インターフェイスで受信した DHCP 要求を 1 つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。DHCP クライアントは、最初の DHCPDISCOVER メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワークセグメントにクライアントがある場合、Firepower Threat Defense デバイスはブロードキャストトラフィックを転送しないため、UDP ブロードキャストは通常転送されません。DHCP リレー エン



ントを使用して、ブロードキャストを受信している Firepower Threat Defense デバイスのインターフェイスが DHCP 要求を別のインターフェイスの DHCP サーバに転送するように設定できます。

## DDNS について

DDNS 更新では、DNS を DHCP に組み込みます。これら2つのプロトコルは相互補完します。DHCP は、IP アドレス割り当てを集中化および自動化します。DDNS アップデートは、割り当てられたアドレスとホスト名の間のアソシエーションを事前定義された間隔で自動的に記録します。DDNS は、頻繁に更新されるアドレスとホスト名の関連付けを頻繁に更新できるようにします。これにより、たとえばモバイルホストは、ユーザまたは管理者が操作することなく、ネットワーク内を自由に移動できます。DDNS は、DNS サーバ上で、名前からアドレスへのマッピングと、アドレスから名前へのマッピングを動的に更新して、同期します。

DDNS の名前とアドレスのマッピングは、DHCP サーバ上で2つのリソースレコード (RR) で行われます。RR では、名前から IP アドレスへのマッピングが保持され、PTR RR では、アドレスから名前へのマッピングが行われます。DDNS 更新を実行するための2つの方式 (RFC 2136 で規定されている IETF 標準規格、および一般的な HTTP 方式) のうち、Firepower Threat Defense デバイスでは、IETF 方式をサポートしています。



(注) DDNS は BVI またはブリッジグループメンバーインターフェイスではサポートされません。

## DDNS 更新設定

2つの最も一般的な DDNS 更新設定は次のとおりです。

- DHCP クライアントは A RR を更新し、DHCP サーバは PTR RR を更新します。
- DHCP サーバは、A RR と PTR RR の両方を更新します。

通常、DHCP サーバはクライアントの代わりに DNS PTR RR を保持します。クライアントは、必要なすべての DNS 更新を実行するように設定できます。サーバは、これらの更新を実行するかどうかを設定できます。DHCP サーバは、PTR RR を更新するクライアントの完全修飾ドメイン名 (FQDN) を認識する必要があります。クライアントは Client FQDN と呼ばれる DHCP オプションを使用して、サーバに FQDN を提供します。

## UDP パケットサイズ

DDNS は、DNS 要求者が UDP パケットのサイズをアダプティブできるようにし、512 オクテットより大きいパケットの転送を容易にします。DNS サーバは UDP 上で要求を受信すると、OPT RR から UDP パケットサイズを識別し、要求者により指定された最大 UDP パケットサイズにできるだけ多くのリソースレコードを含めることができるよう、応答のサイズを調整します。DNS パケットのサイズは、BIND の場合は最大 4096 バイト、Windows 2003 DNS サーバの場合は 1280 バイトです。

# DHCP サービスと DDNS サービスのガイドライン

この項では、DHCP および DDNS サービスを設定する前に確認する必要があるガイドラインおよび制限事項について説明します。

## ファイアウォール モード

- DHCP リレーは、トランスペアレント ファイアウォール モード。
- DHCP サーバは、ブリッジ グループ メンバー インターフェイス上のトランスペアレント ファイアウォール モードでサポートされます。
- DDNS は、トランスペアレント ファイアウォール モード。

## IPv6

DHCP サーバでサポートされます。DHCP リレーの IPv6 はサポートされます。

## DHCPv4 サーバ

- 使用可能な DHCP の最大プールは 256 アドレスです。
- インターフェイスごとに 1 つの DHCP サーバのみを設定できます。各インターフェイスは、専用のアドレス プールのアドレスを使用できます。しかし、DNS サーバ、ドメイン名、オプション、ping のタイムアウト、WINS サーバなど他の DHCP 設定はグローバルに設定され、すべてのインターフェイス上の DHCP サーバによって使用されます。
- DHCP クライアントや DHCP リレー サービスは、サーバがイネーブルになっているインターフェイス上では設定できません。また、DHCP クライアントは、サーバがイネーブルになっているインターフェイスに直接接続する必要があります。
- Firepower Threat Defense デバイスは、QIP DHCP サーバと DHCP プロキシ サービスとの併用をサポートしません。
- DHCP サーバもイネーブルになっている場合、リレーエージェントをイネーブルにすることはできません。
- DHCP サーバは、BOOTP 要求をサポートしていません。

## DHCP リレー

- グローバルおよびインターフェイス固有のサーバを合わせて 10 台までの DHCPv4 リレーサーバを設定できます。インターフェイスごとには、4 台まで設定できます。
- 10 台までの DHCPv6 リレー サーバを設定できます。IPv6 のインターフェイス固有のサーバはサポートされません。
- DHCP サーバもイネーブルになっている場合、リレーエージェントをイネーブルにできません。

- DHCP リレー サービスは、トランスペアレントファイアウォールモード。ただし、アクセスルールを使用して DHCP トラフィックを通過させることはできません。DHCP 要求と応答が Firepower Threat Defense デバイスを通過できるようにするには、2つのアクセスルールを設定する必要があります。1つは内部インターフェイスから外部（UDP 宛先ポート 67）への DHCP 要求を許可するもので、もう1つは逆方向（UDP 宛先ポート 68）に向かうサーバからの応答を許可するためのものです。
- IPv4 の場合、クライアントは直接 Firepower Threat Defense デバイスに接続する必要があります。他のリレーエージェントやルータを介して要求を送信できません。IPv6 の場合、Firepower Threat Defense デバイスは別のリレーサーバからのパケットをサポートします。
- DHCP クライアントは、Firepower Threat Defense デバイスが要求をリレーする DHCP サーバとは別のインターフェイスに存在する必要があります。
- トラフィックゾーン内のインターフェイスで DHCP リレーを有効にできません。

## DHCP サーバの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。

**ステップ 2** [DHCP] > [DHCP サーバ (DHCP Server)] を選択します。

**ステップ 3** 次の DHCP サーバのオプションを設定します。

- [Ping タイムアウト (Ping Timeout)] : Firepower Threat Defense デバイスが DHCP ping 試行のタイムアウトを待つ時間をミリ秒単位で入力します。有効値の範囲は 10 ~ 10000 ミリ秒です。デフォルト値は、50 ミリ秒です。

アドレスの衝突を避けるために、Firepower Threat Defense デバイスは、1つのアドレスに ICMP ping パケットを 2 回送信してから、そのアドレスを DHCP クライアントに割り当てます。

- [リース長 (Lease Length)] : リースの期間が終了する前に、割り当て IP アドレスをクライアントが使用できる秒単位の時間。有効な値の範囲は、300 ~ 1048575 秒です。デフォルト値は 3600 秒 (1 時間) です。

- (ルーテッドモード) [自動設定 (Auto-configuration)] : Firepower Threat Defense デバイスでDHCP自動設定を有効にします。自動設定では、指定したインターフェイスで動作しているDHCPクライアントから取得したDNSサーバ、ドメイン名、およびWINSサーバの情報が、DHCPサーバからDHCPクライアントに提供されます。自動設定にしない場合は、自動設定を無効にして、手順4で値を追加することもできます。
- [インターフェイス (Interface)] : Firepower Threat Defense デバイスが指定インターフェイス (通常は外側) 上でDHCPクライアントとして動作している場合に、自動コンフィギュレーションのためのDNS、WINS、ドメイン名情報を提供するDHCPクライアントのインターフェイス。トランスペアレントモードでは、ブリッジグループメンバーインターフェイスを指定します。

**ステップ4** 自動設定をオーバーライドするには、以下を実行します。

- インターフェイスのドメイン名を入力します。たとえば、デバイスは `Your_Company` ドメインにあるかもしれません。
- ドロップダウンリストから、インターフェイスに設定されたDNSサーバ (プライマリおよびセカンダリ) を選択します。DNSサーバを新たに追加する手順については、[ネットワークオブジェクトの作成 \(434 ページ\)](#) を参照してください。
- ドロップダウンリストから、インターフェイスに設定されたWINSサーバ (プライマリおよびセカンダリ) を選択します。WINSサーバを新たに追加する手順については、[ネットワークオブジェクトの作成 \(434 ページ\)](#) を参照してください。

**ステップ5** [サーバ (Server)] タブを選択して、[追加 (Add)] をクリックし、以下のオプションを設定します。

- ドロップダウンリストからインターフェイスを選択します。
- [アドレスプール (Address Pool)] : DHCPサーバが使用するIPアドレスの最下位から最上位の間の範囲です。IPアドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身のIPアドレスを含めることはできません。
- [DHCPサーバを有効にする (Enable DHCP Server)] : 選択したインターフェイスのDHCPサーバを有効にします。

**ステップ6** [OK] をクリックして、DHCPサーバの設定を保存します。

**ステップ7** (オプション) [詳細 (Advanced)] タブを選択して、[追加 (Add)] をクリックし、DHCPクライアントに戻すオプションの情報のタイプを指定します。

- [オプションコード (Option Code)] : Firepower Threat Defense デバイスは、RFC 2132、RFC 2562、およびRFC 5510に記載されている情報を送信するDHCPオプションをサポートしています。オプション1、12、50～54、58～59、61、67、82を除き、すべてのDHCPオプション (1～255) がサポートされています。DHCPオプションコードの詳細については、[DHCPv4サーバについて \(705 ページ\)](#) を参照してください。

(注) Firepower Threat Defense デバイスは、指定されたオプションのタイプおよび値が、RFC 2132 に定義されているオプション コードに対して期待されているタイプおよび値と一致するかどうかは確認しません。オプションコードと、コードに関連付けられたタイプおよび期待値の詳細については、RFC 2132 を参照してください。

- [タイプ (Type) ] : DHCP のオプションのタイプ。使用できるオプションには、IP、ASCII、および HEX が含まれます。IP を選択する場合、[IP アドレス (IP Address) ] フィールドに IP アドレスを追加する必要があります。ASCII を選択する場合、[ASCII] フィールドに [ASCII] 値を追加する必要があります。HEX を選択する場合、[HEX] フィールドに [HEX] 値を追加する必要があります。
- [IP アドレス 1 (IP Address 1) ] および [IP アドレス 2 (IP Address 2) ] : このオプションコードで戻る IP アドレス。IP アドレスを新たに追加する手順については、[ネットワーク オブジェクトの作成 \(434 ページ\)](#) を参照してください。
- [ASCII] : DHCP クライアントに戻る ASCII 値。文字列にスペースを含めることはできません。
- [HEX] : DHCP クライアントに戻る HEX 値。文字列はスペースなしの偶数でなければなりません。0x プレフィックスを使用する必要はありません。

ステップ 8 [OK] をクリックして、オプション コードの設定を保存します。

ステップ 9 DHCP ページで [保存 (Save) ] をクリックして変更を保存します。

## DHCP リレー エージェントの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

インターフェイスで受信した DHCP 要求を 1 つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。DHCP クライアントは、最初の DHCPDISCOVER メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワークセグメントにクライアントがある場合、Firepower Threat Defense デバイスはブロードキャストトラフィックを転送しないため、UDP ブロードキャストは通常転送されません。

ブロードキャストを受信している Firepower Threat Defense デバイスのインターフェイスが DHCP 要求を別のインターフェイスの DHCP サーバに転送するように設定すると、この状況を改善できます。



(注) DHCP リレーは、トランスペアレント ファイアウォール モードまたはでは、サポートされません。

#### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。

**ステップ 2** [DHCP] > [DHCP リレー (DHCP Relay)] を選択します。

**ステップ 3** [タイムアウト (Timeout)] フィールドでは、Firepower Threat Defense デバイスが DHCP リレー エージェントのタイムアウトを待つ時間を秒単位で入力します。有効な値の範囲は、1 ~ 3600 秒です。デフォルト値は 60 秒です。

タイムアウトは、ローカル DHCP リレー エージェントを介すアドレス ネゴシエーション用です。

**ステップ 4** [DHCP リレー エージェント (DHCP Relay Agent)] タブで、[追加 (Add)] をクリックして、以下のオプションを設定します。

- [インターフェイス (Interface)] : DHCP クライアントに接続されているインターフェイス。
- [DHCP リレーを有効にする (Enable DHCP Relay)] : このインターフェイスで IPv4 DHCP リレーを有効にします。
- [ルート設定 (Set Route)] : (IPv4 用) サーバからの DHCP メッセージのデフォルトゲートウェイアドレスを、元の DHCP 要求をリレーした DHCP クライアントに最も近い Firepower Threat Defense デバイスのインターフェイスのアドレスに変更します。このアクションを行うと、クライアントは、自分のデフォルトルートを設定して、DHCP サーバで異なるルータが指定されている場合でも、Firepower Threat Defense デバイスをポイントすることができます。パケット内にデフォルトのルータ オプションがなければ、Firepower Threat Defense デバイスは、そのインターフェイスのアドレスを含んでいるデフォルトルータを追加します。
- [IPv6 リレーを有効にする (Enable IPv6 Relay)] : このインターフェイスで IPv6 DHCP リレーを有効にします。

**ステップ 5** [OK] をクリックして、DHCP リレー エージェントの変更を保存します。

**ステップ 6** [DHCP サーバ (DHCP Servers)] タブで、[追加 (Add)] をクリックして、以下のオプションを設定します。

IPv4 サーバアドレスおよび IPv6 サーバアドレスが同じサーバに属していても、個別のエントリとして追加します。

- [サーバ (Server) ] : DHCP サーバの IP アドレス。ドロップダウンリストから IP アドレスを選択します。新たに加えるには、次を参照してください。 [ネットワーク オブジェクトの作成 \(434 ページ\)](#)
- [インターフェイス (Interface) ] : 指定の DHCP サーバが接続されるインターフェイス。DHCP リレー エージェントと DHCP サーバを、同じインターフェイスに設定することはできません。

**ステップ 7** [OK] をクリックして、DHCP サーバの変更を保存します。

**ステップ 8** DHCP ページで [保存 (Save) ] をクリックして変更を保存します。

## DDNS の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ダイナミック DNS (DDNS) アップデートにより、DNS を DHCP に組み込みます。DDNS 更新プログラムは割り当て済みアドレスとホスト名間のアソシエーションを自動的に記録し、頻繁に変更されるアドレスとホスト名間のアソシエーションを効果的に更新できるようにします。

### 始める前に

- 概要については、[DDNS について \(707 ページ\)](#) を参照してください。
- DDNS は、トランスペアレント ファイアウォール モードでサポートされていません。

### 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、Firepower Threat Defense デバイスを編集します。

**ステップ 2** [DHCP] > [DDNS] を選択して、次の DDNS オプションを設定します。

- [DHCP クライアントが記録更新を DHCP サーバに要求 (DHCP Client Requests DHCP Server to update Records) ] : DHCP サーバによる指定の記録の更新を DHCP クライアントが要求するよう設定します。使用可能なオプションは、[選択なし (Not Selected) ]、[更新なし (No Update) ]、[PTR のみ (Only PTR) ]、[A と PTR 記録 (Both A and PTR Records) ] です。A および PTR 記録の説明については、[DDNS について \(707 ページ\)](#) を参照してください。

- [DHCP クライアントブロードキャストを有効にする (Enable DHCP Client Broadcast) ] : DHCP クライアントが DHCP サーバに到達するためにブロードキャストアドレスを使用することを有効にします。
- [ダイナミック DNS 更新 (Dynamic DNS Update) ] : DHCP サーバの DDNS 更新に使用する記録を選択します。使用可能なオプションは、[選択なし (Not Selected) ]、[PTR のみ (Only PTR) ]、[A と PTR 記録 (Both A and PTR Records) ] です。
- [DHCP クライアント要求のオーバーライド (Override DHCP Client Requests) ] : DHCP サーバのアクションが、DHCP クライアントによって要求された更新アクションをオーバーライドするよう指定します。

**ステップ 3** [DHCP クライアント ID インターフェイス (DHCP Client ID Interface) ] タブで、[使用可能なインターフェイス (Available Interfaces) ] リストからインターフェイスを選択し、[追加 (Add) ] をクリックして、インターフェイスを [選択されたインターフェイス (Selected Interfaces) ] リストに移動します。

**ステップ 4** [DDNS インターフェイス設定 (DDNS Interface Settings) ] タブで、[追加 (Add) ] をクリックし、以下のオプションを設定します。

- [インターフェイス (Interface) ] : 設定済みのそれぞれのインターフェイスに DDNS 設定を追加するには、ドロップダウンリストからインターフェイスを選択します。
- [方法名 (Method Name) ] : インターフェイスに割り当てられた DDNS 更新方法。
- [ホスト名 (Host Name) ] : DDNS クライアントのホスト名。
- [DHCP クライアントが更新要求を DHCP サーバに要求 (DHCP Client requests DHCP server to update requests) ] : DHCP サーバによる指定の記録の更新を DHCP クライアントが要求するよう設定します。使用可能なオプションは、[選択なし (Not Selected) ]、[更新なし (No Update) ]、[PTR のみ (Only PTR) ]、[A と PTR 記録 (Both A and PTR Records) ] です。A および PTR 記録の説明については、[DDNS について \(707 ページ\)](#) を参照してください。
- [ダイナミック DNS 更新 (Dynamic DNS Update) ] : DHCP サーバの DDNS 更新に使用する記録を選択します。使用可能なオプションは、[選択なし (Not Selected) ]、[PTR のみ (Only PTR) ]、[A と PTR 記録 (Both A and PTR Records) ] です。
- [DHCP クライアント要求のオーバーライド (Override DHCP Client Requests) ] : DHCP サーバのアクションが、DHCP クライアントによって要求された更新アクションをオーバーライドするよう指定します。

**ステップ 5** [OK] をクリックして、DDNS のインターフェイスの変更を保存します。

**ステップ 6** [DDNS 更新方法 (DDNS Update Methods) ] タブで、[追加 (Add) ] をクリックし、以下のオプションを設定します。

- [方法名 (Method Name) ] : インターフェイスに割り当てられた DDNS 更新方法。
- [更新間隔 (Update Interval) ] : 日 (0 ~ 364) 、時 (0 ~ 23) 、分 (0 ~ 59) 、秒 (0 ~ 59) で設定される DNS の更新試行の整数の更新間隔。これらの単位は、追加式です。つ



まり、日数に 0、時間数に 0、分数に 5、秒数に 15 を入力した場合、この更新方法がアクティブである限り、5 分 15 秒ごとに更新が試行されます。

- [更新記録 (Update Records)] : DNS クライアントによるサーバリソース記録の更新を保存します。使用可能なオプションは、[定義なし (Not Defined)]、[A と PTR 記録 (Both A and PTR Records)]、[A 記録 (A Records)] です。

**ステップ 7** [OK] をクリックして、DDNS の更新方法の変更を保存します。

**ステップ 8** DHCP ページで [保存 (Save)] をクリックして変更を保存します。

---





## 第 29 章

# Firepower Threat Defense 用の Quality of Service (QoS)

以下のトピックでは、Firepower Threat Defense デバイスを使ってネットワーク トラフィックを管理するために Quality of Service (QoS) 機能を使用する方法について説明します。

- [QoS の概要 \(717 ページ\)](#)
- [QoS ポリシーについて \(718 ページ\)](#)
- [QoS ポリシーによるレートの制限 \(719 ページ\)](#)

## QoS の概要

Quality of Service (QoS) は、アクセス制御によって許可または信頼されている (ポリシーの) ネットワーク トラフィックをレート制限します。システムはファストパスされたトラフィックにレート制限は行いません。

QoS は、Firepower Threat Defense デバイスのルーテッドインターフェイスのみでサポートされています。

### レート制限された接続のロギング

QoS 用のロギング設定はありません。接続はロギングなしでレート制限することができ、またレート制限されているという理由だけで接続をロギングすることはできません。接続イベントで QoS 情報を表示するには、適切な接続の終了を Firepower Management Center データベースに個別にロギングする必要があります。[設定可能な接続ロギング \(2504 ページ\)](#) を参照してください。

レート制限された接続の接続イベントには、どの程度のトラフィックがドロップされ、どの QoS の設定がトラフィックを制限したかについての情報が含まれています。この情報はイベントビュー (ワークフロー)、ダッシュボード、レポートで確認できます。

## QoS ポリシーについて

管理対象デバイスに展開する QoS ポリシーによりレート制限が決まります。各 QoS ポリシーは、複数のデバイスを対象にすることができます。各デバイスで同時に展開可能な QoS ポリシーは 1 つです。

QoS ポリシーでは、最大 32 の QoS ルールがネットワークトラフィックを処理します。システムは指定した順序で QoS ルールをトラフィックと照合します。システムは、すべての条件がトラフィックに一致する最初のルールに従ってトラフィックをレート制限します。どのルールにも一致しないトラフィックは、レート制限を受けません。

QoS ルールは、送信元または接続先（ルーティング先）インターフェイスによって制約を設ける必要があります。システムは、これらの個別のインターフェイスでそれぞれ独立したレート制限を行います。複数のインターフェイスにまとめてレート制限を指定することはできません。

QoS ルールでは、その他のネットワーク特性や、アプリケーション、URL、およびユーザ ID などのコンテキスト情報によってトラフィックのレート制限を行うこともできます。

トラフィックのアップロードやダウンロードのレート制限を個別に行うことが可能です。システムは、接続インシエータを基準としてダウンロードかアップロードかを判別します。



(注) QoS はマスターアクセス制御設定に従属するものではありません。QoS は個別に設定します。ただし、同じデバイスに展開されたアクセスコントロールポリシーおよび QoS ポリシーはアイデンティティ設定を共有します。[アクセス制御への他のポリシーの関連付け \(1340 ページ\)](#) を参照してください。

### QoS ポリシーとマルチテナンシー

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

先祖ドメインの管理者は、異なる子孫ドメインのデバイスに、同じ QoS ポリシーを展開できます。子孫ドメインの管理者は、この先祖ドメインから展開された読み取り専用 QoS ポリシーを使用するか、またはローカルポリシーに置き換えることができます。

## QoS ポリシーによるレートの制限

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Admin/Access Admin/Network Admin

ポリシー ベースのレート制限を実行するために、管理対象デバイスに QoS ポリシーを設定して展開します。各 QoS ポリシーは複数のデバイスをターゲットにすることができます。各デバイスに同時に展開できる QoS ポリシーは 1 つです。

ポリシーの編集は、1つのブラウザウィンドウを使用して、一度に1人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシーエディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

### 手順

**ステップ 1** [デバイス (Devices)] > [QoS] を選択します。

**ステップ 2** [新規ポリシー (New Policy)] をクリックして、新しい QoS ポリシーを作成して、必要に応じてターゲットデバイスを割り当てます。詳細については、[QoS ポリシーの作成 \(720 ページ\)](#) を参照してください。

また、既存のポリシーをコピー (📄) または編集 (✏️) することもできます。

**ステップ 3** QoS ルールを設定します。[QoS ルールの設定 \(722 ページ\)](#) または [ルール管理：共通の特性 \(369 ページ\)](#) を参照してください。

QoS ポリシー エディタの [ルール (Rules)] タブには、各ルールが評価順にリストされ、ルール条件とレート制限の設定の概要が表示されます。右クリックのメニューには、ルールの管理オプション (移動、有効化、無効化など) があります。

大規模な展開では、特定のデバイスまたはデバイスのグループに影響するルールのみを表示する、[デバイス基準のフィルタ (Filter by Device)] が役に立ちます。また、ルールの検索とルール内の検索も可能です。システムは、[ルールの検索 (Search Rules)] フィールドに入力されたテキストをルールの名前および条件値と照合します。これには、オブジェクトとオブジェクトグループが含まれます。

(注) ルールを適切に作成して順序付けることは複雑なタスクですが、効果的な展開を構築する上で不可欠なタスクです。慎重に計画していないと、ルールが別のルールをプリエンプション処理したり、追加のライセンスが必要になったり、ルールに無効な設定が含まれる場合があります。アイコンにより、コメント、警告、およびエラーが表示されます。問題があれば、[警告の表示 (Show Warnings)] をクリックしてリストを表示します。詳細については、[ルールのパフォーマンスに関するガイドライン \(412 ページ\)](#) を参照してください。

**ステップ 4** [ポリシーの割り当て (Policy Assignments)] をクリックして、ポリシーがターゲットにしている管理対象デバイスを特定します。詳細については、[QoS ポリシーのターゲットデバイスの設定 \(721 ページ\)](#) を参照してください。

ポリシーの作成中にデバイス ターゲットを特定した場合は、選択内容を確認します。

**ステップ 5** QoS ポリシーを保存します。

**ステップ 6** 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## QoS ポリシーの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Admin Access Admin Network Admin

ルールのない新規 QoS ポリシーは、レート制限を実行しません。

### 手順

**ステップ 1** [デバイス (Devices)] > [QoS] を選択します。

**ステップ 2** [新しいポリシー (New Policy)] をクリックします。

**ステップ 3** [名前 (Name)] を入力し、必要に応じて [説明 (Description)] を入力します。

**ステップ 4** (オプション) ポリシーを展開する [使用可能なデバイス (Available Devices)] を選択し、[ポリシーに追加 (Add to Policy)] をクリックするか、[選択されたデバイス (Selected Devices)] にドラッグアンドドロップします。表示されるデバイスを絞り込むには、[検索 (Search)] フィールドに検索文字列を入力します。

ポリシーを展開する前に、デバイスを割り当てる必要があります。

**ステップ 5** [保存 (Save)] をクリックします。

## 次のタスク

- QoS ポリシーを設定および展開します。[QoS ポリシーによるレート制限 \(719 ページ\)](#) を参照してください。

## QoS ポリシーのターゲット デバイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Admin Access Admin Network Admin

各 QoS ポリシーは複数のデバイスをターゲットにすることができます。各デバイスに同時に展開できる QoS ポリシーは 1 つです。

## 手順

**ステップ 1** QoS ポリシー エディタで、[ポリシーの割り当て (Policy Assignments)] をクリックします。

**ステップ 2** ターゲット リストを作成します。

- 追加: 1 つ以上の [使用可能なデバイス (Available Devices)] を選択して、[ポリシーに追加 (Add to Policy)] をクリックするか、[選択したデバイス (Selected Devices)] のリストにドラッグアンドドロップします。
- 削除: 1 つのデバイスの横にある削除アイコン (🗑️) をクリックするか、複数のデバイスを選択して、右クリックしてから [選択済み項目の削除 (Delete Selected)] を選択します。
- 検索: 検索フィールドに検索文字列を入力します。検索をクリアするには、クリア (✖) をクリックします。

**ステップ 3** [OK] をクリックしてポリシーの割り当てを保存します。

**ステップ 4** [保存 (Save)] をクリックしてポリシーを保存します。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## QoS ルールの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Admin/Access Admin/Network Admin

ルールを作成または編集するときに、一般的なルールプロパティを設定するには、ルールエディタの上部を使用します。ルール条件とコメントを設定するには、下部のタブを使用します。

### 手順

**ステップ 1** QoS ポリシー エディタの [ルール (Rules) ] タブで、次の操作を実行します。

- ルールの追加 : [ルールの追加 (Add Rule) ] をクリックします。
- ルールの編集 : 編集アイコン (✎) をクリックします。

**ステップ 2** 名前を入力します。

**ステップ 3** ルール コンポーネントを設定します。

- [有効化 (Enabled) ] : ルールを有効にするかどうかを指定します。
- [QoS の適用 (Apply QoS On) ] : レート制限するインターフェイス ([宛先インターフェイス オブジェクトのインターフェイス (Interfaces in Destination Interface Objects) ] または [送信元インターフェイス オブジェクトのインターフェイス (Interfaces in Source Interface Objects) ]) を選択します。選択するインターフェイスは、入力されたインターフェイス 制約 (任意ではなく) と一致する必要があります。
- [インターフェイスごとのトラフィック制限 (Traffic Limit Per Interface) ] : ダウンロード/アップロード制限を Mb/s 単位で入力します。ダウンロードトラフィックとアップロードトラフィックに異なる制限を入力するには、[詳細 (Advanced) ] をクリックします。[無制限 (Unlimited) ] のデフォルト値にすると、一致するトラフィックはレート制限されません。
- [条件 (Conditions) ] : 追加する条件に対応するタブをクリックします。[QoS の適用 (Apply QoS On) ] の選択内容に対応する、送信元インターフェイスまたは宛先インターフェイスの条件を設定する必要があります。
- [コメント (Comments) ] : [コメント (Comments) ] タブをクリックします。コメントを追加するには、[新規コメント (New Comment) ] をクリックしてコメントを入力し、[OK] をクリックします。ルールを保存するまでこのコメントを編集または削除できます。

ルールコンポーネントの詳細については、[QoS ルールコンポーネント \(723 ページ\)](#) を参照してください。

**ステップ 4** ルールを保存します。



**ステップ 5** ポリシーエディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリックメニューを使用してカットアンドペーストを実行します。

ルールには1から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワークトラフィックの処理に必要なリソースが削減され、ルールのプリエンブションを回避できます。

**ステップ 6** [保存 (Save) ] をクリックしてポリシーを保存します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[ルールのパフォーマンスに関するガイドライン \(412 ページ\)](#)

## QoS ルール コンポーネント

### 状態 (有効/無効)

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

### インターフェイス (QoS の適用対象)

すべてのトラフィックがレート制限されている QoS のルールは保存できません。QoS のルールごとに、次のいずれかに QoS を適用する必要があります：

- 送信元インターフェイスオブジェクトのインターフェイス：レートは、ルールの送信元インターフェイスを介するトラフィックに制限されます。このオプションを選択すると、少なくとも1つの送信元インターフェイスの制約を追加する必要があります (どんな制約であってもよいわけではありません)。
- 宛先インターフェイスオブジェクト：レートは、ルールの宛先インターフェイスを介するトラフィックに制限されます。このオプションを選択すると、少なくとも1つの宛先インターフェイスの制約を追加する必要があります (どんな制約であってもよいわけではありません)。

### インターフェイスごとのトラフィック制限

QoS ルールでは、[Apply QoS On (QoS の適用対象) ] オプションで指定するインターフェイスごとに個別にレートを制限します。インターフェイスのセットに対して集約レート制限を指定することはできません。

トラフィックのレート制限を M ビット/秒とします。[無制限 (Unlimited) ] のデフォルト値では、一致したトラフィックのレートは制限されません。

詳細設定により、トラフィックのアップロードやダウンロードのレート制限を個別に行うことが可能です。システムは、接続インシエータに基づいてダウンロード方向とアップロード方向を決定します。

インターフェースの最大スループットを超える制限を指定すると、システムは一致しているトラフィックのレート制限は行いません。最大スループットはインターフェースのハードウェア構成による影響を受ける可能性があり、各デバイス（**[デバイス (Devices)] > [デバイス管理 (Device Management)]**）のプロパティに指定します。

### 条件 (Conditions)

条件は、ルールが処理する特定のトラフィックを指定します。各ルールには複数の条件を設定できます。トラフィックは、ルールに一致するすべての条件に適合する必要があります。各条件の種類には、ルールエディタ内に独自のタブがあります。以下を使用して、トラフィックをレート制限できます：

- [インターフェイス条件 \(374 ページ\)](#) (ルート設定済みの場合のみ、必須)
- [ネットワーク条件 \(377 ページ\)](#)
- [ポートおよび ICMP コードの条件 \(382 ページ\)](#)
- [アプリケーション条件 \(アプリケーション制御\) \(386 ページ\)](#)
- [URL 条件 \(URL フィルタリング\) \(393 ページ\)](#)
- [ユーザ条件、レルム条件、および ISE 属性条件 \(ユーザ制御\) \(401 ページ\)](#)

### 説明

ルールで変更を保存するたびに、コメントを追加することができます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。

ポリシー エディタでは、システムがそのルールのコメント数を表示します。ルール エディタでは、**[コメント (Comments)]** タブを使用して、既存のコメントを表示し、新しいコメントを追加します。



## 第 **IX** 部

# Firepower Threat Defense のハイ アベイラビリティと拡張性

- [Firepower Threat Defense ハイ アベイラビリティ \(727 ページ\)](#)
- [Firepower 9300 の Firepower Threat Defense クラスタ \(757 ページ\)](#)





## 第 30 章

# Firepower Threat Defense ハイ アベイラビリティ

次のトピックでは、Cisco Firepower Threat Defense のハイ アベイラビリティを達成するためにアクティブ/スタンバイ フェールオーバーを設定する方法について説明します。

- [ハイ アベイラビリティ Firepower Threat Defense について \(727 ページ\)](#)
- [ハイ アベイラビリティ のガイドライン \(744 ページ\)](#)
- [Firepower Threat Defense ハイ アベイラビリティ ペアの追加 \(745 ページ\)](#)
- [オプションの高可用性パラメータの設定 \(747 ページ\)](#)
- [ハイ アベイラビリティ の管理 \(750 ページ\)](#)
- [ハイ アベイラビリティ のモニタリング \(754 ページ\)](#)

## ハイ アベイラビリティ Firepower Threat Defense について

フェールオーバーとも呼ばれるハイアベイラビリティを設定するには、専用フェールオーバーリンク（および任意でステートリンク）を介して相互に接続された2つの同じFirepower Threat Defense デバイスが必要です。Firepower Threat Defense は一方の装置がアクティブ装置としてトラフィックを通過させる、アクティブ/スタンバイ フェールオーバーをサポートします。スタンバイ装置は、アクティブにトラフィックを通過させることはありませんが、アクティブ装置の設定やその他の状態情報を同期しています。フェールオーバーが発生すると、アクティブ装置がスタンバイ装置にフェールオーバーし、そのスタンバイ装置がアクティブになります。

アクティブ装置（ハードウェア、インターフェイス、ソフトウェアおよび環境ステータス）の状態は、特定のフェールオーバー条件に一致しているかどうかを確認するためにモニタされます。所定の条件に一致すると、フェールオーバーが行われます。



(注) Amazon Web Services 上で実行される Firepower Threat Defense Virtual では、ハイ アベイラビリティはサポートされません。

## ハイ アベイラビリティ のシステム要件

この項では、ハイ アベイラビリティ コンフィギュレーションにある Firepower Threat Defense デバイスのハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。

### ハードウェア要件

ハイ アベイラビリティ コンフィギュレーションの 2 台の装置は、次の条件を満たしている必要があります。

- 同じモデルであること。
- Firepower 9300 シャーシでは、ハイ アベイラビリティ ペアの両方のユニットで同じインターフェイスがハイ アベイラビリティ 論理デバイスに割り当てられている必要があります。
- インターフェイスの数とタイプが同じであること。Firepower 9300 シャーシでは、ハイ アベイラビリティ を有効にする前に、すべてのインターフェイスが FXOS で同一に事前構成されている必要があります。

ハイ アベイラビリティ コンフィギュレーションで装置に異なるサイズのフラッシュ メモリを使用している場合、小さい方のフラッシュ メモリを取り付けた装置に、ソフトウェア イメージファイルおよびコンフィギュレーション ファイルを格納できる十分な容量があることを確認してください。十分な容量がない場合、フラッシュ メモリの大きい装置からフラッシュ メモリの小さい装置にコンフィギュレーションの同期が行われると、失敗します。

### ソフトウェア要件

ハイ アベイラビリティ コンフィギュレーションの 2 台の装置は、次の条件を満たしている必要があります。

- ファイアウォール モードが同じであること（ルーテッドまたは透過）。
- ソフトウェアバージョンが、メジャー（最初の番号）、マイナー（2 番目の番号）およびメンテナンス（3 番目の番号）が同じであること。
- Firepower Management Center 上で、同じドメインまたはグループに入っていること。
- 同じ NTP コンフィギュレーションであること。[脅威に対する防御のための NTP 時刻同期の設定（1066 ページ）](#) を参照してください。
- 非コミットの変更で、Firepower Management Center 上で完全に展開していること。
- どのインターフェイスでも、DHCP または PPPoE は変更していないこと。

### ライセンス要件

ハイ アベイラビリティ構成での Firepower Threat Defense デバイスは、すべて同じライセンスである必要があります。ハイ アベイラビリティを確立する前に、どのライセンスがセカンダリ/

スタンバイ デバイスに割り当てられているかどうかは問題にはなりません。ハイ アベイラビリティの設定中に、Firepower Management Center はスタンバイに割り当てられている不要なライセンスをすべて削除し、プライマリ/アクティブ デバイスに割り当てられているのと同じライセンスで置き換えます。たとえば、アクティブ デバイスは基本ライセンスと Threat ライセンスであり、スタンバイ デバイスは基本ライセンスだけの場合、Firepower Management Center は Cisco Smart Software Manager と通信して、アカウントからスタンバイ デバイス用に使用可能な Threat ライセンスを取得します。スマート ライセンス アカウントで十分な数の資格が購入されていない場合は、正しい数のライセンスを購入するまで、アカウントは非準拠の状態になります。ハイアベイラビリティ構成には、2つのスマートライセンス資格（ペアを構成するデバイスごとに1つ）が必要です。

## フェールオーバー リンクとステートフル フェールオーバー リンク

フェールオーバー リンクとオプションのステートフル フェールオーバー リンクは、2つの装置間の専用接続です。フェールオーバー リンクとステートフルフェールオーバー リンクでは、両方のデバイスで同じインターフェイスを使用する必要があります。

### フェールオーバー リンク

フェールオーバー ペアの2台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。

#### フェールオーバー リンク データ

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態（アクティブまたはスタンバイ）
- hello メッセージ（キープアライブ）
- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期

#### フェールオーバー リンクのインターフェイス

使用されていないデータインターフェイス（物理、冗長、または EtherChannel）はどれも、フェールオーバーリンクとして使用できます。フェールオーバーリンクインターフェイスは、通常のネットワークインターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバーリンク用にのみ使用できます（ステートリンク用としても使用できます）。Firepower Threat Defense デバイスは、ユーザデータとフェールオーバーリンク間でのインターフェイスの共有はサポートしません。フェールオーバーリンクには、別の物理、EtherChannel、または冗長インターフェイスを使用する必要があります。



- (注) フェールオーバーまたはステートフルリンクとして EtherChannel または冗長インターフェイスを使用している場合、ハイアベイラビリティを確立する前に、両方のデバイスで同じメンバーインターフェイスを備えた同じポート チャネルが存在していることを確認する必要があります。

フェールオーバーリンクとして使用される冗長インターフェイスについては、冗長性の増強による次の利点を参照してください:

- フェールオーバー ユニットが起動すると、メンバー インターフェイスを交互に実行し、アクティブ ユニットを検出します。
- メンバー インターフェイスの 1 つにあるピアからのキープアライブ メッセージの受信をフェールオーバー ユニットが停止した場合、別のメンバー インターフェイスに切り替えます。

フェールオーバーリンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバーリンクとして使用中の EtherChannel の設定は変更できません。

## フェールオーバー リンクの接続

フェールオーバーリンクを次の 2 つの方法のいずれかで接続します。

- Firepower Threat Defense デバイスのフェールオーバー インターフェイスと同じネットワーク セグメント (ブロードキャスト ドメインまたは VLAN) に他のデバイスのないスイッチを使用する。
- イーサネットケーブルを使用してユニットを直接接続する。外部スイッチは必要ありません。

ユニット間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらのユニットのものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

Firepower Threat Defense デバイスは、銅線イーサネットポートで Auto-MDI/MDIX をサポートしているため、クロスオーバー ケーブルまたはストレート ケーブルのいずれかを使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

## ステートフル フェールオーバー リンク

ステートフルフェールオーバーを使用するには、接続ステート情報を渡すためのステートフルフェールオーバーリンク (ステートリンクとも呼ばれる) を設定する必要があります。



## フェールオーバー リンクの共有

インターフェイスを節約するための最適な方法はフェールオーバー リンクを共有することです。このインターフェイスでパフォーマンス上の問題が発生した場合は、別のインターフェイスをステート リンク専用にすることを検討してください。

## ステートフル フェールオーバー リンクの専用インターフェイス

ステートリンク専用のデータ インターフェイス（物理、冗長、または EtherChannel）を使用できます。ステートリンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。

次の 2 つの方法のいずれかで、専用のステート リンクを接続します。

- Firepower Threat Defense デバイスのフェールオーバー インターフェイスと同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）に他のデバイスのないスイッチを使用する。
- イーサネット ケーブルを使用してアプライアンスを直接接続します。外部スイッチは必要ありません。

ユニット間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらのユニットのものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

Firepower Threat Defense デバイスは、銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているため、クロスオーバー ケーブルまたはストレート ケーブルのいずれかを使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

長距離のフェールオーバーを使用する場合のステートリンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要があります。遅延が 10 ミリ秒を上回る場合、フェールオーバー メッセージの再送信によって、パフォーマンスが低下する可能性があります。

## フェールオーバー リンクとデータ リンクの中断の回避

すべてのインターフェイスで同時に障害が発生する可能性を減らすために、フェールオーバー リンクとデータ インターフェイスは異なるパスを通すことを推奨します。フェールオーバー リンクがダウンした場合、フェールオーバーが必要かどうかの決定に、Firepower Threat Defense デバイスはデータ インターフェイスを使用できます。その後、フェールオーバー動作は、フェールオーバー リンクの正常性が復元されるまで停止されます。

耐障害性フェールオーバー ネットワークの設計については、次の接続シナリオを参照してください。

## シナリオ 1 : 非推奨

2つの Firepower Threat Defense デバイス間のフェールオーバーとデータ インターフェイスの両方を接続するために1つのスイッチまたは一連のスイッチを使用している場合、スイッチまたはスイッチ間リンクがダウンしていると、両方の Firepower Threat Defense デバイスがアクティブになります。したがって、次の図で示されている次の2つの接続方式は推奨しません。

図 6: 単一のスイッチを使用した接続 : 非推奨

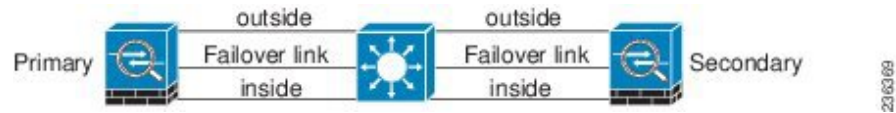
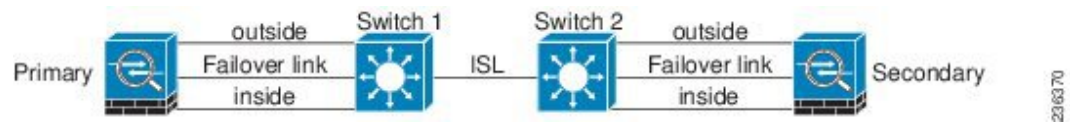


図 7: 2つのスイッチを使用した接続 : 非推奨



## シナリオ 2 : 推奨

フェールオーバー リンクには、データ インターフェイスと同じスイッチを使用しないことを推奨します。代わりに、次の図に示すように、別のスイッチを使用するか直接ケーブルを使用して、フェールオーバー リンクを接続します。

図 8: 異なるスイッチを使用した接続

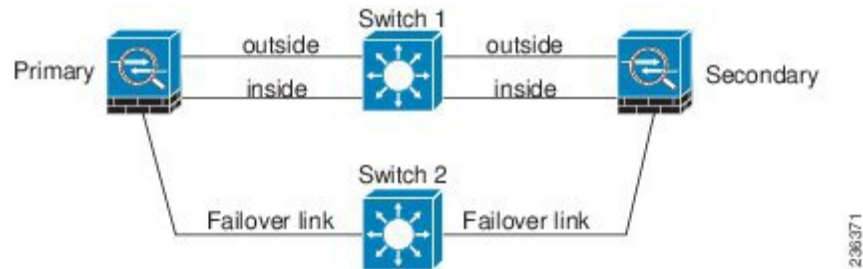
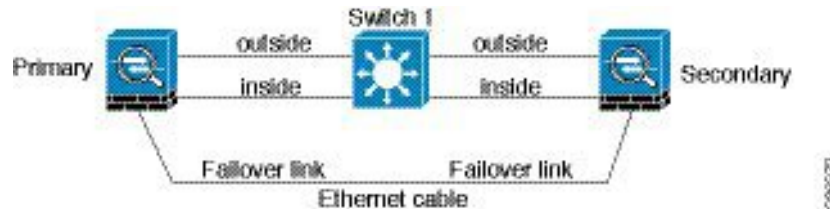


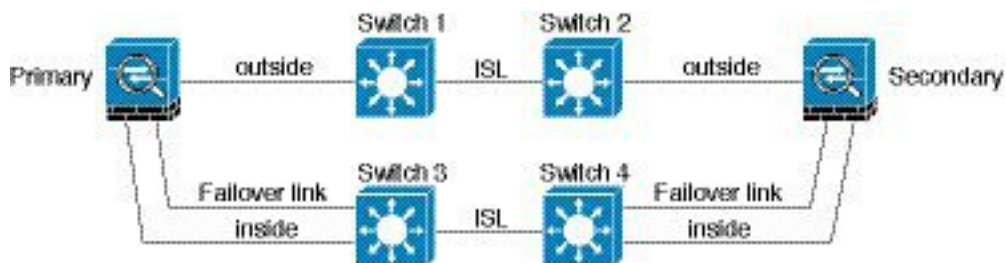
図 9: ケーブルを使用した接続



## シナリオ 3 : 推奨

Firepower Threat Defense データ インターフェイスが複数セットのスイッチに接続されている場合、フェールオーバー リンクはいずれかのスイッチに接続できます。できれば、次の図に示すように、ネットワークのセキュアな側（内側）のスイッチに接続します。

図 10:セキュアスイッチを使用した接続



シナリオ 4 : 推奨

最も信頼性の高いフェールオーバー構成では、次の図に示すように、フェールオーバーリンクに冗長インターフェイスを使用します。

図 11:冗長インターフェイスを使用した接続

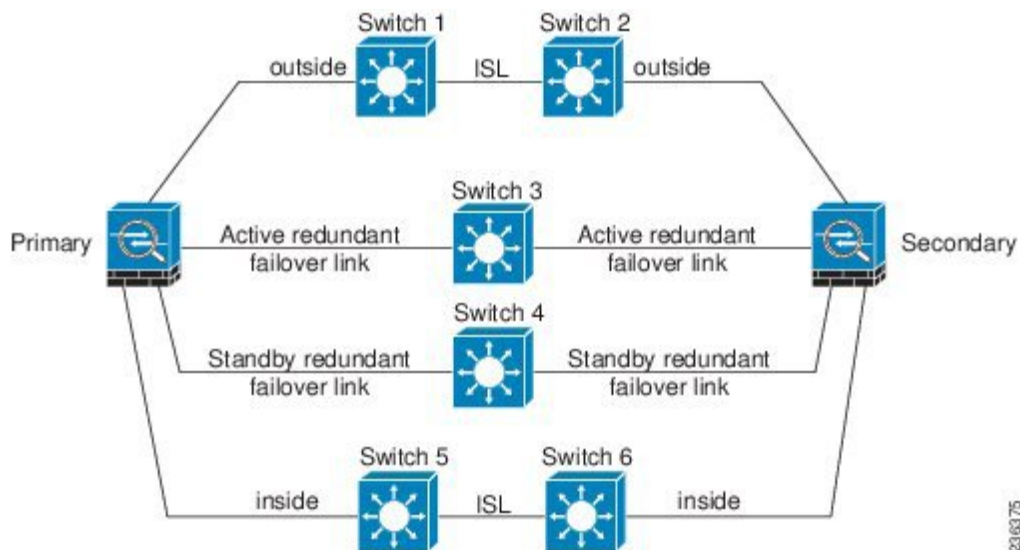
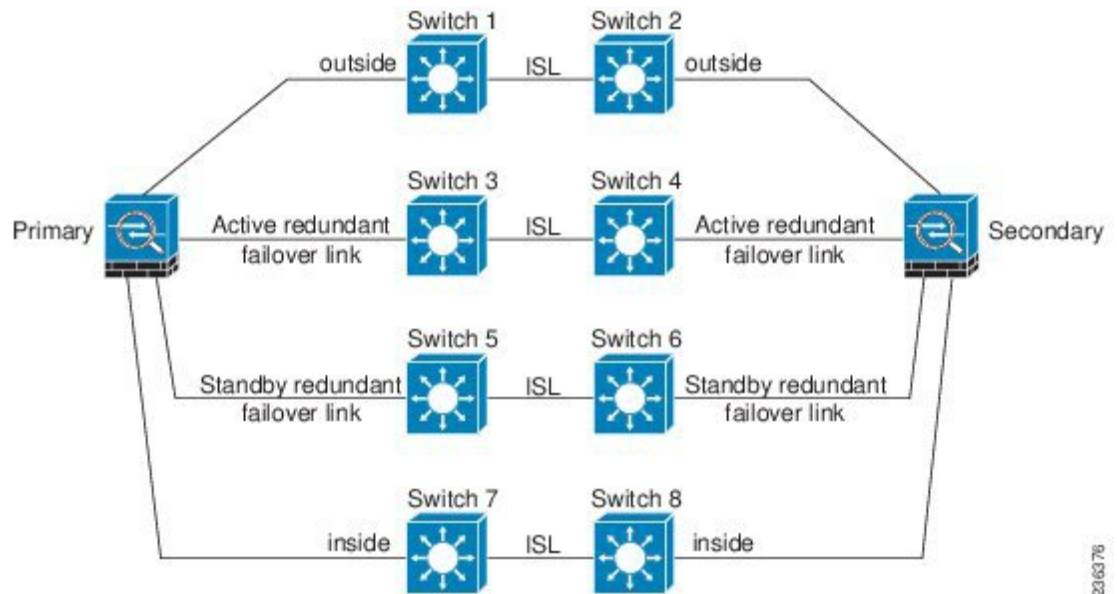


図 12: Inter-Switch Link (ISL) を使用した接続



## フェールオーバーでの MAC アドレスおよび IP アドレス

インターフェイスを設定する場合、同じネットワーク上のアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。スタンバイアドレスを設定することが推奨されていますが、必須ではありません。スタンバイ IP アドレスがないと、アクティブ装置はスタンバイインターフェイスの状態を確認するためのネットワーク テストを実行できません。リンク ステートのみ追跡できます。また、管理目的でそのインターフェイスのスタンバイ装置に接続することもできません。

1. プライマリ装置に障害が発生すると、セカンダリ装置はプライマリ ユニットの IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。
2. 現在スタンバイになっている装置が、スタンバイの IP アドレスと MAC アドレスを引き継ぎます。

ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

セカンダリ装置がプライマリ装置を検出せずにブートした場合、セカンダリ装置がアクティブ装置になります。プライマリ装置の MAC アドレスを認識していないため、自分の MAC アドレスを使用します。しかし、プライマリ装置が使用可能になると、セカンダリ (アクティブ) 装置は MAC アドレスをプライマリ装置の MAC アドレスに変更します。これによって、ネットワークトラフィックが中断されることがあります。同様に、プライマリ装置を新しいハードウェアと交換すると、新しい MAC アドレスが使用されます。

仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。手動で仮想 MAC アドレスを設定できます。

仮想 MAC アドレスを設定しなかった場合、トラフィックフローを復元するために、接続されたルータの ARP テーブルをクリアする必要がある場合があります。Firepower Threat Defense デバイスは MAC アドレスを変更するときに、スタティック NAT アドレスに対して Gratuitous ARP を送信しません。そのため、接続されたルータはこれらのアドレスの MAC アドレスの変更を認識できません。

ステートリンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。唯一の例外は、ステートリンクが通常のデータインターフェイスに設定されている場合です。

## ステートフル フェールオーバー

ステートフェールオーバー中にアクティブ装置は接続ごとのステート情報をスタンバイ装置に継続的に渡します。フェールオーバーの発生後も、新しいアクティブ装置で同じ接続情報が利用できます。サポートされているエンドユーザのアプリケーションでは、同じ通信セッションを保持するために再接続する必要はありません。

## サポートされる機能

ステートフル フェールオーバーが有効にされている場合、次のステート情報がスタンバイ Firepower Threat Defense デバイスに渡されます。

- NAT 変換テーブル
- TCP 接続状態
- UDP 接続状態
- Snort 接続状態
- 厳密な TCP の適用
- ARP テーブル
- レイヤ 2 ブリッジテーブル (ブリッジ グループ用)
- HTTP 接続テーブル
- ISAKMP および IPSec SA テーブル
- SIP シグナリングセッション
- Snort インスペクション
- スタティック ルート
- ダイナミック ルーティング プロトコル: ステートフル フェールオーバーはダイナミック ルーティング プロトコル (OSPF や EIGRP など) に参加するため、アクティブ装置上の

ダイナミック ルーティング プロトコルによる学習ルートが、スタンバイ装置の Routing Information Base (RIB) テーブルに維持されます。フェールオーバー イベントで、アクティブなセカンダリ Firepower Threat Defense デバイスには最初にプライマリ Firepower Threat Defense デバイスをミラーリングする規則があるため、パケットは通常は最小限の中断でトラフィックに移動します。フェールオーバーの直後に、新しくアクティブになった装置で再コンバージェンス タイマーが開始されます。次に、RIB テーブルのエポック番号が増加します。再コンバージェンス中に、OSPF および EIGRP ルートは新しいエポック番号で更新されます。タイマーが期限切れになると、失効したルート エントリ (エポック番号によって決定される) はテーブルから削除されます。これで、RIB には新しくアクティブになった装置での最新のルーティング プロトコル 転送情報が含まれています。



(注) ルートは、アクティブ装置上のリンクアップまたはリンクダウン イベントの場合のみ同期されます。スタンバイ装置上でリンクがアップまたはダウンすると、アクティブ装置から送信されたダイナミックルートが失われることがあります。これは正常な予期された動作です。

- DHCP サーバ (DHCP Server)
- ARP インスペクション
- AVC : App-id 判定は複製されますが、検出状態は複製されません。したがって、フェールオーバーが発生する前に、App-id 判定が完了および同期されていれば正常に同期は行われます。
- URL
- 位置情報 (GeoLocation)
- URL フィルタリング
- IPS 検出状態 : フェールオーバーの際、フロー中にピックアップが発生すると、新しいインスペクションは完了しますが、古い状態は失われます。
- ファイル マルウェア ブロッキング : ファイルの処分は、フェールオーバー前にできるようになる必要があります。
- ファイル タイプ検出およびブロック : ファイル タイプは、フェールオーバー前に特定される必要があります。元のアクティブ デバイスでファイルを特定している間にフェールオーバーが発生すると、ファイル タイプの同期は失われます。ファイル ポリシーでそのファイル タイプがブロックされている場合でも、新しいアクティブ デバイスはファイルをダウンロードします。
- 復号されていない TLS セッション
- TLS URL
- ユーザ エージェント

- ISE のセッション ディレクトリ
- アイデンティティ/キャプティブ ポータル：既存のユーザ セッションは、フェールオーバー後に正しく動作します。フェールオーバーが発生した場合の進行中の認証には、キャプティブ ポータル フローとフェールオーバー スイッチの間の競合状態によって、2 つの起こりうる結果があります。
  - フェールオーバーが発生する前に、ユーザは認証していません。この場合、ブラウザ セッションは失敗します。更新の際、セッションは新しいアクティブユニットに移動し、キャプティブ ポータルの設定ページに戻されます。
  - ユーザはすでに元のアクティブユニットと認証されましたが、フェールオーバーが発生し、ブラウザ セッションが失敗します。更新の際、新しいアクティブ ユニットでもう一度認証するために、キャプティブ ポータルの設定ページに戻されます。
- 署名ルックアップ：ファイルの送信中にフェールオーバーが発生した場合、ファイルイベントは生成されず、検出も発生しません。
- ファイル ストレージ：ファイルの保存中にフェールオーバーが発生した場合、元のアクティブ デバイスに保存されます。ファイルの保存中に元のアクティブなデバイスがダウンした場合、ファイルは保存されません。
- ファイル Pre-class（ローカル分析）：分類前にフェールオーバーが発生した場合、検出は失敗します。
- ファイル ダイナミック分析、クラウドとの接続性：フェールオーバーが発生しても、システムはクラウドにファイルを提出できます。
- アーカイブ ファイル サポート：分析中にフェールオーバーが発生した場合、システムはファイル/アーカイブ内の可視性を失います。
- カスタム ブラックリスト：フェールオーバーが発生した場合、イベントは生成されません。
- IP レピュテーション
- URL レピュテーション
- DNS シンクホール
- フラグメント設定

## サポートされない機能

ステートフルフェールオーバーが有効な場合、次のステート情報はスタンバイ Firepower Threat Defense デバイスに渡されません。

- プレーン テキスト トンネル内のセッション
- 復号後のインスペクション
- TLS 復号状態

- DHCP クライアント
- DHCP サーバアドレスのリース
- マルチキャストルーティング

## フェールオーバーのトランスペアレント ファイアウォール モードブリッジグループ要件

ブリッジグループを使用する場合は、フェールオーバーに関して特別な考慮事項があります。アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパンニング ツリー プロトコル (STP) を実行している接続済みスイッチ ポートが、トポロジの変化を検出すると 30 ~ 50 秒間ブロッキング状態になる可能性があります。ポートがブロッキング状態の間のトラフィックの損失を回避するために、次の回避策のいずれかを設定できます。

- スイッチの STP PortFast 機能を有効にします。

```
interface interface_id
  spanning-tree portfast
```

PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディングモードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがグループの一部になる場合、最終的には STP ブロッキングモードに遷移します。

- インターフェイスのモニタリングを無効にします。
- Firepower Threat Defense デバイスがフェールオーバーする前に、インターフェイスの保留時間を STP が収束可能になる大きい値に増やします。
- STP がインターフェイスの保留時間よりも速く収束するように、STP タイマーを減らします。

## フェールオーバーのヘルス モニタリング

Firepower Threat Defense デバイスは、各装置について全体的なヘルスおよびインターフェイスヘルスをモニタします。この項では、各装置の状態を判断するために、Firepower Threat Defense デバイスがテストを実行する方法について説明します。

### 装置のヘルス モニタリング

Firepower Threat Defense デバイスは、hello メッセージでフェールオーバー リンクをモニタして相手装置のヘルスを判断します。装置がフェールオーバー リンクで 3 回連続して hello メッセージを受信しなかったときは、装置はフェールオーバー リンクを含む各データ インターフェイスで LANTEST メッセージを送信し、ピアが応答するかどうかを確認します。Firepower Threat Defense デバイスが行うアクションは、相手装置からの応答によって決まります。次の可能なアクションを参照してください。



- Firepower Threat Defense デバイスがフェールオーバー リンクで応答を受信した場合、フェールオーバーは行われません。
- Firepower Threat Defense デバイスがフェールオーバー リンクで応答を受信せず、データ インターフェイスで応答を受信した場合、装置のフェールオーバーは行われません。フェールオーバー リンクは故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイにフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
- Firepower Threat Defense デバイスがどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブ モードに切り替わり、相手装置を故障に分類します。

## インターフェイス モニタリング

装置が、2回のポーリング期間中にモニタ対象のインターフェイス上でhello メッセージを受信しない場合、インターフェイステストを実行します。1つのインターフェイスに対するすべてのインターフェイステストがすべて失敗したが、相手装置のこの同じインターフェイスが正常にトラフィックを渡し続けている場合、そのインターフェイスは故障しているとは見なされません。故障したインターフェイスがしきい値を超えている場合は、フェールオーバーが行われません。相手装置のインターフェイスでもすべてのネットワークテストに失敗した場合、両方のインターフェイスは「Unknown」状態になり、フェールオーバーの限界値に向けてのカウントは行われません。

インターフェイスは、何らかのトラフィックを受信すると、再度動作状態になります。故障したデバイスは、インターフェイス障害しきい値が満たされなくなった場合、スタンバイ モードに戻ります。

インターフェイスに IPv4 および IPv6 アドレスが設定されている場合、デバイスは IPv4 を使用してヘルス モニタリングを実行します。

インターフェイスに IPv6 アドレスだけが設定されている場合、デバイスは ARP ではなく IPv6 ネイバー探索を使用してヘルス モニタリングテストを実行します。ブロードキャスト ping テストの場合、デバイスは IPv6 全ノードアドレス (FE02::1) を使用します。

## インターフェイス テスト

Firepower Threat Defense デバイスでは、次のインターフェイス テストが使用されます。

1. リンクアップ/ダウンテスト：インターフェイスステータスのテストです。リンクアップ/ダウンテストでインターフェイスがダウンしていることが示された場合、デバイスは障害が発生したと見なします。ステータスがアップの場合、デバイスはネットワークアクティビティテストを実行します。
2. ネットワークアクティビティテスト：ネットワークの受信アクティビティのテストです。このテストの目的は、LANTEST メッセージを使用してネットワーク トラフィックを生成し、障害が発生しているユニット（いずれか1つ）を特定することです。テストの開始時に、各装置はインターフェイスの受信パケットカウントをリセットします。ユニットがテスト中にパケットを受信したらすぐに（最大5秒）、そのインターフェイスは動作可能と見なされます。いずれか一方の装置だけがトラフィックを受信している場合は、トラフィック

クを受信しなかった装置が故障していると思なされます。どちらの装置もトラフィックを受信しなかった場合、デバイスは ARP テストを開始します。

3. ARP テスト：取得したエントリの最後の 2 つの装置 ARP キャッシュの読み取り。装置は、ネットワーク トラフィックを発生させるために、1 回に 1 つずつ、これらのマシンに ARP 要求を送信します。各要求後、装置は最大 5 秒間受信したトラフィックをすべてカウントします。トラフィックが受信されれば、インターフェイスは正常に動作していると思なされます。トラフィックが受信されなければ、ARP 要求が次のマシンに送信されます。リストの最後まで、まったくトラフィックが受信されなかった場合、デバイスは ping テストを開始します。
4. ブロードキャスト ping テスト：このテストでは、ブロードキャスト ping 要求が送信されます。装置は、最大 5 秒間、すべての受信パケット数をカウントします。この時間間隔の間にパケットが受信されると、インターフェイスが正常に動作しているものと思なされ、テストは停止します。トラフィックが受信されなければ、ARP テストからやり直します。

## インターフェイス ステータス

モニタ対象のインターフェイスには、次のステータスがあります。

- **Unknown**：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合があります。
- **Normal**：インターフェイスはトラフィックを受信しています。
- **Normal (Waiting)**：インターフェイスは起動していますが、ピアユニットの対応するインターフェイスからまだ hello パケットを受信していません。
- **Normal (Not-Monitored)**：インターフェイスは動作中ですが、フェールオーバープロセスによってモニタされていません。
- **Testing**：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- **Link Down**：インターフェイスまたは VLAN は管理上ダウンしています。
- **Link Down (Waiting)**：インターフェイスまたは VLAN は管理上ダウンしており、ピアユニットの対応するインターフェイスからまだ hello パケットを受信していません。
- **Link Down (Not-Monitored)**：インターフェイスまたは VLAN は管理上ダウンしていますが、フェールオーバープロセスによってモニタされていません。
- **No Link**：インターフェイスの物理リンクがダウンしています。
- **No Link (Waiting)**：インターフェイスの物理リンクがダウンしており、ピアユニットの対応するインターフェイスから hello パケットをまだ受信していません。
- **No Link (Not-Monitored)**：インターフェイスの物理リンクがダウンしていますが、フェールオーバープロセスによってモニタされていません。
- **Failed**：インターフェイスではトラフィックを受信していませんが、ピアインターフェイスではトラフィックを検出しています。

## フェールオーバー トリガーおよび検出タイミグ

次の表は、フェールオーバー トリガー イベントおよび関連する障害検出タイミグを示します。フェールオーバーが発生した場合、フェールオーバーの理由およびその他のハイ アベイラビリティ ペアに関するさまざまな作業をメッセージセンターで表示できます。

表 59: Firepower Threat Defense フェールオーバー時間

フェールオーバートリガー イベント	最小	デフォルト	最大数
アクティブ ユニットで電源切断が生じる、または通常の動作が停止する。	800 ミリ秒	15 秒	45 秒
アクティブ ユニット インターフェイス物理リンクがダウンする。	500 ミリ秒	5 秒	15 秒
アクティブ ユニットのインターフェイスは実行されているが、接続の問題によりインターフェイス テストを行っている。	5 秒	25 秒	75 秒

## アクティブ/スタンバイ フェールオーバーについて

アクティブ/スタンバイ フェールオーバーでは、障害が発生した装置の機能を、スタンバイ Firepower Threat Defense デバイスに引き継ぐことができます。アクティブ装置が故障すると、スタンバイ状態に変わり、そしてスタンバイ装置がアクティブ状態に変わります。

## プライマリ/セカンダリの役割とアクティブ/スタンバイ ステータス

アクティブ/スタンバイ フェールオーバーを設定する場合、1つのユニットをプライマリとして設定し、もう1つのユニットをセカンダリとして設定します。設定中に、プライマリユニットのポリシーは、セカンダリユニットに同期されます。この時点で、2つのユニットは、デバイスおよびポリシー設定に関して単一のデバイスとして機能します。ただし、イベント、ダッシュボード、レポートおよびヘルスマonitoringに関しては、別々のデバイスとして引き続き表示されます。

フェールオーバーペアの2つのユニットの主な相違点は、どちらのユニットがアクティブでどちらのユニットがスタンバイであるか、つまりどちらの IP アドレスを使用するか、およびどちらのユニットがアクティブにトラフィックを渡すかということに関連します。

しかし、プライマリ ユニット（設定で指定）とセカンダリ ユニットとの間には、いくつかの相違点があります。

- 両方のユニットが同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、プライマリ ユニットが常にアクティブ ユニットになります。
- プライマリ ユニットの MAC アドレスは常に、アクティブ IP アドレスと結び付けられています。このルールの例外は、セカンダリ ユニットがアクティブであり、フェールオーバー リンク経由でプライマリ ユニットの MAC アドレスを取得できない場合に発生します。この場合、セカンダリ ユニットの MAC アドレスが使用されます。

## 起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時に起動された場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。

## フェールオーバー イベント

アクティブ/スタンバイ フェールオーバーでは、フェールオーバーはユニットごとに行われます。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ ユニットが行うアクション、スタンバイ ユニットが行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 60: フェールオーバー イベント

障害イベント	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記 (Notes)
アクティブユニットが故障（電源またはハードウェア）	フェールオーバー	適用対象外	アクティブになる アクティブに故障とマークする	モニタ対象インターフェイスまたはフェールオーバー リンクで hello メッセージは受信されません。
以前にアクティブであったユニットの復旧	フェールオーバーなし	スタンバイになる	動作なし	なし。

障害イベント	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記 (Notes)
スタンバイユニットが故障 (電源またはハードウェア)	フェールオーバーなし	スタンバイに故障とマークする	適用対象外	スタンバイユニットが故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブユニットはフェールオーバーを行いません。
動作中にフェールオーバーリンクに障害が発生した	フェールオーバーなし	フェールオーバーリンクに故障とマークする	フェールオーバーリンクに故障とマークする	フェールオーバーリンクがダウンしている間、ユニットはスタンバイユニットにフェールオーバーできないため、できるだけ早くフェールオーバーリンクを復元する必要があります。
スタートアップ時にフェールオーバーリンクに障害が発生した	フェールオーバーなし	フェールオーバーリンクに故障とマークする	アクティブになる	スタートアップ時にフェールオーバーリンクがダウンしていると、両方のユニットがアクティブになります。
ステートリンクの障害	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。
アクティブユニットにおけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブに故障とマークする	アクティブになる	なし。
スタンバイユニットにおけるしきい値を超えたインターフェイス障害	フェールオーバーなし	動作なし	スタンバイに故障とマークする	スタンバイユニットが故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブユニットはフェールオーバーを行いません。

# ハイ アベイラビリティ のガイドライン

## モデルのサポート

- ASA 5506W-X : 内部 GigabitEthernet 1/9 インターフェイスのインターフェイス モニタリングを無効にする必要があります。これらのインターフェイスは、デフォルトのインターフェイス モニタリング チェックを実行するために通信することができないため、予期されたインターフェイス通信の障害により、スイッチがアクティブからスタンバイに切り替えられ、元に戻ります。
- Firepower 9300 での Firepower Threat Defense : シャーシ内ハイ アベイラビリティはサポートされません。
- Microsoft Azure や Amazon Web Services などのパブリック クラウド ネットワーク上の Firepower Threat Defense Virtual では、レイヤ 2 接続が必要なため、ハイ アベイラビリティはサポートされません。

## その他のガイドライン

- アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパンニング ツリー プロトコル (STP) を実行している接続済みスイッチポートが、トポロジの変化を検出すると 30 ~ 50 秒間ブロッキング状態になる可能性があります。ポートがブロッキング状態である間のトラフィック損失を防ぐには、スイッチで STP PortFast 機能を有効にします。

### `interface interface_idspanning-tree portfast`

この回避策は、ルーテッド モードおよびブリッジ グループ インターフェイスの両方に接続されているスイッチに適用されます。PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- ローカル CA サーバが設定されている場合、フェールオーバーを有効にできません。 `no crypto ca server` コマンドを使用して、CA 設定を削除します。
- Firepower Threat Defense フェールオーバー ペアに接続されたスイッチ上でポートセキュリティを設定すると、フェールオーバー イベントが発生したときに通信の問題が起きることがあります。この問題は、あるセキュア ポートで設定または学習されたセキュア MAC アドレスが別のセキュア ポートに移動し、スイッチのポートセキュリティ機能によって違反フラグが付けられた場合に発生します。
- アクティブ/スタンバイ ハイ アベイラビリティ と VPN IPsec トンネルの場合、SNMP を使用して VPN トンネル上でアクティブ ユニットとスタンバイ ユニットの両方をモニタすることはできません。スタンバイ ユニットにはアクティブ VPN トンネルがないため、NMS に向けられたトラフィックはドロップされます。代わりに暗号化付き SNMPv3 を使用すれば、IPsec トンネルが不要になります。

- ハイ アベイラビリティ ペアの各ユニットが一意のホスト名を使用していることを確認してください。Firepower Management Center では、セカンダリ ユニットの名前がプライマリ ユニットと同じである場合、セカンダリ ユニットの追加できません。

## Firepower Threat Defense ハイ アベイラビリティ ペアの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	任意 (Any)	Admin/Network Admin

アクティブ/スタンバイの高可用性ペアを確立するには、一方のデバイスをプライマリ、他方をセカンダリとして指定します。システムは、マージした設定を、ペア内のデバイスに適用します。競合する場合、システムはプライマリとして指定されたデバイスの構成を適用します。

マルチドメインの導入環境では、高可用性ペアのデバイスが同じドメインに属している必要があります。



- (注) ステートフル フェールオーバー リンクがピア間のアプリケーション コンテンツの同期に使用されている場合には、システムはフェールオーバー リンクを使用して構成を同期します。高可用性が確立された後に、選択したインターフェイスリンクと暗号化設定の変更を行うと、高可用性のペアが壊れ、再設定が必要になります。



- 注意** Firepower Threat Defense のハイ アベイラビリティ ペアを作成または破棄すると、プライマリおよびセカンダリ デバイスの Snort プロセスが直ちに再起動され、両方のデバイスのトラフィック インспекションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。ハイ アベイラビリティ ペアの作成を続けると、プライマリ デバイスとセカンダリ デバイスで Snort プロセスが再起動され、キャンセルすることができるという警告が表示されます。

### 始める前に

以下の点について両方のデバイスを確認してください。

- 同じモデルであること。

- インターフェイスの数とタイプが同じであること。
- ドメインおよびグループが同じであること。
- 通常のヘルス ステータスであり、同じソフトウェアを実行していること。
- ルーティングされているか、またはトランスペアレントモードであること。
- NTP 設定が同じであること。 [脅威に対する防御のための NTP 時刻同期の設定 \(1066 ページ\)](#) を参照してください。
- 未確定の変更がない状態で、完全に展開されていること。
- すべてのインターフェイスで DHCP または PPPoE が設定されていないこと。

## 手順

- ステップ 1** [Firepower Management Center へのデバイスの追加 \(550 ページ\)](#) に従って、両方のデバイスを Firepower Management Center に追加します。
- ステップ 2** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 3** [追加 (Add)] ドロップダウンメニューから、[高可用性の追加 (Add High Availability)] を選択します。
- ステップ 4** 高可用性ペアの表示用の [名前 (Name)] を入力してください。
- ステップ 5** [デバイス タイプ (Device Type)] では、[Firepower Threat Defense] を選択します。
- ステップ 6** 高可用性ペアの [プライマリ ピア (Primary Peer)] デバイスを選択します。
- ステップ 7** 高可用性ペアの [セカンダリ ピア (Secondary Peer)] デバイスを選択します。
- ステップ 8** [続行 (Continue)] をクリックします。
- ステップ 9** LAN フェールオーバー リンクでは、フェールオーバーの通信のための十分な帯域幅の [インターフェイス (Interface)] を選択します。
 

(注) 論理名がなくセキュリティゾーンに属さないインターフェイスのみが、[ハイアベイラビリティペアの追加 (Add High Availability Pair)] ダイアログの [インターフェイス (Interface)] ドロップダウンに一覧表示されます。
- ステップ 10** 識別するための任意の [論理名 (Logical Name)] を入力します。
- ステップ 11** アクティブなユニットの、フェールオーバー リンクの [プライマリ IP (Primary IP)] アドレスを指定します。このアドレスは、未使用のサブネット上になければなりません。
 

(注) 169.254.0.0/16 および fd00:0:0::\*:/64 は内部で使用されるサブネットです。フェールオーバーやステート リンクにはこれらを使用できません。
- ステップ 12** 必要に応じて、[IPv6 アドレスを使用 (Use IPv6 Address)] を選択します。
- ステップ 13** スタンバイユニットのフェールオーバー リンクの [セカンダリ IP (Secondary IP)] アドレスを指定します。この IP アドレスはプライマリ IP アドレスのように、同じサブネット内になければなりません。



- ステップ 14** IPv4 アドレスを使用する場合、プライマリとセカンダリの IP アドレス両方に適用されるサブネットマスクを入力します。
- ステップ 15** 必要に応じて、ステートフル フェールオーバー リンクでは、同じインターフェイスを選択するか、または別のインターフェイスを選択し、高可用性の設定情報を入力します。
- (注) 169.254.0.0/16 および fd00:0:0::\*:/64 は内部で使用されるサブネットです。フェールオーバーやステート リンクにはこれらを使用できません。
- ステップ 16** 必要に応じて、フェールオーバー リンク間の IPsec 暗号化について、[有効 (Enabled)] を選択し、さらに [キー生成 (key generate)] メソッドを選択します。
- ステップ 17** [OK] をクリックします。システム データの同期が行われるため、このプロセスが完了するまでに数分かかります。

## オプションの高可用性パラメータの設定

最初の高可用性構成を Firepower Management Center で確認できます。高可用性ペアを解除して再設定しないと、これらの設定を編集することはできません。

フェールオーバーの結果を改善するために、フェールオーバー トリガー条件を編集できます。インターフェイス モニタリングでは、どのインターフェイスがフェールオーバーに適しているかを判断できます。

## インターフェイス モニタリングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	任意 (Any)	Admin/Network Admin

デフォルトでは、論理名が設定されているすべての物理インターフェイスでモニタリングが有効化されています。重要度の低いネットワークに接続されているインターフェイスがフェールオーバー ポリシーに影響を与えないようにできます。

### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** 編集するデバイスハイアベイラビリティペアの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [ハイ アベイラビリティ (High Availability)] を選択します。

**ステップ 4** [インタフェースのモニタ (Monitor Interfaces)] で、編集アイコン (✎) をクリックします。

**ステップ 5** [このインターフェイスの障害をモニタする (Monitor this interface for failures)] を選択します。

**ステップ 6** [OK] をクリックします。

## ハイ アベイラビリティ フェールオーバー条件の編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	任意 (Any)	Admin/Network Admin

ネットワーク配置に基づいてフェールオーバー条件をカスタマイズできます。

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 編集するデバイスハイ アベイラビリティ ペアの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [ハイ アベイラビリティ (High Availability)] を選択します。

**ステップ 4** [フェールオーバートリガー条件 (Failover Trigger Criteria)] の横にある編集アイコン (✎) をクリックします。

**ステップ 5** [インターフェイス障害しきい値 (Interface Failure Threshold)] で、デバイスがフェールオーバーする条件となるインターフェイスの失敗の数または割合を選択します。

**ステップ 6** [hello パケット間隔 (Hello packet Intervals)] で、フェールオーバーリンクを介して送信される hello パケットの頻度を選択します。

**ステップ 7** [OK] をクリックします。

## 仮想 MAC アドレスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	任意 (Any)	Admin/Network Admin

フェールオーバーのため、以下の Firepower Management Center の 2 か所にアクティブ MAC アドレスとスタンバイ MAC アドレスを設定できます。

- [インターフェイスの編集 (Edit Interface)] ページの [詳細 (Advanced)] タブ。 [MAC アドレスの設定 \(688 ページ\)](#) を参照してください。
- [高可用性 (High Availability)] ページからアクセスする [インターフェイス MAC アドレスの追加 (Add Interface MAC Address)] ページ。次を参照してください。

アクティブ MAC アドレスとスタンバイ MAC アドレスが両方の場所で設定されている場合、フェールオーバーではインターフェイスの設定で定義されたアドレスが優先されます。

物理インターフェイスにアクティブ MAC アドレスとスタンバイ MAC アドレスを指定することでフェールオーバー中のトラフィック喪失を最低に抑えることができます。この機能は、フェールオーバーのための IP アドレスのマッピングに冗長性を提供します。

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 編集するデバイスハイアベイラビリティペアの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [高可用性 (High Availability)] を選択します。

**ステップ 4** インターフェイス MAC アドレスの横にある追加アイコン (+) を選択します。

**ステップ 5** [物理インターフェイス (Physical Interface)] を選択します。

**ステップ 6** [アクティブインターフェイス MAC アドレス (Active Interface Mac Address)] を入力します。

**ステップ 7** [スタンバイインターフェイス MAC アドレス (Standby Interface Mac Address)] を入力します。

**ステップ 8** [OK] をクリックします。

## ハイ アベイラビリティの管理

この項では、ハイ アベイラビリティの設定を変更する方法、ある装置から別の装置にフェールオーバーを強制実行する方法など、ハイ アベイラビリティを有効化した後にハイ アベイラビリティ装置を管理する方法について説明します。

### Firepower Threat Defense ハイ アベイラビリティ ペアにおけるアクティブ ピアの切り替え

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	任意 (Any)	Admin/Network Admin

Firepower Threat Defense ハイ アベイラビリティ ペアを確立した後、アクティブ ユニットとスタンバイ ユニートを手動で切り替えることができます。そうすることで、現在のアクティブ ユニットにおける持続的な障害やヘルスイベントなどに起因するフェールオーバーを効果的に実施できます。この手順を実行する前に、両方のユニットを完全に展開しておく必要があります。

#### 手順

- 
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン (🔄) をクリックします。
- ステップ 3** 次の操作を実行できます。
- ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい (Yes)] をクリックします。
  - キャンセルして [デバイス管理 (Device Management)] ページに戻る場合は、[いいえ (No)] をクリックします。
- 

## ハイ アベイラビリティの中断と再開

CLI を使用して、ハイ アベイラビリティ ペアの 1 つのユニットを中断できます。これは、次の場合に役立ちます。

- 両方のユニットがアクティブ - アクティブ状態にあり、そのうち一方を中断する場合。
- アクティブユニットまたはスタンバイユニットをトラブルシューティングする間、ユニットのフェールオーバーを発生させたくない場合。

フェールオーバーを中断するハイ アベイラビリティ ペアの特定のユニットで、次の CLI コマンドを使用します。

```
configure failover suspend
```

このコマンドは、ハイアベイラビリティの設定を確認し、それを一時停止します。デバイスがアクティブ状態にある場合は、そのデバイスがスタンバイユニットに接続されていればフェールオーバーが発生します。ユニットがピアノードのないアクティブノードの場合、そのユニットは中断状態になり、それ以降トラフィックの処理は行いません。ユニットがスタンバイユニットの場合、そのユニットは中断状態になります。

フェールオーバーを再開するには、次のコマンドを使用します。

```
configure failover resume
```



(注) フェールオーバーの一時停止は永続的な状態ではありません。ユニットをリロードした場合は、ユニットが自動的に再開し、スタンダアロンユニットに戻ります。

## ユニットの交換

Firepower Threat Defense の高可用性ペアにおいて、故障したユニットを交換する必要がある場合、[ブレイクを強制 (Force Break) ] オプション選択して、このペアを分離する必要があります。ユニットを交換するか、修理した後、Firepower Management Center のデバイスを登録し、高可用性を再度確立する必要があります。このプロセスは、デバイスがプライマリ、セカンダリであるかによって異なります。

### プライマリユニットの交換

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	任意 (Any)	Admin/Network Admin

次に示す手順に従って、Firepower Threat Defense の高可用性ペアで障害が発生したプライマリユニットを交換します。ここに示した手順に従わないと、既存の高可用性設定を上書きする可能性があります。

## 手順

- 
- ステップ 1** [強制切断 (Force Break) ]を選択して、高可用性ペアを分離します。[ハイ アベイラビリティ ペアにおけるユニットの分離 \(753 ページ\)](#) を参照してください。
- ステップ 2** 障害が発生したプライマリ Firepower Threat Defense デバイスの登録を Firepower Management Center から解除します。[Firepower Management Center からのデバイスの削除 \(552 ページ\)](#) を参照してください。
- ステップ 3** 交換した Firepower Threat Defense を Firepower Management Center に登録します。[Firepower Management Center へのデバイスの追加 \(550 ページ\)](#) を参照してください。
- ステップ 4** 登録時には、既存のセカンダリ/アクティブユニットをプライマリ デバイスとして使用し、交換したデバイスをセカンダリ/スタンバイ デバイスとして使用して、高可用性を設定します。[Firepower Threat Defense ハイ アベイラビリティ ペアの追加 \(745 ページ\)](#) を参照してください。
- 

## 次のタスク

## セカンダリ ユニットの交換

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	任意 (Any)	Admin/Network Admin

次に示す手順に従って、Firepower Threat Defense の高可用性ペアで障害が発生したセカンダリ ユニットの交換します。

## 手順

- 
- ステップ 1** [強制切断 (Force Break) ]を選択して、高可用性ペアを分離します。[ハイ アベイラビリティ ペアにおけるユニットの分離 \(753 ページ\)](#) を参照してください。
- ステップ 2** セカンダリ Firepower Threat Defense デバイスの登録を Firepower Management Center から解除します。[Firepower Management Center からのデバイスの削除 \(552 ページ\)](#) を参照してください。
- ステップ 3** 交換した Firepower Threat Defense を Firepower Management Center に登録します。[Firepower Management Center へのデバイスの追加 \(550 ページ\)](#) を参照してください。
- ステップ 4** 登録時には、既存のプライマリ/アクティブユニットをプライマリ デバイスとして使用し、交換したデバイスをセカンダリ/スタンバイ デバイスとして使用して、高可用性を設定します。

Firepower Threat Defense ハイ アベイラビリティ ペアの追加 (745 ページ) を参照してください。

## ハイ アベイラビリティ ペアにおけるユニットの分離

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	任意 (Any)	Admin/Network Admin

高可用性ペアを分断しても、アクティブなデバイスは完全な展開の機能を維持します。スタンバイデバイスは、フェールオーバー設定とインターフェイス設定を失って、スタンドアロンのデバイスになります。



(注) Firepower Management Center を使用して高可用性ペアにアクセスできない場合は、CLI コマンド `configure failover disable` を使用して、両方のデバイスからフェールオーバー設定を削除します。

### 手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 分断する高可用性ペアの横にある HA の分断アイコン (🔪) をクリックします。
- ステップ 3 必要に応じて、スタンバイ ペアが応答しなかった場合に、強制的に分断するためのチェックボックスをオンにします。
- ステップ 4 [Yes] をクリックします。デバイスの高可用性ペアが分離されます。

## ハイ アベイラビリティ ペアの登録解除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	任意 (Any)	Admin/Network Admin

各ユニットで CLI を使用することによって、Firepower Management Center からペアを削除し、ハイ アベイラビリティを無効にすることができます。

### 始める前に

この手順では、CLI アクセスが必要です。

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 登録解除するハイ アベイラビリティ ペアの横にある削除アイコン (🗑️) をクリックします。

**ステップ 3** [Yes] をクリックします。デバイス ハイ アベイラビリティ ペアが削除されます。

**ステップ 4** 各ユニットで、Firepower Threat Defense CLI にアクセスし、次のコマンドを入力します。

#### configure high-availability disable

このコマンドを入力しない場合、ユニットを再登録して、新しい HA ペアを形成することはできません。

(注) ファイアウォールモードを変更する前に、このコマンドを入力します。モードを変更すると、ユニットでは **configure high-availability disable** コマンドを入力できなくなります。Firepower Management Center では、このコマンドを使用せずに HA ペアを再形成することはできません。

## ハイ アベイラビリティのモニタリング

このセクションの手順に従うことで、ハイアベイラビリティのステータスをモニタできます。

### フェールオーバー履歴の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	任意 (Any)	Admin/Network Admin

ハイアベイラビリティの両方のデバイスに関するフェールオーバーの履歴を1つのビューに表示できます。履歴は古いものから順番に表示され、すべてのフェールオーバーの理由が示されます。



## 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。

**ステップ 2** 編集するデバイスハイ アベイラビリティ ペアの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [サマリー (Summary) ] を選択します。

**ステップ 4** [全般 (General) ] の下で、表示アイコン (🔍) をクリックします。

## ステートフル フェールオーバーの統計情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	任意 (Any)	Admin/Network Admin

ハイ アベイラビリティ ペアのプライマリとセカンダリ デバイス両方のステートフルフェールオーバー リンク統計情報を表示できます。

## 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。

**ステップ 2** 編集するデバイスハイ アベイラビリティ ペアの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [ハイ アベイラビリティ (High Availability) ] を選択します。

**ステップ 4** ステートフル フェールオーバー リンクの下にある表示アイコン (🔍) をクリックします。

**ステップ 5** 統計情報を表示するデバイスを選択します。





## 第 31 章

# Firepower 9300 の Firepower Threat Defense クラスタ

クラスタリングを利用すると、複数の Firepower Threat Defense 装置をグループ化して 1 つの論理デバイスにすることができます。クラスタリングは、Firepower 9300 上の Firepower Threat Defense デバイスでのみサポートされます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。



(注) Firepower Threat Defense デバイスは、複数のシャーシにわたる（シャーシ間）クラスタをサポートしていません。シャーシ内クラスタリングのみがサポートされています。



(注) クラスタリングを使用する場合、一部の機能はサポートされません。クラスタリングでサポートされない機能（766 ページ）を参照してください。

- [Firepower 9300 シャーシでのクラスタリングについて（757 ページ）](#)
- [Firepower 9300 シャーシでのクラスタ化前提条件（769 ページ）](#)
- [Firepower 9300 シャーシ上のクラスタリングのガイドライン（769 ページ）](#)
- [Firepower 9300 シャーシでのクラスタリングのデフォルト（770 ページ）](#)
- [Firepower 4100/9300 シャーシのクラスタリング設定（770 ページ）](#)
- [クラスタリングの履歴（775 ページ）](#)

## Firepower 9300 シャーシでのクラスタリングについて

クラスタは、1 つの論理ユニットとして機能する複数のデバイスから構成されます。クラスタを Firepower 9300 シャーシに展開すると、以下の処理が実行されます。

- ユニット間通信用のクラスタ制御リンク（デフォルトではポート チャネル 48）を作成します。シャーシ内クラスタリングでは、このリンクは、クラスタ通信に Firepower 9300 バックプレーンを使用します。
- アプリケーション内のクラスタブートストラップコンフィギュレーションを作成します。クラスタを展開すると、クラスタ名、クラスタ制御リンク インターフェイス、およびその他のクラスタ設定を含む各ユニットに対して、最小限のブートストラップ コンフィギュレーションが Firepower 9300 シャーシ スーパーバイザからプッシュされます。
- スパンドインターフェイスとして、クラスタにデータインターフェイスを割り当てます。シャーシ内クラスタリングでは、スパンドインターフェイスは、EtherChannel に制限されません。Firepower 9300 スーパーバイザは共有インターフェイスの複数のモジュールにトラフィックをロードバランシングするために内部で EtherChannel テクノロジーを使用するため、スパンドモードではあらゆるタイプのデータ インターフェイスが機能します。



(注) 管理インターフェイス以外の個々のインターフェイスはサポートされていません。

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

ここでは、クラスタリングの概念と実装について詳しく説明します。

## パフォーマンス スケーリング係数

複数のユニットをクラスタに結合した場合、期待できる合計クラスタパフォーマンスの概算値は次のようになります。

- TCP または CPS の合計スループットの 80 %
- 合計 UDP スループットの 90 %
- トラフィックの組み合わせに応じて、イーサネット MIX (EMIX) の合計スループットの 60 %
- たとえば、TCP スループットについては、3つのモジュールを備えた Firepower 9300 が処理できる実際のファイアウォールトラフィックは、単独動作時は約 135 Gbps となります。2 シャーシの場合、合計スループットの最大値は約 270 Gbps (2 シャーシ × 135 Gbps) の 80 %、つまり 216 Gbps となります。

## ブートストラップコンフィギュレーション

クラスタを展開すると、クラスタ名、クラスタ制御リンク インターフェイス、およびその他のクラスタ設定を含む最小限のブートストラップコンフィギュレーションが Firepower 9300 シャーシ スーパーバイザから各ユニットに対してプッシュされます。

## クラスタ メンバー

クラスタ メンバーは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を達成します。ここでは、各メンバーのロールの特長について説明します。

### マスターおよびスレーブ ユニットのロール

クラスタ内のメンバの 1 つがマスター ユニットです。マスター ユニットは自動的に決定されます。他のすべてのメンバはスレーブ ユニットです。

すべてのコンフィギュレーション作業はマスターユニット上でのみ実行する必要があります。コンフィギュレーションはその後、スレーブ ユニットに複製されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能についてはマスターユニットがすべてのトラフィックを処理します。[クラスタリングの中央集中型機能 \(766 ページ\)](#) を参照してください。

### マスター ユニット選定

クラスタのメンバは、クラスタ制御リンクを介して通信してマスターユニットを選定します。方法は次のとおりです。

1. クラスタを展開すると、各ユニットは選定要求を 3 秒ごとにブロードキャストします。
2. 優先順位が高い他のユニットがこの選定要求に応答します。優先順位はクラスタの展開時に設定され、設定の変更はできません。
3. 45 秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットがマスターになります。
4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的にマスター ユニットになることはありません。既存のマスター ユニットは常にマスターのままです。ただし、マスターユニットが応答を停止すると、その時点で新しいマスター ユニットが選定されます。



(注) 特定のユニットを手動で強制的にマスターにすることができます。中央集中型機能については、マスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

## クラスタ インターフェイス

シャーシ内クラスタリングでは、物理インターフェイスと EtherChannel (ポートチャネルとも呼ばれる) の両方を割り当てることができます。クラスタに割り当てられたインターフェイスはクラスタ内のすべてのメンバーのトラフィックのロード バランシングを行うスパンドインターフェイスです。

管理インターフェイス以外の個々のインターフェイスはサポートされていません。

## VSS または vPC への接続

インターフェイスの冗長性を確保するため、EtherChannel を VSS または vPC に接続することを推奨します。

## クラスタ制御リンク

クラスタ制御リンクはユニット間通信用の EtherChannel（ポートチャネル48）です。シャーシ内クラスタリングでは、このリンクは、クラスタ通信に Firepower 9300 バックプレーンを使用します。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。制御トラフィックには次のものが含まれます。

- マスター選定。
- 設定の複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- 状態の複製。
- 接続所有権クエリおよびデータ パケット転送。

## クラスタ制御リンク ネットワーク

Firepower 9300 シャーシは、シャーシ ID とスロット ID（127.2.chassis\_id.slot\_id）に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。この IP アドレスは、FXOS でもアプリケーション内でも手動で設定することはできません。クラスタ制御リンク ネットワークでは、ユニット間にルータを含めることはできません。レイヤ 2 スイッチングだけが許可されています。

## クラスタ内のハイ アベイラビリティ

クラスタリングは、シャーシ、ユニットとインターフェイスの正常性を監視し、ユニット間で接続状態を複製することにより、ハイ アベイラビリティを提供します。

## シャーシアプリケーションのモニタリング

シャーシアプリケーションのヘルス モニタリングは常に有効になっています。Firepower 9300 シャーシ スーパーバイザは、Firepower Threat Defense アプリケーションを定期的に確認します（毎秒）。Firepower Threat Defense デバイスが作動中で、Firepower 9300 シャーシ スーパーバイザと 3 秒間通信できなければ、Firepower Threat Defense デバイスは syslog メッセージを生成して、クラスタを離れます。

Firepower 9300 シャーシ スーパーバイザが 45 秒後にアプリケーションと通信できなければ、Firepower Threat Defense デバイスをリロードします。Firepower Threat Defense デバイスがスーパーバイザと通信できなければ、自身をクラスタから削除します。

## 装置のヘルス モニタリング

マスターユニットは、各スレーブユニットをモニタするために、クラスタ制御リンク経由でキープアライブメッセージを定期的送信します。各スレーブユニットは、同じメカニズムを使用してマスターユニットをモニタします。装置のヘルスチェックが不合格になると、その装置はクラスタから削除されます。

## インターフェイス モニタリング

各ユニットは、使用中のすべてのハードウェア インターフェイスのリンク ステータスをモニタし、ステータス変更をマスターユニットに報告します。ヘルス モニタリングを有効にすると、デフォルトですべての物理インターフェイスがモニタされます (EtherChannel インターフェイスの主要な EtherChannel を含む)。アップ状態の名前付きインターフェイスのみモニタできます。たとえば、名前付き EtherChannel がクラスタから削除されるまでは、EtherChannel のすべてのメンバー ポートは失敗しなければなりません。

あるモニタ対象のインターフェイスが、特定のユニット上では障害が発生したが、別のユニットではアクティブの場合は、そのユニットはクラスタから削除されます。Firepower Threat Defense デバイスがメンバーをクラスタから削除するまでの時間は、そのユニットが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。Firepower Threat Defense デバイスは、ユニットがクラスタに参加する最初の 90 秒間はインターフェイスを監視しません。この間にインターフェイスのステータスが変化しても、Firepower Threat Defense デバイスはクラスタから削除されません。設定済みのメンバーの場合は、500 ミリ秒後にユニットが削除されます。

## 障害後のステータス

クラスタ内のユニットで障害が発生したときに、そのユニットでホスティングされている接続は他のユニットにシームレスに移管されます。トラフィックフローの状態情報は、クラスタ制御リンクを介して共有されます。

マスターユニットで障害が発生した場合は、そのクラスタの他のメンバーのうち、プライオリティが最高 (番号が最小) のものがマスターユニットになります。

障害イベントに応じて、Firepower Threat Defense デバイスは自動的にクラスタへの再参加を試みます。



(注) Firepower Threat Defense デバイスが非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータ インターフェイスがシャットダウンされます。管理/診断インターフェイスのみがトラフィックを送受信できます。

## クラスタへの再参加

クラスタメンバがクラスタから削除された後、クラスタに再参加するための方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害：クラスタ制御リンクの問題を解決した後、クラスタリングを再び有効にして、手動でクラスタに再参加する必要があります。
- データ インターフェイスの障害：Firepower Threat Defense アプリケーションは自動的に最初は5分後、次に10分後、最終的に20分後に再参加を試みます。20分後に参加できない場合、Firepower Threat Defense アプリケーションはクラスタリングを無効にします。データ インターフェイスの問題を解決した後、手動でクラスタリングを有効にする必要があります。
- ユニットの障害：ユニットがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ユニットは再起動するとクラスタに再参加します。Firepower Threat Defense アプリケーションは5秒ごとにクラスタへの再参加を試みます。
- シャーシアプリケーション通信の障害：Firepower Threat Defense アプリケーションはシャーシアプリケーションの状態が回復したことを検出すると、自動的にクラスタへの再参加を試みます。
- 内部エラー：内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーションステータスなどがあります。問題の解決後、クラスタリングを再度有効にして手動でクラスタに再参加する必要があります。

## データ パス接続状態の複製

どの接続にも、1つのオーナーおよび少なくとも1つのバックアップオーナーがクラスタ内にあります。バックアップオーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP の状態情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップオーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上の状態情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 61: クラスタ全体で複製される機能

トラフィック	状態のサポート	注記 (Notes)
アップタイム	○	システムアップタイムをトラッキングします。
ARP テーブル	○	
MAC アドレス テーブル	○	



トラフィック	状態のサポート	注記 (Notes)
ユーザ ID	○	—
IPv6 ネイバー データベース	○	—
ダイナミック ルーティング	○	—
SNMP エンジン ID	なし	—
中央集中型 VPN (サイト間)	なし	VPN セッションは、マスターユニットで障害が発生すると切断されます。

## コンフィギュレーションの複製

クラスタ内のすべてのユニットは、単一の設定を共有します。設定変更を加えることができるのはマスターユニット上だけであり、変更は自動的にクラスタ内の他のすべてのユニットに同期されます。

## 管理インターフェイス

管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンドインターフェイスではなく、特別な個別インターフェイスです。管理インターフェイスによって各ユニットに直接接続できます。この管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。これは、**Firepower Management Center** にデバイスを設定し、登録するために使用されます。管理インターフェイスは、独自のローカル認証、IP アドレス、およびスタティックルーティングを使用します。クラスタの各メンバーは、管理ネットワーク上で、それぞれに異なる IP アドレスを使用します。これらの IP アドレスは、ブートストラップ構成の一部としてユーザが設定します。

管理インターフェイスは、管理論理インターフェイスと診断論理インターフェイスの間で共有されます。診断論理インターフェイスはオプションであり、ブートストラップ構成の一部としては設定されません。診断インターフェイスは、他のデータインターフェイスと併せて設定できます。診断インターフェイスを設定する場合、メインクラスタ IP アドレスを、そのクラスタの固定アドレス（常に現在のマスターユニットに属するアドレス）として設定します。アドレス範囲も設定して、現在のマスターを含む各ユニットがその範囲内のローカルアドレスを使用できるようにします。このメインクラスタ IP アドレスによって、診断アクセスのアドレスが一本化されます。マスターユニットが変更されると、メインクラスタ IP アドレスは新しいマスターユニットに移動するので、クラスタへのアクセスをシームレスに続行できます。TFTP や syslog などの発信管理トラフィックの場合、マスターユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバに接続します。

## クラスタが接続を管理する方法

接続をクラスタの複数のメンバーにロードバランスできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

### 接続ロール

各接続に定義されている次のロールを参照してください。

- **オーナー**：通常、最初に接続を受信するユニット。オーナーは、TCP 状態を保持し、パケットを処理します。1つの接続に対してオーナーは1つだけです。最初のオーナーに障害が発生すると、新しいユニットがその接続からパケットを受信したときに、ディレクタがそれらのユニットの中から新しいオーナーを選択します。
- **バックアップ オーナー**：オーナーから受信した TCP/UDP 状態情報を保存して、障害発生時に接続を新しいオーナーにシームレスに転送できるようにするユニット。バックアップ オーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合は、その接続からパケットを受け取る最初のユニット（ロードバランシングに基づく）がバックアップ オーナーに問い合わせ、関連する状態情報を取得します。これでそのユニットが新しいオーナーになることができます。

ディレクタ（下記参照）がオーナーと同じユニットでないかぎり、ディレクタもバックアップ オーナーです。オーナーが自分をディレクタとして選択した場合は、別のバックアップ オーナーが選択されます。

- **ディレクタ**：フォワーダからのオーナーバックアップ要求を処理するユニット。オーナーが新しい接続を受信すると、オーナーは、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにメッセージをそのディレクタに送信します。パケットがオーナー以外のユニットに到着した場合は、そのユニットはどのユニットがオーナーかをディレクタに問い合わせます。これで、パケットを転送できるようになります。1つの接続に対してディレクタは1つだけです。ディレクタに障害が発生すると、オーナーは新しいディレクタを選択します。

ディレクタがオーナーと同じユニットでないかぎり、ディレクタもバックアップ オーナーです（上記参照）。オーナーが自分をディレクタとして選択した場合は、別のバックアップ オーナーが選択されます。

- **フォワーダ**：パケットをオーナーに転送するユニット。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください。（TCP シーケンスのランダム化を無効にした場合は、SYN Cookie は使用されないため、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえば DNS や ICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループット

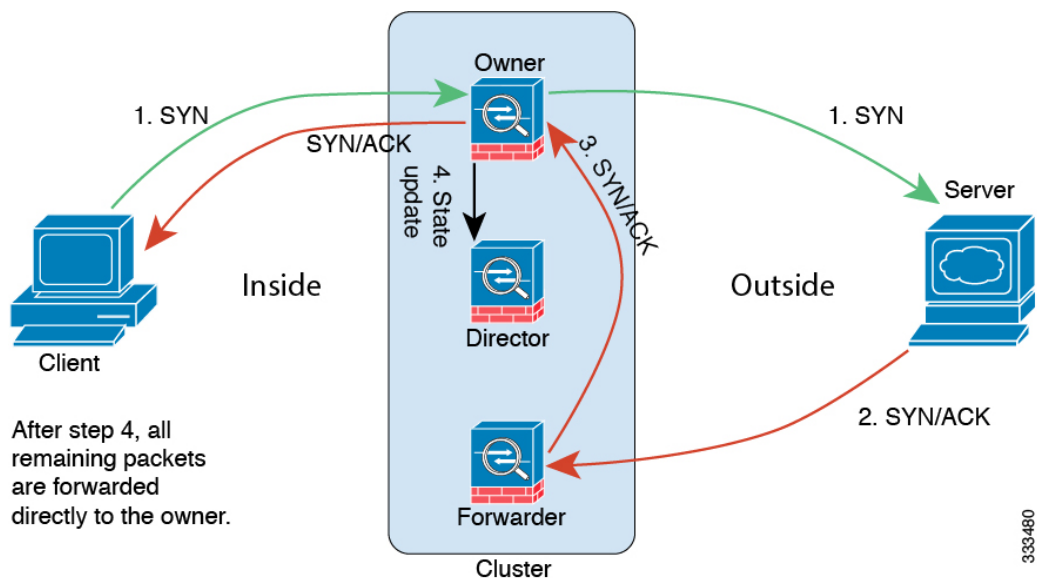
を実現できるのは、フォワーダが1つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

## 新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのメンバに送信される場合は、そのユニットがその接続の両方向のオーナーとなります。接続のパケットが別のユニットに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーユニットに転送されます。逆方向のフローが別のユニットに到着した場合は、元のユニットにリダイレクトされます。

## サンプル データ フロー

次の例は、新しい接続の確立を示します。



1. SYN パケットがクライアントから発信され、Firepower Threat Defense デバイスの1つ（ロードバランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の Firepower Threat Defense デバイス（ロードバランシング方法に基づく）に配信されます。この Firepower Threat Defense デバイスはフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。

5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP 状態情報を記録します。ディレクタは、この接続のバックアップオーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のユニットに配信された場合は、そのユニットはディレクタに問い合わせさせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

## Firepower Threat Defense の機能とクラスタリング

Firepower Threat Defense の一部の機能はクラスタリングではサポートされず、一部はマスターユニットのみでサポートされます。その他の機能については適切な使用に関する警告があります。

### クラスタリングでサポートされない機能

これらの機能は、クラスタリングが有効なときは設定できず、コマンドは拒否されます。

- サイト間 VPN
- DHCP クライアント、サーバ、およびプロキシ。DHCP リレーはサポート対象です。
- 高可用性

### クラスタリングの中央集中型機能

次の機能は、マスターユニット上だけでサポートされます。クラスタの場合もスケーリングされません。



- (注) 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバユニットからマスターユニットに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、マスター以外のユニットに転送されることがあります。この場合は、トラフィックがマスターユニットに送り返されます。

中央集中型機能については、マスターユニットで障害が発生するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

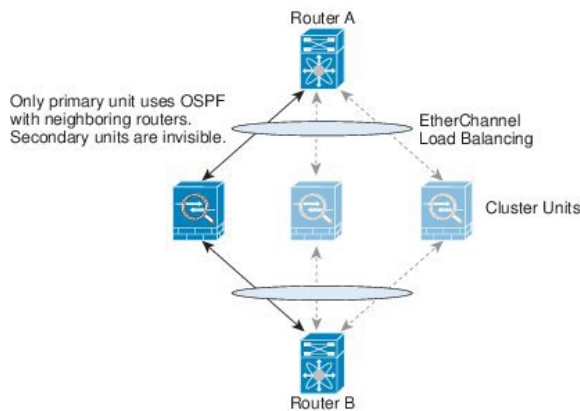
- 次のアプリケーション インспекション：
  - DCERPC
  - NetBIOS

- RSH
  - SUNRPC
  - TFTP
  - XDMCP
- ダイナミック ルーティング
  - スタティック ルート モニタリング

## ダイナミック ルーティングとクラスタリング

ルーティング プロセスはマスター ユニット上だけで実行されます。ルートはマスター ユニットを介して学習され、セカンダリに複製されます。ルーティング パケットがスレーブに到着した場合は、マスター ユニットにリダイレクトされます。

図 13: ダイナミック ルーティング



スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスター ユニットからスレーブ ユニットに同期されません。マスターユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します。必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

## NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、クラスタ内のそれぞれ別の Firepower Threat Defense デバイスに送信されることがあります。ロード バランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用される場合は、インバウンドとアウトバウンドとで、パケットの IP アドレスやポートが異なるからです。接続のオーナーではない Firepower Threat

Defense デバイス に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるので、大量のトラフィックがクラスタ制御リンク上で発生します。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- **ダイナミック PAT 用 NAT プールアドレス分散** : マスターユニットは、アドレスをクラスタ全体に均等に分配します。接続を受信したメンバーにアドレスが1つも残っていない場合、他のメンバーには使用可能なアドレスがまだ残っていても、接続はドロップされません。最低でも、クラスタ内のユニットと同数の NAT アドレスが含まれていることを確認してください。各ユニットが確実に1つのアドレスを受け取るようにするためです。
- **ラウンドロビンなし** : PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- **マスターユニットによって管理されるダイナミック NAT xlate** : マスターユニットが xlate テーブルを維持し、スレーブユニットに複製します。ダイナミック NAT を必要とする接続をスレーブユニットが受信したときに、その xlate がテーブル内にない場合は、スレーブはマスターユニットに xlate を要求します。スレーブユニットが接続を所有します。
- 次のインспекション用のスタティック PAT はありません。
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP

## SIP インспекションとクラスタリング

制御フローは、任意のユニットで作成できますが（ロードバランシングのため）、その子データフローは同じユニットに存在する必要があります。

## syslog とクラスタリング

- クラスタの各ユニットは自身の syslog メッセージを生成します。各ユニットの syslog メッセージヘッダーフィールドで使用されるデバイス ID を同一にするか、別にするかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのユニットに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合は、どのユニットで生成された syslog メッセージも1つのユニットからのように見えます。クラスタブートストラップ設定で割り当てられたローカルユニット名をデバイス ID として使用するようにロギングを設定した場合は、syslog メッセージはそれぞれ別のユニットからのように見えます。

## SNMP とクラスタリング

SNMP エージェントは、個々の Firepower Threat Defense デバイスを、その診断インターフェイスのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メインクラスタ IP アドレスではなく、常にローカルアドレスを使用してください。SNMP エージェントがメインクラスタ IP アドレスをポーリングする場合は、新しいマスターが選定されたときに、新しいマスターユニットのポーリングに失敗します。

## FTP とクラスタリング

- FTPD チャンネルとコントロールチャンネルのフローがそれぞれ別のクラスタメンバーによって所有されている場合は、D チャンネルのオーナーは定期的にアイドルタイムアウトアップデートをコントロールチャンネルのオーナーに送信し、アイドルタイムアウト値を更新します。ただし、コントロールフローのオーナーがリロードされて、コントロールフローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロールフローのアイドルタイムアウトは更新されません。

## Cisco TrustSec とクラスタリング

マスターユニットだけがセキュリティグループタグ (SGT) 情報を学習します。マスターユニットからこの SGT がスレーブに渡されるので、スレーブは、セキュリティポリシーに基づいて SGT の一致決定を下せます。

# Firepower 9300 シャーシでのクラスタ化前提条件

### スイッチ前提条件

- Firepower 4100/9300 シャーシでクラスタリングを設定する前に、必ずスイッチの設定を完了し、シャーシからのすべての EtherChannel をスイッチに正常に接続してください。
- サポートされているスイッチのリストについては、「[Cisco FXOS Compatibility](#)」を参照してください。

# Firepower 9300 シャーシ上のクラスタリングのガイドライン

### ハイ アベイラビリティ

ハイ アベイラビリティは、クラスタリングではサポートされません。

### その他のガイドライン

- ユニットの既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンドインターフェイスに接続された Windows 2003 サーバを使用している場合、syslog サーバポートがダウンし、サーバが ICMP エラーメッセージを制限しないと、大量の ICMP メッセージがクラスタに返送されます。このようなメッセージにより、クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラーメッセージを調節することを推奨します。

## Firepower 9300 シャーシでのクラスタリングのデフォルト

- クラスタのヘルスチェック機能は、デフォルトで有効になり、ホールド時間は3秒です。インターフェイスヘルスモニタリングは、デフォルトで、すべてのインターフェイス上で有効です。

## Firepower 4100/9300 シャーシのクラスタリング設定

クラスタは、Firepower 4100/9300 シャーシスーパーバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。その後、ユニットを Management Center に追加し、1つのクラスタにグループ化できます。

## Firepower 4100/9300 シャーシスーパーバイザからのクラスタの展開

クラスタリングの設定手順についての詳細は、Firepower 4100/9300 シャーシのドキュメンテーションを参照してください。

論理デバイスを Firepower 9300 シャーシに追加するときは、スタンドアロンユニットまたはクラスタのどちらを展開するかを選択できます。



## Management Center へのクラスタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

論理デバイスを Management Center に追加し、これらをクラスタにグループ化します。

### 始める前に

- どのユニットがマスター ユニットであるかを確認するには、Firepower Chassis Manager の [論理デバイス (Logical Devices)] 画面を参照します。
- すべてのクラスタ ユニットは、Management Center に追加する前に、FXOS 上の正常に形成されたクラスタ内に存在している必要があります。

### 手順

**ステップ 1** Management Center で、[デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択し、[追加 (Add)] > [デバイスの追加 (Add Device)] の順に選択して、クラスタを展開したときに割り当てた管理 IP アドレスを使用して、各ユニットを別個の管理対象デバイスとして追加します。

(注) Management Center のハイ アベイラビリティを使用する場合、スタンバイ Management Center にも各ユニットが正常に登録されていることを確認してから、アクティブな Management Center 上での作業を継続し、クラスタを形成します。各ユニットの登録ステータスを確認するために、スタンバイ Management Center にログインします。

**ステップ 2** [追加 (Add)] > [クラスタの追加 (Add Cluster)] の順に選択し、ユニットをクラスタにグループ化します。

a) ドロップダウンリストから [マスター (Master)] デバイスを選択します。

対象となる他のすべてのメンバーは、[スレーブデバイス (Slave Devices)] ボックスに追加されます。

b) クラスタの [名前 (Name)] を指定します。

c) [OK] をクリックします。

クラスタ オブジェクトが [デバイス (Devices)] 画面に追加され、メンバー ユニットがその下に表示されます。現在のマスター ユニットは、ユニット名の後の「(マスター) (master)」で表示されます。

(注) 後から FXOS シャーシのクラスタにさらにユニットを追加する場合は、Management Center に各ユニットを追加し、その後すぐにそれらをクラスタのスレーブノードとして追加する必要があります。

**ステップ 3** デバイス固有の設定を行うには、クラスタの編集アイコン (✎) をクリックします。クラスタを全体として設定することはできませんが、クラスタのメンバー ユニットは設定できません。

**ステップ 4** [デバイス (Devices)] > [デバイス管理 (Device Management)] > [クラスタ (Cluster)] タブから、[全般 (General)]、[ライセンス (License)]、[システム (System)]、および [ヘルス (Health)] の設定を確認できます。このタブは、ライセンス付与の設定をする際に役立ちます。[デバイス (Devices)] タブでは、マスター ユニットのみの管理 IP アドレスを変更できます。

**ステップ 5** (任意) 診断インターフェイスを設定するには、次の手順を実行します。

診断インターフェイスは、個別インターフェイスモードで実行できる唯一のインターフェイスです。syslog メッセージや SNMP などに、このインターフェイスを使用できます。

- a) 診断インターフェイスを編集するには、[インターフェイス (Interfaces)] タブをクリックします。
- b) [IPv4] タブで、[仮想 IP アドレス (Virtual IP Address)] とマスクを入力します。この IP アドレスは、そのクラスタの固定アドレスで、常に現在のマスターユニットに属します。
- c) [開始アドレス (Start Address)] と [終了アドレス (End Address)] に、IP アドレスプールの開始アドレスと終了アドレスを入力します。この範囲に含まれるアドレスの 1 つが、インターフェイスの各クラスタユニットに指定されます。

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。仮想 IP アドレスはこのプールには含まれませんが、同一ネットワーク上に存在している必要があります。各ユニットに割り当てられる正確なローカルアドレスを事前に決定することはできません。

- d) [マスク (Mask)] に、クラスタ IP プールのサブネットマスクを入力します。
- e) [IPv6] タブで、[基本 (Basic)] > [クラスタ IPv6 プール (Cluster IPv6 Pool)] の下の、[アドレス (Address)] に *ipv6-address/prefix-length* を指定し、[カウント (Count)] にプール内のアドレス数を指定します。
- f) 通常どおり、他のインターフェイス設定を行います。

**ステップ 6** 必要に応じて他のデバイスレベルの設定も行います。

**ステップ 7** [保存 (Save)]、[展開 (Deploy)] の順にクリックします。

## クラスタ メンバーの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

Firepower 9300 デバイスにモジュールを追加する場合などには、既存のクラスタに新しいクラスタ メンバーを追加できます。

### 始める前に

FXOS シャーシのクラスタにさらにユニットを追加するときには、Management Center に各ユニットを追加し、その後すぐにそれらをクラスタのスレーブ ノードとして追加する必要があります。

### 手順

- 
- ステップ 1** Management Center で、[デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択し、[追加 (Add)] > [デバイスの追加 (Add Device)] の順に選択して、新しい論理デバイスを追加します。
- ステップ 2** [追加 (Add)] > [クラスタの追加 (Add Cluster)] を選択します。 >
- ステップ 3** ドロップダウン リストから現在の [マスター (Master)] デバイスを選択します。
- クラスタにすでに含まれているマスター デバイスを選択した場合、既存のクラスタの名前が自動入力され、[スレーブ デバイス (Slave Devices)] ボックスに選択可能なすべてのスレーブ デバイスが表示されます。これには、Management Center に追加したばかりの新しいユニットが含まれます。
- ステップ 4** [追加 (Add)] をクリックし、次に [導入 (Deploy)] をクリックします。
- クラスタが更新され、新しいメンバーが追加されます。
-

## スレーブメンバーの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

クラスタメンバーを削除する必要がある場合（たとえば、Firepower 9300 でモジュールを削除する場合は、Management Center からメンバーを削除する必要があります。そのメンバーが引き続きクラスタの正常な構成要素であると Firepower Chassis Manager に示されている場合は、メンバーを削除しないでください。Management Center から削除しても、そのメンバーは引き続きクラスタの有効な構成要素であるため、これがマスターユニットになって Management Center でそれを管理できなくなる場合に問題が発生する可能性があります。

### 手順

**ステップ 1** Management Center で、[デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、スレーブユニットの横にあるごみ箱をクリックします。

**ステップ 2** ユニットの削除を確認します。

ユニットがクラスタから削除され、Management Center デバイスリストからも削除されます。

## クラスタへの再参加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

障害が発生したインターフェイスなど、ユニットがクラスタから削除された場合、ユニット CLI にアクセスして、クラスタに手動で再参加させる必要があります。クラスタへの再参加を試行する前に、障害が解決されていることを確認します。クラスタからユニットが削除される理由の詳細については、[クラスタへの再参加 \(762 ページ\)](#) を参照してください。

## 手順

**ステップ 1** クラスタに再参加させる必要のあるユニットの CLI に、コンソールポートからアクセスするか、管理インターフェイスへの SSH を使用してアクセスします。ユーザ名 **admin** と、初期セットアップ時に設定したパスワードを使用してログインします。

**ステップ 2** クラスタリングを有効にします。

```
cluster enable
```

## クラスタリングの履歴

機能	バージョン (Version)	詳細 (Details)
Firepower 9300 用シャーシ内クラスタリング	6.0.1	<p>FirePOWER 9300 シャーシ内では、最大3つのセキュリティモジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。</p> <p>新しい/変更された画面：</p> <p>[デバイス (Devices)] &gt; [デバイス管理 (Device Management)] &gt; [追加 (Add)] &gt; [クラスタの追加 (Add Cluster)]</p> <p>[デバイス (Devices)] &gt; [デバイス管理 (Device Management)] &gt; [クラスタ (Cluster)]</p> <p>サポートされているプラットフォーム：Firepower 9300 の Firepower Threat Defense</p>





## 第 **X** 部

# Firepower Threat Defense のルーティング

- [Firepower Threat Defense のルーティングの概要 \(779 ページ\)](#)
- [Firepower Threat Defense のスタティック ルートとデフォルト ルート \(793 ページ\)](#)
- [Firepower Threat Defense 用の OSPF \(799 ページ\)](#)
- [Firepower Threat Defense の BGP \(831 ページ\)](#)
- [Firepower Threat Defense 用の RIP \(851 ページ\)](#)
- [Firepower Threat Defense 用のマルチキャスト ルーティング \(859 ページ\)](#)







## 第 32 章

# Firepower Threat Defense のルーティングの概要

この章では、Cisco Firepower Threat Defense 内でのルーティング動作の基本概念と、サポートされているルーティングプロトコルについて説明します。ルーティングは、送信元から宛先にネットワーク経由で情報を移動する行為のことです。その間に、通常は少なくとも1つの中間ノードがあります。ルーティングには、最適なルーティングパスの決定と、ネットワーク経由のパケットの転送という2つの基本的なアクティビティが含まれます。

- [パスの決定 \(779 ページ\)](#)
- [サポートされるルート タイプ \(780 ページ\)](#)
- [Firepower Threat Defense 内でのルーティングの仕組み \(782 ページ\)](#)
- [ルーティングでサポートされるインターネット プロトコル \(784 ページ\)](#)
- [着信サービス一覧 \(Routing Table\) \(785 ページ\)](#)
- [管理トラフィック用ルーティングテーブル \(790 ページ\)](#)
- [ルート マップについて \(790 ページ\)](#)

## パスの決定

ルーティングプロトコルでは、メトリックを使用して、パケットの移動に最適なパスを評価します。メトリックは、宛先への最適なパスを決定するためにルーティングアルゴリズムが使用する、パスの帯域幅などの測定基準です。パスの決定プロセスを支援するために、ルーティングアルゴリズムは、ルート情報が格納されるルーティングテーブルを初期化して保持します。ルート情報は、使用するルーティングアルゴリズムによって異なります。

ルーティングアルゴリズムにより、さまざまな情報がルーティングテーブルに入力されます。宛先またはネクスト ホップの関連付けにより、最終的な宛先に達するまで、「ネクスト ホップ」を表す特定のルータにパケットを送信することによって特定の宛先に最適に到達できることがルータに示されます。ルータは、着信パケットを受信すると宛先アドレスを確認し、このアドレスとネクスト ホップとを関連付けようとします。

ルーティングテーブルには、パスの妥当性に関するデータなど、他の情報を格納することもできます。ルータは、メトリックを比較して最適なルートを決めます。これらのメトリックは、使用しているルーティングアルゴリズムの設計によって異なります。

ルータは互いに通信し、さまざまなメッセージの送信によりそのルーティングテーブルを保持しています。ルーティング アップデート メッセージはそのようなメッセージの1つで、通常はルーティング テーブル全体か、その一部で構成されています。ルーティング アップデートを他のすべてのルータから分析することで、ルータはネットワーク トポロジの詳細な全体像を構築できます。ルータ間で送信されるメッセージのもう1つの例であるリンクステートアドバタイズメントは、他のルータに送信元のリンクの状態を通知します。リンク情報も、ネットワークの宛先に対する最適なルートをルータが決定できるように、ネットワーク トポロジの全体像の構築に使用できます。

## サポートされるルートタイプ

ルータが使用できるルートタイプには、さまざまなものがあります。Firepower Threat Defense デバイス では、次のルートタイプが使用されます。

- スタティックとダイナミックの比較
- シングルパスとマルチパスの比較
- フラットと階層型の比較
- リンクステートと距離ベクトル型の比較

## スタティックとダイナミックの比較

スタティックルーティングアルゴリズムは、実はネットワーク管理者が確立したテーブルマップです。このようなマッピングは、ネットワーク管理者が変更するまでは変化しません。スタティック ルートを使用するアルゴリズムは設計が容易であり、ネットワーク トラフィックが比較的予想可能で、ネットワーク設計が比較的単純な環境で正しく動作します。

スタティック ルーティング システムはネットワークの変更に対応できないため、一般に、変化を続ける大規模なネットワークには不向きであると考えられています。主なルーティングアルゴリズムのほとんどはダイナミック ルーティング アルゴリズムであり、受信したルーティング アップデート メッセージを分析することで、変化するネットワーク環境に適合します。メッセージがネットワークが変化したことを示している場合は、ルーティングソフトウェアはルートを再計算し、新しいルーティングアップデートメッセージを送信します。これらのメッセージはネットワーク全体に送信されるため、ルータはそのアルゴリズムを再度実行し、それに従ってルーティング テーブルを変更します。

ダイナミック ルーティング アルゴリズムは、必要に応じてスタティック ルートで補足できます。たとえば、ラストリゾート ルータ（ルーティングできないすべてのパケットが送信されるルータのデフォルトルート）を、ルーティングできないすべてのパケットのリポジトリとして機能するように指定し、すべてのメッセージを少なくとも何らかの方法で確実に処理することができます。

## シングルパスとマルチパスの比較

一部の高度なルーティングプロトコルは、同じ宛先に対する複数のパスをサポートしています。シングルパスアルゴリズムとは異なり、これらのマルチパスアルゴリズムでは、複数の回線でトラフィックを多重化できます。マルチパスアルゴリズムの利点は、スループットと信頼性が大きく向上することであり、これは一般に「ロードシェアリング」と呼ばれています。

## フラットと階層型の比較

ルーティングアルゴリズムには、フラットなスペースで動作するものと、ルーティング階層を使用するものがあります。フラットルーティングシステムでは、ルータは他のすべてのルータのピアになります。階層型ルーティングシステムでは、一部のルータが実質的なルーティングバックボーンを形成します。バックボーン以外のルータからのパケットはバックボーンルータに移動し、宛先の一般エリアに達するまでバックボーンを通じて送信されます。この時点で、パケットは、最後のバックボーンルータから、1つ以上のバックボーン以外のルータを通じて最終的な宛先に移動します。

多くの場合、ルーティングシステムは、ドメイン、自律システム、またはエリアと呼ばれるノードの論理グループを指定します。階層型のシステムでは、ドメイン内の一部のルータは他のドメインのルータと通信できますが、他のルータはそのドメイン内のルータ以外とは通信できません。非常に大規模なネットワークでは、他の階層レベルが存在することがあり、最も高い階層レベルのルータがルーティングバックボーンを形成します。

階層型ルーティングの第一の利点は、ほとんどの企業の組織を模倣しているため、そのトラフィックパターンを適切にサポートするという点です。ほとんどのネットワーク通信は、小さい企業グループ（ドメイン）内で発生します。ドメイン内ルータは、そのドメイン内の他のルータだけを認識していれば済むため、そのルーティングアルゴリズムを簡素化できます。また、使用しているルーティングアルゴリズムに応じて、ルーティングアップデートトラフィックを減少させることができます。

## リンクステートと距離ベクトル型の比較

リンクステートアルゴリズム（最短パス優先アルゴリズムとも呼ばれる）は、インターネットワークのすべてのノードにルーティング情報をフラッドします。ただし、各ルータは、それ自体のリンクのステートを記述するルーティングテーブルの一部だけを送信します。リンクステートアルゴリズムでは、各ルータはネットワークの全体像をそのルーティングテーブルに構築します。距離ベクトル型アルゴリズム（Bellman-Fordアルゴリズムとも呼ばれる）では、各ルータが、そのネイバーだけに対してそのルーティングテーブル全体または一部を送信するように要求されます。つまり、リンクステートアルゴリズムは小規模なアップデートを全体に送信しますが、距離ベクトル型アルゴリズムは、大規模なアップデートを隣接ルータだけに送信します。距離ベクトル型アルゴリズムは、そのネイバーだけを認識します。通常、リンクステートアルゴリズムは OSPF ルーティングプロトコルとともに使用されます。

# Firepower Threat Defense 内でのルーティングの仕組み

Firepower Threat Defense デバイスは NAT の設定に応じて、ルーティングの判断のために、ルーティング テーブルまたは NAT (xlate) テーブルを使用します。

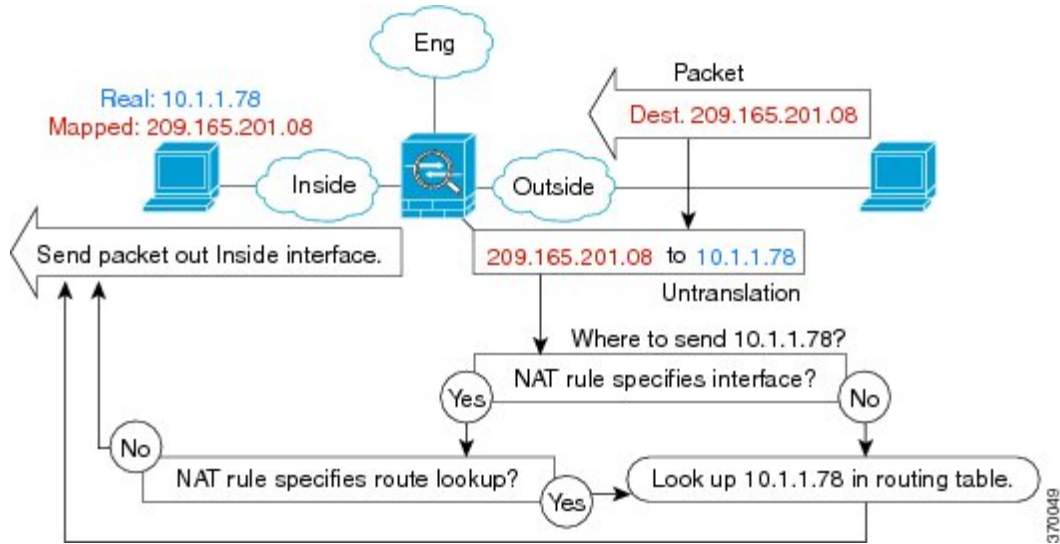
## 出インターフェイスの決定

NAT を使用していて、Firepower Threat Defense デバイスがマッピングアドレスのトラフィックを受信する場合、Firepower Threat Defense デバイスは NAT ルールに従って宛先アドレスを逆変換し、実際のアドレスにパケットを送信します。Firepower Threat Defense デバイスは、次の方法でパケットの出インターフェイスを決定します。

- トランスペアレントモードのブリッジグループインターフェイス：Firepower Threat Defense デバイスは NAT ルールを使用して実際のアドレスの出インターフェイスを決定します。NAT ルールの一部として送信元、宛先のブリッジグループ メンバー インターフェイスを指定する必要があります。
- ルーテッドモードの通常インターフェイス：Firepower Threat Defense デバイスは、次のいずれかの方法で出インターフェイスを決定します。
  - NAT ルールでインターフェイスを設定する：Firepower Threat Defense デバイスは NAT ルールを使用して出インターフェイスを決定します。ただし、代わりにオプションとして常にルート ルックアップを使用することもできます。一部のシナリオでは、ルート ルックアップの上書きが必要になる場合があります。
  - NAT ルールでインターフェイスを設定しない：Firepower Threat Defense デバイスはルート ルックアップを使用して出インターフェイスを決定します。

次の図に、ルーテッドモードでの出インターフェイスの選択方法を示します。ほとんどの場合、ルート ルックアップは NAT ルールのインターフェイスと同じです。ただし、一部の構成では、2つの方法が異なる場合があります。

図 14: NATによるルーテッドモードでの出インターフェイスの選択



## ネクスト ホップの選択プロセス

前述のいずれかの方法を使用して出力インターフェイスを選択した後、さらにルートルックアップが実行され、これまでに選択した出力インターフェイスに属する適切なネクストホップが検出されます。選択されたインターフェイスに明示的に属するルートがルーティングテーブルにない場合は、パケットがドロップされてレベル 6 の syslog メッセージ 110001（ホストへのルートなし）が生成されます（別の出力インターフェイスに属する、指定の宛先ネットワークへの別のルートがあるかどうかにかかわらず）。選択した出力インターフェイスに属するルートが見つかり、パケットは対応するネクストホップに転送されます。

Firepower Threat Defense デバイスでのロードシェアリングは、1つの出力インターフェイスを使用して複数のネクストホップが使用できる場合に限り可能です。ロードシェアリングでは、複数の出力インターフェイスの共有はできません。

ダイナミックルーティングが Firepower Threat Defense デバイスで使用されており、XLATE の作成後にルートテーブルが変更された場合も（ルートフラップなど）、宛先変換トラフィックは、XLATE がタイムアウトするまでは、ルートテーブルではなく古い XLATE を使用して転送されます。トラフィックが、正しくないインターフェイスに転送されたり、ドロップされてレベル 6 の syslog メッセージ 110001（ホストへのルートなし）が生成されたりすることもあります（ルーティングプロセスによって古いルートが古いインターフェイスから削除されて別のインターフェイスに接続された場合）。

Firepower Threat Defense デバイス自体でルートフラップが発生していないにもかかわらず、その周りで一部のルーティングプロセスがフラッピングし、発信元変換された、同じフローに属するパケットを、別のインターフェイスを使用して Firepower Threat Defense デバイス 経由で送信する場合は、同様の問題が発生することがあります。宛先変換された返送パケットは、間違った出力インターフェイスを使用して戻されることがあります。

セキュリティトラフィック構成によっては、この問題が高い確率で発生します。具体的には、ほぼすべてのトラフィックが、フローの最初のパケットの方向に応じて、発信元変換されるか宛先変換されるような構成です。ルートフラップの後にこの問題が発生した場合は、XLATEのタイムアウトによって自動的に解決することもできます。XLATEのタイムアウトは、必要に応じて小さくできます。この問題がほとんど発生しないようにするには、Firepower Threat Defense デバイス やその周りでルートフラップが発生しないようにします。つまり、同じフローに属する宛先変換されたパケットが必ず同じ方法でFirepower Threat Defense デバイス を通して転送されることを確認します。

## ECMP ルーティング

Firepower Threat Defense デバイスは、等コスト マルチパス (ECMP) ルーティングをサポートしています。

インターフェイスごとに最大3の等コストのスタティック ルートまたはダイナミック ルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスで複数のデフォルトルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

この場合、トラフィックは、10.1.1.2、10.1.1.3 と 10.1.1.4 間の外部インターフェイスでロードバランスされます。トラフィックは、送信元 IP アドレスおよび宛先 IP アドレスをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

ECMP は複数のインターフェイス間ではサポートされないため、異なるインターフェイスで同じ宛先へのルートを定義することはできません。上記のルートのいずれかを設定すると、次のルートは拒否されます。

```
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.1
```

## ルーティングでサポートされるインターネットプロトコル

Firepower Threat Defense デバイスは、ルーティングに対してさまざまなインターネットプロトコルをサポートしています。この項では、各プロトコルについて簡単に説明します。

- Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP は、IGRP ルータとの互換性とシームレスな相互運用性を提供するシスコ独自のプロトコルです。自動再配布メカニズムにより、IGRP ルートを Enhanced IGRP に、または

Enhanced IGRP からインポートできるため、Enhanced IGRP を既存の IGRP ネットワークに徐々に追加できます。

- Open Shortest Path First (OSPF)

OSPF は、インターネットプロトコル (IP) ネットワーク向けに、インターネット技術特別調査委員会 (IETF) の Interior Gateway Protocol (IGP) 作業部会によって開発されたルーティングプロトコルです。OSPF は、リンクステートアルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

- Routing Information Protocol (RIP)

RIP は、ホップカウントをメトリックとして使用するディスタンスベクトルプロトコルです。RIP は、グローバルなインターネットでトラフィックのルーティングに広く使用されている Interior Gateway Protocol (IGP) です。つまり、1 つの自律システム内部でルーティングを実行します。

- ボーダー ゲートウェイ プロトコル (BGP)

BGP は自律システム間のルーティングプロトコルです。BGP は、インターネットのルーティング情報を交換するために、インターネットサービスプロバイダー (ISP) 間で使用されるプロトコルです。カスタマーは ISP に接続し、ISP は BGP を使用してカスタマーおよび ISP ルートを交換します。自律システム (AS) 間で BGP を使用する場合、このプロトコルは外部 BGP (EBGP) と呼ばれます。サービスプロバイダーが BGP を使用して AS 内のルートを交換する場合、このプロトコルは内部 BGP (IBGP) と呼ばれます。

## 着信サービス一覧 (Routing Table)

ここでは、ルーティングテーブルについて説明します。

### ルーティングテーブルへの入力方法

Firepower Threat Defense デバイスのルーティングテーブルには、スタティックに定義されたルート、直接接続されているルート、およびダイナミックルーティングプロトコルで検出されたルートを入力できます。Firepower Threat Defense デバイスは、ルーティングテーブルに含まれるスタティックルートと接続されているルートに加えて、複数のルーティングプロトコルを実行できるため、同じルートが複数の方法で検出または入力される可能性があります。同じ宛先への 2 つのルートがルーティングテーブルに追加されると、ルーティングテーブルに残るルートは次のように決定されます。

- 2 つのルートのネットワークプレフィックス長 (ネットワークマスク) が異なる場合は、どちらのルートも固有と見なされ、ルーティングテーブルに入力されます。入力された後は、パケット転送ロジックが 2 つのうちどちらを使用するかを決定します。

たとえば、RIP プロセスと OSPF プロセスが次のルートを検出したとします。

- RIP : 192.168.32.0/24
- OSPF : 192.168.32.0/19

OSPF ルートのアドミニストレーティブディスタンスの方が適切であるにもかかわらず、これらのルートのプレフィックス長（サブネットマスク）はそれぞれ異なるため、両方のルートがルーティングテーブルにインストールされます。これらは異なる宛先と見なされ、パケット転送ロジックが使用するルートを決定します。

- Firepower Threat Defense デバイスが、1つのルーティングプロトコル（RIP など）から同じ宛先に複数のパスがあることを検知すると、（ルーティングプロトコルが判定した）メトリックがよい方のルートがルーティングテーブルに入力されます。

メトリックは特定のルートに関連付けられた値で、ルートを最も優先されるものから順にランク付けします。メトリックの判定に使用されるパラメータは、ルーティングプロトコルによって異なります。メトリックが最も小さいパスは最適パスとして選択され、ルーティングテーブルにインストールされます。同じ宛先への複数のパスのメトリックが等しい場合は、これらの等コストパスに対してロードバランシングが行われます。

- Firepower Threat Defense デバイスが、ある宛先へのルーティングプロトコルが複数あることを検知すると、ルートのアドミニストレーティブディスタンスが比較され、アドミニストレーティブディスタンスが最も小さいルートがルーティングテーブルに入力されます。

## ルートのアドミニストレーティブディスタンス

ルーティングプロトコルによって検出されるルート、またはルーティングプロトコルに再配布されるルートのアドミニストレーティブディスタンスは変更できます。2つの異なるルーティングプロトコルからの2つのルートのアドミニストレーティブディスタンスが同じ場合、デフォルトのアドミニストレーティブディスタンスが小さい方のルートがルーティングテーブルに入力されます。EIGRP ルートと OSPF ルートの場合、EIGRP ルートと OSPF ルートのアドミニストレーティブディスタンスが同じであれば、デフォルトで EIGRP ルートが選択されます。

アドミニストレーティブディスタンスは、2つの異なるルーティングプロトコルから同じ宛先への異なるルートが複数存在する場合に、ASA がベストパスの選択に使用するルートパラメータです。ルーティングプロトコルには、他のプロトコルとは異なるアルゴリズムに基づくメトリックがあるため、異なるルーティングプロトコルによって生成された、同じ宛先への2つのルートについて常にベストパスを判定できるわけではありません。

各ルーティングプロトコルには、アドミニストレーティブディスタンス値を使用して優先順位が付けられています。次の表に、ASA がサポートするルーティングプロトコルのデフォルトアドミニストレーティブディスタンス値を示します。

表 62: サポートされるルーティングプロトコルのデフォルトアドミニストレーティブディスタンス

ルートの送信元	デフォルトアドミニストレーティブディスタンス
接続中のインターフェイス	[0]



ルートの送信元	デフォルトアドミニストレーティブディスタンス
スタティック ルート	1
EIGRP 集約ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
RIP	120
EIGRP 外部ルート	170
内部 BGP	200
不明	255

アドミニストレーティブディスタンス値が小さいほど、プロトコルの優先順位が高くなります。たとえば、ASA が OSPF ルーティングプロセス（デフォルトアドミニストレーティブディスタンスが 110）と RIP ルーティングプロセス（デフォルトアドミニストレーティブディスタンスが 120）の両方から特定のネットワークへのルートを受信すると、OSPF ルーティングプロセスの方が優先度が高いため、ASA は OSPF ルートを選択します。この場合、ルータは OSPF バージョンのルートをルーティングテーブルに追加します。

この例では、OSPF 導出ルートの送信元が（電源遮断などで）失われると、ASA は、OSPF 導出ルートが再度現れるまで、RIP 導出ルートを使用します。

アドミニストレーティブディスタンスはローカルの設定値です。たとえば、OSPF を通して取得したルートのアドミニストレーティブディスタンスを変更するために **distance-ospf** コマンドを使用する場合、その変更は、コマンドが入力された ASA のルーティングテーブルにだけ影響します。アドミニストレーティブディスタンスがルーティングアップデートでアドバタイズされることはありません。

アドミニストレーティブディスタンスは、ルーティングプロセスに影響を与えません。EIGRP、OSPF、RIP および BGP ルーティングプロセスは、そのルーティングプロセスによって検出されたルートまたはそのルーティングプロセスに再配布されたルートのみをアドバタイズします。たとえば、RIP ルーティングプロセスは、ASA のルーティングテーブルで OSPF ルーティングプロセスによって検出されたルートが使用されていても、RIP ルートをアドバタイズしません。

## バックアップルート

ルートを最初にルーティングテーブルにインストールしようとしたとき、他のルートがインストールされているためにインストールできなかった場合、そのルートはバックアップルートとして登録されます。ルーティングテーブルにインストールされたルートに障害が発生すると、ルーティングテーブルメンテナンスプロセスが、登録されたバックアップルートを持つ各

ルーティングプロトコルプロセスを呼び出し、ルーティングテーブルにルートを再インストールするように要求します。障害が発生したルートに対して、登録されたバックアップルートを持つプロトコルが複数ある場合、アドミニストレーティブディスタンスに基づいて優先ルートが選択されます。

このプロセスのため、ダイナミックルーティングプロトコルによって検出されたルートに障害が発生したときにルーティングテーブルにインストールされるフローティングスタティックルートを作成できます。フローティングスタティックルートとは、単に、Firepower Threat Defense デバイスで動作しているダイナミックルーティングプロトコルよりも大きなアドミニストレーティブディスタンスが設定されているスタティックルートです。ダイナミックルーティングプロセスで検出された対応するルートに障害が発生すると、このスタティックルートがルーティングテーブルにインストールされます。

## 転送の決定方法

転送は次のように決定されます。

- 宛先が、ルーティングテーブル内のエン트리と一致しない場合、パケットはデフォルトルートに指定されているインターフェイスを通して転送されます。デフォルトルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティングテーブル内の1つのエン트리と一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。
- 宛先が、ルーティングテーブル内の複数のエン트리と一致し、パケットはネットワークプレフィックス長がより長いルートに関連付けられているインターフェイスから転送されます。

たとえば、192.168.32.1宛てのパケットが、ルーティングテーブルの次のルートを使用してインターフェイスに到着したとします。

- 192.168.32.0/24 gateway 10.1.1.2
- 192.168.32.0/19 gateway 10.1.1.3

この場合、192.168.32.1は192.168.32.0/24ネットワークに含まれるため、192.168.32.1宛てのパケットは10.1.1.2宛てに送信されます。このアドレスはまた、ルーティングテーブルの他のルートにも含まれますが、ルーティングテーブル内では192.168.32.0/24の方が長いプレフィックスを持ちます(24ビットと19ビット)。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先されます。



(注) ルートの変更が原因で新しい同様の接続が異なる動作を引き起こしたとしても、既存の接続は設定済みのインターフェイスを使用し続けます。

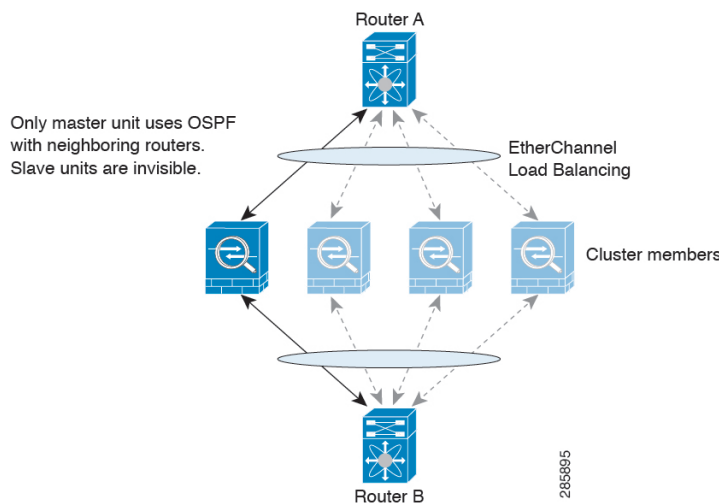
## ダイナミックルーティングおよびハイアベイラビリティ

アクティブなユニットでルーティングテーブルが変更されると、スタンバイユニットでダイナミックルートが同期されます。これは、アクティブユニットのすべての追加、削除、または変更がただちにスタンバイユニットに伝播されることを意味します。スタンバイユニットがアクティブ/スタンバイの待受中ハイアベイラビリティペアでアクティブになると、ルートはハイアベイラビリティバルク同期および連続複製プロセスの一部として同期されるため、そのユニットには以前のアクティブユニットと同じルーティングテーブルがすでに作成されています。

## クラスタリングでのダイナミックルーティング

ルーティングプロセスはマスターユニット上だけで実行されます。ルートはマスターユニットを介して学習され、スレーブに複製されます。ルーティングパケットがスレーブに到着した場合は、マスターユニットにリダイレクトされます。

図 15: クラスタリングでのダイナミックルーティング



スレーブメンバがマスターユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスターユニットからスレーブユニットに同期されません。マスターユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します。必須ではありませんが、スタティックルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップフォワーディング機能を参照してください。

## 管理トラフィック用ルーティングテーブル

標準的なセキュリティ実践として、データトラフィックを管理トラフィックから分離しなければならない場合があります。この分離を実現するために、Firepower Threat Defense デバイスは管理専用トラフィックとデータトラフィックに個別のルーティングテーブルを使用します。

管理ルーティングテーブルは、データインターフェイスルーティングテーブルとは分離したダイナミックルーティングをサポートします。ダイナミックルーティングプロセスは管理専用インターフェイスまたはデータインターフェイスで実行されなければなりません。両方のタイプを混在させることはできません。

HTTP、SCP、TFTP などを使用してリモートファイルを開くすべての機能に関しては、インターフェイスを指定していない場合、Firepower Threat Defense デバイスは管理専用ルーティングテーブルを確認します。一致がない場合はデータルーティングテーブルを確認します。

その他のすべての機能に関しては、インターフェイスを指定しなかった場合、Firepower Threat Defense デバイスはデータルーティングテーブルを確認し、一致するものが見つからなければ、管理専用ルーティングテーブルを確認します。たとえば、ping、DNS、DHCP などがあります。

管理専用インターフェイスには、すべての診断 x/x インターフェイス、および管理専用として設定したすべてのインターフェイスが含まれています。

## ルートマップについて

ルートマップは、ルートを OSPF、RIP、EIGRP、または BGP ルーティングプロセスに再配布するとき使用します。また、OSPF ルーティングプロセスにデフォルトルートを生成するときにも使用します。ルートマップは、指定されたルーティングプロトコルのどのルートを対象ルーティングプロセスに再配布できるのかを定義します。

ルートマップは、広く知られた ACL と共通の機能を数多く持っています。両方に共通する主な特性は次のとおりです。

- いずれも、それぞれが許可または拒否の結果を持つ個別のステートメントの順序シーケンスです。ACL またはルートマップの評価は、事前に定義された順序でのリストのスキャンと、一致する各ステートメントの基準の評価で構成されています。リストのスキャンは、ステートメントの一致が初めて見つかり、そのステートメントの一致に関連付けられたアクションが実行されると中断します。
- これらは汎用的なメカニズムです。基準照合と一致解釈は、適用方法とこれらを使用する機能によって決定します。同じルートマップであっても異なる機能に適用されると、解釈が異なる場合があります。

次のように、ルートマップと ACL には違いがいくつかあります。

- ルートマップは ACL よりも柔軟性が高く、ACL が確認できない基準に基づいてルートを確認できます。たとえば、ルート マップはルート タイプが内部であるかどうかを確認できます。
- 設計規則により、各 ACL は暗黙の deny ステートメントで終了します。照合中にルートマップの終わりに達した場合、そのルート マップの特定の適用によって結果が異なります。再配布に適用されるルート マップの動作は ACL と同じです。ルートがルートマップのどの句とも一致しない場合は、ルートマップの最後に deny ステートメントが含まれている場合と同様に、ルート再配布が拒否されます。

## permit 句と deny 句

ルートマップでは permit 句と deny 句を使用できます。deny 句は、ルートの照合の再配布を拒否します。ルートマップでは、一致基準として ACL を使用できます。ACL には permit 句と deny 句もあるので、パケットが ACL と一致した場合に次のルールが適用されます。

- ACL の permit + ルートマップの permit : ルートは再配布されます。
- ACL の permit + ルートマップの deny : ルートは再配布されません。
- ACL の deny + ルートマップの permit または deny : ルートマップの句は一致せず、次のルートマップ句が評価されます。

## match 句と set 句の値

各ルート マップ句には、次の 2 種類の値があります。

- match 値は、この句が適用されるルートを選択します。
- set 値は、ターゲット プロトコルに再配布される情報を変更します。

再配布される各ルートについて、ルータは最初にルートマップの句の一致基準を評価します。一致基準が満たされると、そのルートは、permit 句または deny 句に従って再配布または拒否され、そのルートの一部の属性が、set コマンドによって設定された値で変更されます。一致基準が満たされないと、この句はルートに適用されず、ソフトウェアはルートマップの次の句でルート进行评估します。ルートマップのスキューン、ルートと一致する句が見つかるまで、もしくはルートマップの最後に到達するまで続行します。

次のいずれかの条件が満たされる場合は、各句の match 値または set 値を省略したり、何回か繰り返したりできます。

- 複数の match エントリが句に含まれる場合に、特定のルートが句に一致するためには、そのルートですべての照合に成功しなければなりません（つまり、複数の match コマンドでは論理 AND アルゴリズムが適用される）。
- match エントリが 1 つのエントリの複数のオブジェクトを指している場合は、そのいずれかが一致していなければなりません（論理 OR アルゴリズムが適用される）。
- match エントリがない場合は、すべてのルートが句に一致します。

- ルートマップの **permit** 句に **set** エントリが存在しない場合、ルートは、その現在の属性を変更されずに再配布されます。



---

(注) ルートマップの **deny** 句では **set** エントリを設定しないでください。 **deny** 句を指定するとルートの再配布が禁止され、情報が何も変更されないからです。

---

**match** エントリまたは **set** エントリがないルートマップ句はアクションを実行します。空の **permit** 句を使用すると、変更を加えずに残りのルートの再配布が可能になります。空の **deny** 句では、他のルートの再配布はできません。これは、ルートマップがすべてスキャンされたときに、明示的な一致が見つからなかったときのデフォルトアクションです。



## 第 33 章

# Firepower Threat Defense のスタティックルートとデフォルトルート

この章では、Firepower Threat Defense でスタティックルートとデフォルトルートを設定する方法について説明します。

- [スタティックルートとデフォルトルートについて \(793 ページ\)](#)
- [スタティックルートとデフォルトルートのガイドライン \(796 ページ\)](#)
- [スタティックルートの追加 \(796 ページ\)](#)

## スタティックルートとデフォルトルートについて

接続されていないホストまたはネットワークにトラフィックをルーティングするには、スタティックルーティングとダイナミックルーティングのどちらかを使用して、ホストまたはネットワークへのルートを定義する必要があります。通常は、少なくとも1つのスタティックルート、つまり、他の方法でデフォルトのネットワークゲートウェイにルーティングされていない、すべてのトラフィック用のデフォルトルート（通常、ネクストホップルータ）を設定する必要があります。

### デフォルトルート

最も単純なオプションは、すべてのトラフィックを上流に位置するルータに送信するようにデフォルトルートを設定して、トラフィックのルーティングをルータに任せることです。デフォルトルートは、ASA が既知のルートもスタティックルートも指定されていないすべての IP パケットを送信するゲートウェイ IP アドレスを特定します。デフォルトスタティックルートは、宛先 IP アドレスとして 0.0.0.0/0 が指定された単純なスタティックルートです。

### スタティックルート

次の場合は、スタティックルートを使用します。

- ネットワークがサポート対象外のルータ ディスカバリ プロトコルを使用している。

- ネットワークが小規模でスタティック ルートを容易に管理できる。
- ルーティング プロトコルが関係するトラフィックまたは CPU のオーバーヘッドをなくす必要がある。
- 場合によっては、デフォルトルートだけでは不十分である。デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティック ルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部の場合、デフォルトルートは、Firepower Threat Defense デバイスに直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。
- ダイナミック ルーティング プロトコルをサポートしていない機能を使用している。

## 不要なトラフィックを「ブラックホール化」するための null0 インターフェイスへのルート

アクセスルールを使用すると、ヘッダーに含まれている情報に基づいてパケットをフィルタ処理することができます。null0 インターフェイスへのスタティック ルートは、アクセスルールを補完するソリューションです。null0 ルートを使用して、不要なトラフィックや望ましくないトラフィックを「ブラックホール」に転送できるため、トラフィックがドロップされます。

スタティック null0 ルートには、推奨パフォーマンス プロファイルが割り当てられます。また、スタティック null0 ルートを使用して、ルーティング ループを回避することもできます。BGP では、リモート トリガ型ブラック ホールルーティングのためにスタティック null0 ルートを活用できます。

## ルートのプライオリティ

- 特定の宛先が特定されたルートはデフォルト ルートより優先されます。
- 宛先が同じルートが複数存在する場合（スタティックまたはダイナミック）、ルートのアドミニストレーティブディスタンスによってプライオリティが決まります。スタティック ルートは 1 に設定されるため、通常、それらが最もプライオリティの高いルートです。
- 宛先かつアドミニストレーティブ ディスタンスが同じスタティック ルートが複数存在する場合は、[ECMP ルーティング \(784 ページ\)](#) を参照してください。
- [トンネル化 (Tunneled) ] オプションを使用してトンネルから出力されるトラフィックの場合、このルートが他の設定済みルートまたは学習されたデフォルトルートをすべてオーバーライドします。

## トランスペアレント ファイアウォール モードのルート

ブリッジ グループ メンバー インターフェイスを通じて直接には接続されていないネットワークに向かう Firepower Threat Defense デバイス で発信されるトラフィックの場合、Firepower Threat Defense デバイス がどのブリッジ グループ メンバー インターフェイスからトラフィッ



クを送信するかを認識するように、デフォルト ルートまたはスタティック ルートを設定する必要があります。Firepower Threat Defense デバイス で発信されるトラフィックには、syslog サーバまたはSNMPサーバへの通信が含まれることもあります。1つのデフォルトルートで到達できないサーバがある場合、スタティックルートを設定する必要があります。トランスペアレントモードの場合、ゲートウェイインターフェイスとしてBVIを指定できません。つまり、メンバー インターフェイスのみを使用できます。詳細については、[MAC アドレスとルート ルックアップ \(643 ページ\)](#) を参照してください。

## スタティック ルート トラッキング

スタティックルートの問題の1つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。スタティック ルートは、ネクスト ホップ ゲートウェイが使用できなくなった場合でも、ルーティングテーブルに保持されています。スタティックルートの、Firepower Threat Defense デバイス 上の関連付けられたインターフェイスがダウンした場合に限りルーティング テーブルから削除されます。

スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリ ルートがダウンした場合のバックアップルートをインストールするための方式が用意されています。たとえば、ISPゲートウェイへのデフォルトルートを定義し、かつ、プライマリ ISP が使用できなくなった場合に備えて、セカンダリ ISP へのバックアップデフォルトルートを定義できます。

Firepower Threat Defense デバイス では、Firepower Threat Defense デバイス が ICMP エコー要求を使用してモニタする宛先ネットワーク上でモニタリング対象ホストにスタティックルートを関連付けることでスタティックルートトラッキングを実装します。指定された時間内にエコー応答がない場合は、そのホストはダウンしていると思われ、関連付けられたルートはルーティングテーブルから削除されます。削除されたルートに代わって、メトリックが高い追跡対象外のバックアップルートの使用されます。

モニタリング対象の選択時には、その対象が ICMP エコー要求に応答できることを確認してください。対象には任意のネットワークオブジェクトを選択できますが、次のものを使用することを検討する必要があります。

- ISP ゲートウェイ アドレス (デュアル ISP サポート用)
- ネクストホップゲートウェイアドレス (ゲートウェイの使用可能状況に懸念がある場合)
- Firepower Threat Defense デバイスが通信する必要のある対象ネットワーク上のサーバ (syslog サーバなど)
- 宛先ネットワーク上の永続的なネットワーク オブジェクト



(注) 夜間にシャットダウンする PC は適しません。

スタティック ルート トラッキングは、スタティックに定義されたルートや、DHCP または PPPoE を通じて取得したデフォルトルートに対して設定することができます。設定済みのルー

トトラッキングでは、複数のインターフェイス上の PPPoE クライアントだけを有効化することができます。

## スタティックルートとデフォルトルートのガイドライン

### ファイアウォールモードとブリッジグループ

- トランスペアレントモードでは、スタティックルートはブリッジグループメンバーインターフェイスをゲートウェイとして使用する必要があります。BVIを指定することはできません。
- スタティックルートトラッキングは、ブリッジグループメンバーインターフェイスをサポートされません。

### IPv6

- IPv6 では、スタティックルートトラッキングはサポートされません。

### クラスタリング

クラスタリングでは、スタティックルートモニタリングはプライマリユニットでのみサポートされます。

## スタティックルートの追加

スタティックルートは、特定の宛先ネットワークのトラフィックの送信先を定義します。少なくともデフォルトルートを定義する必要があります。デフォルトルートは、宛先 IP アドレスが 0.0.0.0/0 のスタティックルートです。

### 手順

- 
- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。
  - ステップ 2 [ルーティング (Routing)] タブをクリックします。
  - ステップ 3 コンテンツのテーブルから [スタティックルート (Static Route)] を選択します。
  - ステップ 4 [ルートを追加 (Add Routes)] をクリックします。
  - ステップ 5 追加するスタティックルートのタイプに応じて、[IPv4] または [IPv6] オプションボタンをクリックします。
  - ステップ 6 このスタティックルートを適用する [インターフェイス (Interface)] を選択します。

トランスペアレント モードの場合は、ブリッジグループのメンバー インターフェイスの名前を選択します。不要なトラフィックを「ブラック ホール化」するには、**Null0** インターフェイスを選択します。

- ステップ 7** [利用可能なネットワーク (Available Network) ]リストで、宛先ネットワークを選択します。デフォルト ルートを定義するには、アドレス 0.0.0.0/0 のオブジェクトを作成し、ここでそれを選択します。
- ステップ 8** [ゲートウェイ (Gateway) ]または [IPv6 ゲートウェイ (IPv6 Gateway) ]フィールドで、このルートのネクスト ホップであるゲートウェイ ルータを入力または選択します。IP アドレスまたはネットワーク/ホスト オブジェクトを指定できます。
- ステップ 9** [メトリック (Metric) ]フィールドに、宛先ネットワークへのホップの数を入力します。有効値の範囲は 1 ~ 255 で、デフォルト値は 1 です。メトリックは、特定のホストが存在するネットワークへのホップ数 (ホップ カウント) に基づくルートの「コスト」を示す測定値です。ホップ カウントは、ネットワーク パケットが最終的な宛先に到達するまでに通過する必要があるネットワークの数であり、宛先ネットワークも含まれます。メトリックは、複数のルーティングプロトコル間でルートを比較するために使用されます。スタティックルートのデフォルトのアドミニストレーティブ ディスタンスは 1 で、ダイナミック ルーティングプロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPF で検出されるルートのデフォルトのアドミニストレーティブ ディスタンスは 110 です。スタティック ルートとダイナミック ルートのアドミニストレーティブ ディスタンスが同じ場合、スタティック ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。
- ステップ 10** (任意) デフォルトルートの場合は、[トンネル型 (Tunneled) ]チェックボックスをオンにして、VPN トラフィック用に別個のデフォルト ルートを定義します。
- VPN トラフィックに非 VPN トラフィックとは別のデフォルト ルートを使用する必要がある場合は、VPN トラフィック用の別個のデフォルト ルートを定義できます。その場合、たとえば VPN 接続からの着信トラフィックは内部ネットワークに転送する一方、内部ネットワークからのトラフィックは外部に転送するといった設定を簡単に行うことができます。[トンネル型 (tunneled) ]オプションを使用してデフォルト ルートを作成すると、デバイスに着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティックルートをを使用してルーティングできない場合、このルートに送信されます。設定できるデフォルトのトンネルゲートウェイは、デバイスごとに 1 つのみです。トンネルトラフィックの ECMP はサポートされません。
- ステップ 11** (IPv4 スタティック ルートのみ) ルートの可用性をモニタするには、モニタリング ポリシーを定義する SLA (サービス レベル契約) モニタ オブジェクトの名前を [ルート トラッキング (Route Tracking) ]フィールドで入力または選択します。
- [SLA モニタ オブジェクト \(499 ページ\)](#) を参照してください。
- ステップ 12** [OK] をクリックします。





## 第 34 章

# Firepower Threat Defense 用の OSPF

この章では、Open Shortest Path First (OSPF) ルーティングプロトコルを使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Firepower Threat Defense を設定する方法について説明します。

- [Firepower Threat Defense 用の OSPF \(799 ページ\)](#)
- [OSPF のガイドライン \(803 ページ\)](#)
- [OSPFv2 の設定 \(804 ページ\)](#)
- [OSPFv3 の設定 \(818 ページ\)](#)

## Firepower Threat Defense 用の OSPF

この章では、Open Shortest Path First (OSPF) ルーティングプロトコルを使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Firepower Threat Defense を設定する方法について説明します。

### OSPF について

OSPF は、パスの選択にディスタンス ベクターではなくリンク ステートを使用する Interior Gateway Routing Protocol です。OSPF は、ルーティング テーブル更新ではなく、リンクステート アドバタイズメントを伝達します。ルーティング テーブル全体ではなく LSA だけが交換されるため、OSPF ネットワークは RIP ネットワークよりも迅速に収束します。

OSPF は、リンクステート アルゴリズムを使用して、すべての既知の接続先までの最短パスを構築し、計算します。OSPF エリア内の各ルータには、同一のリンクステート データベース (ルータが使用可能なインターフェイスおよび到達可能なネイバーの各一覧) が置かれています。

RIP と比べ OSPF には次の利点があります。

- OSPF では、リンクステート データベースの更新が RIP ほど頻繁に送信されません。また、ステート情報がタイムアウトすると、リンクステート データベースは徐々にではなく、すぐに更新されます。

- ルーティングはコスト、つまり特定のインターフェイスを介してパケットを送信するために必要なオーバーヘッドに基づいて決定されます。Firepower Threat Defense デバイスは、インターフェイスのコストをリンク帯域幅に基づいて計算し、接続先までのホップ数は使用しません。コストを設定して優先パスを指定することができます。

最短パスを優先するアルゴリズムの欠点は、CPU サイクルとメモリが大量に必要になることです。

Firepower Threat Defense デバイスは、OSPF プロトコルのプロセスを2つ同時に異なるインターフェイスセット上で実行できます。同じ IP アドレスを使用する複数のインターフェイス (NAT ではこのようなインターフェイスが共存可能ですが、OSPF ではアドレスは重複できません) がある場合に、2つのプロセスを実行できます。あるいは、一方のプロセスを内部で実行しながら別のプロセスを外部で実行し、ルートの子セットをこの2つのプロセス間で再配布することもできます。同様に、プライベートアドレスをパブリックアドレスから分離する必要がある場合もあります。

OSPF ルーティング プロセスには、別の OSPF ルーティング プロセスや RIP ルーティング プロセスから、または OSPF 対応インターフェイスに設定されているスタティックルートおよび接続ルートから、ルートを再配布できます。

Firepower Threat Defense デバイス では、次の OSPF の機能がサポートされています。

- エリア内ルート、エリア間ルート、および外部ルート (タイプ I とタイプ II) 。
- 仮想リンク。
- LSA フラッドイング。
- OSPF パケットの認証 (パスワード認証と MD5 認証の両方) 。
- Firepower Threat Defense デバイスの代表ルータまたはバックアップ代表ルータとしての設定。Firepower Threat Defense デバイスは、ABR として設定することもできます。
- スタブエリアと Not-So-Stubby Area。
- エリア境界ルータのタイプ 3 LSA フィルタリング。

OSPF は、MD5 およびクリアテキスト ネイバー認証をサポートします。OSPF と他のプロトコル (RIP など) の間のルート再配布にあたっては、攻撃者によるルーティング情報の悪用の可能性があるため、できる限りすべてのルーティングプロトコルで認証を行う必要があります。

NAT を使用していて、OSPF がパブリック エリアおよびプライベート エリアで動作している場合、またアドレス フィルタリングが必要な場合は、2つの OSPF プロセス (1つはパブリック エリア用、1つはプライベート エリア用) を実行する必要があります。

複数のエリアにインターフェイスを持つルータは、エリア境界ルータ (ABR) と呼ばれます。ゲートウェイとして動作し、OSPF を使用しているルータと他のルーティングプロトコルを使用しているルータ間でトラフィックを再配布するルータは、自律システム境界ルータ (ASBR) と呼ばれます。

ABR は LSA を使用して、使用可能なルートに関する情報を他の OSPF ルータに送信します。ABR タイプ 3 LSA フィルタリングを使用して、ABR として機能する ASA により、プライベ

トエリアとパブリックエリアを分けることができます。タイプ3LSA（エリア間ルート）は、プライベートネットワークをアドバタイズしなくても NAT と OSPF を一緒に使用できるように、1つのエリアから他のエリアにフィルタリングできます。



- (注) フィルタリングできるのはタイプ3LSAのみです。プライベートネットワーク内の ASBR として設定されている Firepower Threat Defense デバイスは、プライベートネットワークを記述するタイプ5LSAを送信しますが、これはAS全体（パブリックエリアも含む）にフラッドイングされます。

NATが採用されているが、OSPFがパブリックエリアだけで実行されている場合は、パブリックネットワークへのルートを、デフォルトまたはタイプ5AS外部LSAとしてプライベートネットワーク内で再配布できます。ただし、Firepower Threat Defense デバイスにより保護されているプライベートネットワークにはスタティックルートを設定する必要があります。また、同一の Firepower Threat Defense デバイス インターフェイス上で、パブリックネットワークとプライベートネットワークを混在させることはできません。

Firepower Threat Defense デバイスでは、2つの OSPF ルーティング プロセス（1つの RIP ルーティング プロセスと1つの EIGRP ルーティング プロセス）を同時に実行できます。

## fast hello パケットに対する OSPF のサポート

fast hello パケットに対する OSPF のサポートには、1秒未満のインターバルで hello パケットの送信を設定する方法が用意されています。このような設定により、Open Shortest Path First (OSPF) ネットワークでのコンバージェンスがより迅速になります。

### Fast Hello パケットに対する OSPF サポートの前提条件

OSPF がネットワークですでに設定されているか、Fast Hello パケット機能向けの OSPF のサポートと同時に設定される必要があります。

### OSPF Hello インターバルと dead 間隔

OSPF hello パケットとは、OSPF プロセスがネイバーとの接続を維持するために OSPF ネイバーに送信するパケットです。hello パケットは、設定可能なインターバル（秒単位）で送信されます。デフォルトのインターバルは、イーサネットリンクの場合 10 秒、ブロードキャスト以外のリンクの場合 30 秒です。hello パケットには、dead 間隔中に受信したすべてのネイバーのリストが含まれます。dead 間隔も設定可能なインターバル（秒単位）で送信されます。デフォルトは Hello インターバルの値の 4 倍です。Hello インターバルの値は、ネットワーク内ですべて同一にする必要があります。dead 間隔の値も、ネットワーク内ですべて同一にする必要があります。

この2つのインターバルは、リンクが動作していることを示すことにより、接続を維持するために連携して機能します。ルータが dead 間隔内にネイバーから hello パケットを受信しない場合、ルータはこのネイバーがダウンしていると判定します。

## OSPF fast hello パケット

OSPF fast hello パケットとは、1秒よりも短い間隔で送信される hello パケットのことです。fast hello パケットを理解するには、OSPF hello パケット インターバルと dead 間隔との関係についてあらかじめ理解しておく必要があります。[OSPF Hello インターバルと dead 間隔 \(801 ページ\)](#) を参照してください。

OSPF fast hello パケットは、`ospf dead-interval` コマンドで設定されます。dead 間隔は1秒に設定され、hello-multiplier の値は、その1秒間に送信する hello パケット数に設定されるため、1秒未満の「fast」hello パケットになります。

インターフェイスで fast hello パケットが設定されている場合、このインターフェイスから送出される hello パケットでアドバタイズされる Hello インターバルは0に設定されます。このインターフェイス経由で受信した hello パケットの Hello インターバルは無視されます。

dead 間隔は、1つのセグメント上で一貫している必要があります。1秒に設定するか（fast hello パケットの場合）、他の任意の値を設定します。dead 間隔内に少なくとも1つの hello パケットが送信される限り、hello multiplier がセグメント全体で同じである必要はありません。

## OSPF Fast Hello パケットの利点

OSPF Fast Hello パケット機能を利用すると、ネットワークがこの機能を使用しない場合よりも、コンバージェンス時間が短くなります。この機能によって、失われたネイバーを1秒以内に検出できるようになります。この機能は、ネイバーの損失がオープン システム相互接続 (OSI) 物理層またはデータリンク層で検出されないことがあっても、特に LAN セグメントで有効です。

## OSPFv2 および OSPFv3 間の実装の差異

OSPFv3 には、OSPFv2 との後方互換性はありません。OSPF を使用して、IPv4 および IPv6 トラフィックの両方をルーティングするには、OSPFv2 および OSPFv3 の両方を同時に実行する必要があります。これらは互いに共存しますが、相互に連携していません。

OSPFv3 では、次の追加機能が提供されます。

- リンクごとのプロトコル処理。
- アドレッシング セマンティックの削除。
- フラッドイング スコープの追加。
- リンクごとの複数インスタンスのサポート。
- ネイバー探索およびその他の機能に対する IPv6 リンクローカル アドレスの使用。
- プレフィックスおよびプレフィックス長として表される LSA。
- 2つの LSA タイプの追加。
- 未知の LSA タイプの処理。



- RFC-4552 で指定されている OSPFv3 ルーティング プロトコル トラフィックの IPsec ESP 標準を使用する認証サポート。

## OSPF のガイドライン

### ファイアウォール モードのガイドライン

OSPF は、ルーテッドファイアウォール モードのみをサポートしています。OSPF は、トランスパレント ファイアウォール モードをサポートしません。

### ハイ アベイラビリティ ガイドライン

OSPFv2 および OSPFv3 は、ステートフルハイ アベイラビリティ をサポートしています。

### IPv6 のガイドライン

- OSPFv2 は IPv6 をサポートしません。
- OSPFv3 は IPv6 をサポートしています。
- OSPFv3 は、IPv6 を使用して認証を行います。
- Firepower Threat Defense デバイス は、OSPFv3 ルートが最適なルートの場合、IPv6 RIB にこのルートをインストールします。

### クラスタリングのガイドライン

- OSPFv3 暗号化はサポートされていません。クラスタリング環境で OSPFv3 暗号化を設定しようとする、エラー メッセージが表示されます。
- スパンドインターフェイス モードでは、ダイナミック ルーティングは管理専用インターフェイスではサポートされません。
- クラスタでマスター ロールの変更が発生した場合、次の挙動が発生します。
  - スパンドインターフェイス モードでは、ルータ プロセスはマスターユニットでのみアクティブになり、スレーブ ユニットでは停止状態になります。コンフィギュレーションがマスターユニットと同期されているため、各クラスタユニットには同じルータ ID があります。その結果、隣接ルータはロール変更時のクラスタのルータ ID の変更を認識しません。

### マルチプロトコル ラベル スイッチング (MPLS) と OSPF のガイドライン

MPLS 設定ルータから送信されるリンク ステート (LS) アップデート パケットに、Opaque Type-10 リンクステートアドバタイズメント (LSA) が含まれており、この LSA に MPLS ヘッダーが含まれている場合、認証は失敗し、アプライアンスはアップデートパケットを確認せず

にサイレントにドロップします。ピアルータは確認応答を受信していないため、最終的にネイバー関係を終了します。

ネイバー関係の安定を維持するため、アプライアンスでノンストップフォワーディング (NSF) が無効であることを確認します。

- Firepower Management Center の [ノンストップ転送 (Non Stop Forwarding) ] タブに移動します ([デバイス (Devices) ] > [デバイス管理 (Device Management) ] (目的のデバイスを選択) > [ルーティング (Routing) ] > [OSPF] > [詳細設定 (Advanced) ] > [ノンストップ転送 (Non Stop Forwarding) ] ) 。

[ノンストップ転送機能 (Non Stop Forwarding Capability) ] のボックスがオンになっていないことを確認します。

### その他のガイドライン

- OSPFv2 および OSPFv3 は 1 つのインターフェイス上での複数インスタンスをサポートしています。
- OSPFv3 は、非クラスタ環境での ESP ヘッダーを介した暗号化をサポートしています。
- OSPFv3 は非ペイロード暗号化をサポートします。
- OSPFv2 は RFC 4811、4812 および 3623 でそれぞれ定義されている、Cisco NSF グレースフルリスタートおよび IETF NSF グレースフルリスタートメカニズムをサポートします。
- OSPFv3 は RFC 5187 で定義されているグレースフルリスタートメカニズムをサポートします。
- 配布可能なエリア内 (タイプ 1) ルートの数は限られています。これらのルートでは、1 つのタイプ 1 LSA にすべてのプレフィックスが含まれています。システムではパケットサイズが 35 KB に制限されているため、3000 ルートの場合、パケットがこの制限を超過します。2900 本のタイプ 1 ルートが、サポートされる最大数であると考えてください。

## OSPFv2 の設定

ここでは、OSPFv2 ルーティングプロセスの設定に関連するタスクについて説明します。

### OSPF エリア、範囲、仮想リンクの設定

認証の設定、スタブエリアの定義、デフォルトの集約ルートへの特定コストの割り当てが含まれる複数の OSPF エリア パラメータを設定できます。最大 2 つの OSPF プロセスインスタンスを有効にできます。各 OSPF プロセスには、独自のエリアとネットワークが関連付けられます。認証では、エリアへの不正アクセスに対してパスワードベースで保護します。

スタブエリアは、外部ルートの情報が送信されないエリアです。その代わりに、ABR で生成されるデフォルトの外部ルートがあり、このルートは自律システムの外部の宛先としてスタブ

エリアに送信されます。OSPF スタブ エリアのサポートを活用するには、デフォルトのルーティングをスタブ エリアで使用する必要があります。

#### 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ 2** [ルーティング (Routing) ] > [OSPF] を選択します。
- ステップ 3** [プロセス 1 (Process 1) ] を選択します。それぞれのコンテキストで最大 2 つの OSPF プロセスインスタンスを有効にできます。エリアパラメータを設定するには、OSPF プロセスを選択する必要があります。
- ステップ 4** OSPF の権限をドロップダウンリストから選択し、次のフィールドにそれぞれの説明を入力します。オプションは、[内部 (Internal) ]、[ABR]、[ASBR]、[ABR および ASBR (ABR and ASBR) ] です。OSPF の権限の説明については、[OSPF について \(799 ページ\)](#) を参照してください。
- ステップ 5** [エリア (Area) ] タブを選択し、[追加 (Add) ] をクリックします。
- エリアを切り取り、コピー、貼り付け、挿入、削除するには、編集アイコン (✎) をクリックするか、右クリックしてメニューを表示、選択します。
- ステップ 6** 以下のエリアのオプションを、それぞれの OSPF プロセスで設定します。
- [OSPF プロセス (OSPF Process) ] : 1 または 2 を選択します。
  - [エリア ID (Area ID) ] : ルートをサマライズするエリアの接続先。
  - [エリア タイプ (Area Type) ] : 次のいずれかを選択します。
    - [ノーマル (Normal) ] : (デフォルト) 標準 OSPF エリア。
    - [スタブ (Stub) ] : スタブ エリアには、その向こう側にルータまたはエリアはありません。スタブ エリアは、自律システム (AS) External LSA (タイプ 5 LSA) がスタブ エリアにフラッドイングされないようにします。スタブ エリアを作成すると、[サマリースタブ (Summary Stub) ] チェックボックスをオフにすることによって、集約 LSA (タイプ 3 および 4) がそのエリアにフラッドイングされるのを防ぐことができます。
    - [NSSA] : エリアを Not-So-Stubby Area にします。NSSA は、タイプ 7 LSA を受け入れます。[再配布 (Redistribute) ] チェックボックスをオフにし、[デフォルト情報起点 (Default Information Originate) ] チェックボックスをオンにすることで、ルートの再配布をディセーブルにすることができます。[集約 NSSA (Summary NSSA) ] チェックボックスをオフにすることによって、集約 LSA でエリアへのフラッドイングを防止できます。
  - [メトリック値 (Metric Value) ] : デフォルトルートの生成に使用するメトリックを指定します。デフォルト値は 10 です。有効なメトリック値の範囲は、0 ~ 16777214 です。

- [メトリック タイプ (Metric Type) ]: メトリック タイプは、OSPF ルーティング ドメイン にアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。
- [使用可能なネットワーク (Available Network) ]: 使用可能なネットワークのいずれかを選択して [追加 (Add) ] をクリックするか、追加アイコン (⊕) をクリックして新しいネットワーク オブジェクトを追加します。ネットワークの追加手順については、[ネットワーク オブジェクト \(433 ページ\)](#) を参照してください。
- [認証 (Authentication) ]: OSPF 認証を選択します。
  - [なし (None) ]: (デフォルト) OSPF エリアの認証を無効にします。
  - [パスワード (Password) ]: クリアテキストパスワードがエリア認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。
  - [MD5] : MD5 認証を許可します。
- [デフォルト コスト (Default Cost) ]: 接続先までの最短パスを割り出す OSPF エリアのデフォルトのコスト。有効な値の範囲は 0 ~ 65535 です。デフォルト値は 1 です。

**ステップ 7** [OK] をクリックして、エリア設定を保存します。

**ステップ 8** [範囲 (Range) ] タブを選択し、[追加 (Add) ] をクリックします。

- 使用可能なネットワークのいずれかを選択して、アドバタイズするかを決めます。
- または、追加アイコン (⊕) をクリックして、新しいネットワーク オブジェクトを加えます。ネットワークの追加手順については、[ネットワーク オブジェクト \(433 ページ\)](#) を参照してください。

**ステップ 9** [OK] をクリックして、範囲設定を保存します。

**ステップ 10** [仮想リンク (Virtual Link) ] タブを選択して、[追加 (Add) ] をクリックし、それぞれの OSPF プロセスに以下のオプションを設定します。

- [ピア ルータ (Peer Router) ]: ピア ルータの IP アドレスを選択します。新しいピア ルータを追加するには、追加アイコン (⊕) をクリックします。ネットワークの追加手順については、[ネットワーク オブジェクト \(433 ページ\)](#) を参照してください。
- [Hello 間隔 (Hello Interval) ]: hello パケットがインターフェイスで送信される秒単位の間隔です。hello 間隔は、hello パケットでアドバタイズされる符号なし整数です。値は、特定のネットワーク上のすべてのルータおよびアクセス サーバで同じにする必要があります。有効な値の範囲は 1 ~ 65535 です。デフォルトは 10 です。

hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。

- [送信遅延 (Transmit Delay) ] : インターフェイス上で LSA パケットを送信するのに必要な秒単位の予想時間です。ゼロよりも大きい整数値を指定します。有効な値の範囲は 1 ~ 8192 です。デフォルトは 1 です。

アップデート パケット内の LSA 自体の経過時間は、転送前にこの値の分だけ増分されません。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。

- [再送信間隔 (Retransmit Interval) ] : インターフェイスに属する隣接関係の LSA 再送信間の秒単位の時間です。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延より大きくなり、1 ~ 65535 の範囲で指定できます。デフォルトは 5 です。

ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータでは LSA を再送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

- [デッド間隔 (Dead Interval) ] : ルータがダウンしていることをネイバーが示す前に hello パケットを非表示にする秒単位の時間。Dead 間隔は符号なし整数です。デフォルトは hello 間隔の 4 倍または 40 秒です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバで同じであることが必要です。有効な値の範囲は 1 ~ 65535 です。

- [認証 (Authentication) ] : 以下から OSPF 仮想リンクの認証を選択します。

- [なし (None) ] : (デフォルト) 仮想リンク エリアの認証を無効にします。
- [エリア認証 (Area Authentication) ] : MD5 を使用して、エリア認証を有効にします。[追加 (Add) ] ボタンをクリックして、キー ID とキーを入力し、キーを確認し、[OK] をクリックします。
- [パスワード (Password) ] : クリアテキストパスワードが仮想リンクの認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。
- [MD5] : MD5 認証を許可します。[追加 (Add) ] ボタンをクリックして、キー ID とキーを入力し、キーを確認し、[OK] をクリックします。

**ステップ 11** [OK] をクリックして、仮想リンクの設定を保存します。

**ステップ 12** ルーティング ページで [保存 (Save) ] をクリックして変更を保存します。

## 次のタスク

[OSPF 再配布の設定](#) を続けます。

## OSPF 再配布の設定

Firepower Threat Defense デバイスは、OSPF ルーティング プロセス間のルート再配布を制御できます。1つのルーティング プロセスから OSPF ルーティング プロセスへの再配布ルートのルールが表示されます。RIP および BGP で検出されたルートを、OSPF ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、OSPF ルーティング プロセスに再配布できます。

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング (Routing)] > [OSPF] を選択します。

**ステップ 3** [再配布 (Redistribution)] タブを選択し、[追加 (Add)] をクリックします。

編集アイコン (✎) をクリックするか、右クリックメニューを使用して、エリアの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

**ステップ 4** OSPF プロセスごとに、次の再配布オプションを設定します。

- [OSPF プロセス (OSPF Process)] : 1 または 2 を選択します。
- [ルート タイプ (Route Type)] : 次のいずれかのタイプを選択します。
  - [スタティック (Static)] : スタティック ルートを OSPF ルーティング プロセスに再配布します。
  - [接続済み (Connected)] : 接続されたルート (インターフェイス上で IP アドレスを有効にすることによって自動的に確立されるルート) を OSPF ルーティング プロセスに再配布します。接続済みルートは、デバイスの外部として再配布されます。[オプション (Optional)] リストのサブネットを使用するかどうかを選択できます。
  - [OSPF] : 別の OSPF ルーティング プロセスからルートを再配布します (内部、外部 1 と 2、NSSA 外部 1 と 2、またはサブネットを使用するかどうか)。[オプション (Optional)] リストでこれらのオプションを選択できます。
  - [BGP] : BGP ルーティング プロセスからルートを再配布します。AS 番号およびサブネットを使用するかどうかを追加します。
  - [RIP] : RIP ルーティング プロセスからルートを再配布します。[オプション (Optional)] リストのサブネットを使用するかどうかを選択できます。
- [メトリック値 (Metric Value)] : 再配布するルートのメトリック値。デフォルト値は 10 です。有効な値の範囲は 0 ~ 16777214 です。

同じデバイス上で 1つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは1つのプロセスから他のプロセスへ存続します。

他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。

- [メトリック タイプ (Metric Type) ]: メトリック タイプは、OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。
- [タグ値 (Tag Value) ]: タグは 32 ビット 10 進数値を指定します。この値は、OSPF 自身では使用されないが ASBR 間の情報伝達に使用できる外部ルートのそれぞれに関連付けられます。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用されます。その他のプロトコルについては、ゼロが使用されます。有効な値は 0 ~ 4294967295 です。
- [RouteMap]: 送信元ルーティングプロトコルから現在のルーティングプロトコルへのルートのインポートのフィルタリングをチェックします。このパラメータを指定しない場合、すべてのルートが再配布されます。このパラメータを指定し、ルート マップ タグが表示されていない場合、ルートはインポートされません。または、追加アイコン (🟢) をクリックして新しいルートマップを追加できます。新しいルートマップの追加については、「[ルート マップ](#)」を参照してください。

**ステップ 5** [OK] をクリックして、再配布設定を保存します。

**ステップ 6** [ルーティング (Routing) ] ページで [保存 (Save) ] をクリックして変更を保存します。

#### 次のタスク

[OSPF エリア間フィルタリングの設定 \(809 ページ\)](#) に進みます。

## OSPF エリア間フィルタリングの設定

ABR のタイプ 3 LSA フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されているときは、指定されたプレフィックスのみが OSPF エリア間で送信されます。その他のすべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックス リストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。デフォルトでは、シーケンス番号は自動的に生成され、開始値は 5 で 5 ずつ増えていきます。

## 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、Firepower Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング (Routing) ] > [OSPF] を選択します。

**ステップ 3** [エリア間 (InterArea) ] タブを選択し、[追加 (Add) ] をクリックします。

編集アイコン (✎) をクリックするか、右クリックメニューを使用して、エリア間の切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

**ステップ 4** OSPF プロセスごとに、次のエリア間フィルタリング オプションを設定します。

- [OSPF プロセス (OSPF Process) ] : 1 または 2 を選択します。
- [エリア ID (Area ID) ] : ルートを要約するエリア。
- [PrefixList] : プレフィックスの名前。新しいプレフィックスリストオブジェクトを追加するには、ステップ 5 を参照してください。
- [トラフィックの方向 (Traffic Direction) ] : 着信または発信。OSPF エリアへの LSA をフィルタリングするには [着信 (Inbound) ] を選択し、OSPF エリアからの LSA をフィルタリングするには [発信 (Outbound) ] を選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。

**ステップ 5** 追加アイコン (+) をクリックして、新しいプレフィックスリストの名前と、オーバーライドを許可するかどうかを入力します。

プレフィックスルールを設定する前に、プレフィックスリストを設定する必要があります。

**ステップ 6** [追加 (Add) ] をクリックしてプレフィックスルールを設定し、次のパラメータを設定します。

- [アクション (Action) ] : 再配布アクセスに対して [ブロック (Block) ] または [許可 (Allow) ] を選択します。
- [シーケンス番号 (Sequence No) ] : ルーティングシーケンス番号。デフォルトでは、シーケンス番号は自動的に生成され、開始値は 5 で 5 ずつ増えていきます。
- [IP アドレス (IP Address) ] : プレフィックス番号を IP アドレス/マスク長の形式で指定します。
- [最小プレフィックス長 (Min Prefix Length) ] : (オプション) 最小のプレフィックス長。
- [最大プレフィックス長 (Max Prefix Length) ] : (オプション) 最大のプレフィックス長。

**ステップ 7** [OK] をクリックして、エリア間フィルタリング設定を保存します。

**ステップ 8** [ルーティング (Routing) ] ページで [保存 (Save) ] をクリックして変更を保存します。



### 次のタスク

[OSPF のフィルタ ルールの設定 \(811 ページ\)](#) に進みます。

## OSPF のフィルタ ルールの設定

OSPF プロセスごとに ABR タイプ 3 LSA フィルタを設定できます。ABR タイプ 3 LSA フィルタを設定すると、指定したプレフィックスだけが1つのエリアから別のエリアに送信され、その他のプレフィックスはすべて制限されます。このタイプのエリアフィルタリングは、特定の OSPF エリアから、特定の OSPF エリアへ、または同じ OSPF エリアへ同時に適用できます。OSPF ABR タイプ 3 LSA フィルタリングによって、OSPF エリア間のルート再配布の制御が向上します。

### 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、Firepower Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング (Routing) ] > [OSPF] を選択します。

**ステップ 3** [フィルタ ルール (Filter Rule) ] タブを選択し、[追加 (Add) ] をクリックします。

編集アイコン (✎) をクリックするか、右クリック メニューを使用して、フィルタ ルールの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

**ステップ 4** OSPF プロセスごとに、次のフィルタ ルール オプションを設定します。

- [OSPF プロセス (OSPF Process) ] : 1 または 2 を選択します。
- [アクセス リスト (Access List) ] : この OSPF プロセスのアクセス リスト。新しい標準アクセス リスト オブジェクトを追加するには、追加アイコン (+) をクリックし、[標準 ACL オブジェクトの設定 \(510 ページ\)](#) を参照してください。
- [トラフィックの方向 (Traffic Direction) ] : フィルタリングするトラフィックの方向として [イン (In) ] または [アウト (Out) ] を選択します。OSPF エリアへの LSA をフィルタリングするには [イン (In) ] を選択し、OSPF エリアからの LSA をフィルタリングするには [アウト (Out) ] を選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。
- [インターフェイス (Interface) ] : このフィルタ ルールのインターフェイス。

**ステップ 5** [OK] をクリックしてルール設定を保存します。

**ステップ 6** [ルーティング (Routing) ] ページで [保存 (Save) ] をクリックして変更を保存します。

### 次のタスク

[OSPF サマリー アドレスの設定 \(812 ページ\)](#) に進みます。

## OSPF サマリー アドレスの設定

他のプロトコルからのルートを OSPF に再配布する場合、各ルートは外部 LSA で個別にアドバタイズされます。ただし、再配布されるルートのうち、指定のネットワークアドレスとマスクに含まれるすべてのものを1つのルートで表し、そのルートだけをアドバタイズするように Firepower Threat Defense デバイスを設定することができます。この設定によって OSPF リンクステートデータベースのサイズが小さくなります。指定した IP アドレス マスク ペアと一致するルートは抑制できます。ルートマップで再配布を制御するために、タグ値を一致値として使用できます。

他のルーティングプロトコルから学習したルートをサマライズできます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。集約ルートは、ルーティング テーブルのサイズを削減するのに役立ちます。

OSPF の集約ルートを使用すると、OSPF ASBR は、そのアドレスでカバーされるすべての再配布ルートの集約として、1つの外部ルートをアドバタイズします。OSPF に再配布されている、他のルーティングプロトコルからのルートだけをサマライズできます。

### 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、Firepower Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング (Routing) ] > [OSPF] を選択します。

**ステップ 3** [サマリー アドレス (Summary Address) ] タブを選択し、[追加 (Add) ] をクリックします。

編集アイコン (✎) をクリックして編集するか、右クリック メニューを使用して、サマリーアドレスの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

**ステップ 4** OSPF プロセスごとに、次のサマリー アドレス オプションを設定します。

- [OSPF プロセス (OSPF Process) ] : 1 または 2 を選択します。
- [利用可能なネットワーク (Available Networks) ] : サマリーの IP アドレス。利用可能なネットワーク リストから 1 つを選択して [追加 (Add) ] をクリックするか、追加アイコン (+) をクリックして新しいネットワークを追加します。ネットワークを追加する手順については、[ネットワーク オブジェクト \(433 ページ\)](#) を参照してください。
- [タグ (Tag) ] : 各外部ルートに付加される 32 ビットの 10 進数値。この値は OSPF 自身には使用されませんが、ASBR 間の情報伝達に使用できます。
- [アドバタイズ (Advertise) ] : 集約ルートをアドバタイズします。サマリーアドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェック ボックスはオンになっています。

**ステップ 5** [OK] をクリックしてサマリー アドレス設定を保存します。

ステップ 6 [ルーティング (Routing)] ページで [保存 (Save)] をクリックして変更を保存します。

#### 次のタスク

[OSPF インターフェイスとネイバーの設定 \(813 ページ\)](#) に進みます。

## OSPF インターフェイスとネイバーの設定

必要に応じて一部のインターフェイス固有の OSPFv2 パラメータを変更できます。これらのパラメータを変更することは必須ではありませんが、hello インターバル、Dead 間隔、認証キーというインターフェイスパラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

ポイントツーポイントの非ブロードキャストネットワークを介して OSPFv2 ルートをアドバタイズするには、スタティック OSPFv2 ネイバーを定義する必要があります。この機能により、OSPFv2 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

#### 手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。

ステップ 2 [ルーティング (Routing)] > [OSPF] を選択します。

ステップ 3 [インターフェイス (Interface)] タブを選択し、[追加 (Add)] をクリックします。

編集アイコン (✎) をクリックするか、右クリックメニューを使用して、エリアの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 4 OSPF プロセスごとに、次のインターフェイス オプションを設定します。

- [インターフェイス (Interface)] : 設定するインターフェイス。
- [デフォルトコスト (Default Cost)] : インターフェイスを介したパケット送信のコスト。デフォルト値は 10 です。
- [優先順位 (Priority)] : ネットワークの代表ルータを指定します。有効な値の範囲は 0 ~ 255 です。デフォルト値は 1 です。この設定に 0 を入力すると、適切でないルータが指定ルータになったり、指定ルータのバックアップが行われたりします。

2 つのルータがネットワークに接続している場合、両方が指定ルータになろうとします。ルータ優先順位の高いデバイスが指定ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。この設定は、ポイントツーポイントのインターフェイスとして設定されているインターフェイスには適用されません。

- [MTU 無視 (MTU Ignore) ] : OSPF は、共通のインターフェイス上でネイバーが同一の MTU を使用しているかどうかをチェックします。このチェックは、ネイバーによる DBD パケットの交換時に行われます。DBD パケット内の受信した MTU が、受信インターフェイスに設定されている IP MTU より大きい場合は、OSPF 隣接関係は確立されません。
- [データベースフィルタ (Database Filter) ] : この設定は、同期とフラッディングのときに発信 LSA インターフェイスをフィルタリングするのに使用します。デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。完全メッシュ化トポロジでは、このフラッディングによって帯域幅が浪費されて、リンクおよび CPU の過剰使用につながることがあります。このチェックボックスをオンにすると、選択されているインターフェイスでは OSPF の LSA フラッディングが行われなくなります。
- [Hello 間隔 (Hello Interval) ] : インターフェイス上で送信される hello パケットの間隔を秒単位で指定します。有効な値の範囲は、1 ~ 8192 秒です。デフォルト値は 10 秒です。  
hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバで同じである必要があります。
- [伝送遅延 (Transmit Delay) ] : インターフェイス上で LSA パケットを送信するのに必要な予想時間 (秒単位) 。有効な値の範囲は、1 ~ 65535 秒です。デフォルト値は 1 秒です。  
更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。
- [再送信間隔 (Retransmit Interval) ] : インターフェイスに属する隣接関係の LSA 再送信間の時間 (秒単位) 。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効な値の範囲は、1 ~ 65535 秒です。デフォルトは 5 秒です。  
ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータでは LSA を再送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。
- [Dead 間隔 (Dead Interval) ] : hello パケットが確認されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間 (秒単位) 。この値はネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ~ 65535 秒です。
- [Hello 乗数 (Hello Multiplier) ] : 1 秒ごとに送信される hello パケットの数を指定します。有効な値は、3 ~ 20 です。
- [ポイント ツー ポイント (Point-to-Point) ] : VPN トンネルで OSPF ルートを送信できません。

- [認証 (Authentication)] : 認証アルゴリズムのタイプ。サポートされる値は、[SHA-1] および [MD5] です。[追加 (Add)] をクリックし、キー ID とキーを入力して、キーを確認します。
- [パスワードの入力 (Enter Password)] : 認証のタイプとして [パスワード (Password)] を選択した場合に、設定するパスワード。
- [パスワードの確認 (Confirm Password)] : 選択したパスワードを確認します。

**ステップ 5** [ネイバー (Neighbor)] タブを選択し、[追加 (Add)] をクリックします。

編集アイコン (✎) をクリックするか、右クリックメニューを使用して、エリアの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

**ステップ 6** OSPF プロセスごとに、次のパラメータを設定します。

- [OSPF プロセス (OSPF Process)] : 1 または 2 を選択します。
- [ネイバー (Neighbor)] : ドロップダウンリストでネイバーの 1 人を選択するか、追加アイコン (+) をクリックして新しいネイバーを追加します。名前、説明、ネットワーク、およびオーバーライドを許可するかどうかを入力し、[保存 (Save)] をクリックします。
- [インターフェイス (Interface)] : ネイバーに関連付けられたインターフェイスを選択します。

**ステップ 7** [OK] をクリックして、ネイバー設定を保存します。

**ステップ 8** [ルーティング (Routing)] ページで [保存 (Save)] をクリックして変更を保存します。

## OSPF 詳細プロパティの設定

[高度なプロパティ (Advanced Properties)] タブを使用すると、syslog メッセージ生成、アドミニストレーティブルートディスタンス、LSA タイマー、グレースフルリスタートなどのオプションを設定できます。

### グレースフルリスタート

Firepower Threat Defense デバイスでは、既知の障害状況が発生することがあります。これにより、スイッチングプラットフォーム全体でパケット転送に影響を与えることがあってはなりません。Non-Stop Forwarding (NSF) 機能では、ルーティングプロトコル情報を復元している間に、既知のルートへのデータ転送が続行されます。この機能は、スケジュール済みヒットレスソフトウェアアップグレードがあるときに便利です。NSF Cisco (RFC 4811 および RFC 4812) または NSF IETF (RFC 3623) のいずれかを使用して、OSPFv2 上でグレースフルリスタートを設定できます。



(注) NSF 機能は HA モードとクラスタリングでも役立ちます。

NSF グレースフルリスタート機能の設定には、機能の設定と NSF 対応または NSF 認識としてのデバイスの設定という2つのステップが伴います。NSF 対応デバイスは、ネイバーに対して独自のリスタート アクティビティを示すことができ、NSF 認識デバイスはネイバーのリスタートをサポートすることができます。

デバイスは、いくつかの条件に応じて、NSF 対応または NSF 認識として設定できます。

- デバイスは、現在のデバイスのモードに関係なく、NSF 認識デバイスとして設定できます。
- デバイスを NSF 対応として設定するには、デバイスはフェールオーバーまたはスパンド EtherChannel (L2) クラスタ モードのいずれかである必要があります。
- デバイスを NSF 認識または NSF 対応にするには、必要に応じて opaque リンク ステート アドバタイズメント (LSA) / リンク ローカル シグナリング (LLS) ブロックの機能を使って設定する必要があります。

## 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、Firepower Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング (Routing) ] > [OSPF] を選択し、[詳細 (Advanced) ] をクリックします。

**ステップ 3** [一般 (General) ] タブを選択し、次のように設定します。

- [ルータ ID (Router Id) ] : ルータ ID に [自動 (Automatic) ] または [IP アドレス (IP address) ] を選択します。[IP アドレス (IP address) ] を選択する場合は、[IP アドレス (IP Address) ] フィールドに IP アドレスを入力します。
- [LSA MOSPF を無視 (Ignore LSA MOSPF) ] : ルートがサポートされていない LSA タイプ 6 マルチキャスト OSPF (MOSPF) パケットを受信した場合、syslog メッセージを抑制します。
- [RFC 1583 互換 (RFC 1583 Compatible) ] : 集約ルートのコストを計算するための手段として RFC 1583 の互換性を設定します。RFC 1583 の互換性が有効な場合、ルーティンググループが発生することがあります。ルーティンググループを防止するには、これを無効にします。OSPF ルーティング ドメイン内のすべての OSPF ルータの RFC 互換設定が同じである必要があります。
- [隣接関係の変更 (Adjacency Changes) ] : syslog メッセージが送信される隣接関係の変更内容を定義します。

デフォルトでは、OSPF ネイバーがアップ状態またはダウン状態になったときに、syslog メッセージが生成されます。OSPF ネイバーがダウンしたときに syslog メッセージを送信するようルータを設定することも、状態ごとに syslog を送信するように設定することもできます。

- [隣接関係の変更のログ記録 (Log Adjacency Changes) ] : OSPF ネイバーが起動または停止したときに、Firepower Threat Defense デバイスによって syslog メッセージが送信されるようになります。この設定は、デフォルトでオンになっています。
- [隣接関係の変更の詳細のログ記録 (Log Adjacency Change Details) ] : ネイバーがアップ状態またはダウン状態になったときだけでなく、状態の変更が発生したときにも Firepower Threat Defense デバイスによって syslog メッセージが送信されるようになります。デフォルトでは、この設定はオフになっています。
- [アドミニストレーティブルートディスタンス (Administrative Route Distances) ] : エリア間、エリア内、および外部 IPv6 ルートのアドミニストレーティブルートディスタンスの設定に使用された設定を変更できます。アドミニストレーティブルートディスタンスは 1 ~ 254 の整数です。デフォルトは 110 です。
- [LSA グループ ペーシング (LSA Group Pacing) ] : LSA をグループにまとめてリフレッシュ、チェックサム計算、エージングする間隔を秒単位で指定します。有効な値の範囲は 10 ~ 1800 です。デフォルト値は 240 です。
- [デフォルト情報の発信を有効にする (Enable Default Information Originate) ] : デフォルトの外部ルートを OSPF ルーティングドメインに生成するには、[有効化 (Enable) ] チェックボックスをオンにして、次のオプションを設定します。
  - [デフォルト ルートを常にアドバタイズする (Always advertise the default route) ] : デフォルト ルートが常にアドバタイズされるようにします。
  - [メトリック (Metric) ] : デフォルト ルートを生成するために使用するメトリック。有効なメトリック値の範囲は、0 ~ 16777214 です。デフォルト値は 10 です。
  - [メトリック タイプ (Metric Type) ] : OSPFv3 ルーティングドメインにアドバタイズされるデフォルトルートに関連付けられた外部リンクタイプ。有効な値は 1 (タイプ 1 の外部ルート) および 2 (タイプ 2 の外部ルート) です。デフォルトはタイプ 2 外部ルートです。
  - [ルート マップ (Route Map) ] : ルート マップが満たされている場合にデフォルト ルートを生成するルーティングプロセスを選択するか、追加アイコン (+) をクリックして、新しいルーティングプロセスを追加します。新しいルート マップの追加については、「[ルート マップ](#)」を参照してください。

**ステップ 4** [OK] をクリックして、一般設定を保存します。

**ステップ 5** [Non Stop Forwarding] タブを選択し、NSF 対応または NSF 認識デバイスに対して、OSPFv2 の Cisco NSF グレースフルリスタートを設定します。

(注) OSPFv2 には、Cisco NSF と IETF NSF の 2 つのグレースフルリスタートメカニズムがあります。OSPF インスタンスに対しては、これらのグレースフルリスタートメカニズムのうち一度に設定できるのは 1 つだけです。NSF 認識デバイスは、Cisco NSF ヘルパーと IETF NSF ヘルパーの両方として設定できますが、NSF 対応デバイスは OSPF インスタンスに対して、Cisco NSF または IETF NSF モードのいずれかとして設定できます。

- a) [Cisco Non Stop Forwarding 機能を有効にする (Enable Cisco Non Stop Forwarding Capability) ] チェックボックスをオンにします。
- b) (オプション) 必要に応じて、[非 NSF 認識隣接ネットワークング デバイスが検出されたときに NSF リスタートをキャンセルする (Cancel NSF restart when non-NSF-aware neighboring networking devices are detected) ] チェックボックスをオンにします。
- c) (オプション) [Cisco Non Stop Forwarding ヘルパー モードを有効にする (Enable Cisco Non Stop Forwarding Helper mode) ] チェックボックスをオフにして、NSF 認識デバイスでのヘルパー モードを無効にします。

**ステップ 6** NSF 対応または NSF 認識デバイスに対して、OSPFv2 の IETF NSF グレースフルリスタートを設定します。

- a) [IETF Non Stop Forwarding 機能を有効にする (Enable IETF Non Stop Forwarding Capability) ] チェックボックスをオンにします。
- b) [グレースフルリスタート間隔 (秒) (Length of graceful restart interval (seconds)) ] フィールドにリスタート間隔を秒単位で入力します。デフォルト値は 120 秒です。30 秒以下のリスタート間隔の場合、グレースフルリスタートは終了します。
- c) (オプション) [ヘルパー モードの IETF Nonstop Forwarding (NSF) を有効にする (Enable IETF nonstop forwarding (NSF) for helper mode) ] チェックボックスをオフにして、NSF 認識デバイスでの IETF NSF ヘルパー モードを無効にします。
- d) [厳密なリンク ステートのアドバタイズメント チェックを有効にする (Enable Strict Link State advertisement checking) ] : 有効にすると、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフルリスタートプロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させます。
- e) [IETF Non Stop Forwarding を有効にする (Enable IETF Non Stop Forwarding) ] : スイッチオーバー後にルーティングプロトコル情報が復元される間、データのパケットの転送が既知のルートで続行される Non Stop Forwarding を有効にします。OSPF は OSPF プロトコルの拡張を使用して、隣接する OSPF デバイスからステートを回復します。リカバリが機能するためには、ネイバーが NSF プロトコル拡張をサポートし、再起動するデバイスの「ヘルパー」として積極的に動作する必要があります。ネイバーはまた、プロトコルステートのリカバリが行われる間、再起動するデバイスにデータトラフィックを転送し続ける必要があります。

## OSPFv3 の設定

ここでは、OSPFv3 ルーティングプロセスの設定に関連するタスクについて説明します。

### OSPFv3 エリア、ルート集約、および仮想リンクの設定

OSPFv3 を有効にするには、OSPFv3 ルーティングプロセスを作成し、OSPFv3 用のエリアを作成して、OSPFv3 のインターフェイスを有効にする必要があります。その後、ターゲットの OSPFv3 ルーティングプロセスにルートを再配布する必要があります。



## 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ 2** [ルーティング (Routing) ] > [OSPFv3] を選択します。
- ステップ 3** デフォルトでは、[プロセス 1 を有効にする (Enable Process 1) ] が選択されています。最大 2 つの OSPF プロセス インスタンスを有効にできます。
- ステップ 4** OSPFv3 ロールをドロップダウンリストから選択し、それに対応する説明を入力します。オプションは、[内部 (Internal) ]、[ABR]、[ASBR]、[ABR および ASBR (ABR and ASBR) ] です。OSPFv3 ロールの説明については、[OSPF について \(799 ページ\)](#) を参照してください。
- ステップ 5** [エリア (Area) ] タブを選択し、[追加 (Add) ] をクリックします。
- 編集アイコン (✎) をクリックするか、右クリックメニューを使用して、エリアの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。
- ステップ 6** [一般 (General) ] タブを選択し、各 OSPF プロセスについて次のオプションを設定します。
- [エリア ID (Area ID) ] : ルートを要約するエリア。
  - [Cost (コスト) ] : この集約ルートのメトリックまたはコスト。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効な値の範囲は 0 ~ 16777215 です。
  - [タイプ (Type) ] : [標準 (Normal) ]、[NSSA]、[スタブ (Stub) ] を指定します。[標準 (Normal) ] を選択した場合、設定するその他のパラメータはありません。[スタブ (Stub) ] を選択した場合、エリアでサマリー LSA を送信することができます。[NSSA] を選択した場合、次の 3 つのオプションを設定できます。
    - [このエリアへのサマリー LSA の送信を許可する (Allow Sending summary LSA into this area) ] : エリアにサマリー LSA を送信することを許可します。
    - [標準および NSSA エリアにインポートルートを再配布する (Redistribute imports routes to normal and NSSA area) ] : 再配布でルートをスタブ エリアでなく標準エリアにインポートできるようになります。
    - [デフォルト情報生成 (Defaults information originate) ] : OSPFv3 ルーティング ドメインへのデフォルト外部ルートを生成します。
  - [メトリック (Metric) ] : デフォルトルートを生成するために使用するメトリック。デフォルト値は 10 です。有効なメトリック値の範囲は、0 ~ 16777214 です。
  - [メトリック タイプ (Metric Type) ] : メトリック タイプは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。
- ステップ 7** [OK] をクリックして、一般設定を保存します。

**ステップ 8** [ルート集約 (Route Summary)] タブを選択し、[ルート集約の追加 (Add Route Summary)] をクリックします。

編集アイコン (✎) をクリックするか、右クリックメニューを使用して、ルート集約の切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

**ステップ 9** OSPF プロセスごとに、次のルート集約オプションを設定します。

- [IPv6 プレフィックス/長さ (IPv6 Prefix/Length)] : IPv6 プレフィックス。新しいネットワーク オブジェクトを追加するには、追加アイコン (+) をクリックします。ネットワークを追加する手順については、[ネットワーク オブジェクト \(433 ページ\)](#) を参照してください。
- [コスト (Cost)] : この集約ルートのもトリックまたはコスト。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効な値の範囲は 0 ~ 16777215 です。
- [アドバタイズ (Advertise)] : 集約ルートアドバタイズします。サマリーアドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェックボックスはオンになっています。

**ステップ 10** [OK] をクリックして、ルート集約設定を保存します。

**ステップ 11** [仮想リンク (Virtual Link)] タブを選択し、[仮想リンクの追加 (Add Virtual Link)] をクリックして、各 OSPF プロセスについて次のオプションを設定します。

- [ピア ルータ ID (Peer RouterID)] : ピア ルータの IP アドレスを選択します。新しいネットワーク オブジェクトを追加するには、追加アイコン (+) をクリックします。ネットワークを追加する手順については、[ネットワーク オブジェクト \(433 ページ\)](#) を参照してください。
- [TTL セキュリティ (TTL Security)] : TTL セキュリティチェックを有効にします。このホップカウントの値は、1 ~ 254 の数値です。デフォルトは 1 です。  
OSPF は、IP ヘッダー存続可能時間 (TTL) の値が 255 の発信パケットを送信し、設定可能なしきい値よりも低い TTL 値の入力パケットを廃棄します。IP パケットを転送する各デバイスは TTL が低下するため、直接 (1 ホップ) 接続により受信されたパケットの TTL 値は 255 になります。2つのホップを通過するパケットの値は 254 というようになります。受信しきい値は、パケットが移動する可能性がある最大ホップ数で設定されます。
- [Dead 間隔 (Dead Interval)] : hello パケットが届かなかった場合にネイバーがルータのダウンを示すまでの時間 (秒単位)。デフォルトは hello 間隔の 4 倍または 40 秒です。有効な値の範囲は 1 ~ 65535 です。  
Dead 間隔は符号なし整数です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバで同じである必要があります。
- [Hello 間隔 (Hello Interval)] : hello パケットがインターフェイスで送信される間隔 (秒単位)。有効な値の範囲は 1 ~ 65535 です。デフォルトは 10 です。  
hello 間隔は、hello パケットでアドバタイズされる符号なし整数です。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバで同じである必要があります。

hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。

- [再転送間隔 (Retransmit Interval) ]: インターフェイスに属する隣接関係の LSA 再送信間の時間 (秒単位)。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延より大きくなり、1 ~ 65535 の範囲で指定できます。デフォルトは 5 です。

ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータでは LSA を再送します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

- [転送遅延 (Transmit Delay) ]: インターフェイス上で LSA パケットを送信するために必要と推定される時間 (秒単位)。ゼロよりも大きい整数値を指定します。有効な値の範囲は 1 ~ 8192 です。デフォルトは 1 です。

アップデート パケット内の LSA 自体の経過時間は、転送前にこの値の分だけ増分されません。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。

**ステップ 12** [OK] をクリックして、仮想リンク設定を保存します。

**ステップ 13** [ルータ (Router) ] ページで [保存 (Save) ] をクリックして変更を保存します。

---

### 次のタスク

[OSPFv3 再配布の設定](#) を続けます。

## OSPFv3 再配布の設定

Firepower Threat Defense デバイスは、OSPF ルーティング プロセス間のルート再配布を制御できます。1 つのルーティング プロセスから OSPF ルーティング プロセスへの再配布ルートのルールが表示されます。RIP および BGP で検出されたルートを、OSPF ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、OSPF ルーティング プロセスに再配布できます。

### 手順

---

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、Firepower Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング (Routing) ] > [OSPF] を選択します。

**ステップ 3** [再配布 (Redistribution) ] タブを選択し、[追加 (Add) ] をクリックします。

編集アイコン (✎) をクリックするか、右クリックメニューを使用して、エリアの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

**ステップ 4** OSPF プロセスごとに、次の再配布オプションを設定します。

- [ソース プロトコル (Source Protocol) ]: ルートの再配布元となるソース プロトコル。サポートされるプロトコルは、接続済み、OSPF、スタティック、BGPです。OSPFを選択した場合は、[プロセス ID (Process ID) ]フィールドにプロセス IDを入力する必要があります。BCPを選択した場合は、[AS 番号 (AS Number) ]フィールドに AS 番号を追加する必要があります。
- [メトリック (Metric) ]: 配布されるルートのメトリック値。 デフォルト値は 10 です。有効な値の範囲は 0 ~ 16777214 です。  
  
同じデバイス上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。
- [メトリック タイプ (Metric Type) ]: メトリック タイプは、OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。
- [タグ (Tag) ]: タグは 32 ビット 10 進数値を指定します。この値は、OSPF 自身では使用されないが ASBR 間の情報伝達に使用できる外部ルートのそれぞれに関連付けられます。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用されます。その他のプロトコルについては、ゼロが使用されます。有効な値は 0 ~ 4294967295 です。
- [ルート マップ (Route Map) ]: 送信元ルーティング プロトコルから現在のルーティング プロトコルへのルートのインポートのフィルタリングをチェックします。このパラメータを指定しない場合、すべてのルートが再配布されます。このパラメータを指定し、ルート マップタグが表示されていない場合、ルートはインポートされません。または、追加アイコン (⊕) をクリックして新しいルート マップを追加できます。新しいルート マップを追加する手順については、[ルート マップ \(504 ページ\)](#) を参照してください。
- [プロセス ID (Process ID) ]: OSPF プロセス ID。1 または 2。  
  
(注) プロセス ID が有効であると、OSPFv3 プロセスは別の OSPFv3 プロセスから認識したルートを再配布します。
- [一致 (Match) ]: OSPF ルートを他のルーティング ドメインに再配布できるようにします。
  - [内部 (Internal) ] は、特定の自律システムの内部にあるルートです。
  - [外部 1 (External 1) ] は、自律システムの外部であるが、OSPFv3 にタイプ 1 外部ルートとしてインポートされるルートです。

- [外部2 (External2)] は、自律システムの外部であるが、OSPFv3 にタイプ2 外部ルートとしてインポートされるルートです。
- [NSSA 外部1 (NSSA External 1)] は、自律システムの外部であるが、IPv6 用の NSSA の OSPFv3 にタイプ1 の外部ルートとしてインポートされるルートです。
- [NSSA 外部2 (NSSA External 2)] は、自律システムの外部であるが、IPv6 用の NSSA の OSPFv3 にタイプ2 の外部ルートとしてインポートされるルートです。

**ステップ 5** [OK] をクリックして、再配布設定を保存します。

**ステップ 6** [ルーティング (Routing)] ページで [保存 (Save)] をクリックして変更を保存します。

### 次のタスク

[OSPFv3 サマリー プレフィックスの設定 \(823 ページ\)](#) に進みます。

## OSPFv3 サマリー プレフィックスの設定

指定された IPv6 プレフィックスとマスクのペアに一致するルートをアドバタイズするように Firepower Threat Defense デバイスを設定できます。

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング (Routing)] > [OSPFv3] を選択します。

**ステップ 3** [サマリー プレフィックス (Summary Prefix)] タブを選択し、[追加 (Add)] をクリックします。

編集アイコン (✎) をクリックするか、右クリックメニューを使用して、サマリープレフィックスの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

**ステップ 4** OSPF プロセスごとに、次のサマリープレフィックス オプションを設定します。

- [IPv6 プレフィックス/長さ (IPv6 Prefix/Length)] : IPv6 プレフィックスとプレフィックス長のラベル。リストから1つを選択するか、追加 (+) アイコンをクリックして新しいネットワークオブジェクトを追加します。ネットワークを追加する手順については、[ネットワークオブジェクト \(433 ページ\)](#) を参照してください。
- [アドバタイズ (Advertise)] : 指定されたプレフィックスとマスクのペアに一致するルートをアドバタイズします。このチェックボックスをオフにすると、指定されたプレフィックスとマスク ペアと一致するルートが抑制されます。
- (オプション) [タグ (Tag)] : ルートマップで再配布を制御するための「match」値として使用できるタグ値。

**ステップ 5** [OK] をクリックして、サマリープレフィックス設定を保存します。

**ステップ 6** [ルーティング (Routing)] ページで [保存 (Save)] をクリックして変更を保存します。

### 次のタスク

[OSPFv3 インターフェイス、認証、およびネイバーの設定 \(824 ページ\)](#) に進みます。

## OSPFv3 インターフェイス、認証、およびネイバーの設定

必要に応じて特定のインターフェイス固有の OSPFv3 パラメータを変更できます。これらのパラメータを必ずしも変更する必要はありませんが、hello interval と dead interval というインターフェイスパラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ 2** [ルーティング (Routing)] > [OSPFv3] を選択します。
- ステップ 3** [インターフェイス (Interface)] タブを選択し、[追加 (Add)] をクリックします。
- [鉛筆 (Pencil)] アイコンをクリックして編集するか、右クリックメニューを使用して、エリアの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。
- ステップ 4** 各 OSPFv3 プロセスについて、次のインターフェイス オプションを設定します。
- [インターフェイス (Interface)] : 設定するインターフェイス。
  - [OSPFv3 を有効にする (Enable OSPFv3)] : OSPFv3 を有効にします。
  - [OSPF プロセス (OSPF Process)] : 1 または 2 を選択します。
  - [エリア (Area)] : このプロセスのエリア ID。
  - [インスタンス (Instance)] : インターフェイスに割り当てるエリア インスタンス ID を指定します。インターフェイスは、OSPFv3 エリアを 1 つだけ保有できます。複数のインターフェイスで同じエリアを使用でき、各インターフェイスは異なるエリア インスタンス ID を使用できます。
- ステップ 5** [プロパティ (Properties)] タブを選択し、各 OSPFv3 プロセスについて次のオプションを設定します。
- [発信リンク ステート アドバタイズメントをフィルタ (Filter Outgoing Link Status Advertisements)] : OSPFv3 インターフェイスへの発信 LSA をフィルタ処理します。デフォルトでは、すべての発信 LSA がインターフェイスにフラッドされます。

- [MTU 不一致検出を無効にする (Disable MTU mismatch detection) ] : DBD パケットが受信された場合、OSPF MTU 不一致検出を無効にします。OSPF MTU 不一致検出は、デフォルトで有効になっています。
- [フラッドの削減 (Flood Reduction) ] : エリア全体で 3600 秒ごとにフラッディングしないように、標準の LSA を [LSA をエージングしない (Do Not Age LSAs) ] に変更します。  
OSPF LSA は 3600 秒ごとに更新されます。大規模な OSPF ネットワークでは、これにより大量の不要な LSA フラッディングがエリアからエリアに発生する可能性があります。
- [ポイントツーポイント ネットワーク (Point-to-Point Network) ] : OSPF ルートを VPN トンネル経由で送信できます。インターフェイスをポイントツーポイント、非ブロードキャストとして設定すると、次の制限が適用されます。
  - インターフェイスにはネイバーを 1 つだけ定義できます。
  - ネイバーは手動で設定する必要があります。
  - クリプト エンドポイントを指すスタティック ルートを定義する必要があります。
  - トンネル経由の OSPF がインターフェイスで実行中である場合は、アップストリーム ルータを使用する通常の OSPF を同じインターフェイス上で実行することはできません。
  - OSPF ネイバーを指定する前に、クリプト マップをインターフェイスにバインドする必要があります。これは、OSPF アップデートが VPN トンネルを通過できるようにするためです。OSPF ネイバーを指定した後でクリプト マップをインターフェイスにバインドした場合は、**clear local-host all** コマンドを使用して OSPF 接続をクリアします。これで、OSPF 隣接関係を VPN トンネル経由で確立できるようになります。
- [ブロードキャスト (Broadcast) ] : インターフェイスがブロードキャストインターフェイスであることを指定します。デフォルトでは、イーサネットインターフェイスの場合はこのチェックボックスがオンになっています。このチェックボックスをオフにすると、インターフェイスをポイントツーポイントの非ブロードキャストインターフェイスとして指定したことになります。インターフェイスをポイントツーポイントの非ブロードキャストとして指定すると、OSPF ルートを VPN トンネル経由で送信できます。
- [コスト (Cost) ] : インターフェイスでパケットを送信するコストを指定します。この設定の有効値の範囲は 0 ~ 255 です。デフォルト値は 1 です。この設定に 0 を入力すると、適切でないルータが指定ルータになったり、指定ルータのバックアップが行われたりします。この設定は、ポイントツーポイントの非ブロードキャストインターフェイスとして設定されているインターフェイスには適用されません。  
2 つのルータがネットワークに接続している場合、両方が指定ルータになろうとします。ルータ優先順位の高いデバイスが指定ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。
- [優先順位 (Priority) ] : ネットワークの代表ルータを指定します。有効な値の範囲は 0 ~ 255 です。

- [Dead 間隔 (Dead Interval) ] : hello パケットが確認されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間 (秒単位)。この値はネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ~ 65535 です。
- [ポーリング間隔 (Poll Interval) ] : ネイバーとの隣接関係が確立される前にルータが送信する OSPF パケット間の期間 (秒単位)。ルーティングデバイスがアクティブなネイバーを検出すると、hello パケット間隔はポーリング間隔で指定された時間から Hello 間隔で指定された時間に変更されます。有効な値の範囲は、1 ~ 65535 秒です。
- [再送信間隔 (Retransmit Interval) ] : インターフェイスに属する隣接関係の LSA 再送信間の時間 (秒単位)。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効な値の範囲は、1 ~ 65535 秒です。デフォルトは 5 秒です。
- [転送遅延 (Transmit Delay) ] : インターフェイス上でリンクステート更新パケットを送信する予想時間 (秒単位)。有効な値の範囲は、1 ~ 65535 秒です。デフォルト値は 1 秒です。

**ステップ 6** [OK] をクリックして、プロパティ設定を保存します。

**ステップ 7** [認証 (Authentication) ] タブを選択し、各 OSPFv3 プロセスについて次のオプションを設定します。

- [タイプ (Type) ] : 認証のタイプ。使用可能なオプションは、[エリア (Area) ]、[インターフェイス (Interface) ]、[なし (None) ] です。[なし (None) ] オプションを選択すると、認証が行われません。
- [セキュリティパラメータインデックス (Security Parameters Index) ] : 256 ~ 4294967295 の数値。タイプとして [インターフェイス (Interface) ] を選択した場合、このオプションを設定します。
- [認証 (Authentication) ] : 認証アルゴリズムのタイプ。サポートされる値は、[SHA-1] および [MD5] です。タイプとして [インターフェイス (Interface) ] を選択した場合、このオプションを設定します。
- [認証キー (Authentication Key) ] : MD5 認証を使用する場合、キーの長さは 32 桁の 16 進数 (16 バイト) である必要があります。SHA-1 認証を使用する場合、キーの長さは 40 桁の 16 進数 (20 バイト) である必要があります。
- [認証キーを暗号化する (Encrypt Authentication Key) ] : 認証キーの暗号化を有効にします。
- [暗号化を含める (Include Encryption) ] : 暗号化を有効にします。
- [暗号化アルゴリズム (Encryption Algorithm) ] : 暗号化アルゴリズムのタイプ。サポートされる値は DES です。ヌルのエントリーは暗号化されません。[暗号化を含める (Include Encryption) ] を選択した場合、このオプションを設定します。
- [暗号化キー (Encryption Key) ] : 暗号キーを入力します。[暗号化を含める (Include Encryption) ] を選択した場合、このオプションを設定します。



- [キーを暗号化する (Encrypt Key) ] : キーを暗号化できるようにします。

**ステップ 8** [OK] をクリックして、認証設定を保存します。

**ステップ 9** [ネイバー (Neighbor) ] タブを選択し、[追加 (Add) ] をクリックして、各 OSPFv3 プロセスについて次のオプションを設定します。

- [リンク ローカルアドレス (Link Local Address) ] : スタティック ネイバーの IPv6 アドレス。
- [コスト (Cost) ] : コストを有効にします。アドバタイズする場合は、[コスト (Cost) ] フィールドにコストを入力し、[発信リンクステートアドバタイズメントをフィルタ (Filter Outgoing Link State Advertisements) ] をオンにします。
- (オプション) [ポーリング間隔 (Poll Interval) ] : ポーリング間隔を有効にします。[優先順位 (Priority) ] レベルと [ポーリング間隔 (Poll Interval) ] (秒単位) を入力します。

**ステップ 10** [追加 (Add) ] をクリックして、ネイバーを追加します。

**ステップ 11** [OK] をクリックして、インターフェイス設定を保存します。

## OSPFv3 詳細プロパティの設定

[高度なプロパティ (Advanced Properties) ] タブを使用すると、syslog メッセージ生成、アドミニストレーティブ ルート ディスタンス、パッシブ OSPFv3 ルーティング、LSA タイマー、グレースフル リスタートなどのオプションを設定できます。

### グレースフル リスタート

Firepower Threat Defense デバイスでは、既知の障害状況が発生することがあります。これにより、スイッチングプラットフォーム全体でパケット転送に影響を与えることがあってはなりません。Non-Stop Forwarding (NSF) 機能では、ルーティング プロトコル情報を復元している間に、既知のルートへのデータ転送が継続されます。この機能は、スケジュール済みヒットレス ソフトウェア アップグレードがあるときに便利です。グレースフル リスタート (RFC 5187) を使用して、OSPFv3 上でグレースフル リスタートを設定できます。



(注) NSF 機能は HA モードとクラスタリングでも役立ちます。

NSF グレースフル リスタート機能の設定には、機能の設定と NSF 対応または NSF 認識としてのデバイスの設定という 2 つのステップが伴います。NSF 対応デバイスは、ネイバーに対して独自のリスタート アクティビティを示すことができ、NSF 認識デバイスはネイバーのリスタートをサポートすることができます。

デバイスは、いくつかの条件に応じて、NSF 対応または NSF 認識として設定できます。

- デバイスは、現在のデバイスのモードに関係なく、NSF 認識デバイスとして設定できます。
- デバイスを NSF 対応として設定するには、デバイスはフェールオーバーまたはスパンド EtherChannel (L2) クラスタ モードのいずれかである必要があります。
- デバイスを NSF 認識または NSF 対応にするには、必要に応じて opaque リンク ステート アドバタイズメント (LSA) / リンク ローカル シグナリング (LLS) ブロックの機能を使って設定する必要があります。

## 手順

- 
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ 2** [ルーティング (Routing)] > [OSPFv3] を選択し、[詳細 (Advanced)] をクリックします。
- ステップ 3** [ルータ ID (Router ID)] には、[自動 (Automatic)] または [IP アドレス (IP address)] を選択します。[IP アドレス (IP address)] を選択する場合は、[IP アドレス (IP Address)] フィールドに IP アドレスを入力します。
- ステップ 4** ルートがサポートされていない LSA タイプ 6 Multicast OSPF (MOSPF) パケットを受信する場合に syslog メッセージを抑制するには、[LSA MOSPF を無視 (Ignore LSA MOSPF)] チェックボックスをオンにします。
- ステップ 5** [一般 (General)] タブを選択し、次のように設定します。
- [隣接関係の変更 (Adjacency Changes)] : syslog メッセージが送信される隣接関係の変更内容を定義します。  
デフォルトでは、OSPF ネイバーがアップ状態またはダウン状態になったときに、syslog メッセージが生成されます。OSPF ネイバーがダウンしたときに syslog メッセージを送信するようルータを設定することも、状態ごとに syslog を送信するように設定することもできます。
  - [隣接関係の変更 (Adjacency Changes)] : OSPF ネイバーが起動または停止したときに、Firepower Threat Defense デバイスによって syslog メッセージが送信されるようになります。この設定は、デフォルトでオンになっています。
  - [詳細を含める (Include Details)] : ネイバーがアップ状態またはダウン状態になったときだけでなく、状態の変更が発生したときにも Firepower Threat Defense デバイスによって syslog メッセージが送信されるようになります。デフォルトでは、この設定はオフになっています。
  - [アドミニストレーティブルート ディスタンス (Administrative Route Distances)] : エリア間、エリア内、および外部 IPv6 ルートのアドミニストレーティブルート ディスタンスの設定に使用された設定を変更できます。アドミニストレーティブルート ディスタンスは 1 ~ 254 の整数です。デフォルトは 110 です。

- [デフォルト情報の発信 (Default Information Originate) ] : デフォルトの外部ルートを OSPFv3 ルーティング ドメインに生成するには、[有効化 (Enable) ] チェックボックスをオンにして、次のオプションを設定します。
  - [常にアドバタイズする (Always Advertise) ] : デフォルト ルートが存在するかどうかにかかわらず、常にアドバタイズします。
  - [メトリック (Metric) ] : デフォルト ルートを生成するために使用するメトリック。有効なメトリック値の範囲は、0 ~ 16777214 です。デフォルト値は 10 です。
  - [メトリック タイプ (Metric Type) ] : OSPFv3 ルーティング ドメインにアドバタイズされるデフォルトルートに関連付けられた外部リンクタイプ。有効な値は1 (タイプ 1 の外部ルート) および 2 (タイプ 2 の外部ルート) です。デフォルトはタイプ 2 外部ルートです。
  - [ルート マップ (Route Map) ] : ルート マップが満たされている場合にデフォルト ルートを生成するルーティングプロセスを選択するか、追加アイコン (+) をクリックして、新しいルーティングプロセスを追加します。新しいルート マップを追加するには、[ルート マップ \(504 ページ\)](#) を参照してください。

**ステップ 6** [OK] をクリックして、一般設定を保存します。

**ステップ 7** [パッシブ インターフェイス (Passive Interfaces) ] タブを選択して、[使用可能なインターフェイス (Available Interfaces) ] リストからパッシブ OSPFv3 ルーティングを有効にするインターフェイスを選択し、[追加 (Add) ] をクリックして [選択したインターフェイス (Selected Interfaces) ] リストにこれらを移動します。

パッシブルーティングは、OSPFv3 ルーティング情報のアドバタイズメントの制御に有効であり、インターフェイスでの OSPFv3 ルーティング更新の送受信を無効にします。

**ステップ 8** [OK] をクリックしてパッシブ インターフェイス設定を保存します。

- ステップ 9** [タイマー (Timer) ] タブを選択し、次の LSA ペーシングと SPF 計算タイマーを設定します。
- [到着 (Arrival) ] : ネイバーから到着する同一 LSA の最短受信間隔をミリ秒単位で指定します。有効な範囲は 0 ~ 6000,000 ミリ秒です。デフォルトは 1000 ミリ秒です。
  - [フラッド ペーシング (Flood Pacing) ] : フラッディング キュー内の LSA が更新間にペーシング処理される時間を指定します (ミリ秒単位) 。設定できる範囲は 5 ~ 100 ミリ秒です。デフォルト値は、33 ミリ秒です。
  - [グループ ペーシング (Group Pacing) ] : LSA をグループにまとめてリフレッシュ、チェックサム計算、エージングする間隔を秒単位で指定します。有効な値の範囲は 10 ~ 1800 です。デフォルト値は 240 です。
  - [再送信ペーシング (Retransmission Pacing) ] : 再送信キュー内の LSA がペースされる時間をミリ秒単位で指定します。設定できる範囲は 5 ~ 200 ミリ秒です。デフォルト値は、66 ミリ秒です。
  - [LSA スロットル (LSA Throttle) ] : LSA の最初のオカレンスを生成する遅延を指定します (ミリ秒単位) 。デフォルト値は、0 ミリ秒です。最小値は、同じ LSA を送信する最小

遅延をミリ秒単位で指定します。デフォルト値は、5000 ミリ秒です。最大値は、同じ LSA を送信する最大遅延をミリ秒単位で指定します。デフォルト値は、5000 ミリ秒です。

(注) LSA スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

• [SPF スロットル (SPF Throttle) ] : SPF 計算の変更を受信する遅延をミリ秒単位で指定します。デフォルト値は、5000 ミリ秒です。最小値は、最初と 2 番目の SPF 計算の間の遅延をミリ秒単位で指定します。デフォルト値は、10000 ミリ秒です。最大値は、SPF 計算の最大待機時間をミリ秒単位で指定します。デフォルト値は、10000 ミリ秒です。

(注) SPF スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

**ステップ 10** [OK] をクリックして LSA タイマー設定を保存します。

**ステップ 11** [Non Stop Forwarding] タブを選択し、[グレースフルリスタートヘルパーを有効にする (Enable graceful-restart helper) ] チェックボックスをオンにします。このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスでグレースフルリスタートヘルパーモードを無効にするには、このチェックボックスをオフにします。

**ステップ 12** [リンクステートアドバタイズメントを有効にする (Enable link state advertisement) ] チェックボックスをオンにして、厳密なリンクステートアドバタイズメントチェックを有効にします。

有効にすると、再起動ルータにフラグディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフルリスタートプロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパールータはルータの再起動プロセスを終了させることを示します。

**ステップ 13** [グレースフルリスタートを有効にする (スパンドクラスタまたはフェールオーバーが設定されている場合に使用) (Enable graceful-restart (Use when Spanned Cluster or Failover Configured)) ] をオンにして、グレースフルリスタート間隔を秒単位で入力します。範囲は 1 ~ 1800 です。デフォルト値は 120 秒です。30 秒未満の再起動間隔では、グレースフルリスタートが中断します。

**ステップ 14** [OK] をクリックしてグレースフルリスタート設定を保存します。

**ステップ 15** [ルーティング (Routing) ] ページで [保存 (Save) ] をクリックして変更を保存します。



## 第 35 章

# Firepower Threat Defense の BGP

この項では、Border Gateway Protocol (BGP) を使用してデータのルーティング、認証の実行、ルーティング情報の再配布を行うように Firepower Threat Defense を設定する方法について説明します。

- [BGP について \(831 ページ\)](#)
- [BGP のガイドライン \(835 ページ\)](#)
- [BGP の設定 \(835 ページ\)](#)

## BGP について

BGP は相互および内部の自律システムのルーティング プロトコルです。自律システムとは、共通の管理下にあり、共通のルーティング ポリシーを使用するネットワークまたはネットワーク グループです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー (ISP) 間で使用されるプロトコルです。

## ルーティング テーブルの変更

BGP ネイバーは、ネイバー間で最初に TCP 接続を確立する際に、完全なルーティング情報を交換します。ルーティングテーブルで変更が検出された場合、BGP ルータはネイバーに対し、変更されたルートのみを送信します。BGP ルータは、定期的にルーティング アップデートを送信しません。また BGP ルーティング アップデートは、宛先ネットワークに対する最適パスのアドバタイズのみを行います。

BGP により学習されたルートには、特定の宛先に対して複数のパスが存在する場合、宛先に対する最適なルートを決定するために使用されるプロパティが設定されています。これらのプロパティは BGP 属性と呼ばれ、ルート選択プロセスで使用されます。

- [重要度 (Weight) ]: これは、シスコ定義の属性で、ルータに対してローカルです。[重要度 (Weight) ] 属性は、隣接ルータにアドバタイズされません。ルータが同じ宛先への複数のルートがあることを学習すると、[重要度 (Weight) ] 属性値が最も大きいルートが優先されます。

- [ローカルプリファレンス (Local preference) ]: この属性は、ローカル AS からの出力点を選択するために使用されます。[重要度 (Weight) ]属性とは異なり、[ローカルプリファレンス (Local preference) ]属性は、ローカル AS 全体に伝搬されます。AS からの出力点が複数ある場合は、[ローカルプリファレンス (Local preference) ]属性値が最も高い出力点が特定のルートの出力点として使用されます。
- [Multi-Exit 識別子 (Multi-exit discriminator) ]: メトリック属性である Multi-Exit 識別子 (MED) は、メトリックをアドバタイズしている AS への優先ルートに関して、外部 AS への提案として使用されます。これが提案と呼ばれるのは、MEDを受信している外部 AS がルート選択の際に他の BGP 属性も使用している可能性があるためです。MED メトリックが小さい方のルートが優先されます。
- [発信元 (Origin) ]: この属性は、BGP が特定のルートについてどのように学習したかを示します。[発信元 (Origin) ]属性は、次の 3 つの値のいずれかに設定することができ、ルート選択に使用されます。
  - [IGP]: ルートは発信側 AS の内部にあります。この値は、ネットワーク ルータ コンフィギュレーションコマンドを使用して BGP にルートを挿入する際に設定されます。
  - [EGP]: ルートは Exterior Border Gateway Protocol (EBGP) を使用して学習されます。
  - [未完了 (Incomplete) ]: ルートの送信元が不明であるか、他の方法で学習されていません。未完了の発信元は、ルートが BGP に再配布される時に発生します。
- [AS\_path]: ルートアドバタイズメントが自律システムを通過すると、ルートアドバタイズメントが通過した AS 番号が AS 番号の順序付きリストに追加されます。AS\_path リストが最も短いルートのみ、IP ルーティングテーブルにインストールされます。
- [ネクストホップ (Next hop) ]: EBGP の [ネクストホップ (Next hop) ]属性は、アドバタイズしているルータに到達するために使用される IP アドレスです。EBGP ピアの場合、ネクストホップアドレスは、ピア間の接続の IP アドレスです。IBGP の場合、EBGP のネクストホップアドレスがローカル AS に伝送されます。
- [コミュニティ (Community) ]: この属性は、ルーティングの決定 (承認、優先度、再配布など) を適用できる宛先をグループ化する方法、つまりコミュニティを提供します。ルートマップは、[コミュニティ (Community) ]属性を設定するために使用されます。定義済みの [コミュニティ (Community) ]属性は次のとおりです。
  - [no-export]: EBGP ピアにこのルートをアドバタイズしません。
  - [no-advertise]: このルートをどのピアにもアドバタイズしない。
  - [インターネット (internet) ]: インターネットコミュニティにこのルートをアドバタイズします。ネットワーク内のすべてのルートがこのコミュニティに属します。

## BGP を使用する状況

大学や企業などの顧客ネットワークでは、そのネットワーク内でルーティング情報を交換するために OSPF などの内部ゲートウェイプロトコル (IGP) を通常使用しています。顧客は ISP

に接続し、ISP は BGP を使用して顧客のルートと ISP のルートを交換します。自律システム (AS) 間で BGP を使用する場合は、このプロトコルは外部 BGP (EBGP) と呼ばれます。サービスプロバイダーが BGP を使用して AS 内でルートを交換する場合は、このプロトコルは内部 BGP (IBGP) と呼ばれます。

BGP は、IPv6 ネットワーク上で IPv6 プレフィックスのルーティング情報を伝送するために使用することもできます。

## BGP パスの選択

BGP は、異なる送信元から同じルートの複数のアドバタイズメントを受信する場合があります。BGP はベストパスとして 1 つのパスだけを選択します。このパスを選択すると、BGP は IP ルーティングテーブルに選択したパスを格納し、そのネイバーにパスを伝搬します。BGP は次の基準を使用して (示されている順序で)、宛先へのパスを選択します。

- パスで指定されているネクストホップが到達不能な場合、この更新はドロップされます。
- ウェイトが最大のパスが優先されます。
- ウェイトが同じである場合、ローカルの優先順位が最大のパスが優先されます。
- ローカルの優先順位が同じである場合、このルータで動作している BGP により発信されたパスが優先されます。
- ルートが発信されていない場合、AS\_path が最短のルートが優先されます。
- すべてのパスの AS\_path の長さが同じである場合、起点タイプが最下位のパス ([IGP] は [EGP] よりも低く、[EGP] は [不完全 (Incomplete)] よりも低い) が優先されます。
- 起点コードが同じである場合、最も小さい MED 属性を持つパスが優先されます。
- パスの MED が同じである場合、内部パスより外部パスが優先されます。
- それでもパスが同じである場合、最も近い IGP ネイバーを経由するパスが優先されます。
- [BGP マルチパス \(833 ページ\)](#) のルーティングテーブルで、複数のパスのインストールが必要かどうかを判断します。
- 両方のパスが外部の場合、最初に受信したパス (最も古いパス) が優先されます。
- BGP ルータ ID で指定された、IP アドレスが最も小さいパスが優先されます。
- 送信元またはルータ ID が複数のパスで同じである場合、クラスタリストの長さが最小のパスが優先されます。
- 最も小さいネイバー アドレスから発信されたパスが優先されます。

## BGP マルチパス

BGP マルチパスでは、同一の宛先プレフィックスへの複数の等コスト BGP パスを IP ルーティングテーブルに組み込むことができます。その場合、宛先プレフィックスへのトラフィックは、組み込まれたすべてのパス間で共有されます。

これらのパスは、負荷共有のためのベストパスと共にテーブルに組み込まれます。BGP マルチパスは、ベストパスの選択には影響しません。たとえば、ルータは引き続き、アルゴリズムに従っていずれかのパスをベストパスとして指定し、このベストパスをルータの BGP ピアにアドバタイズします。

同一宛先へのパスをマルチパスの候補にするには、これらのパスの次の特性がベストパスと同等である必要があります。

- Weight
- ローカルプリファレンス
- AS-PATH の長さ
- オリジン コード
- Multi Exit Discriminator (MED)
- 次のいずれかです。
  - ネイバー AS またはサブ AS (BGP マルチパスの追加前)
  - AS-PATH (BGP マルチパスの追加後)

一部の BGP マルチパス機能では、マルチパス候補に要件が追加されます。

- パスは外部ネイバーまたは連合外部ネイバー (eBGP) から学習される必要があります。
- BGP ネクストホップへの IGP メトリックは、ベストパス IGP メトリックと同等である必要があります。

内部 BGP (iBGP) マルチパス候補の追加要件を次に示します。

- 内部ネイバー (iBGP) からパスが学習される必要があります。
- ルータが不等コスト iBGP マルチパス用に設定されていない限り、BGP ネクストホップへの IGP メトリックは、ベストパス IGP メトリックと同等です。

BGP はマルチパス候補から最近受信したパスのうち、最大  $n$  本のパスを IP ルーティングテーブルに挿入します。この  $n$  は、BGP マルチパスの設定時に指定した、ルーティングテーブルに組み込まれるルートの数です。マルチパスが無効な場合のデフォルト値は 1 です。

不等コストロードバランシングの場合、BGP リンク帯域幅も使用できます。



(注) 内部ピアへの転送前に、eBGP マルチパスで選択されたベストパスに対し、同等の next-hop-self が実行されます。



# BGP のガイドライン

## ファイアウォール モードのガイドライン

トランスペアレント ファイアウォール モードはサポートされません。BGP は、ルータ モードでのみサポートされています。

## IPv6 のガイドライン

IPv6 をサポートします。グレースフル リスタートは、IPv6 アドレス ファミリではサポートされません。

# BGP の設定

BGP を設定するには、以下のトピックを参照してください。

## 手順

- ステップ 1 [BGP 基本設定 \(835 ページ\)](#)
- ステップ 2 [BGP 一般設定 \(838 ページ\)](#)
- ステップ 3 [BGP ネイバーの設定 \(840 ページ\)](#)
- ステップ 4 [BGP 集約アドレス設定 \(845 ページ\)](#)
- ステップ 5 [BGPv4 フィルタリング設定 \(846 ページ\)](#)

(注) フィルタリング セクションは、IPv4 設定にのみ適用されます。

- ステップ 6 [BGP ネットワーク設定 \(847 ページ\)](#)
- ステップ 7 [BGP 再配布設定 \(847 ページ\)](#)
- ステップ 8 [BGP ルート注入の設定 \(848 ページ\)](#)

## BGP 基本設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

BGP の多くの基本設定が可能です。

## 手順

- 
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ 2** [ルーティング (Routing)] タブを選択します。
- ステップ 3** [BGP] を選択します。
- ステップ 4** [BGP を有効にする (Enable BGP)] チェックボックスを選択して、BGP ルーティング プロセスを有効にします。
- ステップ 5** [AS 番号 (AS Number)] フィールドに、BGP プロセスの自律システム (AS) 番号を入力します。AS 番号内部には、複数の自律番号が含まれます。AS 番号には、1 ~ 4294967295 または 1.0 ~ 65535.65535 を指定できます。AS 番号は固有に割り当てられた値であるため、インターネットの各ネットワークが識別されます。
- ステップ 6** (オプション) **General** でさまざまな BGP 設定を編集します。これらの設定のデフォルトはほとんどの場合で適切ですが、ネットワークのニーズに合わせて調整できます。[編集 (Edit)] (鉛筆) ボタンをクリックして、グループの設定を編集します。
- a) [ルータ ID (Router ID)] ドロップダウンリストで、[自動 (Automatic)] または [手動 (Manual)] を選択します。自動を選択すると、Firepower Threat Defense デバイス上で最上位の IP アドレスがルータ ID として使用されます。固定ルータ ID を使用するには、[手動 (Manual)] を選択して、[IP アドレス (IP Address)] フィールドに IPv4 アドレスを入力します。デフォルト値は [自動 (Automatic)] です。
  - b) [AS\_パス属性の AS 番号の数 (number of AS numbers in AS\_PATH attribute)] を入力します。AS パス属性は、移動パケットの最短ルートになる送信元と宛先のルータ間の中間 AS 番号のシーケンスです。有効な値は、1 ~ 254 です。デフォルト値は None です。
  - c) [ログ ネイバー変更 (Log Neighbor Changes)] チェックボックスをオンにして、BGP ネイバーの変更 (アップ状態またはダウン状態) およびリセットのログギングをイネーブルにします。これは、ネットワーク接続の問題をトラブルシューティングしたり、ネットワークの安定性を評価する際に役に立ちます。この設定はデフォルトで有効になっています。
  - d) [TCP パス MTU ディスカバリ使用 (Use TCP path MTU discovery)] チェックボックスをオンにし、パス MTU 手法を使用して 2 つの IP ホスト間のネットワークパスにおける最大伝送単位 (MTU) のサイズを決定します。これにより、IP フラグメンテーションが回避されます。この設定はデフォルトで有効になっています。
  - e) [フェールオーバー後すぐにセッションをリセット (Reset session upon Failover)] チェックボックスをオンにして、リンク障害の発生時に外部 BGP セッションをただちにリセットします。この設定はデフォルトで有効になっています。
  - f) [最初の AS を EBGП ルートのピアの AS として実行 (Enforce that first AS is peer's AS for EBGП routes)] チェックボックスをオンにして、その AS 番号を AS\_path 属性の 1 つ目のセグメントとしてリストしていない外部 BGP ピアから受信した着信アップデートを破棄します。これにより、誤って設定されたピアや許可されていないピアが、別の自律システムから送信されたかのようにルートをアドバイタイズしてトラフィックを誤った宛先に送信することがなくなります。この設定はデフォルトで有効になっています。
  - g) [AS 番号のドット表記を使用 (Use dot notation for AS numbers)] チェックボックスをオンにして、完全なバイナリ 4 バイトの AS 番号を、ドットで区切られた 16 ビットの 2 文字ず

つに分割します。0～65535のAS番号は10進数で表され、65535を超えるAS番号はドット付き表記を使用して表されます。これは、デフォルトでは無効になっています。

- h) [OK] をクリックします。

**ステップ7** (オプション) [ベストパス選択 (Best Path Selection)] セクションを編集します。

- a) [デフォルト ローカル優先度 (Default Local Preference)] で0～4294967295の値を入力します。デフォルト値は100です。値が大きいほど、優先度が高いことを示します。この優先度は、ローカル自律システム内のすべてのルータおよびアクセスサーバに送信されます。
- b) [異なるネイバーからのMED比較を許可 (Allow comparing MED from different neighbors)] チェックボックスをオンにして、さまざまな自律システムのネイバーからのパスにおいてMulti-exit discriminator (MED) の比較ができるようにします。これは、デフォルトでは無効になっています。
- c) [同一EBGPパスのルータIDを比較 (Compare Router ID for identical EBGP paths)] チェックボックスをオンにして、最適なパスの選択プロセス中に、外部BGPピアから受信した類似のパスを比較し、最適なパスをルータIDが最も小さいルートに切り替えます。これは、デフォルトでは無効になっています。
- d) [隣接するASがアドバタイズしたパス間の最適MEDを選別 (Pick the best MED path among paths advertised from the neighboring AS)] チェックボックスをオンにして、連合ピアから学習したパス間におけるMED比較を有効にします。MED間の比較は、外部の自律システムがパスに存在しない場合にのみ行われます。これは、デフォルトでは無効になっています。
- e) [欠落MEDを最低優先度として処理 (Treat missing MED as the least preferred one)] チェックボックスをオンにして、欠落しているMED属性は無限大の値を持つものとみなし、このパスを最も推奨度の低いパスにします。したがって、MEDが欠落しているパスが最も優先度が低くなります。これは、デフォルトでは無効になっています。
- f) [OK] をクリックします。

**ステップ8** (オプション) [ネイバータイマー (Neighbor Timers)] セクションを編集します。

- a) [キープアライブインターバル (Keepalive interval)] フィールドでキープアライブメッセージを送信しなかった場合に、その後BGPネイバーがアクティブな状態を維持する時間間隔を入力します。このキープアライブインターバルが終わると、メッセージが送信されない場合、BGPピアはデッドとして宣言されます。デフォルト値は60秒です。
- b) [維持時間 (Hold Time)] フィールドで、BGP接続が開始、設定されている間、BGPネイバーがアクティブな状態を維持する時間間隔を入力します。デフォルト値は180秒です。
- c) (オプション) [最小維持時間 (Min Hold time)] フィールドで、BGP接続が開始、設定されている間、BGPネイバーがアクティブな状態を維持する最小時間間隔を入力します。0～65535の値を指定します。
- d) [OK] をクリックします。

**ステップ9** (オプション) [グレースフルリスタート (Graceful Restart)] セクションを編集します。

- (注) このセクションは、Firepower Threat Defenseデバイスがフェールオーバーまたはスタンドクラスタモードになっているときのみ使用できます。フェールオーバー設定のデバイスの1つが失敗した場合に、トラフィックフローの packets でドロップがないように行われるものです。

- a) [グレースフルリスタートを有効にする (Enable Graceful Restart)] チェックボックスをオンにして、Firepower Threat Defense ピアがスイッチオーバー後のルートフラップを回避できるようにします。
- b) [リスタート時間 (Restart Time)] フィールドで BGP オープン メッセージが受信される前に、Firepower Threat Defense ピアが古いルート削除するまでの待機時間を入力します。デフォルト値は 120 秒です。有効な値は 1 ~ 3600 秒です。
- c) [Stalepath 時間 (Stalepath Time)] フィールドで、リスタートする Firepower Threat Defense から End Of Record (EOR) メッセージを受信した後、Firepower Threat Defense が古いルート削除するまでの待機時間を入力します。デフォルト値は 360 秒です。有効な値は 1 ~ 3600 秒です。
- d) [OK] をクリックします。

ステップ 10 [保存 (Save)] をクリックします。

## BGP 一般設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ルートマップ、アドミニストレーティブルートディスタンス、同期、ネクストホップ、パケット転送を設定します。これらの設定のデフォルトはほとんどの場合で適切ですが、ネットワークのニーズに合わせて調整できます。

### 手順

ステップ 1 [ルーティング (Routing)] > [BGP] > [IPv4] または [Ipv6] に進み、[一般 (General)] タブを選択します。

ステップ 2 [一般 (General)] タブで、次のセクションを更新します。

- a) [設定 (Settings)] セクションで、[ルートマップ (Route Map)] オブジェクトを入力または選択して、ネクストホップ検証用の BGP ルータの [スキャンインターバル (Scanning Interval)] を入力します。有効な値は 5 ~ 60 秒です。デフォルト値は 60 です。[OK] をクリックします。

(注) [ルートマップ (Route Map)] フィールドは、IPv4 設定にのみ適用されます。

- b) [ルートと同期化 (Routes and Synchronization)] セクションで、必要に応じて以下を更新し、[OK] をクリックします。

- (オプション) [デフォルト ルートの生成 (Generate Default Routes)] : これを選択して、デフォルトルート (ネットワーク 0.0.0.0) を配布するように BGP ルーティング プロセスを設定します。
  - (オプション) [サブネットルートのネットワーク レベルルートへの集約 (Summarize subnet routes into network-level routes)] : これを選択して、ネットワーク レベルのルートへのサブネットルートの自動集約を設定します。このチェックボックスを適用できるのは、IPv4 設定だけです。
  - (オプション) [非アクティブなルートのアドバタイズ (Advertise inactive routes)] : これを選択して、ルーティング情報ベース (RIB) にインストールされていないルートをアドバタイズします。
  - (オプション) [BGP と IGP システム間の同期化 (Synchronise between BGP and IGP system)] : これを選択して、BGP と内部ゲートウェイプロトコル (IGP) システムの間の同期を有効にします。通常、ルートがローカルであるか IGP に存在する場合を除き、BGP スピーカーは外部ネイバーにルートをアドバタイズしません。この機能により、自律システム内のルータおよびアクセス サーバは、BGP が他の自律システムでルートを使用可能にする前にルートを確保できるようになります。
  - (オプション) [IBGP の IGP への再配布 (Redistribute IBGP into IGP)] : これを選択して、OSPF などの内部ゲートウェイプロトコル (IGP) への iBGP の再配布を設定します。
- c) [アドミニストレーティブルート ディスタンス (Administrative Route Distances)] セクションで、必要に応じて以下を更新し、[OK] をクリックします。
- [外部 (External)] : 外部 BGP ルートのアドミニストレーティブ ディスタンスを入力します。外部自律システムから学習されたルートは、外部ルートです。この引数の値の範囲は 1 ~ 255 です。デフォルト値は 20 です。
  - [内部 (Internal)] : 内部 BGP ルートのアドミニストレーティブ ディスタンスを入力します。ローカル自律システムのピアから学習されたルートは、内部ルートです。この引数の値の範囲は 1 ~ 255 です。デフォルト値は 200 です。
  - [ローカル (Local)] : ローカル BGP ルートのアドミニストレーティブ ディスタンスを入力します。ローカルルートは、別のプロセスから再配布されているルータまたはネットワークの、多くの場合バック ドアとして、ネットワーク ルータ表示コマンドによりリストされるネットワークです。この引数の値の範囲は 1 ~ 255 です。デフォルト値は 200 です。
- d) [ネクスト ホップ (Next Hop)] セクションで、必要に応じて BGP ネクストホップ アドレスを有効にする [アドレス追跡を有効にする (Enable address tracking)] チェックボックスを選択し、ルーティング テーブルにインストールされた更新ネクストホップ ルートのチェックの間で [遅延インターバル (Delay Interval)] を入力します。[OK] をクリックします。
- (注) [ネクスト ホップ (Next Hop)] セクションは、IPv4 設定にのみ適用されます。

- e) [多重パスでパケットを転送 (Forward Packets over Multiple Paths)] セクションで、必要に応じて以下を更新し、[OK] をクリックします。
- (オプション) [パスの数 (Number of Paths)] : ルーティング テーブルにインストール可能な Border Gateway Protocol ルートの最大数を指定します。値の範囲は 1 ~ 8 です。デフォルト値は 1 です。
  - (オプション) [IBGP パスの数 (IBGP Number of Paths)] : ルーティング テーブルにインストール可能な並行内部ボーダー ゲートウェイ プロトコル (IBGP) ルートの最大数を指定します。値の範囲は 1 ~ 8 です。デフォルト値は 1 です。

ステップ 3 [保存 (Save)] をクリックします。

## BGP ネイバーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

BGP ルータは更新を交換する前に、各ピアとの接続を確立する必要があります。これらのピアは BGP ネイバーと呼ばれます。[ネイバー (Neighbor)] タブを使用して、BGP IPv4 または IPv6 ネイバーとネイバーの設定を定義します。

### 手順

- ステップ 1 [ルーティング (Routing)] > [BGP] > [IPv4] または [IPv6] を選択し、[ネイバー (Neighbor)] タブをクリックします。
- ステップ 2 [追加 (Add)] をクリックして、BGP ネイバーとネイバーの設定を定義します。
- ステップ 3 BGP ネイバーの IP アドレスを入力します。この IP アドレスは、BGP ネイバー テーブルに追加されます。
- ステップ 4 BGP ネイバーのインターフェイスを入力します。
- (注) [インターフェイス (Interface)] フィールドは、IPv6 の設定にのみ適用されます。
- ステップ 5 [リモート AS (Remote AS)] フィールドに、BGP ネイバーが属する自律システムを入力します。
- ステップ 6 [有効アドレス (Enabled address)] チェックボックスをオンにして、BGP ネイバーとの通信を有効にします。[有効アドレス (Enabled address)] チェックボックスがオンの場合にのみ、追加のネイバー設定が行われます。

- ステップ 7** (オプション) [管理シャットダウン (Shutdown administratively)] チェックボックスをオンにして、ネイバーまたはピア グループを無効化します。
- ステップ 8** (オプション) [グレースフルリスタートの設定 (Configure graceful restart)] チェックボックスをオンにして、このネイバーの BGP グレースフルリスタート機能の設定を有効にします。このオプションを選択した後、[グレースフルリスタート (フェールオーバー/スパンドモード) (Graceful Restart (failover/spanned mode))] オプションを使用して、このネイバーに対してグレースフルリスタートを有効にするか、または無効にするかを指定する必要があります。
- (注) [グレースフルリスタート (graceful restart)] フィールドは、IPv4 の設定にのみ適用されます。
- ステップ 9** (オプション) BGP ネイバーの説明を入力します。
- ステップ 10** (オプション) [ルートフィルタリング (Filtering Routes)] タブで、必要に応じてアクセスリスト、ルートマップ、プレフィックスリスト、および AS パスのフィルタを使用して、BGP ネイバー情報を配布します。次の各セクションを更新します。
- a) 適切な着信または発信 **アクセスリスト** を入力または選択して、BGP ネイバー情報を配布します。
- (注) アクセスリストは、IPv4 の設定にのみ適用されます。
- b) 適切な着信または発信 **ルートマップ** を入力または選択して、着信または発信ルートにルートマップを適用します。
- c) 適切な着信または発信 **プレフィックスリスト** を入力または選択して、BGP ネイバー情報を配布します。
- d) 適切な着信または発信 **AS パス フィルタ** を入力または選択して、BGP ネイバー情報を配布します。
- e) (オプション) [ネイバーから許可されるプレフィックスの数を制限する (Limit the number of prefixes allowed from the neighbor)] チェックボックスをオンにして、ネイバーから受信できるプレフィックスの数を制御します。
- [最大プレフィックス数 (Maximum Prefixes)] フィールドに、特定のネイバーからの許可される最大プレフィックス数を入力します。
  - [しきい値レベル (Threshold Level)] フィールドに、ルータが警告メッセージの生成を開始するパーセンテージ (最大数に対する割合) を入力します。有効な値は 1 ~ 100 の整数です。デフォルト値は 75 です。
- f) [ピアから受信したプレフィックスを制御する (Control prefixes received from the peer)] チェックボックスをオンにし、ピアから受信したプレフィックスに対する追加の制御を指定します。次のいずれかを実行します。
- プレフィックス数の制限値に到達したときに BGP ネイバーを停止するには、[プレフィックス数の制限値を超えたときにピアリングを停止する (Terminate peering when prefix limit is exceeded)] ラジオ ボタンを選択します。[再起動間隔 (Restart interval)] フィールドで、BGP ネイバーが再起動するまでの時間を指定します。

- 最大プレフィックス数の制限値を超えたときにログメッセージを生成するには、[プレフィックス数の制限値を超えたときに警告メッセージのみを表示する (Give only warning message when prefix limit is exceeded)] ラジオボタンを選択します。この場合、BGP ネイバーは終了しません。

g) [OK] をクリックします。

**ステップ 11** (オプション) [ルート (Routes)] タブで、その他のネイバー ルート パラメータを指定します。次を更新します。

- [アドバタイズメントの間隔 (Advertisement Interval)] フィールドに、BGP ルーティング アップデートが送信される最小間隔 (秒) を入力します。有効な値は、1 ~ 600 です。
- [発信ルーティング更新からプライベート AS 番号を削除する (Remove private AS numbers from outbound routing updates)] を選択して、プライベート AS 番号を発信ルートにおけるアドバタイズ対象から除外します。
- [デフォルトルートの生成 (Generate default routes)] チェックボックスをオンにして、ローカルルータにネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルトルートとして使用されるようにします。[ルートマップ (Route map)] フィールドで、ルート 0.0.0.0 が条件に応じて注入されるように許可するルートマップを入力または選択します。
- 条件に応じてアドバタイズされるルートを追加するには、[行を追加 (Add Row)] (+) ボタンをクリックします。[アドバタイズ対象ルートの追加 (Add Advertised Route)] ダイアログボックスで、次の手順を実行します。
  - [アドバタイズマップ (Advertise Map)] フィールドで、exist-map または非存在マップの条件が満たされた場合にアドバタイズされるルートマップを追加または選択します。
  - [exist-map (Exist Map)] ラジオボタンを選択し、[ルートマップオブジェクトセレクタ (Route Map Object Selector)] からルートマップを選択します。このルートマップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。
  - [非存在マップ (Non-Exist Map)] ラジオボタンを選択し、[ルートマップオブジェクトセレクタ (Route Map Object Selector)] からルートマップを選択します。このルートマップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。
  - [OK] をクリックします。

**ステップ 12** [タイマー (Timers)] タブで [BGP ピアの時間を設定する (Set Timers for the BGP Peer)] チェックボックスをオンにし、キープアライブ頻度、保留時間、最小保留時間を設定します。

- [キープアライブインターバル (Keepalive Interval)] : Firepower Threat Defense デバイスがキープアライブメッセージをネイバーに送信する頻度 (秒) を入力します。有効な値は、0 ~ 65535 です。デフォルト値は 60 秒です。



- [保留時間 (Hold time) ]: キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると Firepower Threat Defense デバイスが宣言するまでの時間 (秒) を入力します。有効な値は、0 ~ 65535 です。デフォルト値は 180 秒です。
- [最小保留時間 (Min hold time) ]: (オプション) キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると Firepower Threat Defense デバイスが宣言するまでの最小時間 (秒) を入力します。有効な値は、0 ~ 65535 です。デフォルト値は 0 秒です。

ステップ 13 [詳細 (Advanced) ] タブで、次を更新します。

- a) (オプション) [認証を有効にする (Enable Authentication) ] を選択して、2 つの BGP ピア間の TCP 接続で MD5 認証を有効にします。
  1. [暗号化を有効にする (Enable Encryption) ] ドロップダウンリストから暗号化タイプを選択します。
  2. パスワードを [パスワード (Password) ] フィールドに入力します。[確認 (Confirm) ] フィールドにパスワードを再入力します。パスワードは大文字と小文字を区別し、service password-encryption コマンドが有効な場合は最大 25 文字、service password-encryption コマンドが有効でない場合は最大 81 文字を指定できます。最初の文字を数値にはできません。この文字列には、スペースも含め、あらゆる英数字を使用できます。

(注) 数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。
- b) (オプション) [このネイバーにコミュニティ属性を送信する (Send Community attribute to this neighbor) ] チェックボックスをオンにして、コミュニティ属性を BGP ネイバーに送信することを指定します。
- c) (オプション) [このネイバーのネクスト ホップとして FTD を使用する (Use FTD as next hop for this neighbor) ] チェックボックスをオンにし、ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。
- d) [接続の検証を無効にする (Disable Connection Verification) ] チェックボックスをオンにして、シングルホップで到達可能な eBGP ピアリングセッションについての接続の検証プロセスを無効にします。これにより、ループバックインターフェイスで設定されたピアや直接接続されない IP アドレスが設定されたピアとの間でセッションを確立することができます。オフ (デフォルト) にすると、シングルホップ eBGP ピアリングセッション (TTL=254) について、BGP ルーティング プロセスで接続が検証され、eBGP ピアが同じネットワーク セグメントに直接接続されているかどうか確認されます。ピアが同じネットワーク セグメントに直接接続されていない場合、ピアリングセッションは確立されません。
- e) [直接接続されていないネイバーとの接続を許可する (Allow connections with neighbor that is not directly connected) ] ラジオ ボタンを選択して、直接接続されていないネットワーク上で外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。(オプション) [TTL ホップ (TTL hops) ] フィールドに存続可能時間を入力します。有効な値は、1 ~ 255 です。または、[ネイバーへの TTL ホップの制限数 (Limited number of TTL

hops to neighbor) ] ラジオ ボタンを選択して、BGP ピアリングセッションを保護します。  
[TTL ホップ (TTL hops) ] フィールドに、eBGP ピアを区切るホップの最大数を入力します。  
有効な値は、1 ~ 254 です。

- f) (オプション) [TCP MTU パス検出の使用 (Use TCP MTU path discovery) ] チェックボックスをオンにして、BGP セッションの TCP トランスポートセッションを有効にします。
- g) [TCP トランスポートモード (TCP Transport Mode) ] ドロップダウンリストから TCP 接続モードを選択します。オプションは [デフォルト (Default) ]、[アクティブ (Active) ]、または [パッシブ (Passive) ] です。
- h) (オプション) BGP ネイバー接続のウェイトを入力します。
- i) ドロップダウンリストから Firepower Threat Defense デバイスが受け入れる BGP バージョンを選択します。[4 のみ (4-Only) ] に設定すると、指定されたネイバーとの間でバージョン 4 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。

**ステップ 14** AS 移行を考慮する場合にのみ [移行 (Migration) ] タブを更新します。

(注) AS 移行カスタマイズは、遷移の完了後に削除される必要があります。

- a) (オプション) [ネイバーから受信したルートの AS 番号をカスタマイズする (Customize the AS number for routes received from the neighbor) ] チェックボックスをオンにして、eBGP ネイバーから受信したルートの AS\_path 属性をカスタマイズします。
- b) [ローカル AS 番号 (Local AS number) ] フィールドにローカル自律システム番号を入力します。有効な値は、1 ~ 4294967295 または 1.0 ~ 65535.65535 の有効な自律システム番号です。
- c) (オプション) [ローカル AS 番号をネイバーから受信したルートの前に付加しない (Do not prepend local AS number to routes received from neighbor) ] チェックボックスをオンにして、ローカル AS 番号が eBGP ピアから受信したルートの前に付加されないようにします。
- d) (オプション) [実 AS 番号をネイバーから受信したルートのローカル AS 番号に置き換える (Replace real AS number with local AS number in routes received from neighbor) ] チェックボックスをオンにして、実自律システム番号を eBGP 更新のローカル自律システム番号に置き換えます。ローカル BGP ルーティングプロセスからの自律システム番号は、追加されません。
- e) (オプション) [実 AS 番号またはネイバーから受信したルートのローカル AS 番号を受け入れる (Accept either real AS number or local AS number in routes received from neighbor) ] チェックボックスをオンにして、実自律システム番号 (ローカル BGP ルーティングプロセスより) またはローカル自律システム番号を使用するピアリングセッションを確立するように eBGP ネイバーを設定します。

**ステップ 15** [OK] をクリックします。

**ステップ 16** [保存 (Save) ] をクリックします。

## BGP 集約アドレス設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

BGP ネイバーはルーティング情報を格納し、交換しますが、設定される BGP スピーカーの数が増えるに従って、ルーティング情報の量が増えます。ルート集約は、複数の異なるルートの属性を合成し、1つのルートだけがアドバタイズされるようにするプロセスです。集約プレフィックスは、クラスレスドメイン間ルーティング (CIDR) の原則を使用して、複数の隣接するネットワークを、ルーティングテーブルに要約できる IP アドレスのクラスレスセット 1 つに合成します。結果として、アドバタイズの必要なルートは少なくなります。[集約アドレスの追加/編集 (Add/Edit Aggregate Address)] ダイアログボックスで、特定のルートの 1 つのルートへの集約を定義します。

### 手順

- ステップ 1 Firepower Threat Defense デバイスを編集する際、[ルーティング (Routing)] > [BGP] > [IPv4] または [IPv6] を選択して、[集約アドレス (Aggregate Address)] タブを選択します。
- ステップ 2 [集約アドレス (Aggregate Addresses)] タブをクリックします。
- ステップ 3 [集約タイマー (Aggregate Timer)] フィールドで、集約タイマーの値 (秒) を入力します。有効な値は、0 または 6 ~ 60 の値です。デフォルト値は 30 です。
- ステップ 4 [追加 (Add)] をクリックして、[集約アドレスの追加 (Add Aggregate Address)] ダイアログを更新します。
  - a) [ネットワーク (Network)] : IPv4 アドレスを入力するか、任意のネットワーク/ホスト オブジェクトを選択します。
  - b) [集約マップ (Attribute Map)] : (オプション) 集約ルートの属性の設定に使用されるルート マップを入力または選択します。
  - c) [アドバタイズマップ (Advertise Map)] : (オプション) AS 設定の元のコミュニティを作成するルートの選択に使用されるルート マップを入力または選択します。
  - d) [抑制マップ (Suppress Map)] : (オプション) 抑制するルートの選択に使用されるルート マップを入力または選択します。
  - e) [AS 設定パス情報の生成 (Generate AS set path Information)] : (オプション) 自律システム設定パス情報の生成を有効にするには、チェックボックスを選択します。
  - f) [更新から全ルートをフィルタ処理 (Filter all routes from updates)] : (オプション) 更新からのすべての特定のルートをフィルタ処理するには、チェックボックスを選択します。
  - g) [OK] をクリックします。

## 次のタスク

- BGPv4 設定については、次に進みます。 [BGPv4 フィルタリング設定 \(846 ページ\)](#)
- BGPv6 設定については、次に進みます。 [BGP ネットワーク設定 \(847 ページ\)](#)

## BGPv4 フィルタリング設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

フィルタリング設定は、受信される BGP 更新プログラムのフィルタ処理ルートまたはネットワークに使用されます。フィルタリングは、ルータが学習またはアドバタイズするルーティング情報を制限するために使用されます。

## 始める前に

フィルタリングは、BGP の IPv4 ルーティング ポリシーでのみ適用されます。

## 手順

- 
- ステップ 1** [ルーティング (Routing)] > [BGP] > [IPv4] を選択し、[フィルタリング (Filtering)] タブを選択します。
- ステップ 2** [追加 (Add)] をクリックして、[フィルタの追加 (Add Filter)] ダイアログを更新します。
- [アクセス リスト (Access List)] : 受信されるネットワークとルーティングアップデートで抑制されるネットワークを定義するアクセスコントロールリストを選択します。
  - [指示 (Direction)] : (オプション) インバウンド更新、アウトバウンド更新のどちらにフィルタを適用するかを指定する指示を選択します。
  - [プロトコル (Protocol)] : (オプション) なし、BGP、接続中、OSPF、RIP または静的のルーティングプロセスのうち、フィルタ処理するものを選択します。
  - [プロセス ID (Process ID)] : (オプション) OSPF ルーティング プロトコルのプロセス ID を入力します。
  - [OK] をクリックします。
- ステップ 3** [保存 (Save)] をクリックします。
-

## BGP ネットワーク設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ネットワーク設定は、BGPルーティングプロセスによってアダプタイズされるネットワーク、アダプタイズされるネットワークのフィルタ処理で確認されるルートマップを追加するために使用されます。

### 手順

**ステップ 1** [ルーティング (Routing)] > [BGP] > [IPv4] または [IPv6] に進み、[ネットワーク (Networks)] タブを選択します。

**ステップ 2** [追加 (Add)] をクリックして、[ネットワークの追加 (Add Networks)] ダイアログを更新します。

- a) [ネットワーク (Network)] : BGPルーティングプロセスによってアダプタイズされるネットワークを入力します。
- b) (オプション) [ルートマップ (Route Map)] : アダプタイズされるネットワークをフィルタ処理するために調べる必要のあるルートマップを入力または選択します。この値を指定しない場合、すべてのネットワークが再配布されます。
- c) [OK] をクリックします。

**ステップ 3** [保存 (Save)] をクリックします。

## BGP 再配布設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

再配布設定により、別のルーティングドメインから BGP にルートを再配布する条件を定義できます。

## 手順

- ステップ1 [ルーティング (Routing)] > [BGP > IPv4] または [IPv6] に進み、[再配布 (Redistribution)] タブを選択します。
- ステップ2 [追加 (Add)] をクリックして、[再配布の追加 (Add Redistribution)] ダイアログを更新します。
- [送信元プロトコル (Source Protocol)]: 送信元プロトコルドロップダウンリストから、どのプロトコルからルートを BGP ドメインに再配布するかを選択します。
  - [プロセス ID (Process ID)]: 選択されている送信元プロトコルの識別子を入力します。OSPF プロトコルに適用されます。
  - [メトリック (Metric)]: (オプション) 再配布されているルートのメトリックを入力します。
  - [ルートマップ (Route Map)]: 再配布されるネットワークをフィルタ処理するために調べる必要のあるルートマップを入力または選択します。この値を指定しない場合、すべてのネットワークが再配布されます。
  - [一致 (Match)]: 1 つのルーティング プロトコルから別のルーティング プロトコルへのルート再配布に使用される条件。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。これらのオプションは、OSPF が送信元プロトコルとして選択されているときにのみ有効になります。
    - 内線
    - 外部 1
    - 外部 2
    - NSSA 外部 1
    - NSSA 外部 2
  - f) [OK] をクリックします。

## BGP ルート注入の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ルート注入設定により、条件に応じて BGP ルーティング テーブルに注入されるルートを定義できます。

## 手順

---

- ステップ 1** [ルーティング (Routing)] > [BGP] > [IPv4] または [IPv6] を選択し、[ルート注入 (Route Injection)] タブを選択します。
- ステップ 2** [追加 (Add)] をクリックして、[ルート注入の追加 (Add Route Injection)] ダイアログを更新します。
- a) [マップ注入 (Inject Map)] : ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップを入力または選択します。
  - b) [マップ存在 (Exist Map)] : BGP スピーカーが追跡するプレフィックスを含むルート マップを入力または選択します。
  - c) [注入されたルートが集約ルートの属性を継承 (Injected routes will inherit the attributes of the aggregate route)] : これを選択し、集約ルートの属性を継承するよう注入されたルートを設定します。
  - d) [OK] をクリックします。
- ステップ 3** [保存 (Save)] をクリックします。
-







## 第 36 章

# Firepower Threat Defense 用の RIP

この章では、ルーティング情報プロトコル (RIP) を使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Firepower Threat Defense を設定する方法について説明します。

- [RIP について \(851 ページ\)](#)
- [RIP のガイドライン \(853 ページ\)](#)
- [RIP の設定 \(854 ページ\)](#)

## RIP について

RIP と呼ばれることが多い Routing Information Protocol は、すべてのルーティング プロトコルの中で最も堅牢なもの1つです。RIP には、ルーティング アップデート プロセス、RIP ルーティング メトリック、ルーティング 安定性、ルーティング タイマーの4つの基本的なコンポーネントがあります。RIP をサポートしているデバイスは、ルーティング アップデート メッセージを定期的に、またネットワーク トポロジが変更されたときに送信します。これらの RIP パケットには、デバイスが到達可能なネットワークに関する情報、さらに宛先アドレスに到達するためにパケットが通過しなければならないルータやゲートウェイの数が含まれています。RIP では、生成されるトラフィックは OSPF より多くなりますが、設定は OSPF より容易です。

RIP は、ホップ カウントをパス選択のメトリックとして使用するディスタンス ベクター ルーティング プロトコルです。インターフェイス上で RIP が有効になっている場合、インターフェイスは、ネイバー デバイスと RIP ブロードキャストを交換して、ルートの動的な学習およびアドバタイズを行います。

Firepower Threat Defense デバイスは、RIP バージョン 1 と RIP バージョン 2 の両方をサポートしています。RIP バージョン 1 では、ルーティング アップデートでサブネットマスクは送信されません。RIP バージョン 2 では、ルーティング アップデートでサブネットマスクが送信され、可変長サブネットマスクがサポートされています。さらに、RIP バージョン 2 では、ルーティング アップデートを交換するときのネイバー認証がサポートされています。この認証により、信頼性の高い送信元から信頼できるルーティング情報が Firepower Threat Defense デバイスで受信できるようになります。

RIP は、初期設定が簡単で、トポロジが変更されても設定を更新する必要がないため、スタティックルーティングより有利です。RIP の欠点は、スタティックルーティングよりネットワークや処理オーバーヘッドが大きいことです。

## ルーティングアップデートプロセス

RIP は、ルーティングアップデートメッセージを定期的送信するだけでなく、ネットワークトポロジが変更された場合にも送信します。ルータは、エントリーの変更が含まれるルーティングアップデートを受け取ると、新しいルートを反映するようにそのルーティングテーブルを更新します。パスのメトリック値は1ずつ大きくなり、送信者はネクストホップとして示されます。RIP ルータは、宛先に対する最適なルート（メトリック値が最も小さいルート）だけを保持します。ルータは、そのルーティングテーブルを更新した後、他のネットワークルータに変更を通知するために、ルーティングアップデートの送信をただちに開始します。これらのアップデートは、RIP ルータが送信する定期的スケジュールされたアップデートとは独立して送信されます。

## RIP のルーティングメトリック

RIP は、1つのルーティングメトリック（ホップカウント）を使用して発信元と宛先ネットワークとの距離を測定します。発信元から宛先までのパスの各ホップにはホップカウント値（通常は1）が割り当てられます。ルータが、新しいまたは変更された宛先ネットワークエントリーが含まれるルーティングアップデートを受け取ると、アップデートで示されたメトリック値に1を加算し、そのネットワークをルーティングテーブルに入れます。送信者のIPアドレスがネクストホップとして使用されます。

## RIP 安定性機能

RIP は、送信元から宛先へのパスで許可されるホップ数に制限を導入することにより、ルーティングループが無限に続くことを防止しています。パス内のホップの最大数は15です。新しいまたは変更されたエントリーが含まれるルーティングアップデートをルータが受信し、メトリック値に1を加えた結果、メトリックが無限（つまり16）になる場合は、ネットワークの宛先は到達不能と見なされます。この安定性機能の欠点は、この機能によってRIPネットワークの直径の最大値が16ホップ未満に制限されることです。

RIPには、その他にも、多くのルーティングプロトコルに共通の安定性機能がいくつか含まれます。ネットワークトポロジは急激に変化する可能性があります。これらの機能は、安定性を提供するように設計されています。たとえば、RIPでは、スプリットホライズンとホールddダウンメカニズムを実装して、間違ったルーティング情報が伝搬されることを防止しています。

## RIP タイマー

RIPでは、多数のタイマーを使用してそのパフォーマンスを調整しています。これらのタイマーには、ルーティングアップデートタイマー、ルートタイムアウトタイマー、ルートフラッ

シュタイマーがあります。ルーティングアップデートタイマーは、定期的なルーティングアップデートの間隔を測ります。通常は 30 秒に設定されており、タイマーがリセットされたときにはランダムな時間がわずかに追加されます。これは、すべてのルータがそのネイバーを同時にアップデートしようとした結果発生する輻輳を防ぐためです。ルーティングテーブルの各エントリには、ルートタイムアウト タイマーが関連付けられています。ルートタイムアウト タイマーが期限切れになると、ルートには無効のマークが付きますが、ルートフラッシュ タイマーが期限切れになるまではテーブル内に保持されます。

## RIP のガイドライン

### IPv6 のガイドライン

IPv6 はサポートされません。

### その他のガイドライン

次の情報は、RIP バージョン 2 だけに適用されます。

- ネイバー認証を使用する場合、認証キーとキー ID は、RIP バージョン 2 アップデートをそのインターフェイスに提供するすべてのネイバーデバイス上で同じにする必要があります。
- RIP バージョン 2 の場合、Firepower Threat Defense デバイスは、マルチキャストアドレス 224.0.0.9 を使用してデフォルト ルート アップデートを送受信します。パッシブ モードでは、そのアドレスでルート アップデートが受信されます。
- RIP バージョン 2 がインターフェイス上で設定されると、マルチキャストアドレス 224.0.0.9 がそのインターフェイス上で登録されます。RIP バージョン 2 設定がインターフェイスから削除されると、そのマルチキャストアドレスの登録は解除されます。

### 制限事項

- RIP アップデートは、Firepower Threat Defense デバイスのインターフェイス間を通過できません。
- RIP バージョン 1 では、可変長サブネット マスクがサポートされていません。
- RIP の最大ホップ カウントは 15 です。ホップ カウントが 15 を超えるルートは、到達不能と見なされます。
- RIP の収束は、他のルーティング プロトコルと比べて時間がかかります。
- Firepower Threat Defense デバイス では、RIP プロセスを 1 つだけイネーブルにできます。

# RIP の設定

RIP は、ホップ カウントをメトリックとして使用するディスタンスベクトルルーティング プロトコルです。

## 手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ 2 [ルーティング (Routing)] タブを選択します。
- ステップ 3 コンテンツ テーブルから [RIP] を選択します。
- ステップ 4 [RIP を有効にする (Enable RIP)] チェックボックスをオンにして、RIP を設定します。
- ステップ 5 [RIP バージョン (RIP Version)] ドロップダウン リストから、RIP の更新を送受信するための RIP バージョンを選択します。
- ステップ 6 (オプション) [デフォルト ルートの生成 (Generate Default Route)] チェックボックスをオンにして、指定したルート マップに基づく配布用のデフォルト ルートを生成します。
  - a) [ルート マップ (Route map)] フィールドで、デフォルト ルートの生成に使用するルート マップ名を指定します。

[ルート マップ (Route map)] フィールドで指定したルート マップが存在する場合、特定のインターフェイスで配布されるデフォルト ルート 0.0.0.0/0 が生成されます。
- ステップ 7 [RIP バージョン (RIP Version)] として [バージョン 2 の送受信 (Send and Receive Version 2)] を選択した場合、[自動集約の有効化 (Enable Auto Summary)] オプションが使用可能になります。[自動集約の有効化 (Enable Auto Summary)] チェックボックスをオンにすると、自動ルート集約が有効になります。切断されているサブネット間のルーティングを実行する必要がある場合は、自動サマライズを無効にします。自動サマライズを無効にすると、サブネットがアドバタイズされます。

(注) RIP バージョン 1 では、常に自動サマライズが使用されます。無効にすることはできません。
- ステップ 8 [ネットワーク (Networks)] タブをクリックします。RIP ルーティングに対して 1 つ以上のネットワークを定義します。IP アドレスを入力するか、目的のネットワーク/ホスト オブジェクトを入力または選択します。セキュリティアプライアンスの設定に追加できるネットワーク数に制限はありません。このコマンドで定義されるネットワークに属しているインターフェイスは、RIP ルーティング プロセスに参加します。RIP ルーティング更新は、指定したネットワークのインターフェイスだけを介して送受信されます。また、インターフェイスのネットワークを指定しない場合、インターフェイスは RIP 更新でアドバタイズされません。

(注) RIP では、IPv4 オブジェクトのみがサポートされます。
- ステップ 9 (オプション) [パッシブ インターフェイス (Passive Interfaces)] タブをクリックします。このオプションを使用して、アプライアンスでパッシブインターフェイスを指定してから、アク

タイプ インターフェイスを指定します。デバイスは、そのルーティング テーブルを入力するための情報を使用して、パッシブ インターフェイスでの RIP ルートのブロードキャストをリッスンしますが、パッシブ インターフェイスでのルーティング更新はブロードキャストしません。パッシブとして指定されていないインターフェイスは、更新を送受信します。

**ステップ 10** [再配布 (Redistribution) ] タブをクリックして、再配布ルートを管理します。これらは、他のルーティング プロセスから RIP ルーティング プロセスに再配布されているルートです。

- a) [追加 (Add) ] をクリックして、再配布ルートを指定します。
- b) [プロトコル (Protocol) ] ドロップダウン リストから、RIP ルーティング プロセスに再配布するルーティング プロトコルを選択します。

(注) OSPF プロトコルの場合は、プロセス ID を指定します。同様に、BGP の場合は AS パスとして指定します。[プロトコル (Protocol) ] ドロップダウン リストで [接続済み (Connected) ] オプションを選択すると、直接接続されたネットワークを RIP ルーティング プロセスに再配布できます。

- c) (オプション) OSPF ルートを RIP ルーティング プロセスに再配布する場合、[一致 (Match) ] ドロップダウン リストで、再配布する特定のタイプの OSPF ルートを選択できます。複数のタイプを選択するには、Ctrl を押しながらかlickします。

- [内部 (Internal) ] : 自律システム (AS) の内部のルートが再配布されます。
- [外部 1 (External 1) ] : AS に対して外部のタイプ 1 ルートが再配布されます。
- [外部 2 (External 2) ] : AS に対して外部のタイプ 2 ルートが再配布されます。
- [NSSA 外部 1 (NSSA External 1) ] : Not-So-Stubby Area (NSSA) の外部のタイプ 1 ルートが再配布されます。
- [NSSA 外部 2 (NSSA External 2) ] : NSSA に対して外部のタイプ 2 ルートが再配布されます。

(注) デフォルトの一致は、[内部 (Internal) ]、[外部 1 (External 1) ]、および [外部 2 (External 2) ] です。

- d) [メトリック (Metric) ] ドロップダウン リストから、再配布されたルートに適用する RIP メトリック タイプを選択します。選択肢は次の 2 つです。

- [トランスペアレント (Transparent) ] : 現在のルート メトリックを使用します。
- [指定値 (Specified Value) ] : 特定のメトリック値を割り当てます。[メトリック値 (Metric Value) ] フィールドに 0 ~ 16 の特定の値を入力します。
- [なし (None) ] : メトリックが指定されません。再配布されたルートに適用するメトリック値を使用しないでください。

- e) (オプション) [ルート マップ (Route Map) ] フィールドに、ルートが RIP ルーティング プロセスに再配布される前に満たす必要のあるルートマップの名前を指定します。ルートは、IP アドレスがルートマップ アドレス リストの許可文と一致する場合にのみ再配布されます。

f) [OK] をクリックします。

**ステップ 11** (オプション) [フィルタリング (Filtering)] タブをクリックして、RIP ポリシーのフィルタを管理します。このセクションでは、インターフェイスでのルーティング更新の回避、ルーティング更新でのルートのアドバタイズ制御、ルーティング更新の処理制御、およびルーティング更新の送信元フィルタリングに、フィルタを使用します。

a) [追加 (Add)] をクリックして、RIP フィルタを追加します。

b) [トラフィックの方向 (Traffic Direction)] フィールドでフィルタリングされるトラフィックのタイプ ([着信 (Inbound)] または [発信 (Outbound)]) を選択します。

(注) トラフィックの方向が着信の場合、インターフェイスフィルタだけを定義できません。

c) [フィルタ オン (Filter On)] フィールドで適切なラジオ ボタンを選択して、フィルタがインターフェイスまたはルートのいずれに基づくかを指定します。[インターフェイス (Interface)] を選択した場合、ルーティング更新がフィルタリングされるインターフェイスの名前を入力または選択します。[ルート (Route)] を選択した場合、ルートタイプを選択します。

- [スタティック (Static)] : スタティック ルートだけがフィルタリングされます。

- [接続済み (Connected)] : 接続されたルートだけがフィルタリングされます。

- [OSPF] : 指定した OSPF プロセスによって検出された OSPFv2 ルートだけがフィルタリングされます。フィルタリングされる OSPF プロセスの [プロセス ID (Process ID)] を入力します。

- [BGP] : 指定した BGP プロセスによって検出された BGPv4 ルートだけがフィルタリングされます。フィルタリングされる BGP プロセスの AS パスを入力します。

d) [アクセス リスト (Access List)] フィールドで、許可されるネットワークまたは RIP ルート アドバタイズメントから削除されるネットワークを定義する 1 つ以上のアクセス コントロール リスト (ACL) の名前を入力または選択します。

e) [OK] をクリックします。

**ステップ 12** (オプション) [ブロードキャスト (Broadcast)] タブをクリックして、インターフェイス設定を追加または編集します。[ブロードキャスト (Broadcast)] タブを使用して、インターフェイスごとに送受信するグローバル RIP バージョンをオーバーライドできます。また、有効な RIP アップデートを確認するための認証を実装する場合は、インターフェイスごとの認証パラメータを定義できます。

a) [追加 (Add)] をクリックして、インターフェイス設定を追加します。

b) [インターフェイス (Interface)] フィールドで、このアプライアンスで定義されるインターフェイスを入力または選択します。

c) [送信 (Send)] オプションで、該当するボックスを選択して、RIP バージョン 1、バージョン 2、または両方を使用して更新を送信するように指定します。これらのオプションを使用して、指定されたインターフェイスについて、指定したグローバルな送信バージョンをオーバーライドできます。

- d) [受信 (Receive) ] オプションで、該当するボックスを選択して、RIP バージョン 1、バージョン 2、または両方を使用して更新を受け入れるように指定します。これらのオプションを使用して、指定されたインターフェイスについて、指定したグローバルな受信バージョンをオーバーライドできます。
- e) RIP ブロードキャストに対してこのインターフェイスで使用される認証を選択します。
- [なし (None) ] : 認証はありません。
  - [MD5] : MD5 を使用します。
  - [クリア テキスト (Clear Text) ] : クリア テキスト認証を使用します。
- [MD5] または [クリア テキスト (Clear Text) ] を選択した場合、次の認証パラメータも指定する必要があります。
- [キー ID (Key ID) ] : 認証キーの ID。有効な値は 0 ~ 255 です。
  - [キー (Key) ] : 選択した認証方式で使用されるキー。最大 16 文字まで使用できます
  - [確認 (Confirm) ] : 確認のために、認証キーを再度入力します。
- f) [OK] をクリックします。
-







## 第 37 章

# Firepower Threat Defense 用のマルチキャストルーティング

この章では、マルチキャストルーティングプロトコルを使用するように Firepower Threat Defense デバイスを設定する方法について説明します。

- [マルチキャストルーティングについて \(859 ページ\)](#)
- [マルチキャストルーティングのガイドライン \(864 ページ\)](#)
- [IGMP 機能の設定 \(865 ページ\)](#)
- [PIM 機能の設定 \(871 ページ\)](#)
- [マルチキャストルートの設定 \(879 ページ\)](#)
- [マルチキャスト境界フィルタの設定 \(880 ページ\)](#)

## マルチキャストルーティングについて

マルチキャストルーティングは、単一の情報ストリームを数千もの企業や家庭に同時に配信することでトラフィックを軽減する帯域幅節約型のテクノロジーです。マルチキャストルーティングを活用するアプリケーションには、ビデオ会議、企業通信、遠隔学習に加えて、ソフトウェア、株価、およびニュースの配信などがあります。

マルチキャストルーティングプロトコルでは、競合テクノロジーのネットワーク帯域幅の使用量を最小限に抑えながら、送信元や受信者の負荷を増加させずに発信元のトラフィックを複数の受信者に配信します。マルチキャストパケットは、Protocol Independent Multicast (PIM) やサポートする他のマルチキャストプロトコルを使用した Firepower Threat Defense デバイスによりネットワークで複製されるため、複数の受信者にできる限り高い効率でデータを配信できます。

Firepower Threat Defense デバイスは、スタブマルチキャストルーティングと PIM マルチキャストルーティングの両方をサポートしています。ただし、1つの Firepower Threat Defense デバイスに両方を同時に設定することはできません。



- (注) マルチキャストルーティングでは、UDP トランスポートおよび非 UDP トランスポートの両方がサポートされます。ただし、非 UDP トランスポートでは FastPath 最適化は行われません。

## IGMP プロトコル

IP ホストは、Internet Group Management Protocol (IGMP) を使用して、そのグループメンバーシップを、直接接続されているマルチキャストルータに報告します。IGMP は、マルチキャストグループの個々のホストを特定の LAN にダイナミックに登録するために使用します。ホストは、そのローカルマルチキャストルータに IGMP メッセージを送信することで、グループメンバーシップを識別します。IGMP では、ルータは IGMP メッセージをリッスンし、定期的にクエリを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

IGMP は、グループアドレス (クラス D IP アドレス) をグループ識別子として使用します。ホストグループアドレスは、224.0.0.0 ~ 239.255.255.255 の範囲で使用できます。アドレス 224.0.0.0 がグループに割り当てられることはありません。アドレス 224.0.0.1 は、サブネットのシステムすべてに割り当てられます。アドレス 224.0.0.2 は、サブネットのルータすべてに割り当てられます。



- (注) Firepower Threat Defense デバイスでマルチキャストルーティングを有効にすると、IGMP バージョン 2 がすべてのインターフェイスで自動的に有効になります。

### マルチキャストグループへのクエリメッセージ

Firepower Threat Defense デバイスは、クエリメッセージを送信して、インターフェイスに接続されているネットワークにメンバーを持つマルチキャストグループを検出します。メンバーは、IGMP 報告メッセージで応答して、特定のグループに対するマルチキャストパケットの受信を希望していることを示します。クエリメッセージは、アドレスが 224.0.0.1 で存続可能時間値が 1 の全システムマルチキャストグループ宛に送信されます。

これらのメッセージが定期的送信されることにより、Firepower Threat Defense デバイスに保存されているメンバーシップ情報が更新されます。Firepower Threat Defense デバイスで、ローカルメンバーがいなくなったマルチキャストグループがまだインターフェイスに接続されていることがわかると、そのグループへのマルチキャストパケットを接続されているネットワークに転送するのを停止し、そのパケットの送信元にプルーニングメッセージを戻します。

デフォルトでは、サブネット上の PIM 代表ルータがクエリメッセージの送信を担当します。このメッセージは、デフォルトでは 125 秒間に 1 回送信されます。

クエリ応答時間を変更する場合は、IGMP クエリでアドバタイズする最大クエリ応答所要時間はデフォルトで 10 秒になります。Firepower Threat Defense デバイスがこの時間内にホストクエリの応答を受信しなかった場合、グループを削除します。

## スタブマルチキャストルーティング

スタブマルチキャストルーティングは、ダイナミックホスト登録の機能を提供して、マルチキャストルーティングを容易にします。スタブマルチキャストルーティングを設定すると、Firepower Threat Defense デバイスはIGMPのプロキシエージェントとして動作します。Firepower Threat Defense デバイスは、マルチキャストルーティングに全面的に参加するのではなく、IGMPメッセージをアップストリームのマルチキャストルータに転送し、そのルータがマルチキャストデータの送信をセットアップします。スタブマルチキャストルーティングを設定する場合は、Firepower Threat Defense デバイスを PIM スパースモードまたは双方向モード用に設定できません。IGMPスタブマルチキャストルーティングに参加するインターフェイス上で PIM を有効にする必要があります。

Firepower Threat Defense デバイスは、PIM-SM および双方向 PIM の両方をサポートしています。PIM-SMは、基盤となるユニキャストルーティング情報ベースまたは別のマルチキャスト対応ルーティング情報ベースを使用するマルチキャストルーティングプロトコルです。このプロトコルは、マルチキャストグループあたり1つのランデブーポイント (RP) をルートにした単方向の共有ツリーを構築し、オプションでマルチキャストの発信元ごとに最短パスツリーを作成します。

## PIM マルチキャストルーティング

双方向 PIM は PIM-SM の変形で、マルチキャストの発信元と受信者を接続する双方向の共有ツリーを構築します。双方向ツリーは、マルチキャストトポロジの各リンクで動作する指定フォワード (DF) 選択プロセスを使用して構築されます。DF に支援されたマルチキャストデータは発信元からランデブーポイント (RP) に転送されます。この結果、マルチキャストデータは発信元固有の状態を必要とせず、共有ツリーをたどって受信者に送信されます。DF の選択は RP の検出中に行われ、これによってデフォルトルートが RP に提供されます。



(注) Firepower Threat Defense デバイスが PIM RP の場合は、Firepower Threat Defense デバイスの変換されていない外部アドレスを RP アドレスとして使用してください。

## PIM Source Specific Multicast のサポート

Firepower Threat Defense デバイスは PIM Source Specific Multicast (SSM) の機能や関連設定をサポートしていません。ただし、Firepower Threat Defense デバイスは最終ホップルータとして配置されていない限り、SSM 関連のパケットの通過を許可します。

SSM は、IPTV などの1対多のアプリケーションのデータ送信メカニズムとして分類されます。SSM モデルは、(S, G) ペアで示される「チャンネル」の概念を使用します。S は発信元アドレス、G は SSM 宛先アドレスです。チャンネルに登録するには、IGMPv3 などのグループ管理プロトコルを使用して行います。SSM は、特定のマルチキャスト送信元について学習した後、受信側のクライアントを有効にします。これにより、共有ランデブーポイント (RP) からではなく、直接送信元からマルチキャストストリームを受信できるようになります。アクセス制御

メカニズムは SSM 内に導入され、現在のスパースまたはスパース - デンス モードの実装では提供されないセキュリティ拡張機能を提供します。

PIM-SSM は、RP または共有ツリーを使用しない点で PIM-SM とは異なります。代わりに、マルチキャストグループの発信元アドレスの情報は、ローカル受信プロトコル (IGMPv3) 経由で受信者から提供され、送信元固有のツリーを直接作成するために使用されます。

## マルチキャスト双方向 PIM

マルチキャスト双方向 PIM は、ビデオ会議、WebEx ミーティング、およびグループチャットなどのように、同時に通信を行う送信元と受信者が多く存在し、各参加者がマルチキャストトラフィックの送信元、受信者のどちらにもなりうるネットワークで有効です。PIM 双方向モードを使用すると、RP は共有ツリーの (\*,G) エントリのみを作成します。(S,G) エントリはありません。各 (S,G) エントリの状態テーブルを維持しないので、RP のリソースの節約になります。

PIM スパースモードでは、トラフィックは共有ツリーを下りにのみ流れます。PIM 双方向モードでは、トラフィックは共有ツリーの上りと下りの双方向に流れます。

PIM 双方向モードでは、PIM 登録/登録停止メカニズムを使って RP に送信元の登録をさせません。送信元はそれぞれ、いつでもソースへの送信を開始できます。マルチキャストパケットが RP に到達すると、共有ツリーで下りに転送されるか (受信者がいる場合)、ドロップされず (受信者がいない場合)。ただし、RP から送信元に対してマルチキャストトラフィックの送信停止を命令する方法はありません。

設計の観点から、ネットワークのどこに RP を配置するかを考える必要があります。ネットワーク内の送信元と受信者の中間のどこかに配置する必要があるからです。

PIM 双方向モードには、リバースパスフォワーディング (RPF) のチェックがありません。ループを回避するため、代わりに代表フォワーダ (DF) の概念を使用します。この DF は、セグメント内で唯一、RP にマルチキャストトラフィックの送信を許可されたルータです。マルチキャストトラフィックを転送するルータがセグメントあたり 1 台だけであれば、ループは発生しません。DF は次のメカニズムを使って選択されます。

- RP へのメトリックが最も小さいルータが DF になる。
- メトリックが等しい場合は、IP アドレスが最も大きいルータが DF になる。

## PIM ブートストラップルータ (BSR)

PIM ブートストラップルータ (BSR) は、RP 機能およびグループの RP 情報をリレーするために候補のルータを使用する動的ランデブーポイント (RP) セレクションモデルです。RP 機能には RP の検出が含まれており、RP にデフォルトルートを提供します。これは、一連のデバイスを BSR の選択プロセスに参加する候補の BSR (C-BSR) として設定し、その中から BSR を選択することで実現します。BSR が選択されると、候補のランデブーポイント (C-RP) として設定されたデバイスは、選定された BSR にグループマッピングの送信を開始します。次に、BSR はホップ単位で PIM ルータ間を移動する BSR メッセージ経由で、マルチキャストツリーに至る他のすべてのデバイスにグループ/RP マッピング情報を配布します。

この機能は、RPを動的に学習する方法を提供するため、RPが停止と起動を繰り返す複雑で大規模なネットワークには不可欠です。

## PIM ブートストラップルータ (BSR) の用語

PIM BSR の設定では、次の用語がよく使用されます。

- **ブートストラップルータ (BSR)** : BSR はホップバイホップ ベースの PIM が設定された他のルータに、ランデブーポイント (RP) 情報をアドバタイズします。選択プロセスの後に、複数の候補 BSR の中から 1 つの BSR が選択されます。このブートストラップルータの主な目的は、すべての候補 RP (C-RP) 通知を RP-set というデータベースに収集し、これをネットワーク内の他のすべてのルータに定期的に BSR メッセージとして送信することです (60 秒ごと)。
- **ブートストラップルータ (BSR) メッセージ** : BSR メッセージは、TTL が 1 に設定された All-PIM-Routers グループへのマルチキャストです。これらのメッセージを受信するすべての PIM ネイバーは、メッセージを受信したインターフェイスを除くすべてのインターフェイスからそのメッセージを再送信します (TTL は 1 に設定)。BSR メッセージには、現在アクティブな BSR の RP-set と IP アドレスが含まれています。この方法で、C-RP は C-RP メッセージのユニキャスト先を認識します。
- **候補ブートストラップルータ (C-BSR)** : 候補 BSR として設定されるデバイスは、BSR 選択メカニズムに参加します。最も優先順位の高い C-BSR が BSR として選択されます。C-BSR の最上位の IP アドレスはタイブレーカーとして使用されます。BSR の選択プロセスはプリエンティブです。たとえば、より優先順位の高い C-BSR が新たに見つかり、新しい選択プロセスがトリガーされます。
- **候補ランデブーポイント (C-RP)** : RP はマルチキャストデータの送信元と受信者が対面する場所として機能します。C-RP として設定されているデバイスは、マルチキャストグループマッピング情報を、ユニキャスト経由で直接、選択された BSR に定期的にアドバタイズします。これらのメッセージには、グループ範囲、C-RP アドレス、および保留時間が含まれています。現在の BSR の IP アドレスは、ネットワーク内のすべてのルータが受信した定期的な BSR メッセージから学習されます。このようにして、BSR は現在動作中で到達可能な RP 候補について学習します。



---

(注) C-RP は BSR トラフィックの必須要件ですが、Firepower Threat Defense デバイスは C-RP としては機能しません。ルータのみが C-RP として機能できます。したがって、BSR のテスト機能では、トポロジにルータを追加する必要があります。

---

- **BSR 選択メカニズム** : 各 C-BSR は、BSR 優先順位フィールドを含むブートストラップメッセージ (BSM) を生成します。ドメイン内のルータは、ドメイン全体に BSM をフラグディングします。自身より優先順位の高い C-BSR に関する情報を受け取った BSR は、一定期間、BSM の送信を抑制します。残った単一の C-BSR が選択された BSR となり、その BSM により、選択された BSR に関する通知がドメイン内の他のすべてのルータに対して送信されます。

## マルチキャスト グループの概念

マルチキャストはグループの概念に基づくものです。受信者の任意のグループは、特定のデータストリームを受信することに関心があります。このグループには物理的または地理的な境界がなく、インターネット上のどの場所にホストを置くこともできます。特定のグループに流れるデータの受信に関心があるホストは、IGMPを使用してグループに加入する必要があります。ホストがデータストリームを受信するには、グループのメンバでなければなりません。

## マルチキャスト アドレス

マルチキャストアドレスは、グループに加入し、このグループに送信されるトラフィックの受信を希望する IP ホストの任意のグループを指定します。

## クラスタリング

マルチキャストルーティングは、クラスタリングをサポートします。レイヤ2クラスタリングでは、プライマリ ユニットが、ファーストパス転送が確立されるまで、すべてのマルチキャストルーティング パケットとデータ パケットを送信します。ファーストパス転送が確立されると、従属ユニットがマルチキャストデータ パケットを転送できます。すべてのデータフローは、フルフローです。スタブ転送フローもサポートされます。1つのユニットだけレイヤ2クラスタリングのマルチキャスト パケットを受信するため、プライマリ ユニットへのリダイレクションは共通です。レイヤ3クラスタリングでは、ユニットは個別に機能しません。すべてのデータとルーティング パケットはプライマリ ユニットで処理され、転送されます。従属ユニットは、送信されたすべてのパケットをドロップします。

## マルチキャスト ルーティングのガイドライン

### コンテキスト モード

シングル コンテキスト モードでサポートされています。

### ファイアウォール モード

ルーテッド ファイアウォール モードでのみサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

### IPv6

IPv6 はサポートされません。

### クラスタリング

IGMP および PIM のクラスタリングでは、この機能はプライマリ ユニットでのみサポートされます。

### その他のガイドライン

224.1.2.3 などのマルチキャストホストへのトラフィックを許可するには、インバウンドセキュリティゾーン上のアクセス制御またはプレフィルタールールを設定する必要があります。ただし、ルールの宛先セキュリティゾーンを指定したり、初期接続確認の間にマルチキャストの接続に適用したりすることはできません。

## IGMP 機能の設定

IP ホストは、自身のグループメンバーシップを直接接続されているマルチキャストルータに報告するために IGMP を使用します。IGMP は、マルチキャストグループの個々のホストを特定の LAN にダイナミックに登録するために使用します。ホストは、そのローカルマルチキャストルータに IGMP メッセージを送信することで、グループメンバーシップを識別します。IGMP では、ルータは IGMP メッセージを受信し、定期的にクエリーを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

ここでは、インターフェイス単位で任意の IGMP 設定を行う方法について説明します。

### 手順

- ステップ 1 [マルチキャストルーティングの有効化 \(865 ページ\)](#)
- ステップ 2 [IGMP プロトコルの設定 \(866 ページ\)](#)。
- ステップ 3 [IGMP アクセスグループの設定 \(868 ページ\)](#)。
- ステップ 4 [IGMP スタティックグループの設定 \(869 ページ\)](#)。
- ステップ 5 [IGMP 参加グループの設定 \(870 ページ\)](#)。

## マルチキャストルーティングの有効化

Firepower Threat Defense デバイスでマルチキャストルーティングを有効にすると、デフォルトですべてのインターフェイス上の IGMP と PIM が有効になります。IGMP は、直接接続されているサブネット上にグループのメンバーが存在するかどうか学習するために使用されます。ホストは、IGMP レポートメッセージを送信することにより、マルチキャストグループに参加します。PIM は、マルチキャストデータグラムを転送するための転送テーブルを維持するために使用されます。



(注) マルチキャストルーティングでは、UDP トランスポート層だけがサポートされています。

以下の表に、Firepower Threat Defense デバイスの RAM の量に基づいた特定のマルチキャストテーブルのエントリの最大数を示します。この上限に達すると、新しいエントリは廃棄されます。

表 63: マルチキャスト テーブルのエントリ数の上限

テーブル	16 MB	128 MB	128+ MB
MFIB	[1000]	3000	30000
IGMP グループ	[1000]	3000	30000
PIM ルート	3000	7000	72000

#### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ 2** Choose [ルーティング (Routing)] > [マルチキャスト ルーティング (Multicast Routing)] > [IGMP] を選択します。
- ステップ 3** [マルチキャスト ルーティングの有効化 (Enable Multicast Routing)] チェックボックスをオンにします。

このチェックボックスをオンにすると、Firepower Threat Defense デバイス上で IP マルチキャスト ルーティングが有効になります。このチェックボックスをオフにすると、IP マルチキャスト ルーティングが無効になります。デフォルトでは、マルチキャストは無効になっています。マルチキャストルーティングを有効にすると、すべてのインターフェイス上でマルチキャストが有効になります。

マルチキャストはインターフェイスごとに無効にできます。この情報が役に立つのは、あるインターフェイス上にマルチキャスト ホストがないことがわかっている場合に、そのインターフェイス上で Firepower Threat Defense デバイスからホスト クエリ メッセージが送信されないように設定するときです。

## IGMP プロトコルの設定

転送インターフェイス、クエリ メッセージ、時間間隔などのインターフェイスごとに、IGMP パラメータを設定できます。

#### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ 2** ルーティング (Routing)] > [マルチキャスト ルーティング (Multicast Routing)] > [IGMP] を選択します。
- ステップ 3** [プロトコル (Protocol)] タブで、[追加 (Add)] または [編集 (Edit)] をクリックします。



[IGMP パラメータの追加 (Add IGMP parameters)] ダイアログボックスで、Firepower Threat Defense デバイスに新しい IGMP パラメータを追加します。既存のパラメータを変更する場合は、[IGMP パラメータの編集 (Edit IGMP parameters)] ダイアログボックスを使用します。

**ステップ 4** 次のオプションを設定します。

- [インターフェイス (Interface)] : ドロップダウンリストから、IGMP プロトコルを設定するインターフェイスを選択します。
- [IGMP を有効にする (Enable IGMP)] : IGMP を有効にするには、このチェックボックスをオンにします。

(注) 特定のインターフェイスでの IGMP 無効が役に立つのは、あるインターフェイス上にマルチキャストホストがないことがわかっている場合に、そのインターフェイス上で Firepower Threat Defense デバイスからホストクエリーメッセージが送信されないように設定するときです。

- [インターフェイスの転送 (Forward Interface)] : ドロップダウンリストから、どのインターフェイスから IGMP メッセージを送信するかを選択します。
- [バージョン (Version)] : IGMP バージョン 1 または 2 を選択します。

デフォルトでは、Firepower Threat Defense デバイスで IGMP バージョン 2 が実行されるため、多数の追加機能が使用できるようになります。

(注) サブネットのマルチキャストルータはすべて、同じ IGMP バージョンをサポートしている必要があります。Firepower Threat Defense デバイスが自動的にバージョン 1 ルータを検出してバージョン 1 に切り替えることはありません。ただ、サブネットに IGMP のバージョン 1 のホストとバージョン 2 のホストを混在させることも可能です。IGMP バージョン 2 を実行している Firepower Threat Defense デバイスは、IGMP バージョン 1 のホストが存在しても正常に動作します。

- [クエリー インターバル (Query Interval)] : 指定したルータから IGMP ホストクエリーメッセージが送信される秒単位の時間間隔。指定できる範囲は 1 ~ 3600 です。デフォルトは 125 です。

(注) 指定されたタイムアウト値の時間が経過しても、Firepower Threat Defense デバイスがインターフェイス上でクエリーメッセージを検出できなかった場合は、その Firepower Threat Defense デバイスが指定ルータになり、クエリーメッセージの送信を開始します。

- [応答時間 (Response Time)] : Firepower Threat Defense デバイスでグループが削除される前の秒単位の時間間隔。指定できる範囲は 1 ~ 25 です。デフォルトは 10 です。

Firepower Threat Defense デバイスがこの時間内にホストクエリーの応答を受信しなかった場合、グループを削除します。

- [グループ制限 (Group Limit) ] : インターフェイス上で加入する最大ホスト数。指定できる範囲は 1 ~ 500 です。デフォルトは 500 です。

IGMP メンバーシップ報告の結果の IGMP 状態の数は、インターフェイスごとに制限することができます。設定された上限を超過したメンバーシップ報告は IGMP キャッシュに入力されず、超過した分のメンバーシップ報告のトラフィックは転送されません。

- [クエリータイムアウト (Query Timeout) ] : 秒単位の時間で、前のリクエストがリクエストとしての動作を停止してからこの時間が経過すると、この Firepower Threat Defense デバイスはそのインターフェイスのリクエストの役割を引き継ぎます。指定できる範囲は 60 ~ 300 です。デフォルトは 255 です。

ステップ 5 [OK] をクリックして、IGMP プロトコル構成を保存します。

## IGMP アクセスグループの設定

アクセス コントロール リストを使用して、マルチキャスト グループへのアクセスを制御できます。

### 手順

ステップ 1 [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、Firepower Threat Defense デバイスを編集します。

ステップ 2 [ルーティング (Routing) ] > [マルチキャストルーティング (Multicast Routing) ] > [アクセスグループ (Access Group) ] を選択します。

ステップ 3 [アクセスグループ (Access Group) ] タブで、[追加 (Add) ] または [編集 (Edit) ] をクリックします。

[IGMP アクセスグループパラメータを追加 (Add IGMP Access Group parameters) ] ダイアログボックスを使用して、新しい IGMP アクセスグループをアクセスグループテーブルに追加します。既存のパラメータを変更する場合は、[IGMP アクセスグループパラメータを編集 (Edit IGMP Access Group parameters) ] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス (Interface) ] ドロップダウンリストから、アクセスグループが関連付けられるインターフェイスを選択します。既存のアクセスグループを編集しているときは、関連インターフェイスは変更できません。
- 次のいずれかのオプション ボタンをクリックします。

- [標準アクセスリスト (Standard Access List) ] : [標準アクセスリスト (Standard Access List) ] ドロップダウンリストから、標準 ACL を選択するか、または追加アイコン (+) をクリックして新しい標準 ACL を作成します。手順については、[標準 ACL オブジェクトの設定 \(510 ページ\)](#) を参照してください。

- [拡張アクセスリスト (Extended Access List)] : [拡張アクセスリスト (Extended Access List)] ドロップダウンリストから、拡張 ACL を選択するか、または追加アイコン (➕) をクリックして新しい拡張 ACL を作成します。手順については、[拡張 ACL オブジェクトの設定 \(509 ページ\)](#) を参照してください。

ステップ 5 [OK] をクリックして、アクセスグループ構成を保存します。

## IGMP スタティック グループの設定

グループ メンバーがグループのメンバーシップをレポートできなかつたり、ネットワーク セグメントにグループのメンバーが存在しない場合でも、そのグループのマルチキャスト トラフィックをそのネットワークセグメントに送信しなければならないことがあります。そのようなグループのマルチキャストトラフィックをそのセグメントに送信するには、スタティック加入した IGMP グループを設定します。この方法の場合、Firepower Threat Defense デバイスはパケットそのものを受信せず、転送だけを実行します。そのため、スイッチングが高速に実施されます。発信インターフェイスはIGMP キャッシュ内に存在しますが、このインターフェイスはマルチキャスト グループのメンバーではありません。

### 手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ 2 [ルーティング (Routing)] > [マルチキャスト ルーティング (Multicast Routing)] > [IGMP] を選択します。
- ステップ 3 [スタティック グループ (Static Group)] タブで、[追加 (Add)] または [編集 (Edit)] をクリックします。

インターフェイスに対してマルチキャストグループをスタティックに割り当てる場合は、[IGMP スタティック グループパラメータの追加 (Add IGMP Static Group parameters)] ダイアログボックスを使用します。既存のスタティック グループの割り当てを変更する場合は、[IGMP スタティック グループパラメータの編集 (Edit IGMP Static Group parameters)] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス (Interface)] ドロップダウンリストから、マルチキャストグループをスタティックに割り当てるインターフェイスを選択します。既存のエントリを編集しているときは、値は変更できません。
- [マルチキャストグループ (Multicast Groups)] ドロップダウンリストから、インターフェイスを割り当てるマルチキャストグループを選択するか、追加アイコン (➕) をクリックして、新しいマルチキャストグループを作成します。手順については、[ネットワークオブジェクトの作成](#) を参照してください。

ステップ 5 [OK] をクリックして、スタティック グループ設定を保存します。

## IGMP 参加グループの設定

インターフェイスをマルチキャストグループのメンバーとして設定できます。マルチキャストグループに加入するように Firepower Threat Defense デバイスを設定すると、アップストリームルータはそのグループのマルチキャストルーティングテーブル情報を維持して、このグループをアクティブにするパスを保持します。



(注) [IGMP スタティック グループの設定 \(869 ページ\)](#) を参照して、特定のグループのマルチキャストパケットを特定のインターフェイスに転送する必要がある場合に、Firepower Threat Defense デバイスがそのパケットをそのグループの一部として受け付けることがないようにする方法を確認してください。

### 手順

ステップ 1 [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、Firepower Threat Defense デバイスを編集します。

ステップ 2 [ルーティング (Routing) ] > [マルチキャストルーティング (Multicast Routing) ] > [IGMP] を選択します。

ステップ 3 [参加グループ (Join Group) ] タブで、[追加 (Add) ] または [編集 (Edit) ] をクリックします。

Firepower Threat Defense デバイスをマルチキャストグループのメンバーに設定する場合は、[IGMP 参加グループ パラメータの追加 (Add IGMP Join Group parameters) ] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[IGMP 参加グループ パラメータの編集 (Edit IGMP Join Group parameters) ] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス (Interface) ] ドロップダウンリストから、マルチキャストグループのメンバーにするインターフェイスを選択します。既存のエントリを編集しているときは、値は変更できません。
- [参加グループ (Join Group) ] ドロップダウンリストから、インターフェイスを割り当てるマルチキャストグループを選択するか、[プラス (Plus) ] アイコンをクリックして、新しいマルチキャストグループを作成します。手順については、[ネットワーク オブジェクトの作成](#) を参照してください。

## PIM 機能の設定

ルータは PIM を使用して、マルチキャスト ダイアグラムを転送するために使われる転送テーブルを維持します。Firepower Threat Defense デバイスでマルチキャストルーティングを有効にすると、PIM および IGMP がすべてのインターフェイスで自動的に有効になります。



- (注) PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

ここでは、任意の PIM 設定を行う方法について説明します。

### 手順

- ステップ 1 [PIM プロトコルの設定 \(871 ページ\)](#)
- ステップ 2 [PIM ネイバー フィルタの設定 \(872 ページ\)](#)
- ステップ 3 [PIM 双方向ネイバー フィルタの設定 \(873 ページ\)](#)
- ステップ 4 [PIM ランデブー ポイントの設定 \(875 ページ\)](#)
- ステップ 5 [PIM ルート ツリーの設定 \(876 ページ\)](#)
- ステップ 6 [PIM リクエスト フィルタの設定 \(877 ページ\)](#)
- ステップ 7 [マルチキャスト境界フィルタの設定 \(880 ページ\)](#)

## PIM プロトコルの設定

PIM は、特定のインターフェイスで有効または無効にすることができます。

代表ルータ (DR) のプライオリティを設定することもできます。DR は、PIM 登録メッセージ、PIM 加入メッセージ、およびプルーニング メッセージの RP への送信を担当します。1 つのネットワーク セグメントに複数のマルチキャストルータがある場合は、DR プライオリティに基づいて DR が選択されます。複数のデバイスの DR プライオリティが等しい場合、最上位の IP アドレスを持つデバイスが DR になります。デフォルトでは、Firepower Threat Defense デバイスの DR プライオリティは 1 です。

ルータ クエリ メッセージは、PIM DR の選択に使用されます。PIM DR は、ルータ クエリ メッセージを送信します。デフォルトでは、ルータ クエリ メッセージは 30 秒間隔で送信されます。さらに、60 秒ごとに、Firepower Threat Defense デバイスは PIM 加入メッセージおよびプルーニング メッセージを送信します。

## 手順

- 
- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ 2** [ルーティング (Routing) ] > [マルチキャスト ルーティング (Multicast Routing) ] > [PIM] を選択します。
- ステップ 3** [プロトコル (Protocol) ] タブで、[追加 (Add) ] または [編集 (Edit) ] をクリックします。
- インターフェイスに新しい PIM パラメータを追加する場合は、[PIM パラメータの追加 (Add PIM parameters) ] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[PIM パラメータの編集 (Edit PIM parameters) ] ダイアログボックスを使用します。
- ステップ 4** 次のオプションを設定します。
- [インターフェイス (Interface) ] : ドロップダウンリストから、PIM プロトコルを設定するインターフェイスを選択します。
  - [PIM を有効にする (Enable PIM) ] : PIM を有効にするには、このチェックボックスをオンにします。
  - [DR プライオリティ (DR Priority) ] : 選択したインターフェイスの DR の値。サブネット上のルータのうち、DR プライオリティが最も大きいものが指定ルータになります。有効な値の範囲は 0 ~ 4294967294 です。デフォルトの DR プライオリティは 1 です。この値を 0 に設定した場合は、その Firepower Threat Defense デバイスインターフェイスがデフォルトのルータになることはありません。
  - [Hello 間隔 (Hello Interval) ] : インターフェイスから PIM hello メッセージが送信される時間間隔 (秒単位)。指定できる範囲は 1 ~ 3600 です。デフォルトは 30 です。
  - [参加プルーン間隔 (Join Prune Interval) ] : インターフェイスから PIM の加入アドバタイズメントおよびプルーンアドバタイズメントが送信される時間間隔 (秒単位)。指定できる範囲は 10 ~ 600 です。デフォルトは 60 です。
- ステップ 5** [OK] をクリックして、PIM プロトコル設定を保存します。
- 

## PIM ネイバー フィルタの設定

PIM ネイバーにできるルータの定義が可能です。PIM ネイバーにできるルータをフィルタリングすると、次の制御を行うことができます。

- 許可されていないルータが PIM ネイバーにならないようにする。
- 添付されたスタブルータが PIM に参加できないようにする。

## 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ 2** [ルーティング (Routing) ] > [マルチキャスト ルーティング (Multicast Routing) ] > [PIM] を選択します。
- ステップ 3** [ネイバー フィルタ (Neighbor Filter) ] タブで、[追加 (Add) ] または [編集 (Edit) ] をクリックします。

インターフェイスに新しい PIM ネイバー フィルタを追加する場合は、[PIM ネイバー フィルタの追加 (Add PIM Neighbor Filter) ] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[PIM ネイバー フィルタの編集 (Edit PIM Neighbor Filter) ] ダイアログボックスを使用します。

- ステップ 4** 次のオプションを設定します。

- [インターフェイス (Interface) ] ドロップダウンリストから、PIM ネイバー フィルタを追加するインターフェイスを選択します。
- [標準アクセス リスト (Standard Access List) ] : [標準アクセス リスト (Standard Access List) ] ドロップダウンリストから標準 ACL を選択するか、追加アイコン (+) をクリックして新しい標準 ACL を作成します。手順については、[標準 ACL オブジェクトの設定 \(510 ページ\)](#) を参照してください。

(注) [標準アクセス リスト エントリの追加 (Add Standard Access List Entry) ] ダイアログボックスで [許可 (Allow) ] を選択すると、マルチキャストグループアドバタイズメントはこのインターフェイスを通過できるようになります。[ブロック (Block) ] を選択すると、指定したマルチキャストグループアドバタイズメントはこのインターフェイスを通過できなくなります。インターフェイスに対してマルチキャスト境界を設定すると、ネイバー フィルタ エントリで許可されていない限り、すべてのマルチキャストトラフィックが、インターフェイスの通過を拒否されます。

- ステップ 5** [OK] をクリックして、PIM ネイバー フィルタ設定を保存します。

## PIM 双方向ネイバー フィルタの設定

PIM 双方向ネイバー フィルタは、Designated Forwarder (DF) 選定に参加できるネイバー デバイスを定義する ACL です。PIM 双方向ネイバー フィルタがインターフェイスに設定されていなければ、制限はありません。PIM 双方向ネイバー フィルタが設定されている場合は、ACL で許可されるネイバーだけが DF 選択プロセスに参加できます。

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。DF を選択するために、セグメント内のすべてのマルチキャスト ルータが双方向で有効になっている必要があります。

PIM 双方向ネイバー フィルタが有効な場合、その ACL によって許可されるルータは、双方向に対応しているとみなされます。したがって、次のことが当てはまります。

- 許可されたネイバーが双方向モードをサポートしていない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向モードをサポートしている場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向モードをサポートしていない場合、DF 選択が実行される可能性があります。

## 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。

**ステップ 2** [マルチキャスト ルーティング (Multicast Routing)] > [PIM] を選択します。

**ステップ 3** [双方向ネイバー フィルタ (Bidirectional Neighbor Filter)] タブで、[追加 (Add)] または [編集 (Edit)] をクリックします。

PIM 双方向ネイバー フィルタ ACL の ACL エントリを作成する場合は、[PIM 双方向ネイバー フィルタの追加 (Add PIM Bidirectional Neighbor Filter)] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[PIM 双方向ネイバー フィルタの編集 (Edit PIM Bidirectional Neighbor Filter)] ダイアログボックスを使用します。

**ステップ 4** 次のオプションを設定します。

- [インターフェイス (Interface)] ドロップダウンリストから、PIM 双方向ネイバー フィルタの ACL エントリを設定するインターフェイスを選択します。
- [標準アクセス リスト (Standard Access List)] : [標準アクセス リスト (Standard Access List)] ドロップダウンリストから標準 ACL を選択するか、追加アイコン (+) をクリックして新しい標準 ACL を作成します。手順については、[標準 ACL オブジェクトの設定 \(510 ページ\)](#) を参照してください。

(注) [標準アクセス リスト エントリの追加 (Add Standard Access List Entry)] ダイアログボックスで [許可 (Allow)] を選択すると、指定したデバイスが DR 選択プロセスに参加できます。[ブロック (Block)] を選択すると、指定したデバイスは DR 選択プロセスに参加できなくなります。

**ステップ 5** [OK] をクリックして、PIM 双方向ネイバー フィルタ設定を保存します。



## PIM ランデブーポイントの設定

Firepower Threat Defense デバイスを複数のグループの RP として機能するように設定することができます。ACL に指定されているグループ範囲によって、PIM RP のグループマッピングが決まります。ACL が指定されていない場合は、マルチキャストグループ全体の範囲 (224.0.0.0/4) にグループの RP が適用されます。双方向 PIM の詳細については、[マルチキャスト双方向 PIM \(862 ページ\)](#) を参照してください。

RP には、次の制約事項が適用されます。

- 同じ RP アドレスは、2 度使用できません。
- 複数の RP に対しては、[すべてのグループ (All Groups)] を指定できません。

### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ 2** [ルーティング (Routing)] > [マルチキャストルーティング (Multicast Routing)] > [PIM] を選択します。
- ステップ 3** [ランデブーポイント (Rendezvous Points)] タブで、[追加 (Add)] または [編集 (Edit)] をクリックします。  
  
[ランデブーポイント (Rendezvous Points)] テーブルに新しいエントリを作成する場合は、[ランデブーポイントの追加 (Add Rendezvous Point)] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[ランデブーポイントの編集 (Edit Rendezvous Point)] ダイアログボックスを使用します。
- ステップ 4** 次のオプションを設定します。
  - [ランデブーポイントの IP アドレス (Rendezvous Point IP address)] ドロップダウンリストから、RP として追加する IP アドレスを選択するか、追加アイコン (🟢) をクリックして新しいネットワークオブジェクトを作成します。手順については、[ネットワークオブジェクトの作成](#) を参照してください。
  - [双方向転送の使用 (Use bi-directional forwarding)] チェックボックスをオンにすると、指定されているマルチキャストグループは双方向モードで動作します。双方向モードでは、Firepower Threat Defense デバイスがマルチキャストパケットを受信したときに、直接接続されたメンバーも PIM ネイバーも存在しない場合は、送信元にプルーンメッセージが返されます。
  - 指定した RP をインターフェイス上のすべてのマルチキャストグループに対して使用する場合は、[すべてのマルチキャストグループに対してこの RP を使用する (Use this RP for All Multicast Groups)] オプション ボタンを選択します。
  - [次に指定するようにすべてのマルチキャストグループに対してこの RP を使用する (Use this RP for all Multicast Groups as specified below)] を選択して、指定の RP とともに使用する

るマルチキャスト グループを指定します。次に [標準アクセス リスト (Standard Access List) ] ドロップダウンリストから標準 ACL を選択するか、追加アイコン (+) をクリックして、新しい標準 ACL を作成します。手順については、[標準 ACL オブジェクトの設定 \(510 ページ\)](#) を参照してください。

**ステップ 5** [OK] をクリックして、ランデブー ポイント設定を保存します。

## PIM ルート ツリーの設定

デフォルトでは、PIM リーフルータは、新しい送信元から最初のパケットが到着した直後に、最短パス ツリーに加入します。この方法では、遅延が短縮されますが、共有 ツリーに比べて多くのメモリが必要になります。すべてのマルチキャスト グループまたは特定のマルチキャスト アドレスに対して、Firepower Threat Defense デバイスを最短パス ツリーに加入させるか、共有 ツリーを使用するかを設定できます。

[マルチキャスト グループ (Multicast Groups) ] テーブルで指定されていないグループには最短パス ツリーが使用されます。[マルチキャスト グループ (Multicast Groups) ] テーブルには、共有 ツリーを使用するマルチキャスト グループが表示されます。テーブル エントリは、上から下の順で処理されます。ある範囲のマルチキャスト グループが含まれるエントリを作成し、その範囲の中から特定のグループを除外するには、その除外するグループに対する拒否ルールをテーブルの先頭に配置し、その範囲内のマルチキャスト グループ全体に対する許可ルールを deny 文の下に配置します。



(注) この動作は Shortest Path Switchover (SPT) と呼ばれます。[共有 ツリー (Shared Tree) ] オプションを常に使用することをお勧めします。

### 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、Firepower Threat Defense デバイスを編集します。

**ステップ 2** [ルーティング (Routing) ] > [マルチキャスト ルーティング (Multicast Routing) ] > [PIM] を選択します。

**ステップ 3** [ルート ツリー (Route Tree) ] タブで、ルート ツリーのパスを選択します。

- すべてのマルチキャスト グループに最短パス ツリーを使用する場合は、[最短パス (Shortest Path) ] オプション ボタンをクリックします。
- すべてのマルチキャスト グループに共有 ツリーを使用する場合は、[共有 ツリー (Shared Tree) ] オプション ボタンをクリックします。
- [次に示すグループの共有 ツリー (Shared tree for below mentioned group) ] オプション ボタンをクリックして、[マルチキャスト グループ (Multicast Groups) ] テーブルで指定された

グループを指定します。次に [標準アクセス リスト (Standard Access List)] ドロップダウンリストから標準 ACL を選択するか、追加アイコン (+) をクリックして、新しい標準 ACL を作成します。手順については、[標準 ACL オブジェクトの設定 \(510 ページ\)](#) を参照してください。

ステップ 4 [OK] をクリックして、ルート ツリー設定を保存します。

## PIM リクエスト フィルタの設定

Firepower Threat Defense デバイスが RP として動作しているときは、特定のマルチキャスト送信元を登録できないように制限することができます。このようにすると、未許可の送信元が RP に登録されるのを回避できます。Firepower Threat Defense デバイスが PIM 登録メッセージを受け入れるマルチキャスト送信元を定義できます。

### 手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。

ステップ 2 [ルーティング (Routing)] > [マルチキャスト ルーティング (Multicast Routing)] > [PIM] を選択します。

ステップ 3 [リクエスト フィルタ (Request Filter)] タブで、RP として動作する Firepower Threat Defense デバイ스에登録できるマルチキャスト送信元を定義します。

- [PIM 登録メッセージのフィルタ方法: (Filter PIM register messages using:)] ドロップダウンリストから [なし (None)]、[アクセス リスト (Access List)]、または [ルート マップ (Route Map)] を選択します。
- ドロップダウンリストから [アクセス リスト (Access List)] を選択した場合は、拡張 ACL を選択するか、追加アイコン (+) をクリックして新しい拡張 ACL を作成します。手順については、[拡張 ACL オブジェクトの設定 \(509 ページ\)](#) を参照してください。

(注) [拡張アクセス リスト エントリの追加 (Add Extended Access List Entry)] ダイアログボックスで、ドロップダウンリストから [許可 (Allow)] を選択して、指定したマルチキャストトラフィックの指定した送信元を Firepower Threat Defense デバイ스에登録することを許可するルールを作成します。または、[ブロック (Block)] を選択して、指定したマルチキャストトラフィックの指定した送信元が Firepower Threat Defense デバイ스에登録されることを防ぐルールを作成します。

- [ルート マップ (Route Map)] を選択した場合は、[ルート マップ (Route Map)] ドロップダウンリストからルート マップを選択するか、追加アイコン (+) をクリックして新しいルート マップを作成します。手順については、[ネットワーク オブジェクトの作成](#) を参照してください。

ステップ4 [OK] をクリックして、リクエスト フィルタ設定を保存します。

## Firepower Threat Defense デバイスのブートストラップルータ設定

Firepower Threat Defense デバイスを BSR 候補として設定できます。

### 手順

- ステップ1 [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ2 [ルーティング (Routing) ] > [マルチキャストルーティング (Multicast Routing) ] > [PIM] を選択します。
- ステップ3 [ブートストラップルータ (Bootstrap Router) ] タブで、[この FTD をブートストラップルータ候補として設定 (Configure this FTD as a Candidate Bootstrap Router (C-BSR)) ] チェックボックスをオンにして、C-BSR の設定をします。
- [インターフェイス (Interface) ] ドロップダウンリストから、BSR アドレスが派生する Firepower Threat Defense デバイスのインターフェイスを選択して、候補にします。  
このインターフェイスは PIM を使用して有効化する必要があります。
  - [ハッシュマスク長 (Hash mask length) ] フィールドに、ハッシュ関数が呼び出される前にグループアドレスと論理積をとるマスク長 (最大 32 ビット) を入力します。ハッシュ元が同じであるすべてのグループは、同じ RP に対応します。たとえば、マスク長が 24 の場合、グループアドレスの最初の 24 ビットだけが使用されます。これにより、複数のグループについて 1 つの RP を取得できます。指定できる範囲は 0 ~ 32 です。
  - [優先度 (Priority) ] フィールドに、BSR 候補の優先度を入力します。プライオリティが大きな BSR が優先されます。プライオリティ値が同じ場合は、IP アドレスがより高位であるルータが BSR となります。指定できる範囲は 0 ~ 255 です。デフォルト値は 0 です。
- ステップ4 (オプション) [この FTD をボーダーブートストラップルータとして設定 (Configure this FTD as a Border Bootstrap Router (BSR)) ] セクションで、追加アイコン (+) をクリックして、PIM BSR メッセージを送受信しないインターフェイスを選択します。
- [インターフェイス (Interface) ] ドロップダウンリストから、PIM BSR メッセージを送受信しないインターフェイスを選択します。  
RP または BSR アドバタイズメントは、フィルタリングされている効果的に隔てられた 2 つの RP 情報交換ドメインです。
  - BSR を有効化するには、[ボーダー BSR を有効にする (Enable Border BSR) ] チェックボックスをオンにします。
- ステップ5 [OK] をクリックして、ブートストラップルータ設定を保存します。

## マルチキャスト ルートの設定

スタティック マルチキャスト ルートを設定すると、マルチキャスト トラフィックをユニキャスト トラフィックから分離できます。たとえば、送信元と宛先の間のパスでマルチキャスト ルーティングがサポートされていない場合は、その解決策として、2つのマルチキャスト デバイスの間に GRE トンネルを設定し、マルチキャスト パケットをそのトンネル経由で送信します。

PIM を使用する場合、Firepower Threat Defense デバイスは、ユニキャスト パケットを発信元に返送するときと同じインターフェイスでパケットを受信することを想定しています。マルチキャスト ルーティングをサポートしていないルートをバイパスする場合などは、ユニキャスト パケットで1つのパスを使用し、マルチキャスト パケットで別の1つのパスを使用することもあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ 2** [ルーティング (Routing)] > [マルチキャスト ルーティング (Multicast Routing)] > [マルチキャスト ルート (Multicast Routes)] を選択し、[追加 (Add)] または [編集 (Edit)] をクリックします。

Firepower Threat Defense デバイスに新しいマルチキャスト ルートを追加する場合は、[マルチキャスト ルート設定の追加 (Add Multicast Route Configuration)] ダイアログボックスを使用します。既存のマルチキャスト ルートを変更する場合は、[マルチキャスト ルート設定の編集 (Edit Multicast Route Configuration)] ダイアログボックスを使用します。
- ステップ 3** [送信元ネットワーク (Source Network)] ドロップダウンボックスから、既存のネットワークを選択するか、追加アイコン (+) をクリックして新しいネットワークを追加します。手順については、[ネットワーク オブジェクトの作成](#) を参照してください。
- ステップ 4** ルートを転送するようインターフェイスを設定するには、[インターフェイス (Interface)] オプション ボタンをクリックして、以下のオプションを設定します。
  - [送信元インターフェイス (Source Interface)] ドロップダウンリストから、マルチキャスト ルートの着信インターフェイスを選択します。
  - [発信インターフェイス/デンス (Output Interface/Dense)] ドロップダウンリストから、ルートが転送される宛先インターフェイスを選択します。
  - [距離 (Distance)] フィールドに、マルチキャスト ルートの距離を入力します。指定できる範囲は 0 ~ 255 です。

- ステップ 5** ルートを転送するよう RPF アドレスを設定するには、[アドレス (Address)] オプションボタンをクリックして、以下のオプションを設定します。
- [RPF アドレス (RPF Address)] フィールドに、マルチキャストルートの IP アドレスを入力します。
  - [距離 (Distance)] フィールドに、マルチキャストルートの距離を 0～255 で入力します。
- ステップ 6** [OK] をクリックして、マルチキャストルータの設定を保存します。

## マルチキャスト境界フィルタの設定

アドレス スコーピングは、同じ IP アドレスを持つ RP が含まれるドメインが相互にデータを漏出させることのないように、ドメイン境界フィルタを定義します。スコーピングは、大きなドメイン内のサブネット境界や、ドメインとインターネットの間の境界で実行されます。

インターフェイスでマルチキャスト グループ アドレスの管理スコープ境界フィルタを設定できます。IANA では、239.0.0.0～239.255.255.255 のマルチキャストアドレス範囲が管理スコープアドレスとして指定されています。この範囲のアドレスは、さまざまな組織で管理されるドメイン内で再使用されます。このアドレスはグローバルではなく、ローカルで一意であるとみなされます。

影響を受けるアドレスの範囲は、標準 ACL で定義します。境界フィルタが設定されると、マルチキャスト データ パケットは境界を越えて出入りできなくなります。境界フィルタを定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

管理スコープ境界での Auto-RP 検出および通知のメッセージの設定、検査、フィルタリングを行うことができます。境界の ACL で拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界フィルタを通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスを編集します。
- ステップ 2** [ルーティング (Routing)] > [マルチキャスト ルーティング (Multicast Routing)] > [マルチキャスト境界フィルタ (Multicast Boundary Filter)] を選択し、[追加 (Add)] または [編集 (Edit)] をクリックします。

[マルチキャスト境界フィルタの追加 (Add Multicast Boundary Filter)] ダイアログボックスを使用して、新しいマルチキャスト境界フィルタを Firepower Threat Defense デバイスに追加しま

す。既存のパラメータを変更するには、[マルチキャスト境界フィルタの編集 (Edit Multicast Boundary Filter)] ダイアログボックスを使用します。

管理スコープ マルチキャスト アドレスのマルチキャスト境界を設定できます。マルチキャスト境界により、マルチキャスト データ パケット フローが制限され、同じマルチキャスト グループアドレスを複数の管理ドメインで再利用できるようになります。インターフェイスに対してマルチキャスト境界が定義されている場合、フィルタ ACL により許可されたマルチキャスト トラフィックだけが、そのインターフェイスを通過します。

- ステップ 3** [インターフェイス (Interface)] ドロップダウン リストから、マルチキャスト境界フィルタ ACL を設定するインターフェイスを選択します。
  - ステップ 4** [標準アクセス リスト (Standard Access List)] ドロップダウン リストから、使用する標準 ACL を選択するか、追加アイコン (+) をクリックして新しい標準 ACL を作成します。手順については、[標準 ACL オブジェクトの設定 \(510 ページ\)](#) を参照してください。
  - ステップ 5** 境界 ACL によって拒否されたソースからの Auto-RP メッセージをフィルタするには、[境界によって拒否された Auto-RP パケットからの Auto-RP グループ範囲通知の削除 (Remove any Auto-RP group range announcement from the Auto-RP packets that are denied by the boundary)] チェックボックスをオンにします。このチェックボックスをオンにしていない場合、すべての Auto-RP メッセージが通過します。
  - ステップ 6** [OK] をクリックして、マルチキャスト境界フィルタの設定を保存します。
-







## 第 **XI** 部

# Firepower Threat Defense の VPN

- [VPN の概要 \(885 ページ\)](#)
- [Firepower Threat Defense VPNの導入 \(897 ページ\)](#)
- [Firepower Threat Defense VPN の管理 \(901 ページ\)](#)





## 第 38 章

### VPN の概要

バーチャルプライベートネットワーク（VPN）接続は、インターネットなどのパブリックネットワークを介してエンドポイント間の安全なトンネルを確立します。

この章は、Firepower Threat Defense デバイス上のサイト間 VPN にのみ適用されます。サイト間 VPN の構築に使用される Internet Protocol Security（IPsec）、Internet Security Association and Key Management Protocol（ISAKMP、または IKE）および SSL 規格について説明します。

Firepower Management Center でゲートウェイ VPN または Firepower VPN と呼ばれる、7000 および 8000 シリーズ デバイス上のサイト間 VPN については [ゲートウェイ VPN（1297 ページ）](#) で説明しています。

- [VPN タイプ（885 ページ）](#)
- [VPN の基本（886 ページ）](#)
- [VPN パケットフロー（889 ページ）](#)
- [VPN ライセンス（889 ページ）](#)
- [VPN 接続の安全性を確保する方法（889 ページ）](#)
- [VPN トポロジ オプション（892 ページ）](#)

### VPN タイプ

Firepower Management Center は次のタイプの VPN 接続をサポートします。

- Firepower Threat Defense デバイス上のサイト間 VPN。

サイト間 VPN は、地理的に異なる場所にあるネットワークを接続します。管理対象デバイス間、および管理対象デバイスと関連するすべての規格に準拠するその他のシスコまたはサードパーティのピアとの間で、サイト間 IPsec 接続を作成できます。これらのピアは、IPv4 アドレスと IPv6 アドレスの内部と外部の任意の組み合わせを持つことができます。サイト間トンネルは、Internet Protocol Security（IPsec）プロトコルスイートと IKEv1 または IKEv2 を使用して構築されます。VPN 接続が確立されると、ローカルゲートウェイの背後にあるホストはセキュアな VPN トンネルを介して、リモートゲートウェイの背後にあるホストに接続することができます。

- 7000 および 8000 シリーズ デバイス上のサイト間 VPN。

これらのサイト間 VPN は、Firepower Management Center 内でゲートウェイ VPN または Firepower VPN と呼ばれます。このタイプの VPN 接続については、[ゲートウェイ VPN \(1297 ページ\)](#) を参照してください。

## VPN の基本

トンネリングによって、インターネットなどのパブリック TCP/IP ネットワークの使用が可能となり、リモートユーザとプライベート企業ネットワークとの間でセキュアな接続を作成できます。各セキュアな接続がトンネルと呼ばれます。

IPsec ベースの VPN テクノロジーでは、Internet Security Association and Key Management Protocol (ISAKMP または IKE) と IPsec トンネリングを使用して、トンネルを構築し管理します。ISAKMP と IPsec は、次を実現します。

- トンネルパラメータのネゴシエート。
- トンネルの確立。
- ユーザとデータの認証。
- セキュリティ キーの管理。
- データの暗号化と復号。
- トンネルを経由するデータ転送の管理。
- トンネルエンドポイントまたはルータとしてのインバウンドおよびアウトバウンドのデータ転送の管理。

VPN 内のデバイスは、双方向トンネルエンドポイントとして機能します。プライベートネットワークからプレーンパケットを受信し、それらをカプセル化して、トンネルを作成し、それらをトンネルの他端に送信することができます。そこで、カプセル化が解除され、最終宛先へ送信されます。また、パブリックネットワークからカプセル化されたパケットを受信し、それらをカプセル化解除して、プライベートネットワーク上の最終宛先に送信することもできます。

サイト間 VPN 接続が確立された後、ローカルゲートウェイの背後にあるホストは、セキュアな VPN トンネルを介してリモートゲートウェイの背後にあるホストと接続できます。接続は、2つのゲートウェイの IP アドレスとホスト名、それらの背後にあるサブネット、および2つのゲートウェイが互いを認証するために使用する方式で構成されます。

## インターネット キー エクスチェンジ (IKE)

インターネット キー エクスチェンジ (IKE) は、IPsec ピアを認証し、IPsec 暗号化キーをネゴシエートして配信し、IPsec セキュリティ アソシエーション (SA) を自動的に確立するために使用されるキー管理プロトコルです。

IKE ネゴシエーションは2つのフェーズで構成されています。フェーズ1では、2つのIKEピア間のセキュリティアソシエーションをネゴシエートします。これにより、ピアはフェーズ2で安全に通信できるようになります。フェーズ2のネゴシエーションでは、IKEによってIPsecなどの他のアプリケーション用のSAが確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。

IKE ポリシーは、2つのピアが、ピア間のIKEネゴシエーションの安全性を確保するために使用する一連のアルゴリズムです。IKEネゴシエーションは、共通（共有）IKEポリシーに合意している各ピアによって開始されます。このポリシーは、どのセキュリティパラメータが後続のIKEネゴシエーションを保護するかを規定します。IKEバージョン1 (IKEv1) の場合、IKEポリシーには単一セットのアルゴリズムとモジュラスグループが含まれます。IKEv1とは異なり、IKEv2ポリシーでは、フェーズ1ネゴシエーション中にピアがその中から選択できるように、複数のアルゴリズムとモジュラスグループを選択できます。単一のIKEポリシーを作成できますが、最も必要なオプションにより高い優先順位をつけるために異なるポリシーが必要となる場合もあります。サイト間VPNの場合は、単一のIKEポリシーを作成できます。

IKEポリシーを定義するには、次を指定します。

- 固有の優先順位（1～65,543、1が最高の優先順位）。
- データを保護し、プライバシーを確保するためのIKEネゴシエーションの暗号化方式。
- 送信者のIDを保証し、メッセージが伝送中に変更されないように確保するためのハッシュメッセージ認証コード（HMAC）方式（IKEv2では整合性アルゴリズムと呼ばれる）。
- IKEv2の場合、IKEv2トンネル暗号化に必要なキーの材料とハッシュ操作を派生させるためのアルゴリズムとして使用される個別の擬似乱関数（PRF）。オプションは、ハッシュアルゴリズムで使用されているものと同じです。
- 暗号化キー判別アルゴリズムの強度を決定するDiffie-Hellmanグループ。デバイスは、このアルゴリズムを使用して、暗号化キーとハッシュキーを派生させます。
- ピアのIDを保証するための認証方式。



---

(注) 認証には事前共有キーのみが使用されます。

---

- デバイスが暗号化キーを交換するまでに使用できる時間制限。

IKEネゴシエーションが開始すると、ネゴシエーションを開始するピアはリモートピアにすべてのポリシーを送信し、リモートピアは優先順位順に自身のポリシーとの一致を検索します。ピアが、暗号化、ハッシュ（IKEv2の場合は整合性とPRF）、認証、Diffie-Hellman値を保持し、さらに、送信されたポリシーのライフタイム以下であるSAライフタイムを保持している場合に、IKEポリシー間に一致が存在します。ライフタイムが同じでない場合は、リモートピアポリシーの短い方のライフタイムが適用されます。デフォルトでは、Firepower Management Centerは、正常なネゴシエーションを確保するために、すべてのVPNエンドポイントに対してIKEv1ポリシーを最低優先順位で展開します。

## IPsec

IPsec は、VPN を設定する場合の最も安全な方法の 1 つです。IPsec では、IP パケット レベルでのデータ暗号化が提供され、標準規格に準拠した堅牢なセキュリティソリューションが提供されます。IPsec では、データはトンネルを介してパブリック ネットワーク経由で送信されます。トンネルとは、2 つのピア間のセキュアで論理的な通信パスです。IPsec トンネルを通過するトラフィックは、セキュリティプロトコルとアルゴリズムの組み合わせによって保護されます。

IPsec プロポーザル ポリシーは、IPsec トンネルに必要な設定を定義します。IPsec プロポーザルとは、デバイスの VPN インターフェイスに適用される 1 つ以上の暗号マップの集合です。暗号マップには、IPsec セキュリティ アソシエーションを設定するために必要なすべてのコンポーネントが組み合わされています。これらのコンポーネントには以下のものがあります。

- プロポーザル (またはトランスフォームセット) とは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルおよびアルゴリズムの組み合わせです。IPsec セキュリティ アソシエーション (SA) ネゴシエーション中に、ピアでは、両方のピアに共通するプロポーザルが検索されます。そのようなプロポーザルが検出されると、そのプロポーザルを適用して、その暗号マップのアクセスリストでデータフローを保護する SA が作成され、VPN でトラフィックが保護されます。IKEv1 と IKEv2 には別個の IPsec プロポーザルがあります。IKEv1 プロポーザル (トランスフォームセット) では、パラメータごとに 1 つの値を設定します。IKEv2 プロポーザルでは、単一のプロポーザルに複数の暗号化アルゴリズムと統合アルゴリズムを設定できます。
- 暗号マップには、IPsec ルール、プロポーザル、リモート ピア、IPsec SA を定義するために必要なその他のパラメータを含む、IPsec セキュリティ アソシエーション (SA) を設定するために必要なすべてのコンポーネントが組み合わされています。2 つのピアが SA を確立しようとする場合は、それぞれに少なくとも 1 つの互換暗号マップエントリが必要です。

不明なリモート ピアがローカル ハブとの間の IPsec セキュリティ アソシエーションの開始を試みた場合、ダイナミック暗号マップ ポリシーがサイト間 VPN で使用されます。ハブは、セキュリティ アソシエーション ネゴシエーションを開始できません。ダイナミック暗号ポリシーを使用することによって、ハブがリモートピアのアイデンティティを把握していない場合でも、リモートピアはローカルハブとの間で IPsec トラフィックを交換できます。実質的には、ダイナミック暗号マップポリシーによって、すべてのパラメータが設定されていない暗号マップエントリが作成されます。設定されていないパラメータは、IPsec ネゴシエーションの結果として、リモートピアの要件に合うようにあとで動的に設定されます。

ダイナミック暗号マップポリシーは、ハブアンドスポークおよび完全メッシュ VPN トポロジでのみ適用されます。ポイントツーポイントまたはフルメッシュ VPN トポロジでは、スタティッククリプトマップポリシーのみを適用できます。ポイントツーポイントトポロジでダイナミック暗号マップポリシーをエミュレートするには、2 つのデバイスでハブアンドスポークトポロジを作成します。スポークのダイナミック IP アドレスを指定して、このトポロジでダイナミック暗号マップを有効にします。

## VPN パケットフロー

Firepower Threat Defense デバイスでは、デフォルトでは、明示的な許可なしにいずれのトラフィックもアクセスコントロールを通過できません。VPN トンネルトラフィックも、Snort を通過するまでは、エンドポイントにリレーされません。着信トンネルパケットは復号されてから、Snort プロセスへ送信されます。Snort は、暗号化の前に発信パケットを処理します。

VPN トンネルのエンドポイント ノードごとに保護されたネットワークを識別するアクセス制御は、どのトラフィックが Firepower Threat Defense デバイスをパススルーしてエンドポイントに到達できるかを決定します。

さらに、システムは、トンネルがダウンしている場合は、トンネルトラフィックをパブリックなソースに送信しません。

## VPN ライセンス

Firepower Threat Defense VPN を有効にするための特別なライセンスはありません。デフォルトで利用可能です。

Firepower Management Center は、スマートライセンス サーバから提供される属性に基づいて、Firepower Threat Defense デバイスで強力な暗号の使用を許可するかブロックするかを決定します。

これは、Cisco Smart License Manager に登録するときデバイス上で輸出管理機能を許可するオプションを選択しているかどうかによって制御されます。評価ライセンスを使用している場合、または輸出管理機能を有効にしていない場合は、強力な暗号化を使用できません。

## VPN 接続の安全性を確保する方法

VPN トンネルは通常、インターネットなどのパブリック ネットワークを経由するため、トラフィックを保護するために接続を暗号化する必要があります。IKE ポリシーと IPsec プロポーサルを使用して、暗号化とその他のセキュリティ技術を定義し、適用します。

デバイス ライセンスによって強力な暗号化を適用できる場合は、広範な暗号化とハッシュ アルゴリズム、および Diffie-Hellman グループがあり、その中から選択できます。ただし、一般に、トンネルに適用する暗号化が強力なほど、システムパフォーマンスは低下します。効率を損なうことなく十分な保護を提供するセキュリティとパフォーマンスのバランスを見出します。

シスコでは、どのオプションを選択するかについての特定のガイダンスは提供できません。比較的大規模な企業またはその他の組織内で運用している場合は、すでに、満たす必要がある標準が定義されている可能性があります。定義されていない場合は、時間を割いてオプションを調べてください。

以降のトピックでは、使用可能なオプションについて説明します。

## 使用する暗号化アルゴリズムの決定

IKE ポリシーまたは IPsec プロポーザルに使用する暗号化アルゴリズムを決定する際、選択肢は VPN のデバイスでサポートされるアルゴリズムに限られます。

IKEv2 では、複数の暗号化アルゴリズムを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

IPsec プロポーザルでは、認証、暗号化、およびアンチリプレイ サービスを提供するカプセル化セキュリティプロトコル (ESP) によってアルゴリズムが使用されます。ESP は、IP プロトコルタイプ 50 です。IKEv1 IPsec プロポーザルでは、アルゴリズム名の前に ESP というプレフィックスが付けられます。

デバイスライセンスが強力な暗号化を適用できる場合、次の暗号化アルゴリズムを選択できます。強力な暗号化の対象ではない場合、DES のみ選択できます。

- **AES-GCM**— (IKEv2 のみ) Galois/カウンタ モードの **Advanced Encryption Standard** は、機密性、データの発信元の認証を提供する操作のブロック暗号モードであり、AES よりも優れたセキュリティを提供します。AES-GCM には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。GCM は **NSA Suite B** をサポートするために必要となる AES モードです。NSA Suite B は、暗号化強度に関する連邦標準規格を満たすためにデバイスがサポートすべき一連の暗号化アルゴリズムです。
- **AES-GMAC**— (IKEv2 IPsec プロポーザルのみ)。Advanced Encryption Standard のガロアメッセージ認証コード (GMAC) は、データ発信元認証だけを行う操作のブロック暗号モードです。これは AES-GCM の一種であり、データを暗号化せずにデータ認証が行えます。AES-GMAC には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。
- **AES (Advanced Encryption Standard)** は DES よりも高度なセキュリティを提供する対称暗号化アルゴリズムであり、計算的には 3DES よりも効率的です。AES には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。
- **3DES (トリプル DES)** : 56 ビット キーを使用して暗号化を 3 回行います。異なるキーを使用してデータの各ブロックを 3 回処理するため、DES よりも安全です。ただし、使用するシステムリソースが多くなり、DES よりも速度が遅くなります。
- **DES (データ暗号化標準)** : 56 ビット キーを使用して暗号化する対称秘密鍵ブロックアルゴリズムです。3DES よりも高速であり、使用するシステムリソースも少ないですが、安全性も劣ります。堅牢なデータ機密保持が必要ない場合、およびシステムリソースや速度が重要である場合には、DES を選択します。
- **Null** : ヌル暗号化アルゴリズムは暗号化なしで認証します。通常はテスト目的にのみ使用されます。



## 使用するハッシュ アルゴリズムの決定

IKE ポリシーでは、ハッシュ アルゴリズムがメッセージダイジェストを作成します。これは、メッセージの整合性を保証するために使用されます。IKEv2 では、ハッシュ アルゴリズムは 2 つのオプションに分かれています。1 つは整合性アルゴリズムに使用され、もう 1 つは擬似乱数関数 (PRF) に使用されます。

IPsec プロポーザルでは、ハッシュ アルゴリズムは Encapsulating Security Protocol (ESP) による認証に使用されます。IKEv2 IPsec プロポーザルでは、これは整合性のハッシュと呼ばれます。IKEv1 IPsec プロポーザルでは、アルゴリズム名の接頭辞が「ESP-」となり、「-HMAC」 (Hash Method Authentication Code) という接尾辞も使用されます。

IKEv2 では、複数のハッシュ アルゴリズムを設定できます。各設定が、安全性の高い順に順序付けられ、ピアとのネゴシエーションにはこの順序が使用されます。IKEv1 では、1 つのオプションしか選択できません。

選択可能なハッシュ アルゴリズムは、次のとおりです。

- **SHA (Secure Hash Algorithm) : 160 ビットのダイジェストを生成します。SHA には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。ただし、SHA は MD5 よりもリソース消費量が大きくなります。最大レベルのセキュリティを必要とする実装には、SHA ハッシュ アルゴリズムを使用してください。**

Standard SHA (SHA1) は 160 ビットのダイジェストを生成します。

IKEv2 の設定では、以下の SHA-2 オプションを指定して、より高度なセキュリティを実現することができます。NSA Suite B 暗号化仕様を実装するには、次のいずれかを選択します。

- **SHA256 : 256 ビットのダイジェストを生成するセキュアハッシュ アルゴリズム SHA 2 を指定します。**
- **SHA384 : 384 ビットのダイジェストを生成するセキュアハッシュ アルゴリズム SHA 2 を指定します。**
- **SHA512 : 512 ビットのダイジェストを生成するセキュアハッシュ アルゴリズム SHA 2 を指定します。**
- **[MD5 (Message Digest 5)] : 128 ビットのダイジェストを生成します。MD5 は処理時間が短いため、全体的なパフォーマンスが SHA より高速ですが、SHA より強度は低いと考えられています。**
- **NULL またはなし (NULL、ESP-NONE) : (IPsec プロポーザルのみ) NULL ハッシュ アルゴリズム。通常はテスト目的のみに使用されます。しかし、暗号化オプションとしていずれかの AES-GCM/GMAC オプションを選択した場合は、NULL 整合性アルゴリズムを選択する必要があります。NULL 以外のオプションを選択した場合、これらの暗号化標準に対しては、整合性ハッシュは無視されます。**

## 使用する Diffie-Hellman 係数グループの決定

次の Diffie-Hellman キー導出アルゴリズムを使用して、IPsec Security Association (SA : セキュリティアソシエーション) キーを生成することができます。各グループでは、異なるサイズの係数が使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。両方のピアに、一致する係数グループが存在する必要があります。

AES 暗号化を選択する場合は、AES で必要な大きいキー サイズをサポートするために、Diffie-Hellman (DH : デフィーヘルマン) グループ 5 以降を使用する必要があります。IKEv1 ポリシーではグループ 1、2、5 のみ許可されます。

NSA Suite-B の暗号化の仕様を実装するには、IKEv2 を使用して楕円曲線 Diffie-Hellman (ECDH) オプション : 19、20、21 のいずれか 1 つを選択します。楕円曲線オプションと、2048 ビット係数を使用するグループは、Logjam のような攻撃にさらされる可能性が低くなります。

IKEv2 では、複数のグループを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。

IKEv1 では、単一のオプションのみ選択できます。

- 1 : Diffie-Hellman グループ 1 (768 ビット係数)。
- 2 : Diffie-Hellman グループ 2 (1024 ビット係数)。
- 5 : Diffie-Hellman グループ 5 (1536 ビット係数)。128 ビットのキーでは十分な保護レベルです。
- 14 : Diffie-Hellman グループ 14 (2048 ビット係数)。192 ビットのキーでは十分な保護レベルです。
- 19 : Diffie-Hellman グループ 19 (256 ビット楕円曲線)。
- 20 : Diffie-Hellman グループ 20 (384 ビット楕円曲線)。
- 21 : Diffie-Hellman グループ 21 (521 ビット楕円曲線)。
- 24 : Diffie-Hellman グループ 24 (2048 ビット係数および 256 素数位数サブグループ)。

## VPN トポロジオプション

新しい VPN トポロジを作成するには、最低でも、固有の名前をつけ、トポロジの型を特定し、IKE バージョンを選択する必要があります。それぞれが VPN トンネルグループを含む 3 つの型のトポロジから選択できます。

- ポイントツーポイント (PTP) トポロジでは、2 つのエンドポイント間に VPN トンネルを確立します。
- ハブおよびスポーク トポロジは、ハブエンドポイントをスポークエンドポイントのグループに接続する VPN トンネルグループを確立します。

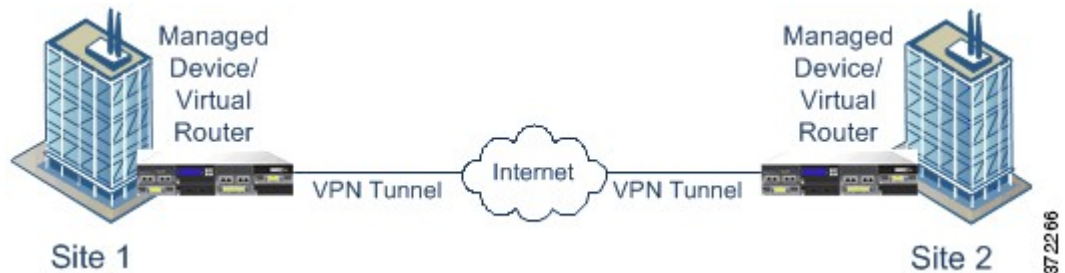
- フルメッシュのトポロジは、エンドポイントのセットの間で VPN トンネルのグループを確立します。

VPN 認証の事前共有キーを手動または自動で定義します。デフォルトのキーはありません。自動を選択すると、Firepower Management Center は事前共有キーを生成して、そのキーをトポロジ内のすべてのノードに割り当てます。

## ポイントツーポイントの VPN トポロジ

ポイントツーポイントの VPN トポロジでは、2つのエンドポイントが相互に直接通信します。2つのエンドポイントをピアデバイスとして設定し、いずれかのデバイスでセキュアな接続を開始することができます。

次の図は、一般的なポイントツーポイントの VPN トポロジを示しています。

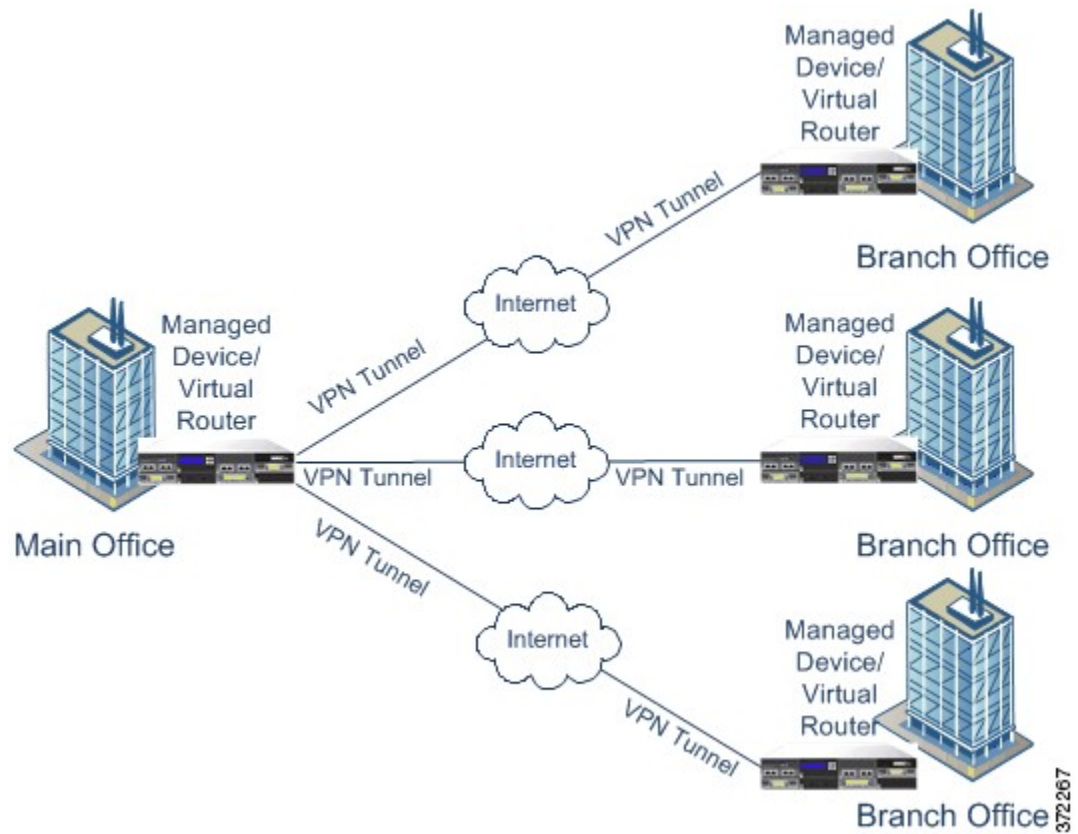


## ハブアンドスポーク VPN トポロジ

ハブアンドスポーク VPN トポロジでは、中央のエンドポイント（ハブノード）が複数のエンドポイント（スポークノード）と接続します。ハブノードと個々のスポークエンドポイント間のそれぞれの接続は、別の VPN トンネルです。いずれかのスポークノードの背後にあるホストは、ハブノードを介して互いに通信できます。

ハブアンドスポークトポロジは一般的に、インターネットや他のサードパーティのネットワークを介してセキュアな接続を使用している組織の本社とブランチオフィスを接続する VPN を表します。これらの展開は、すべての従業員に対して、組織のネットワークへのコントロールされたアクセスを提供します。一般的に、ハブノードは本社に配置します。スポークノードはブランチオフィスに配置し、大半のトラフィックはここから開始されます。

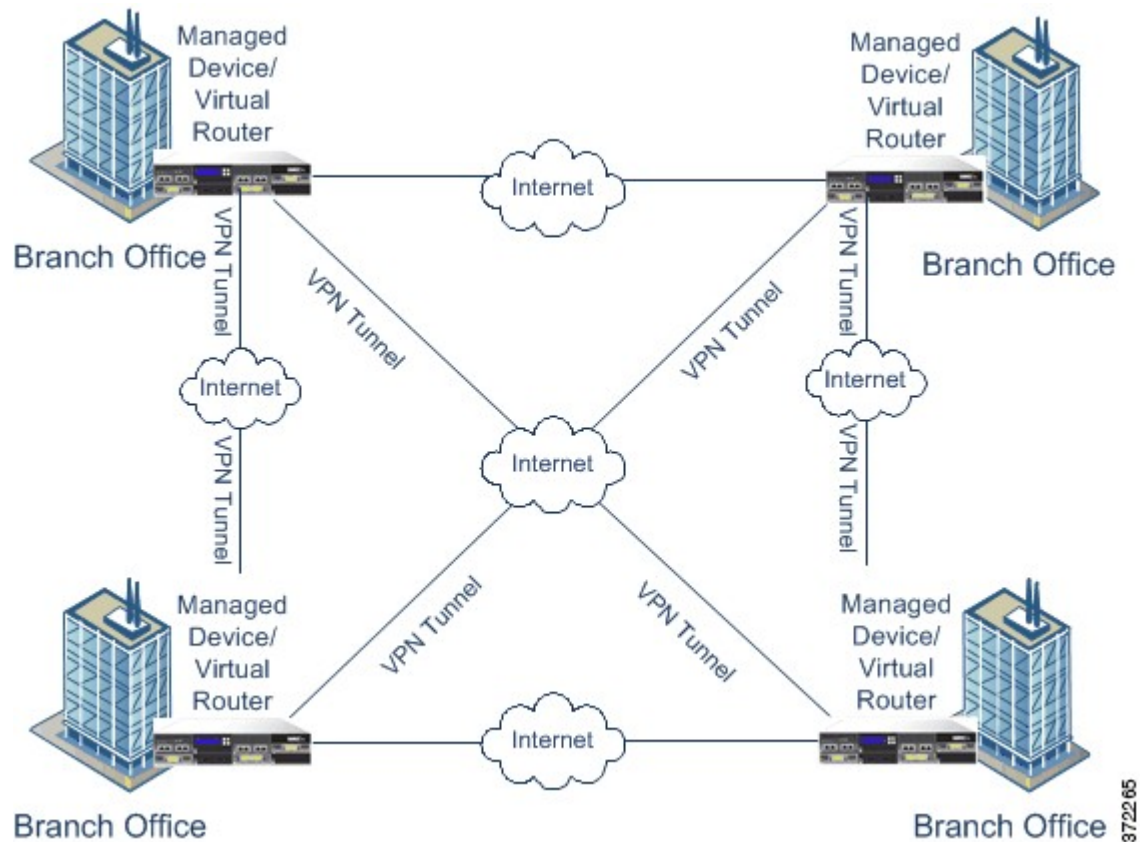
次の図は、一般的なハブアンドスポーク VPN トポロジを示しています。



## フルメッシュ VPN トポロジ

フルメッシュ VPN トポロジでは、すべてのエンドポイントが個々の VPN トンネルによって他のエンドポイントと通信できます。このトポロジにより、あるエンドポイントで障害が発生しても、残りのエンドポイントの相互通信は維持されるように冗長性が提供されます。これは、一般的に分散したブランチ オフィスが配置されたグループを接続する VPN を表します。この設定で展開する VPN 対応の管理対象デバイスの数は、必要な冗長性のレベルによって異なります。

次の図は、一般的なフルメッシュ VPN トポロジを示しています。



372265

## 暗黙的にサポートされるトポロジ

3つの主要なVPNトポロジに加えて、これらのトポロジを組み合わせた他のより複雑なトポロジを作成することもできます。具体的には以下のとおりです。

- 部分メッシュ**：このネットワークでは、一部のデバイスはフルメッシュトポロジに編成され、その他のデバイスは、フルメッシュ構成のデバイスのうちのいくつかとのハブアンドスポーク接続またはポイントツーポイント接続を形成します。部分メッシュには、フルメッシュトポロジほどの冗長性はありませんが、導入コストがより低くなります。部分メッシュトポロジは、フルメッシュ構成のバックボーンに接続するペリフェラルネットワークで使用されます。
- 階層型ハブアンドスポーク**：このネットワークでは、あるデバイスが、1つ以上のトポロジでハブとして動作し、他のトポロジではスパイクとして動作できます。スポークグループからそれらの直近のハブへのトラフィックが許可されます。
- 結合ハブアンドスポーク**：接続して1つのポイントツーポイントトンネルを形成する、2つのトポロジ（ハブアンドスポーク、ポイントツーポイント、またはフルメッシュ）の組み合わせです。たとえば、2つのハブアンドスポークトポロジから構成され、それぞれのハブがポイントツーポイントトポロジのピアデバイスとして動作する結合ハブアンドスポークトポロジを作成できます。





## 第 39 章

# Firepower Threat Defense VPNの導入

- [Firepower Threat Defense サイト間 VPN について \(897 ページ\)](#)
- [VPN ライセンス \(898 ページ\)](#)
- [Firepower Threat Defense サイト間 VPN ガイドラインと制約事項 \(899 ページ\)](#)

## Firepower Threat Defense サイト間 VPN について

Firepower Threat Defense サイト間 VPN では、次の機能がサポートされています。

- IPsec IKEv1 および IKEv2 プロトコルの両方をサポート。
- 自動または手動の事前共有認証キー。
- IPv4 および IPv6。内部、外部のすべての組み合わせをサポート。
- スタティック インターフェイスおよびダイナミック インターフェイス。
- Firepower Management Center および Firepower Threat Defense 両方の HA 環境をサポート。
- トンネルがダウンした際の VPN アラート。
- Firepower Threat Defense 統合 CLI により利用可能なトンネル統計。

### VPN トポロジ

新しいサイト間 VPN トポロジを作成するには、少なくとも、一意の名前を付け、トポロジタイプを指定し、IPsec IKEv1 または IKEv2 あるいはその両方に使用される IKE バージョンを選択する必要があります。また、事前共有キーを指定します。設定したら、Firepower Threat Defense デバイスにトポロジを展開します。Firepower Management Center は、Firepower Threat Defense デバイスのサイト間 VPN のみ設定します。

次の3つのタイプのトポロジから選択することができます。トポロジには、VPN トンネルが1つ以上含まれています。

- ポイントツーポイント (PTP) 型の展開は、2つのエンドポイント間でVPN トンネルを確立します。

- ハブアンドスポーク型の展開は、VPN トンネルのグループを確立し、ハブ エンドポイントをスポーク ノードのグループに接続します。
- フルメッシュ型の展開は、エンドポイントのセット内で VPN トンネルのグループを確立します。

### IPsec と IKE

Firepower Management Center では、サイト間 VPN は、VPN トポロジに割り当てられた IKE ポリシーおよび IPsec プロポーザルに基づいて設定されます。ポリシーとプロポーザルはパラメータのセットであり、これらのパラメータによって、IPsec トンネル内のトラフィックでセキュリティを確保するために使用されるセキュリティ プロトコルやアルゴリズムなど、サイト間 VPN の特性が定義されます。VPN トポロジに割り当て可能な完全な設定イメージを定義するために、複数のポリシー タイプが必要となる場合があります。

### 認証

VPN 認証の事前共有キーを定義します。トポロジ内のすべての VPN ノードに使用するデフォルト キーを手動で指定するか、Firepower Management Center に自動的に生成させることが可能です。

### エクストラネット デバイス

各トポロジタイプには、Firepower Management Center で管理しないデバイスである、エクストラネット デバイスが含まれる可能性があります。これには次が含まれます。

- Firepower Management Center ではサポートされているが、ユーザの部門が担当していないシスコ デバイス。たとえば、社内の他の部門が管理するネットワーク内のスポークや、サービス プロバイダーやパートナー ネットワークへの接続などです。
- シスコ製以外のデバイス。Firepower Management Center を使用して、シスコ製以外のデバイスに対する設定を作成したり、展開したりすることはできません。

シスコ以外のデバイス、または Firepower Management Center で管理されていないシスコ デバイスを VPN トポロジに「その他の」デバイスとして追加します。また、各リモート デバイスの IP アドレスも指定します。

## VPN ライセンス

Firepower Threat Defense VPN を有効にするための特別なライセンスはありません。デフォルトで利用可能です。

Firepower Management Center は、スマートライセンス サーバから提供される属性に基づいて、Firepower Threat Defense デバイスで強力な暗号の使用を許可するかブロックするかを決定します。



これは、Cisco Smart License Manager に登録するときにデバイス上で輸出管理機能を許可するオプションを選択しているかどうかによって制御されます。評価ライセンスを使用している場合、または輸出管理機能を有効にしていない場合は、強力な暗号化を使用できません。

## Firepower Threat Defense サイト間 VPN ガイドラインと制約事項

- PKI 証明書には対応していません。認証にあたっては、事前共有キーにのみ対応していません。
- 現在のドメイン内ではないエンドポイント用のエクストラネットピアを使用するのみ、ドメイン間の VPN 接続が可能です。
- VPN トポロジをドメイン間で移動させることはできません。
- 「範囲」オプションのあるネットワーク オブジェクトは、VPN では対応していません。
- Firepower Threat Defense VPN のバックアップは、Firepower Management バックアップを使用した場合のみ行われます。
- Firepower Threat Defense VPN では、現在、PDF のエクスポートおよびポリシーの比較には対応していません。
- Firepower Threat Defense VPN ではトンネル単位またはデバイス単位の編集オプションはありません。トポロジ全体のみ編集できます。
- クラスタ化環境では、Firepower Threat Defense VPN には対応していません。
- Firepower Management Center では、トンネルの状態はリアルタイムではなく、5 分間隔でアップロードされます。
- トンネルモードにのみ対応し、トランスポートモードには対応していません。IPsec トンネルモードは、新しい IP パケットのペイロードになる元の IP データグラム全体を暗号化します。トンネルモードは、ファイアウォールの背後にあるホストとの間で送受信されるトラフィックをファイアウォールが保護する場合に使用します。トンネルモードは、インターネットなどの非信頼ネットワークを介して接続されている 2 つのファイアウォール（またはその他のセキュリティ ゲートウェイ）間で通常の IPsec が実装される標準の方法です。





## 第 40 章

# Firepower Threat Defense VPN の管理

- [Firepower Threat Defense のサイト間 VPN の管理 \(901 ページ\)](#)
- [Firepower Threat Defense サイト間 VPN の設定 \(902 ページ\)](#)
- [Firepower Threat Defense VPN のモニタリング \(911 ページ\)](#)

## Firepower Threat Defense のサイト間 VPN の管理


スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
エクスポート コンプライアンス	該当なし	Firepower Threat Defense	リーフのみ	Admin

### 手順

[デバイス (Devices)] > [VPN] > [サイト間 (Site To Site)] を選択して、Firepower Threat Defense のサイト間 VPN の設定と展開を管理します。次のオプションから選択します。

- 追加：新しい VPN トポロジを作成するには、 [VPN の追加 (Add VPN)] > [Firepower Threat Defense デバイス (Firepower Threat Defense Device)] をクリックして、[Firepower Threat Defense サイト間 VPN の設定 \(902 ページ\)](#) の手順を実行します。

(注) VPN トポロジは、リーフ ドメインでのみ作成できます。

- 編集：既存の VPN トポロジの設定を変更するには、編集アイコン () をクリックします。変更は設定とほとんど同じです。前述の手順を実行してください。

(注) トポロジタイプは、最初の保存後に編集することはできません。トポロジタイプを変更するには、トポロジを削除してから新しいものを作成します。

2 人のユーザが同じトポロジを同時に編集してはいけません。ただし、Web インターフェイスでは同時編集を防止していません。

- 削除：VPN の展開を削除するには、削除アイコン (🗑️) をクリックします。
- VPN ステータスの表示：このステータスは Firepower の VPN にのみ適用されます。現時点では、Firepower Threat Defense VPN についてはステータスが表示されません。Firepower Threat Defense VPN のステータスを確認するには、[こちら](#) を参照してください。
- 展開：[展開 (Deploy)] をクリックします ([設定変更の導入 \(350 ページ\)](#) を参照)。  
(注) 一部の VPN 設定は、展開時にのみ検証されます。展開が成功したことを確認してください。

## Firepower Threat Defense サイト間 VPN の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
エクスポート コンプライアンス	該当なし	Firepower Threat Defense	リーフのみ	Admin

### 手順

- ステップ 1** [デバイス (Devices)] > [VPN] > [サイト間 (Site To Site)]。その後、[VPN の追加 (Add VPN)] > [Firepower Threat Defense デバイス (Firepower Threat Defense Device)]、またはリストされている VPN トポロジを編集します。を選択します。
- ステップ 2** 一意のトポロジ名を入力します。トポロジには、Firepower Threat Defense VPN であることとトポロジタイプを示す名前を付けることをお勧めします。
- ステップ 3** この VPN のネットワーク トポロジを選択します。
- ステップ 4** IKE ネゴシエーション中に使用する IKE バージョンとして、[IKEv1] または [IKEv2] のいずれかを選択します。
- デフォルトは [IKEv2] です。必要に応じて、いずれかまたは両方のオプションを選択します。トポロジ内のデバイスが IKEv2 をサポートしない場合は、[IKEv1] を選択します。
- ステップ 5** 必須: トポロジの各ノードの追加アイコン (⊕) をクリックして、この VPN 展開のためのエンドポイントを追加します。

[Firepower Threat Defense VPN エンドポイントオプション \(903 ページ\)](#) の説明に従って各エンドポイント フィールドを設定します。

- ポイントツーポイントの場合は、ノード A とノード B を設定します。
- ハブ アンド スポークの場合は、ハブ ノードとスポーク ノードを設定します。

- フル メッシュの場合は、複数のノードを設定します

- ステップ 6** (任意) 次の説明に従って、この展開のデフォルト以外の IKE オプションを指定します [Firepower Threat Defense VPN IKE オプション \(905 ページ\)](#)
- ステップ 7** (任意) 次の説明に従って、この展開のデフォルト以外の IPsec オプションを指定します [Firepower Threat Defense VPN IPsec オプション \(906 ページ\)](#)
- ステップ 8** (任意) [Firepower Threat Defense VPN 展開の詳細オプション \(908 ページ\)](#) の説明に従って、この展開のデフォルト以外の詳細オプションを指定します。
- ステップ 9** [保存 (Save) ] をクリックします。  
エンドポイントが構成に追加されます。

---

### 次のタスク

設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。



(注) 一部の VPN 設定は、展開時にのみ検証されます。展開が成功したことを確認してください。

---

## Firepower Threat Defense VPN エンドポイント オプション

### ナビゲーションパス

[デバイス (Devices) ] > [VPN] > [サイト間 (Site To Site) ]。その後、[VPN の追加 (Add VPN) ] > [Firepower Threat Defense デバイス (Firepower Threat Defense Device) ]、またはリストされている VPN トポロジを編集します。[エンドポイント (Endpoint) ] タブを開きます。

### フィールド

#### Device

展開するエンドポイント ノードを選択します。

- この Firepower Threat Defense で管理する Firepower Management Center デバイス。
- この Firepower Threat Defense で管理する Firepower Management Center ハイ アベイラビリティ コンテナ。
- [エクストラネット (Extranet) ] デバイス。この Firepower Management Center の管理対象ではない任意のデバイス (シスコまたはサードパーティ) 。

#### デバイス名 (Device Name)

エクストラネットデバイスの場合のみ、このデバイスの名前を入力します。シスコでは、管理対象ではないデバイスとして識別できるような名前を付けることを推奨します。

## インターフェイス (Interface)

エンドポイントとして管理対象デバイスを選択した場合は、その管理対象デバイスのインターフェイスを選択します。

### [IPアドレス (IP Address)]

- Firepower Management Center の管理対象ではないデバイスを選択した場合は、エンドポイントの IP アドレスを指定します。
- エンドポイントとして管理対象デバイスを選択した場合は、ドロップダウンリストから 1 つの IPv4 アドレスまたは複数の IPv6 アドレスを選択します（これらはすでにこの管理対象デバイスのこのインターフェイスに割り当てられているアドレスです）。
- トポロジ内のすべてのエンドポイントは、同じ IP アドレッシング方式でなければなりません。IPv4 トンネルは IPv6 トラフィックを伝送でき、逆もまた同様です。保護ネットワークでは、トンネルするトラフィックで使用するアドレッシング方式が定義されます。
- 管理対象デバイスがハイ アベイラビリティ コンテナである場合は、インターフェイスのリストから選択します。

### この IP はプライベートです (This IP is Private)

エンドポイントが、ネットワーク アドレス変換 (NAT) を備えたファイアウォールの背後に配置されている場合は、このチェックボックスをオンにします。

### パブリック IP アドレス (Public IP address)

[この IP はプライベートです (This IP is Private)] チェックボックスがオンの場合は、ファイアウォールのパブリック IP アドレスを指定します。エンドポイントがレスポンドの場合は、この値を指定します。

### 接続タイプ (Connection Type)

許可されるネゴシエーションを、bidirectional、answer-only、または originate-only として指定します。接続タイプのサポートされる組み合わせは次のとおりです。

表 64: 接続タイプのサポートされる組み合わせ

リモートノード	中央ノード
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

### 保護されたネットワーク (Protected Networks)

この VPN エンドポイントによって保護されたネットワークのリストを定義します。追加アイコン (+) をクリックして、使用可能なネットワークオブジェクトから選択するか、ネットワークオブジェクトインラインに追加します。ネットワークオブジェクトの作成

(434 ページ) を参照してください。アクセスコントロールリストがここで選択されたものから生成されます。

VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイントペアの保護されたネットワークは重複することはできません。エンドポイントについて保護されたネットワークのリストに 1 つ以上の IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ（つまり、IPv4 または IPv6）のエントリを少なくとも 1 つ持っていることが必要です。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です。（IPv4 については /32 CIDR アドレスを使用し、IPv6 については /128 CIDR アドレス ブロックを使用します）。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

## Firepower Threat Defense VPN IKE オプション

このトポロジに選択した IKE のバージョンの場合は、[IKEv1/IKEv2 設定 (IKEv1/IKEv2 Settings)] を指定します。



(注) このダイアログの設定は、トポロジ全体、すべてのトンネル、すべての管理対象デバイスに適用されます。

### ナビゲーションパス

[デバイス (Devices)] > [VPN] > [サイト間 (Site To Site)]。その後、[VPN の追加 (Add VPN)] > [Firepower Threat Defense デバイス (Firepower Threat Defense Device)]、またはリストされている VPN トポロジを編集します。[IKE] タブを開きます。

### フィールド

#### ポリシー

事前定義済みの IKEv1 または IKEv2 ポリシー オブジェクトを選択するか、または使用する新しいポリシー オブジェクトを作成します。詳細の参照先：[Firepower Threat Defense IKE ポリシー \(516 ページ\)](#)

#### キータイプ

- [手動 (Manual)] : この VPN に使用される事前共有キーを手動で割り当てます。[キー (Key)] を指定して、[キーの確認 (Confirm Key)] に再入力します。
- [自動 (Automatic)] : 管理センターが、この VPN に使用される事前共有キーを自動的に定義します。[キー長 (Key Length)] を指定します。キーの文字数は 1 ~ 27 文字です。

## Firepower Threat Defense VPN IPsec オプション



- (注) このダイアログの設定は、トポロジ全体、すべてのトンネル、すべての管理対象デバイスに適用されます。

### クリプトマップタイプ (Crypto-Map Type)

クリプトマップには、IPsec Security Association (SA; セキュリティアソシエーション) を設定するために必要なすべてのコンポーネントが組み合わされています。2つのピアがSAを確立しようとする場合は、それぞれに少なくとも1つの互換クリプトマップエントリが必要です。クリプトマップエントリに定義されたプロポーザルは、そのクリプトマップのIPsecルールによって指定されたデータフローを保護するためのIPsecセキュリティネゴシエーションで使用されます。この展開のクリプトマップにスタティックまたはダイナミックを選択します。

- [スタティック (Static) ]: スタティック暗号マップは、ポイントツーポイントまたは完全メッシュVPNトポロジで使用します。
- [ダイナミック (Dynamic) ]: 実質的に、ダイナミック暗号マップによって、すべてのパラメータが設定されていない暗号マップエントリが作成されます。設定されていないパラメータは、IPsecネゴシエーションの結果として、リモートピアの要件に合うようにあとで動的に設定されます。

ダイナミッククリプトマップポリシーは、ハブアンドスポークVPN設定にのみ適用されます。ポイントツーポイントまたはフルメッシュVPNトポロジでは、スタティッククリプトマップポリシーのみを適用できます。2つのデバイスを使用してハブアンドスポークトポロジを作成することで、ポイントツーポイントトポロジでダイナミッククリプトマップの使用をエミュレートします。スポークのダイナミックIPアドレスを指定し、このトポロジでダイナミッククリプトマップを有効にします。

### IKEv2 モード (IKEv2 Mode)

IPsec IKEv2 の場合のみ、カプセル化モードはトンネルにESP暗号化と認証を適用するために指定します。これにより、ESPが適用されるオリジナルのIPパケットの部分が決定されます。

- [トンネルモード (Tunnel mode) ]: (デフォルト) カプセル化モードがトンネルモードに設定されます。トンネルモードでは、ESP暗号化と認証が元のIPパケット全体 (IPヘッダーとデータ) に適用されるため、最終的な送信元アドレスと宛先アドレスが非表示になり、新しいIPパケットでペイロードになります。

トンネルモードの大きな利点は、エンドシステムを変更しなくてもIPsecを利用できるということです。このモードでは、ルータなどのネットワークデバイスがIPsecのプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPsecトンネルを使用して転送します。宛先ルータは元のIPデータグラムを復号化し、宛先システムに転送します。また、トラフィック分析から保護することもできます。トンネルモードを使用すると、攻撃者




にはトンネルのエンドポイントしかわからず、トンネリングされたパケットの本来の送信元と宛先はわかりません（これらがトンネルのエンドポイントと同じ場合でも同様）。

- [転送優先 (Transport preferred)] : ピアがサポートしていない場合、カプセル化モードは、トンネルモードにフォールバックするオプション付きの転送モードに設定されます。転送モードでは IP ペイロードだけが暗号化され、元の IP ヘッダーはそのまま使用されます。したがって、管理者は、VPN インターフェイスの IP アドレスと一致する保護されたネットワークを選択する必要があります。

このモードには、各パケットに数バイトしか追加されず、パブリックネットワーク上のデバイスに、パケットの最終的な送信元と宛先を認識できるという利点があります。転送モードでは、中間ネットワークでの特別な処理（たとえば QoS）を、IP ヘッダーの情報に基づいて実行できるようになります。ただし、レイヤ 4 ヘッダーが暗号化されるため、パケットの検査が制限されます。

- [転送必須 (Transport required)] : カプセル化モードは転送モードのみに設定され、トンネルモードにフォールバックすることはできません。転送モードをサポートしていない 1 つのエンドポイントがあるせいで、エンドポイントが転送モードを正常にネゴシエートできない場合、VPN 接続は行われません。

### プロポーザル (Proposals)

選択した IKEv1 または IKEv2 メソッドのプロポーザルを指定するには、 をクリックします。利用可能な [IKEv1 IPsec プロポーザル (IKEv1 IPsec Proposals)] または [IKEv2 IPsec プロポーザル (IKEv2 IPsec Proposals)] オブジェクトから選択するか、または新しいプロポーザルを作成して選択します。詳細については、「[IKEv1 IPsec プロポーザル オブジェクトの設定 \(521 ページ\)](#)」および「[IKEv2 IPsec プロポーザル オブジェクトの設定 \(522 ページ\)](#)」を参照してください。

### セキュリティ アソシエーション (SA) の強度適用の有効化 (Enable Security Association (SA) Strength Enforcement)

このオプションを有効にすると、子 IPsec SA で使用される暗号化アルゴリズムが、親 IKE SA よりも強くなることはありません（キー内のビット数の観点から）。

### リバース ルート インジェクションを有効にする (Enable Reverse Route Injection)

リバース ルート インジェクション (RRI) により、スタティック ルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。

### Perfect Forward Secrecy の有効化 (Enable Perfect Forward Secrecy)

暗号化された交換ごとに一意のセッション キーを生成および使用するために、Perfect Forward Secrecy (PFS) を使用するかどうかを指定します。固有のセッション キーを使用することで、後続の復号から交換が保護されます。また、交換全体が記録されていて、攻撃者がエンドポイントデバイスで使用されている事前共有キーや秘密キーを入手している場合であっても保護されます。このオプションを選択する場合は、[係数グループ (Modulus Group)] リストで、PFS セッション キーの生成時に使用する Diffie-Hellman キー導出アルゴリズムも選択します。

**係数グループ (Modulus Group)**

2つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2つのピアに、一致する係数グループが設定されている必要があります。オプションの説明の詳細については、[使用する Diffie-Hellman 係数グループの決定 \(892 ページ\)](#) を参照してください。

**ライフタイム(秒) (Lifetime (seconds))**

セキュリティアソシエーションが期限切れになる前に存続できる秒数。デフォルトは 28,800 秒です。

**ライフタイム (KB) (Lifetime (kbytes))**

特定のセキュリティアソシエーションが期限切れになる前にそのセキュリティアソシエーションを使用して IPsec ピア間を通過できるトラフィック量 (KB 単位)。デフォルトは 4,608,000 KB です。無限のデータを指定することはできません。

**ESPv3 設定 (ESPv3 Settings)****着信 ICMP のエラーメッセージを検証 (Validate incoming ICMP error messages)**

IPsec トンネルを介して受信され、プライベート ネットワーク上の内部ホストが宛先の ICMP エラーメッセージを検証するかどうかを選択します。

**「フラグメント禁止」ポリシーを有効にする (Enable 'Do Not Fragment' Policy)**

IP ヘッダーに Do-Not-Fragment (DF) ビットセットを持つ大きなパケットを IPsec サブシステムがどのように処理するかを定義します。

**ポリシー**

- [DF ビットのコピー (Copy DF bit) ] : DF ビットを維持します。
- [DF ビットのクリア (Clear DF bit) ] : DF ビットを無視します。
- [DF ビットの設定 (Set DF bit) ] : DF ビットを設定して使用します。

**トラフィック フロー機密保持 (TFC) パケットを有効にする (Enable Traffic Flow Confidentiality (TFC) Packets)**

トンネルを通過するトラフィック プロファイルをマスクするダミーの TFC パケットを有効にします。[バースト (Burst) ]、[ペイロードサイズ (Payload Size) ]、および [タイムアウト (Timeout) ]パラメータを使用して、指定した SA で不定期にランダムな長さのパケットを生成します。

## Firepower Threat Defense VPN 展開の詳細オプション

次に、展開で指定できる詳細オプションについて説明します。



(注) このダイアログの設定は、トポロジ全体、すべてのトンネル、すべての管理対象デバイスに適用されます。

**[詳細設定 (Advanced) ]> [IKE]> [ISAKMP 設定 (ISAKMP Settings) ]****IKE キープアライブ (IKE Keepalive)**

IKE キープアライブを有効または無効にします。または、[永続的に有効にする (EnableInfinite) ] に設定して、デバイスがキープアライブ モニタリングを開始することがないように指定します。

**しきい値 (Threshold)**

IKE キープアライブの信頼間隔を指定します。これは、キープアライブ モニタリングを開始するまでにピアに許可されるアイドル時間 (秒) です。最小値およびデフォルトは 10 秒で、最大値は 3600 秒です。

**再試行間隔 (Retry Interval)**

IKE キープアライブの再試行から再試行までの待機秒数を指定します。デフォルトは 2 秒で、最大値は 10 秒です。

**ピアに送信される ID: (Identity Sent to Peers:)**

IKE ネゴシエーションでピアが自身の識別に使用する ID を選択します。

- autoOrDN (デフォルト) : 接続タイプによって IKE ネゴシエーションを判別します。事前共有キーの IP アドレスまたは証明書認証の証明書 DN (未サポート) を使用します。
- ipAddress : ISAKMP 識別情報を交換するホストの IP アドレスを使用します。
- ホスト名 (Hostname) : ISAKMP 識別情報を交換するホストの完全修飾ドメイン名を使用します。この名前は、ホスト名とドメイン名で構成されます。

**アグレッシブ モードの有効化 (Enable Aggressive Mode)**

ハブアンドスポーク VPN トポロジでのみ使用できます。IP アドレスが不明であり、デバイスで DNS 解決を使用できない可能性がある場合は、このネゴシエーション方式を選択してキー情報を交換します。ホスト名およびドメイン名に基づいてネゴシエーションが行われます。

**[詳細設定 (Advanced) ]> [IKE]> [IvE2 セキュリティ アソシエーション (SA) 設定 (IvE2 Security Association (SA) Settings) ]**

IKE v2 について、オープン SA の数を制限するさらに詳細なセッション制御を使用することができます。デフォルトでは、SA の数は制限されません。

**クッキー チャレンジ (Cookie Challenge)**

SA 開始パケットの応答としてピアデバイスにクッキー チャレンジを送信するかどうかを指定します。これは、サービス妨害 (DoS) 攻撃の防止に役立つことがあります。デフォルトでは、使用可能な SA の 50% がネゴシエーション中である場合にクッキー チャレンジを使用します。次のオプションのいずれか 1 つを選択します。

- カスタム : (Custom :)
- しない (Never) (デフォルト)
- 常に (Always)

**着信クッキー チャレンジのしきい値 (Threshold to Challenge Incoming Cookies)**

許可されるネゴシエーション中の SA の総数の割合。この設定を指定すると、以降の SA ネゴシエーションに対してクッキーチャレンジがトリガーされます。範囲は 0 ~ 100% です。

**許可されるネゴシエーション中の SA の数 (Number of SAs Allowed in Negotiation)**

一時点でネゴシエーション中にできる SA の最大数を制限します。クッキーチャレンジと共に使用する場合は、有効なクロスチェックが実行されるようにするため、クッキーチャレンジのしきい値をこの制限値よりも低くしてください。

**許可される SA の最大数 (Maximum number of SAs Allowed)**

許可される IKEv2 接続の数を制限します。デフォルトでは無制限です。

**トンネルの切断時の通知を有効にする (Enable Notification on Tunnel Disconnect)**

管理者は、SA で受信された着信パケットがその SA のトラフィックセレクタと一致しない場合のピアへの IKE 通知の送信を有効または無効にすることができます。デフォルトでは、[この通知を送信する (Sending this notification)] は無効になっています。

**すべてのセッションが終了するまで、デバイスを再起動できません。**

オンにすると、すべてのアクティブなセッションが自動的に終了してからシステムが再起動されます。デフォルトでは、無効になっています。

**[詳細設定 (Advanced) ] > [IPsec] > [IPsec 設定 (IPsec Settings) ]****暗号化の前にフラグメンテーションを有効にする (Enable Fragmentation Before Encryption)**

このオプションは、IP フラグメンテーションをサポートしていない NAT デバイス間をトラフィックが通過できるようにします。このオプションを使用しても、IP フラグメンテーションをサポートしていない NAT デバイスの動作が妨げられることはありません。

**パスの最大伝送ユニットのエイジング (Path Maximum Transmission Unit Aging)**

オンにすると、PMTU (パス最大伝送ユニット) のエイジング、つまり、SA (セキュリティアソシエーション) の PMTU リセットまでの時間が有効になります。

**値のリセット間隔 (Value Reset Interval)**

SA (セキュリティアソシエーション) の PMTU 値が元の値にリセットされるまでの時間 (分) を入力します。有効範囲は 10 ~ 30 分です。デフォルトは無制限です。

**[詳細設定 (Advanced) ] > [トンネル (Tunnel) ] > [トンネルオプション (Tunnel Options) ]****ハブ経由のスポーク間接続を有効にする (Enable Spoke to Spoke Connectivity through Hub)****[詳細設定 (Advanced) ] > [トンネル (Tunnel) ] > [NAT 設定 (NAT Settings) ]****キープアライブメッセージトラバーサル (Keepalive Messages Traversal)**

NAT キープアライブメッセージトラバーサルを有効にするかどうかを選択します。VPN 接続ハブとスポークとの間にデバイス (中間デバイス) が配置されている場合、キープアライブメッセージを転送するために NAT トラバーサルキープアライブを使用します。このデバイスでは、IPsec フローで NAT を実行します。このオプションを選択する場合は、セッションがアクティブであることを示すためにスポークと中間デバイス間でキープアライブ信号が送信される間隔 (秒) を設定します。値は、5 ~ 3600 秒の範囲で指定します。デフォルトは 20 秒です。

### インターバル (Interval)

NAT キープアライブ間隔を 5 ~ 3600 秒の範囲で設定します。デフォルトは 20 秒です。

## Firepower Threat Defense VPN のモニタリング

Firepower Threat Defense VPN アクティビティを次のようにモニタします。

- システム メッセージ

メッセージセンターは、モニタリングを開始する場所です。この機能を使用すると、システムの使用状況およびステータスについて継続的に生成されるメッセージを確認できます。メッセージセンターを開くには、メインメニューの [展開 (Deploy)] ボタンのすぐ右側にある [システム ステータス (System Status)] アイコンをクリックします。メッセージセンターの使用方法については、[システムメッセージ \(323 ページ\)](#) を参照してください。

- VPN ヘルス イベント

これらのイベントは、[システム (System)] > [ヘルス (Health)] > [イベント (Events)] > [VPN ステータス (VPN Status)] で、その他のシステム イベントと共に表示されます。システムのヘルス イベントの表示に関する詳細については、[ヘルス モニタリング \(275 ページ\)](#) を参照してください。

- システム ログ

現在、Firepower Management Center は Firepower Threat Defense VPN syslog を読み取る機能を備えていません。これらの syslog は、分析とアーカイブのためにサードパーティ サーバに転送される必要があります。syslog サーバの設定とシステム ログの表示の詳細については、[Syslog の設定 \(1050 ページ\)](#) を参照してください。

- 統一された CLI コマンド、『*Command Reference for Firepower Threat Defense*』を参照してください。

Firepower Threat Defense デバイスで show、clear、および debug コマンドを使用して、VPN アクティビティのモニタおよびトラブルシューティングを行います。

### モニタリングのガイドライン

- 300 以上の Firepower Threat Defense デバイスが Firepower Management Center で設定されている場合、イベント処理の問題が発生する可能性があります。
- 接続が切断している場合、Firepower Threat Defense デバイスと Firepower Management Center の間のイベントが失われている可能性があります。





## 第 **XII** 部

# アプライアンス プラットフォームの設定

- システム設定 (System Configuration) (915 ページ)
- 管理対象デバイス用のプラットフォーム設定ポリシー (999 ページ)
- 従来型デバイス用の Firepower プラットフォーム設定 (1003 ページ)
- Firepower Threat Defense のプラットフォーム設定 (1033 ページ)







## 第 41 章

# システム設定 (System Configuration)

以下のトピックでは、Firepower Management Center および管理対象デバイスでシステム設定を行う方法について説明します。

- システム設定の概要 (916 ページ)
- アプライアンス情報 (919 ページ)
- カスタム HTTPS 証明書 (921 ページ)
- 外部データベース アクセスの設定 (927 ページ)
- データベース イベント数の制限 (929 ページ)
- 管理インターフェイス (931 ページ)
- システムのシャットダウンと再起動 (947 ページ)
- リモート ストレージ管理 (949 ページ)
- 変更調整 (954 ページ)
- ポリシー変更のコメント (956 ページ)
- アクセス リスト (957 ページ)
- 監査ログ (959 ページ)
- カスタム監査ログ クライアント証明書 (963 ページ)
- ダッシュボード設定 (968 ページ)
- DNS キャッシュ (969 ページ)
- 電子メールの通知 (970 ページ)
- 言語の選択 (972 ページ)
- ログイン バナー (973 ページ)
- SNMP ポーリング (974 ページ)
- セキュリティ認定準拠の (976 ページ)
- 時刻および時刻の同期 (981 ページ)
- セッション タイムアウト (986 ページ)
- 脆弱性マッピング (988 ページ)
- リモート コンソールのアクセス管理 (989 ページ)
- REST API 設定 (996 ページ)
- VMware Tools と仮想システム (997 ページ)

## システム設定の概要

システム設定の設定値は、Firepower Management Center またはクラシック管理対象デバイス (7000 および 8000 シリーズ、ASA FirePOWER、NGIPSv) のいずれかに適用されます。

- Firepower Management Center では、これらの構成設定は「ローカル」のシステム設定の一部です。Firepower Management Center 上のシステム設定は単一システムに固有のものであり、Management Center のシステム設定への変更はそのシステムのみに影響する点に注意してください。
- クラシック管理対象デバイスでは、プラットフォーム設定ポリシーの一部として Firepower Management Center から設定を適用します。共有ポリシーを作成して、展開全体で同様の設定になっている可能性の高い、管理対象デバイスに最適なシステム設定の設定値のサブセットを設定します。



**ヒント** 7000 および 8000 シリーズデバイスでは、ローカル Web インターフェイスからコンソール設定やリモート管理などのシステム設定の制限付きタスクを実行できます。これらは、プラットフォーム設定ポリシーを使用して 7000 または 8000 シリーズデバイスに適用される設定とは異なります。

## Firepower Management Center システム設定のナビゲーション

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	グローバルだけ	Admin

システム設定により、Firepower Management Center の基本設定を特定します。

### 手順

**ステップ 1** [システム (System)] > [設定 (Configuration)] を選択します。

**ステップ 2** ナビゲーション ウィンドウを使用して、変更する設定を選択します。詳細については、[表 65 : システム設定 \(917 ページ\)](#) を参照してください。

## システム設定

次の表に Firepower Management Center のシステム設定の説明を示します。この表では、7000 および 8000 シリーズ デバイスについて、デバイスのローカル Web インターフェイスから構成する設定、および Firepower Management Center から展開したプラットフォーム設定ポリシーを使用して構成する設定も示します。

表 65: システム設定

設定	説明	他の設定元	
		プラットフォーム設定	7000 & 8000 シリーズ
情報	アプライアンスに関する最新情報を表示し、表示名を編集します。 <a href="#">アプライアンス情報 (919 ページ)</a> を参照してください。	No	Yes
HTTPS Certificate	必要に応じて、信頼できる認証局の HTTPS サーバ証明書を要求し、システムに証明書をアップロードします。 <a href="#">カスタム HTTPS 証明書 (921 ページ)</a> を参照してください。	No	Yes
外部データベースアクセス	データベースへの外部読み取り専用アクセスを有効にし、ダウンロードするクライアント ドライバを提供します。 <a href="#">外部データベースアクセスの設定 (927 ページ)</a> を参照してください。	No	No
データベース	Firepower Management Center が保存できる各イベントのタイプの最大数を指定します。 <a href="#">データベースイベント数の制限 (929 ページ)</a> を参照してください。	No	No
管理インターフェイス	アプライアンスの IP アドレス、ホスト名、プロキシ設定などのオプションを変更します。 <a href="#">管理インターフェイス (931 ページ)</a> を参照してください。	No	Yes
プロセス	Firepower システム関連のプロセスをシャットダウン、リポート、または再起動します。 <a href="#">システムのシャットダウンと再起動 (947 ページ)</a> を参照してください。	No	Yes
リモートストレージデバイス	バックアップとレポート用のリモートストレージデバイスを設定します。 <a href="#">リモートストレージ管理 (949 ページ)</a> を参照してください。	No	No
リコンサイルの変更	過去 24 時間にわたるシステムへの変更の詳細なレポートを送信するようにシステムを設定します。 <a href="#">変更調整 (954 ページ)</a> を参照してください。	No	Yes
アクセスコントロールの設定	ユーザがアクセスコントロールポリシーを追加または変更する際にユーザにコメントを要求するようにシステムを設定します。 <a href="#">ポリシー変更のコメント (956 ページ)</a> を参照してください。	No	No

設定	説明	他の設定元	
		プラットフォーム設定	7000 & 8000 シリーズ
アクセス リスト	どのコンピュータが特定のポートでシステムにアクセスできるかを制御します。 <a href="#">アクセス リスト (957 ページ)</a> を参照してください。	Yes	No
監査ログ	外部ホストに監査ログを送信するようにシステムを設定します。 <a href="#">監査ログ (959 ページ)</a> を参照してください。	Yes	No
カスタム監査ログクライアント証明書	監査ログを外部ホストにストリーミングする際にチャンネルを保護するようにシステムを設定します。次を参照してください。 <a href="#">カスタム監査ログクライアント証明書 (963 ページ)</a>	Yes	No
ダッシュボード	ダッシュボードのカスタム分析ウィジェットを有効にします。 <a href="#">ダッシュボード設定 (968 ページ)</a> を参照してください。	No	No
DNS キャッシュ	イベント表示ページで IP アドレスを自動的に解決するようにシステムを設定します。 <a href="#">DNS キャッシュ (969 ページ)</a> を参照してください。	No	No
電子メール通知	メール ホストを設定し、暗号化方式を選択して、電子メールベースの通知とレポートに認証クレデンシャルを提供します。 <a href="#">電子メールの通知 (970 ページ)</a> を参照してください。	No	No
外部認証	アカウントが外部認証されるユーザのデフォルトのユーザ ロールを設定します。次を参照してください。 <a href="#">外部認証の設定 (1016 ページ)</a>	Yes	No
侵入ポリシーの設定	ユーザが侵入ポリシーを変更する際にユーザにコメントを要求するようにシステムを設定します。 <a href="#">ポリシー変更のコメント (956 ページ)</a> を参照してください。	No	No
[言語 (Language) ]	Web インターフェイスに異なる言語を指定します。 <a href="#">言語の選択 (972 ページ)</a> を参照してください。	Yes	No
ログインバナー	ユーザがログインすると表示されるカスタム ログインバナーを作成します。 <a href="#">ログインバナー (973 ページ)</a> を参照してください。	Yes	No
ネットワーク分析ポリシーの設定	ユーザがネットワーク分析ポリシーを変更する際にユーザにコメントを要求するようにシステムを設定します。 <a href="#">ポリシー変更のコメント (956 ページ)</a> を参照してください。	No	No
SNMP	Simple Network Management Protocol (SNMP) のポーリングを有効にします。 <a href="#">SNMP ポーリング (974 ページ)</a> を参照してください。	Yes	No
セキュリティ認定準拠	米国国防総省によって設定される特定の要件の順守を有効にします。 <a href="#">セキュリティ認定コンプライアンスの有効化 (979 ページ)</a> を参照してください。	Yes	No

設定	説明	他の設定元	
		プラットフォーム設定	7000 & 8000 シリーズ
時刻 (Time)	現在の時刻設定を確認し、現在のシステム設定の時刻同期の設定が[ローカル設定で手動 (Manually in Local Configuration)]に設定されている場合は、時間を変更します。 <a href="#">時刻および時刻の同期 (981 ページ)</a> を参照してください。	No	Yes
時刻の同期	システムの時刻の同期を管理します。 <a href="#">時刻および時刻の同期 (981 ページ)</a> を参照してください。	Yes	No
シェルタイムアウト	ユーザのログインセッションが非アクティブによりタイムアウトするまでのアイドル時間の長さを分単位で設定します。 <a href="#">セッションタイムアウト (986 ページ)</a> を参照してください。	Yes	No
脆弱性マッピング	ホスト IP アドレスから送受信されるアプリケーションプロトコルトラフィックの脆弱性をそのホスト IP アドレスにマップします。 <a href="#">脆弱性マッピング (988 ページ)</a> を参照してください。	No	No
コンソール設定	VGA またはシリアルポート経由、または Lights-Out Management (LOM) 経由のコンソールアクセスを設定します。 <a href="#">リモート コンソールのアクセス管理 (989 ページ)</a> を参照してください。	No	制限付き
REST API 設定	Firepower REST API 経由の Firepower Management Center へのアクセスを有効または無効にします。 <a href="#">REST API 設定 (996 ページ)</a> を参照してください。	No	No
VMware ツール	VMware ツールを有効にして Firepower Management Center Virtual で使用します。 <a href="#">VMware Tools と仮想システム (997 ページ)</a> を参照してください。	適用対象外	適用対象外

関連トピック

[Firepower プラットフォーム設定の概要 \(1003 ページ\)](#)

## アプライアンス情報

Web インターフェイスの [情報 (Information)] ページには、次の表に示す情報が含まれています。別途記載のない限り、フィールドはすべて読み取り専用です。

フィールド	説明
[名前 (Name) ]	アプライアンスに割り当てられた名前。この名前は Firepower システムのコンテキスト内でのみ使用されることに注意してください。ホスト名をアプライアンスの名前として使用できますが、このフィールドに別の名前を入力しても、ホスト名が変更されることはありません。
製品モデル (Product Model)	アプライアンスのモデル名。
シリアル番号 (Serial Number)	アプライアンスのシリアル番号。
ソフトウェア バージョン (Software Version)	アプライアンスに現在インストールされているソフトウェアのバージョン。
Firepower Management Center へのパケット転送の禁止 (Prohibit Packet Transfer to the)	管理対象デバイスがイベントに合わせてパケット データを送信し、Firepower Management Center 上にデータを保存するかを指定します。この設定は、7000 および 8000 シリーズ デバイスのローカル Web インターフェイスで使用できます。
オペレーティング システム (Operating System)	アプライアンス上で現在実行されているオペレーティング システム。
オペレーティング システム バージョン (Operating System Version)	アプライアンス上で現在実行されているオペレーティング システムのバージョン。
IPv4 アドレス (IPv4 Address)	デフォルト管理インターフェイス (eth0) の IPv4 アドレス。IPv4 の管理が無効になっている場合は、このフィールドにそのことが示されます。
IPv6 アドレス (IPv6 Address)	デフォルト管理インターフェイス (eth0) の IPv6 アドレス。IPv6 の管理が無効になっている場合は、このフィールドに表示されます。
現在のポリシー (Current Policies)	現在展開されているシステム レベルのポリシー。ポリシーが最後に適用された後で更新されていると、ポリシー名がイタリック体で表示されます。
モデル番号 (Model Number)	内部フラッシュ ドライブに保存されているアプライアンス固有のモデル番号。この番号は、トラブルシューティングで重要になる場合があります。

## システム情報の表示および変更

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 7000 & 8000 シリーズ	グローバルだけ	Admin

Firepower Management Center の Web インターフェイスまたは 7000 および 8000 シリーズ ローカル Web インターフェイスの情報ページでは、製品名やモデル番号など、読み取り専用の情報を含むシステムについての情報を提供します。このページでは、システムの表示名の変更を変更することもできます。また、7000 および 8000 シリーズ デバイスの場合、パケット転送を禁止する機能もあります。



(注) パケット転送を禁止することは、侵入ポリシー違反をトリガーしたパケットの具体的な内容について気にする必要がない低帯域幅の展開で、効果を発揮する可能性があります。

### 手順

**ステップ 1** [システム (System)] > [設定 (Configuration)] を選択します。

**ステップ 2** オプションで、以下のシステム情報の設定を変更します。

- 名前：表示名を変更するには、[名前 (Name)] フィールドに名前を入力します。
- パケット転送の禁止：Firepower Management Center にパケットデータを送信しないようにするには、[管理センターへのパケット転送を禁止する (Prohibit Packet Transfer to the Management Center)] チェックボックスをオンにします。このオプションは、7000 または 8000 シリーズ デバイスのローカル Web インターフェイスでのみ使用できます。

**ステップ 3** [保存 (Save)] をクリックします。

## カスタム HTTPS 証明書

Firepower Management Center および 7000 および 8000 シリーズ デバイスは、セキュア ソケット レイヤ (SSL) 証明書によりシステムと Web ブラウザ間に暗号化チャネルを確立することができます。すべての Firepower デバイスにデフォルト証明書が含まれていますが、これはグローバル レベルで既知の CA から信頼された認証局 (CA) によって生成された証明書ではありません。したがって、デフォルト証明書ではなく、グローバル レベルで既知の CA または内部で信頼された CA 署名付きのカスタム証明書の使用を検討してください。

システム情報と指定した ID 情報に基づいて、証明書要求を生成できます。ブラウザによって信頼されている内部認証局 (CA) がインストールされている場合は、生成された要求に対して証明書を自己署名することができます。生成された要求を認証局に送信して、サーバ証明書を要求することもできます。認証局 (CA) から署名付き証明書を取得すると、その証明書をインポートできます。

クライアントブラウザの証明書チェック機能を使用して、Firepower システムの Web サーバへのアクセスを制限できます。ユーザ証明書を有効にすると、Web サーバはユーザのブラウザクライアントで有効なユーザ証明書が選択されていることを確認します。そのユーザ証明書は、サーバ証明書で使用されているのと同じ信頼できる認証局によって生成されている必要があります。以下の状況ではいずれの場合もブラウザは Web インターフェイスをロードできません。

- ユーザがブラウザに無効な証明書を選択する。
- ユーザがブラウザにサーバ証明書に署名した認証局が生成していない証明書を選択する。
- ユーザがブラウザにデバイスの証明書チェーンの認証局が生成していない証明書を選択する。

クライアントブラウザ証明書を確認するには、システムを設定して Online Certificate Status Protocol (OSCP) を使用するか、1 つ以上の証明書失効リスト (CRL) ファイルをロードします。OSCP を使用する場合、Web サーバは接続要求を受信すると、接続を確立する前に認証局と通信して、クライアント証明書の有効性を確認します。サーバに 1 つ以上の CRL をロードするよう設定する場合、Web サーバはクライアント証明書を CRL の一覧に照らして比較します。ユーザが CRL にある失効した証明書の一覧に含まれる証明書を選択した場合、ブラウザは Web インターフェイスをロードできません。



(注) CRL を使用した証明書の確認を選択すると、システムはクライアントブラウザ証明書、監査ログサーバ証明書の両方の検証に同じ CRL を使用します。



**注意** Firepower Management Center は 2048 ビット HTTPS 証明書をサポートしています。Firepower Management Center で使用される証明書が 2048 ビットを超える公開サーバキーを使用して生成されていた場合は、Management Center の Web インターフェイスにログインできなくなります。HTTPS 証明書のバージョン 6.0.0 への更新の詳細については、*Firepower System Release Notes, Version 6.0* の「Update Management Center HTTPS Certificates to Version 6.0」を参照してください。HTTPS 証明書を生成またはインポートしても Management Center Web インターフェイスにログインできない場合は、サポート窓口にご連絡ください。



## 現在の HTTPS サーバ証明書の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 7000 および 8000 シリーズ	グローバルだけ	Admin

ログインしているアプライアンスのサーバ証明書のみを表示できます。

### 手順

**ステップ 1** [システム (System)] > [設定 (Configuration)] を選択します。

**ステップ 2** [HTTPS Certificate] をクリックします。

## HTTPS サーバの証明書署名要求の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center 7000 および 8000 シリーズ	グローバルだけ	Admin

ローカル構成の [HTTPS 証明書 (HTTPS Certificate)] ページから、この手順を使用して証明書要求を生成する場合は、1 つのシステムに対して 1 つの証明書しか生成できません。広く知られている CA または内部的に信頼できる CA によって署名されていない証明書をインストールすると、システムへの接続時にセキュリティ警告が表示されます。

証明書要求用に生成されるキーは、ベース 64 エンコードの PEM 形式です。

### 手順

**ステップ 1** [システム (System)] > [設定 (Configuration)] を選択します。

**ステップ 2** [HTTPS Certificate] をクリックします。

**ステップ 3** [新規 CSR の生成 (Generate New CSR)] をクリックします。

**ステップ 4** [国名 (2 文字のコード) (Country Name (two-letter code))] フィールドに国番号を入力します。

**ステップ 5** [都道府県 (State or Province)] フィールドに、都道府県名を入力します。

- ステップ 6 [市区町村 (Locality or City) ]を入力します。
- ステップ 7 [組織 (Organization) ] の名前を入力します。
- ステップ 8 [組織単位 (部署名) (Organizational Unit (Department)) ] の名前を入力します。
- ステップ 9 [共通名 (Common Name) ] フィールドに、証明書を要求するサーバの完全修飾ドメイン名を入力します。

(注) [共通名 (Common Name) ] フィールドには、証明書に表示されるとおりに、サーバの完全修飾ドメイン名を正確に入力する必要があります。共通名と DNS ホスト名が一致していないと、アプライアンスへの接続時に警告が表示されます。

- ステップ 10 [生成 (Generate) ] をクリックします。
- ステップ 11 テキスト エディタを開きます。
- ステップ 12 証明書要求のテキストブロック全体 (BEGIN CERTIFICATE REQUEST 行と END CERTIFICATE REQUEST 行を含む) をコピーして、空のテキスト ファイルに貼り付けます。
- ステップ 13 このファイルを *servername.csr* として保存します。 *servername* は証明書を使用するサーバの名前です。
- ステップ 14 [閉じる (Close) ] をクリックします。

次のタスク

- 証明機関に証明書要求を送信します。
- 署名された証明書を受け取ったら、Firepower Management Center にインポートします。  
[HTTPS サーバ証明書のインポート \(924 ページ\)](#) を参照してください。

## HTTPS サーバ証明書のインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 7000 および 8000 シリーズ	グローバルだけ	Admin

証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、証明書チェーン (証明書パス) も提供する必要があります。

クライアント証明書が必要な場合、サーバ証明書が次に示すいずれかの条件を満たしていないときに、Web インターフェイス経由でのアプライアンスへのアクセスに失敗します。

- 証明書が、クライアント証明書に署名したものと同一 CA によって署名されている。

- 証明書が、証明書チェーンの中間証明書に署名したものと同一 CA によって署名されている。



**注意** Firepower Management Center は、2048 ビットの HTTPS 証明書をサポートしています。Firepower Management Center で使用される証明書が 2048 ビットを超える公開サーバキーを使用して生成されていた場合は、Management Center の Web インターフェイスにログインできなくなります。HTTPS 証明書のバージョン 6.0.0 への更新の詳細については、*Firepower System Release Notes, Version 6.0* の「Update Management Center HTTPS Certificates to Version 6.0」を参照してください。HTTPS 証明書を生成またはインポートしていて、Management Center の Web インターフェイスにログインできない場合は、サポートまでお問い合わせください。

#### 始める前に

- 証明書署名要求を生成します。[HTTPS サーバの証明書署名要求の作成 \(923 ページ\)](#) を参照してください。
- この CSR ファイルを証明書の要求先となる認証局にアップロードするか、この CSR を使用して自己署名証明書を作成します。

#### 手順

- ステップ 1** [システム (System) ] > [設定 (Configuration) ] を選択します。
- ステップ 2** [HTTPS Certificate] をクリックします。
- ステップ 3** [Import HTTPS Certificate] をクリックします。
- ステップ 4** テキスト エディタでサーバ証明書を開いて、BEGIN CERTIFICATE の行と END CERTIFICATE の行を含むテキストのブロック全体をコピーします。このテキストを [サーバ証明書 (Server Certificate) ] フィールドに貼り付けます。
- ステップ 5** 秘密キーをアップロードする場合は、秘密キー ファイルを開いて、BEGIN RSA PRIVATE KEY の行と END RSA PRIVATE KEY の行を含むテキストのブロック全体をコピーします。このテキストを [秘密キー (Private Key) ] フィールドに貼り付けます。
- ステップ 6** 必要な中間証明書をすべて開いて、それぞれのテキストのブロック全体をコピーして、[証明書チェーン (Certificate Chain) ] フィールドに貼り付けます。
- ステップ 7** [保存 (Save) ] をクリックします。

## 有効な HTTPS クライアント証明書の強制

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 7000 および 8000 シリーズ	グローバルだけ	Admin

システムは、OSCP または PEM (Privacy-enhanced Electronic Mail) 形式でインポートされた CRL を使用した HTTPS クライアント証明書の検証をサポートしています。

CRL を使用する場合は、失効した証明書のリストを最新の状態に保つために、CRL を更新するスケジュールタスクを作成してください。システムは、最後に更新した CRL を表示します。



- (注) クライアント認証を有効にした後で Web インターフェイスにアクセスするには、ブラウザに有効なクライアント証明書が存在している (またはリーダーに CAC が挿入されている) 必要があります。

### 始める前に

- 接続に使用するクライアント証明書に署名したものと同一認証局で署名されたサーバ証明書をインポートします。[HTTPS サーバ証明書のインポート \(924 ページ\)](#) を参照してください。
- サーバ証明書チェーンをインポートします (必要な場合)。[HTTPS サーバ証明書のインポート \(924 ページ\)](#) を参照してください。

### 手順

**ステップ 1** [システム (System)] > [設定 (Configuration)] を選択します。

**ステップ 2** [HTTPS Certificate] をクリックします。

**ステップ 3** [クライアント証明書の有効化 (Enable Client Certificates)] を選択します。プロンプトが表示されたら、ドロップダウンリストから該当する証明書を選択します。

**ステップ 4** 次の 3 つのオプションがあります。

- 1 つ以上の CRL を使用してクライアント証明書を検証する場合は、[CRL のフェッチの有効化 (Enable Fetching of CRL)] を選択して、手順 5 に進みます。
- OSCP を使用してクライアント証明書を検証する場合は、[OSCP の有効化 (Enable OSCP)] を選択して、手順 7 に進みます。
- 失効の確認なしでクライアント証明書を承認する場合は、手順 8 に進みます。

**ステップ 5** 既存の CRL ファイルへの有効な URL を入力して、[CRL の追加 (Add CRL)] をクリックします。最大 25 個まで CRL の追加を繰り返します。

**ステップ 6** [CRL の更新 (Refresh CRL)] をクリックして現在の CRL をロードするか、指定した URL から CRL をロードします。

(注) CRL のフェッチを有効にすると、定期的に CRL を更新するスケジュール タスクが作成されます。このタスクを編集して、更新の頻度を設定します。

**ステップ 7** クライアント証明書がアプライアンスにロードされた認証局によって署名されていることと、サーバ証明書がブラウザの証明書ストアにロードされている認証局によって署名されていることを確認します。(これらは同じ認証局であることが必要です)。

**注意** 有効化したクライアント証明書で設定を保存している場合、ブラウザの証明書ストアに有効なクライアント証明書がないと、アプライアンスへの Web サーバアクセスがすべて無効になります。設定を保存する前に、有効なクライアント証明書がインストールされていることを確認してください。

**ステップ 8** [保存] をクリックします。

#### 関連トピック

[証明書失効リストのダウンロードの設定](#) (223 ページ)

## 外部データベース アクセスの設定

サードパーティ製クライアントによるデータベースへの読み取り専用アクセスを許可するように、Firepower Management Center を設定できます。これによって、次のいずれかを使用して SQL でデータベースを照会できるようになります。

- 業界標準のレポート作成ツール (Actuate BIRT、JasperSoft iReport、Crystal Reports など)
- JDBC SSL 接続をサポートするその他のレポート作成アプリケーション (カスタム アプリケーションを含む)
- シスコが提供する RunQuery と呼ばれるコマンドライン型 Java アプリケーション (インタラクティブに実行することも、1 つのクエリの結果をカンマ区切り形式で取得することもできる)

Firepower Management Center のシステム設定を使用して、データベース アクセスを有効にして、選択したホストにデータベースの照会を許可するアクセスリストを作成します。このアクセスリストは、アプライアンスのアクセスは制御しません。

次のツールを含むパッケージをダウンロードすることもできます。

- RunQuery (シスコが提供するデータベース クエリ ツール)
- InstallCert (アクセスしたい Firepower Management Center から SSL 証明書を取得して受け入れるために使用できるツール)

- データベースへの接続時に使用する必要がある JDBC ドライバ

データベースアクセスを構成するためにダウンロードしたパッケージ内のツールの使用方法については、『*Firepower System Database Access Guide*』を参照してください。

## データベースへの外部アクセスの有効化

スマートライセンス	従来のライセンス	サポートされるドライバ	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	グローバルだけ	Admin

### 手順

- ステップ 1** [システム (System)] > [設定 (Configuration)] を選択します。
- ステップ 2** [外部データベース アクセス (External Database Access)] をクリックします。
- ステップ 3** [外部データベース アクセスの許可 (Allow External Database Access)] チェックボックスをオンにします。
- ステップ 4** [サーバホスト名 (Server Hostname)] フィールドに、適切な値を入力します。サードパーティアプリケーションの要件に応じて、この値は、Firepower Management Center の完全修飾ドメイン名 (FQDN)、IPv4 アドレス、または IPv6 アドレスにできます。
- ステップ 5** [クライアント JDBC ドライバ (Client JDBC Driver)] の横にある [ダウンロード (Download)] をクリックし、ブラウザのプロンプトに従って client.zip パッケージをダウンロードします。
- ステップ 6** 1 つ以上の IP アドレスからのデータベース アクセスを追加するには、[ホストの追加 (Add Hosts)] をクリックします。[アクセスリスト (Access List)] フィールドに [IP アドレス (IP Address)] フィールドが表示されます。
- ステップ 7** [IP アドレス (IP Address)] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、any を入力します。
- ステップ 8** [追加 (Add)] をクリックします。
- ステップ 9** [保存 (Save)] をクリックします。

ヒント 最後に保存されたデータベース設定に戻すには、[更新 (Refresh)] をクリックします。

### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## データベース イベント数の制限

Firepower Management Center が保存できる各イベントタイプの最大数を指定できます。パフォーマンスを向上させるには、定期的に処理するイベント数に合わせてイベント数の制限を調整する必要があります。一部のイベントタイプでは、ストレージを無効にすることができます。

システムは侵入イベント、ディスカバリ イベント、監査レコード、セキュリティインテリジェンスデータ、URL フィルタリングデータをアプライアンスのデータベースから自動的にプルーニングします。イベントが自動的にプルーニングされると自動で電子メール通知を生成するようにシステムを設定できます。また、手動でディスカバリ データベースやユーザ データベースをプルーニングし、Firepower Management Center データベースからディスカバリ データや接続データを消去することもできます。

### データベース イベント数の制限の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	グローバルだけ	Admin

#### 始める前に

- Firepower Management Center のデータベースからイベントがプルーニングされた場合に電子メール通知を受信するには、電子メール サーバを設定する必要があります。[メール リレー ホストおよび通知アドレスの設定 \(971 ページ\)](#) を参照してください。

#### 手順

**ステップ 1** [システム (System) ] > [設定 (Configuration) ] を選択します。

**ステップ 2** [データベース (Database) ] を選択します。

**ステップ 3** 各データベースについて、保存するレコードの数を入力します。

各データベースが保持できるレコード数の詳細については、[データベース イベント数の制限 \(930 ページ\)](#) を参照してください。

**ステップ 4** 必要に応じて、[データ プルーニング通知のアドレス (Data Pruning Notification Address) ] フィールドに、プルーニング通知を受信する電子メール アドレスを入力します。

**ステップ 5** [保存 (Save) ] をクリックします。

## データベース イベント数の制限

次の表に、Firepower Management Center に保存可能な各イベント タイプのレコードの最小数と最大数を示します。

表 66: データベース イベント数の制限

イベントタイプ (Event Type)	上限	下限
侵入イベント	1,000 万 (Management Center Virtual) 2,000 万 (MC750) 3,000 万 (MC1500) 6,000 万 (MC2000) 1 億 5,000 万 (MC3500) 3 億 (MC4000)	10,000
検出イベント	1,000 万 2,000 万 (MC2000 および MC4000)	0 (ストレージを無効化)
接続イベント セキュリティ インテリジェンス イベント	5,000 万 (Management Center 仮想) 5,000 万 (MC750) 1 億 (MC1500) 3 億 (MC2000) 5 億 (MC3500) 10 億 (MC4000)  制限は接続イベントとセキュリティインテリジェンス イベントの間で共有されます。設定済みの最大数の合計がこの制限を超えることはできません。	0 (ストレージを無効化)
接続の要約 (集約された接続イベント)	5,000 万 (Management Center 仮想) 5,000 万 (MC750) 1 億 (MC1500) 3 億 (MC2000) 5 億 (MC3500) 10 億 (MC4000)	0 (ストレージを無効化)
関連イベントおよびコンプライアンスのホワイトリストイベント	100 万 200 万 (MC2000 および MC4000)	1 つ



イベントタイプ (Event Type)	上限	下限
マルウェア イベント	1,000 万 2,000 万 (MC2000 および MC4000)	10,000
ファイル イベント	1,000 万 2,000 万 (MC2000 および MC4000)	0 (ストレージを無効化)
ヘルス イベント	100 万	0 (ストレージを無効化)
監査レコード	100,000	1 つ
修復ステータス イベント	1,000 万	1 つ
ホワイトリスト違反履歴	30 日間の違反履歴	1 日の履歴
ユーザ アクティビティ (ユーザ イベント)	1,000 万	1 つ
ユーザ ログイン (ユーザ履歴)	1,000 万	1 つ
侵入ルール更新のインポートログレコード	100 万	1 つ

## 管理インターフェイス

セットアップの完了後、管理ネットワーク設定を変更することができます。これには、Management Center と管理対象デバイスの両方での管理インターフェイス、ホスト名、検索ドメイン、DNS サーバ、HTTP プロキシの追加が含まれます。

### 管理インターフェイスについて

デフォルトでは、Firepower Management Center はすべてのデバイスを 1 つの管理インターフェイス上で制御します。各デバイスには Management Center と通信するための管理インターフェイスが 1 つ含まれています。

また、初期設定 (Management Center および管理対象デバイスの両方) や、管理者として Management Center にログインする際にも管理インターフェイスで行います。

管理インターフェイスは、スマートライセンスサーバとの通信、更新プログラムのダウンロード、その他の管理機能の実行にも使用します。

## Firepower Management Center 上の管理インターフェイス

Firepower Management Center では、初期セットアップ、管理者の HTTP アクセス、デバイスの管理、ならびにその他の管理機能（ライセンス管理や更新など）に、eth0 インターフェイスが使用されます。

同じネットワーク上、あるいは別のネットワーク上に、追加の管理インターフェイスを設定することもできます。Management Center が管理するデバイスの数が多い場合、管理インターフェイスをさらに追加することで、スループットとパフォーマンスの向上につながります。これらの管理インターフェイスをその他すべての管理機能に使用することもできます。管理インターフェイスごとに、対応する機能を限定することをお勧めします。たとえば、ある特定の管理インターフェイスを HTTP 管理者アクセス用に使用し、別の管理インターフェイスをデバイスの管理に使用するなどです。

デバイス管理用に、管理インターフェイスには2つの別個のトラフィック チャンネルがあります。管理トラフィックチャンネルはすべての内部トラフィック（デバイス管理に固有のデバイス間トラフィックなど）を伝送し、イベントトラフィックチャンネルはすべてイベントトラフィック（Web イベントなど）を伝送します。オプションで、Management Center 上にイベントを処理するためのイベント専用インターフェイスを別個に設定することもできます。設定できるイベント専用インターフェイスは1つだけです。イベントトラフィックは大量の帯域幅を使用する可能性があるため、管理トラフィックからイベントトラフィックを分離することで、Management Center のパフォーマンスを向上させることができます。たとえば、10 GigabitEthernet インターフェイスをイベントインターフェイスとして割り当て、可能なら、1 GigabitEthernet インターフェイスを管理用に使用します。たとえば、イベント専用インターフェイスは完全にセキュアなプライベート ネットワーク上に設定し、通常の管理インターフェイスはインターネットにアクセスできるネットワーク上で使用することをお勧めします。目的がスループットの向上だけである場合は、管理インターフェイスとイベントインターフェイスを同じネットワーク上で使用することもできます。

以下の機能は、デフォルトの管理インターフェイス（eth0）でのみサポートされます。

- DHCP IP アドレッシング。他の管理インターフェイスでは静的 IP アドレスを使用する必要があります。
- 新しいデバイスを登録する際の NAT ID の使用。
- Lights-Out Management

## 管理対象デバイス上の管理インターフェイス

一部のモデルでは、イベントトラフィック専用として設定できる追加管理インターフェイスがあり、Management Center との通信中に管理トラフィックとイベントトラフィックを分離できます。

デバイスをセットアップするときに、接続先とする Management Center の IP アドレスを指定します。初期登録時は、管理トラフィックとイベントトラフィックの両方がこのアドレスに送信されます。注：場合によっては、Management Center が別の管理インターフェイスで初期接続を確立することがあります。その場合、以降の接続では指定した IP アドレスの管理インターフェイスを使用する必要があります。

デバイスと Management Center の両方に別個のイベント インターフェイスが設定されている場合は、デバイスと Management Center が互いのイベント インターフェイスを管理通信中に学習した後、ネットワークで許可されていれば、後続のイベントトラフィックがそれらのインターフェイス間で送られます。イベントネットワークがダウンすると、イベントトラフィックは、通常の管理インターフェイスに戻ります。デバイスは、可能な場合に別個のイベントインターフェイスを使用しますが、管理インターフェイスは常にバックアップです。管理対象デバイス上で1つの管理インターフェイスだけを使用している場合、管理トラフィックを Management Center 管理インターフェイスに送信できませんし、イベントトラフィックを別個の Management Center イベント インターフェイスに送信することもできません。Management Center と管理対象デバイスの両方で別個のイベント インターフェイスを使用する必要があります。

## 管理インターフェイスのサポート

管理インターフェイスの場所については、ご使用のモデルのハードウェアインストールガイドを参照してください。



- (注) Firepower 4100/9300 シャーシ (Firepower 4100 および 9300) の場合、MGMT インターフェイスは Firepower Threat Defense の論理デバイスを管理するためではなく、シャーシを管理するために使用します。mgmt タイプ (または firepower-eventing タイプあるいはその両方) の別個の NIC インターフェイスを設定してから、そのインターフェイスを Firepower Threat Defense 論理デバイスに割り当てる必要があります。



- (注) シャーシ上の Firepower Threat Defense の場合、物理管理インターフェイスは、診断論理インターフェイス (SNMP または syslog に利用できて、Management Center でデータ インターフェイスと併せて設定されます) と、Management Center 通信用の管理論理インターフェイスの間で共有されます。詳細については、[管理/診断インターフェイスとネットワーク配置 \(649ページ\)](#) を参照してください。

Firepower Management Center および管理対象デバイスの各モデルでサポートされる管理インターフェイスについては、以下の表を参照してください。

表 67: Firepower Management Center でサポートされる管理インターフェイス

モデル	管理インターフェイス
MC750、MC1500、MC3500	eth0 (デフォルト) eth1
MC2000、MC4000	eth0 (デフォルト) eth1 eth2 eth3

モデル	管理インターフェイス
Firepower Management Center Virtual	eth0 (デフォルト)

表 68: 管理対象デバイスでサポートされる管理インターフェイス

モデル	管理インターフェイス	オプションのイベントインターフェイス
7000 シリーズ	eth0	サポートなし
8000 シリーズ	eth0	eth1
NGIPSv	eth0	サポートなし
ASA 5585-X 上の ASA FirePOWER サービスモジュール	eth0 (注) eth0 は、管理 1/0 インターフェイスの内部名です。	eth1 (注) eth1 は、管理 1/1 インターフェイスの内部名です。
ASA 5506-X、5508-X、5516-X 上の ASA FirePOWER サービスモジュール	eth0 (注) eth0 は、管理 1/1 インターフェイスの内部名です。	サポートなし
ASA 5512-X ~ 5555-X 上の ASA FirePOWER サービスモジュール	eth0 (注) eth0 は、管理 0/0 インターフェイスの内部名です。	サポートなし
ASA 5506-X、5508-X、5516-X 上の Firepower Threat Defense	br1 (注) br1 は、管理 1/1 インターフェイスの内部名です。	サポートなし
ASA 5512-X ~ ASA 5555-X 上の Firepower Threat Defense	br1 (注) br1 は、管理 0/0 インターフェイスの内部名です。	サポートなし

モデル	管理インターフェイス	オプションのイベント インターフェイス
Firepower 4100 および 9300 上の Firepower Threat Defense	management0 (注) management0 は、物理インターフェイス ID に関わらず、このインターフェイスの内部名です。	management1 (注) management1 は、物理インターフェイス ID に関わらず、このインターフェイスの内部名です。
Firepower Threat Defense Virtual	br1	サポートなし

## 管理インターフェイス上のネットワーク ルート

管理インターフェイスはスタティック ルートのみをサポートします。Management Center または管理対象デバイスをセットアップすると、セットアッププロセスにより、指定したゲートウェイ IP アドレスへデフォルトの管理インターフェイスを介して到達するデフォルトのルートが作成します。このルートを削除することはできません。また、このルートで変更できるのはゲートウェイアドレスのみです。

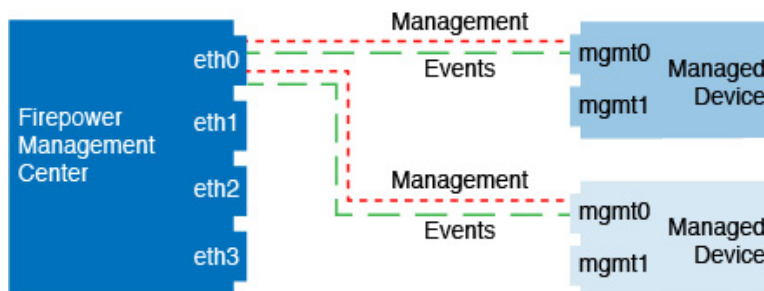
さらにスタティックルートを追加できます。正しいインターフェイスとゲートウェイを指定して、任意のリモート ネットワークへのルートを追加します。

管理インターフェイスのルーティングは、データインターフェイスに対して設定するルーティングとは完全に別のものです。

## 管理およびイベント トラフィック チャンネルの例

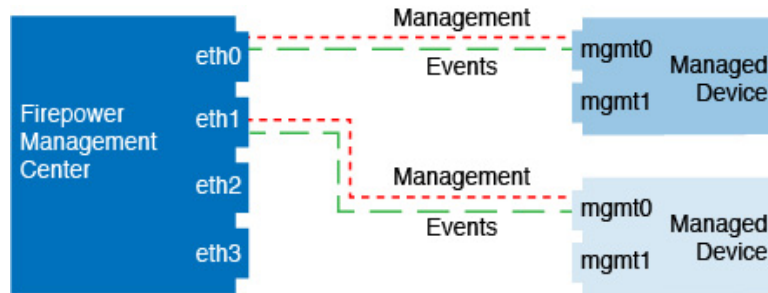
以下に、Firepower Management Center と管理対象デバイスでデフォルト管理インターフェイスのみを使用する例を示します。

図 16: Firepower Management Center 上で単一の管理インターフェイスを使用する場合



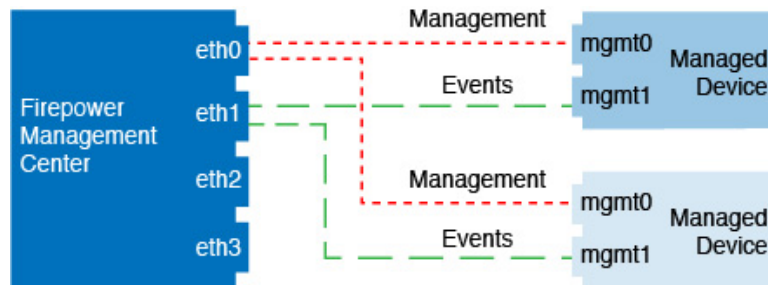
以下に、Firepower Management Center でデバイスごとに別個の管理インターフェイスを使用する例を示します。この場合、各管理対象デバイスが 1 つの管理インターフェイスを使用します。

図 17: Firepower Management Center 上の複数の管理インターフェイスを使用する場合



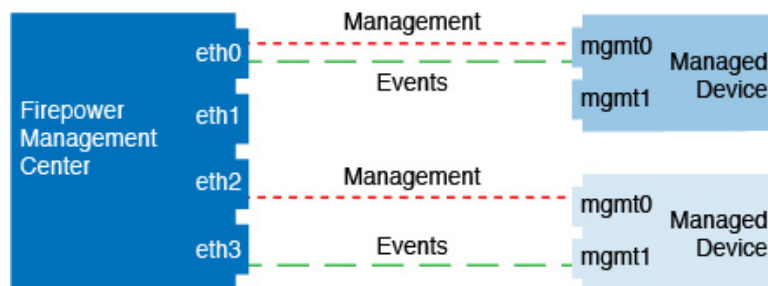
以下に、個別のイベントインターフェイスを使用する Firepower Management Center と管理対象デバイスの例を示します。

図 18: Firepower Management Center 上の個別のイベントインターフェイスと管理対象デバイスを使用する場合



以下に、Firepower Management Center 上で複数の管理インターフェイスと個別のイベントインターフェイスが混在し、個別のイベントインターフェイスを使用する管理対象デバイスと単一の管理インターフェイスを使用する管理対象デバイスが混在する例を示します。

図 19: 管理インターフェイスとイベントインターフェイスを混在させて使用する場合



## 管理インターフェイスの設定

Firepower アプライアンスの管理インターフェイス設定を変更できます。

- Firepower Management Center : Web インターフェイスを使用します。(Firepower Management Center は、Cisco TAC の監督下にある場合に限り、Linux シェル アクセスをサポートします。)
- Firepower Threat Defense デバイス、NGIPSv、ASA FirePOWER : CLI を使用します。

- 7000 & 8000 シリーズ デバイス：制限された Web インターフェイスまたは CLI を使用します。

関連トピック

[通信ポートの要件](#) (2787 ページ)

## Firepower Management Center 管理インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	グローバルだけ	Admin

Firepower Management Center で管理インターフェイスの設定を変更します。オプションとして追加の管理インターフェイスを有効にしたり、イベントのみのインターフェイスを設定したりできます。



**注意**

接続されている管理インターフェイスを変更する場合は十分にご注意ください。設定エラーのために再接続できない場合は、Management Center コンソール ポートにアクセスして、Linux シェルでネットワーク設定を再設定する必要があります。この操作では、Cisco TAC に連絡する必要があります。

手順

- ステップ 1** [システム (System) ] > [設定 (Configuration) ] を選択し、次に [管理インターフェイス (Management Interfaces) ] を選択します。
- ステップ 2** [インターフェイス (Interfaces) ] エリアで、設定するインターフェイスの横にある [編集 (Edit) ] をクリックします。

このセクションでは、利用可能なすべてのインターフェイスがリストされます。インターフェイスをさらに追加することはできません。

それぞれの管理インターフェイスに対して、以下のオプションを設定できます。

- [有効にする (Enabled) ]：管理インターフェイスを有効にします。デフォルト eth0 管理インターフェイスを無効にしないでください。eth0 インターフェイスを必要とするプロセスもあります。
- [チャンネル (Channels) ]：イベントのみのインターフェイスを設定します。Management Center では 1 つのイベント インターフェイスしか設定できません。これを行うには、[管理トラフィック (Management Traffic) ] チェックボックスをオフにし、[イベントトラフィック (Event Traffic) ] チェックボックスをオンのままにします。その他の管理インターフェイスの場合は、両方のチェックボックスをオンにする必要があります。

- [モード (Mode) ]: リンク モードを指定します。GigabitEthernet インターフェイスでは、自動ネゴシエーションの値を変更しても反映されないことに注意してください。
- [MTU]: 最大伝送ユニット (MTU) を設定します。デフォルトは 1500 です。設定可能な MTU の範囲は、モデルとインターフェイスのタイプによって異なる場合があります。  
システムは、設定された MTU 値から自動的に 18 バイトを削減するため、IPv6 の場合、1298 未満の値は MTU の最小値である 1280 に準拠しません。IPv4 の場合は、594 未満の値は MTU の最小値 576 に準拠しません。たとえば、構成値 576 は自動的に 558 に削減されます。
- [MDI/MDIX]: [自動-MDIX (Auto-MDIX) ] を設定します。
- [IPv4 設定 (IPv4 Configuration) ]: IPv4 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック (Static) ]: IPv4 の管理 IP アドレスとネットマスクを手動で入力します。
  - [DHCP]: DHCP を使用するインターフェイスを設定します (eth0 のみ) 。
  - [無効 (Disabled) ]: 無効 IPv4。IPv4 と IPv6 の両方を無効にしないでください。
- [IPv6 設定 (IPv6 Configuration) ]: IPv6 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック (Static) ]: IPv6 の管理 IP アドレスとプレフィックス長を手動で入力します。
  - [DHCP]: DHCPv6 を使用するインターフェイスを設定します (eth0 のみ) 。
  - [ルータ割当て (Router Assigned) ]: ステータス自動設定を有効にします。
  - [無効 (Disabled) ]: IPv6 を無効にします。IPv4 と IPv6 の両方を無効にしないでください。

**ステップ 3** [ルート (Routes) ]エリアで、スタティックルートを編集アイコン (✎) をクリックして編集するか、またはルートを追加アイコン (+) をクリックして追加します。表示アイコン (🔍) をクリックして、ルートの統計を表示します。

(注) デフォルトルートでは、ゲートウェイ IP アドレスのみを変更できます。

次の設定をスタティック ルートに対して設定できます。

- [宛先 (Destination) ]: ルートを作成する宛先ネットワークのアドレスを設定します。
- [ネットマスク (Netmask) ]または[プレフィックス長 (Prefix Length) ]: ネットワークのネットマスク (IPv4) またはプレフィックス長 (IPv6) を設定します。
- [インターフェイス (Interface) ]: 出力管理インターフェイスを設定します。
- [ゲートウェイ (Gateway) ]: ゲートウェイ IP アドレスを設定します。



**ステップ 4** [共有設定 (Shared Settings)] エリアで、すべてのインターフェイスで共有されているネットワーク パラメータを設定します。

(注) eth0 インターフェイスで [DHCP] を選択すると、DHCP サーバから取得する共有設定の一部を手動で指定することができなくなります。

次の共有設定を行うことができます。

- [ホスト名 (Hostname)] : Management Center ホスト名を設定します。ホスト名を変更する場合、syslog メッセージに反映される新しいホスト名を使用するには、Management Center を再起動します。再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。
  - [ドメイン (Domains)] : カンマで区切られた、Management Center の検索ドメインを設定します。これらのドメインは、ping system など、コマンドで完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。
  - [プライマリ DNS サーバ (Primary DNS Serve)]、[セカンダリ DNS サーバ (Secondary DNS Server)]、[ターシャリ DNS サーバ (Tertiary DNS Server)] : 優先度順に使用される DNS サーバを設定します。
  - [リモート管理ポート (Remote Management Port)] : 管理対象デバイスとの通信用のリモート管理ポートを設定します。Management Center および管理対象デバイスは、双方向の SSL 暗号化通信チャネル (デフォルトではポート 8305) を使用して通信します。
- (注) Cisco は、リモート管理ポートをデフォルト設定のままにしておくことを強く推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、展開内の相互に通信する必要があるすべてのデバイスの管理ポートを変更する必要があります。

**ステップ 5** [プロキシ (Proxy)] 領域で、HTTP プロキシを設定します。

Management Center は、ポート TCP/443 (HTTPS) および TCP/80 (HTTP) でインターネットに直接接続するように構成されています。HTTP ダイジェスト経由で認証できるプロキシサーバを使用できます。

(注) NT LAN Manager (NTLM) 認証を使用するプロキシはサポートされません。

- a) [有効 (Enabled)] チェックボックスをオンにします。
- b) [HTTP プロキシ (HTTP Proxy)] フィールドに、プロキシサーバの IP アドレスまたは完全修飾ドメイン名を入力します。
- c) [ポート (Port)] フィールドに、ポート番号を入力します。
- d) [プロキシ認証の使用 (Use Proxy Authentication)] を選択してから [ユーザ名 (User Name)] と [パスワード (Password)] を入力して、認証資格情報を設定します。

**ステップ 6** [保存 (Save)] をクリックします。

## 従来型デバイス Web インターフェイスでのデバイス管理インターフェイスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	7000 & 8000 シリーズ	グローバルだけ	Admin

Web インターフェイスを使用して、管理対象デバイスの管理インターフェイスの設定を変更します。モデルでサポートされている場合に、オプションでイベントインターフェイスを有効にすることができます。



**注意** 慎重に管理インターフェイスに変更を加えてください。構成エラーで再接続できなくなると、デバイスのコンソールポートへのアクセスおよび CLI での再設定が必要になります。

### 手順

**ステップ 1** [システム (System)] > [設定 (Configuration)] を選択して、[管理インターフェイス (Management Interfaces)] を選択します。

**ステップ 2** [インターフェイス (Interfaces)] エリアで、設定するインターフェイスの横にある [編集 (Edit)] をクリックします。

このセクションでは、利用可能なすべてのインターフェイスがリストされます。インターフェイスをさらに追加することはできません。

それぞれの管理インターフェイスに対して、以下のオプションを設定できます。

- [有効にする (Enabled)] : 管理インターフェイスを有効にします。デフォルト eth0 管理インターフェイスを無効にしないでください。eth0 インターフェイスを必要とするプロセスもあります。

- [チャンネル (Channels)] : (8000 シリーズのみ) イベントオンリーのインターフェイスを設定します。8000 シリーズのデバイスで eth1 管理インターフェイスを有効にして、イベントインターフェイスとして機能させることができます。これを設定するには、[管理トラフィック (Management Traffic)] チェックボックスをオフにして、[イベントトラフィック (Event Traffic)] チェックボックスをオンのままにしておきます。eth0 管理インターフェイスを入力するには、両方のチェックボックスをオンのままにしておきます。

管理チャンネルとイベントチャンネルの両方にデフォルト管理インターフェイスを使用することをお勧めします。その後、別個のイベント専用インターフェイスを有効にします。

Firepower Management Center イベント専用インターフェイスは管理チャンネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャンネルを単に無効にしてください。

- [モード (Mode)] : リンク モードを指定します。GigabitEthernet インターフェイスでは、自動ネゴシエーションの値を変更しても反映されないことに注意してください。

- [MTU] : 最大伝送ユニット (MTU) を設定します。デフォルトは 1500 です。設定可能な MTU の範囲は、モデルとインターフェイスのタイプによって異なる場合があります。  
システムは、設定された MTU 値から自動的に 18 バイトを削減するため、IPv6 の場合、1298 未満の値は MTU の最小値である 1280 に準拠しません。IPv4 の場合は、594 未満の値は MTU の最小値 576 に準拠しません。たとえば、構成値 576 は自動的に 558 に削減されます。
- [MDI/MDIX] : [自動-MDIX (Auto-MDIX)] を設定します。
- [IPv4 設定 (IPv4 Configuration)] : IPv4 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック (Static)] : IPv4 の管理 IP アドレスとネットマスクを手動で入力します。
  - [DHCP] : DHCP を使用するインターフェイスを設定します (eth0 のみ)。
  - [無効 (Disabled)] : 無効 IPv4。IPv4 と IPv6 の両方を無効にしないでください。
- [IPv6 設定 (IPv6 Configuration)] : IPv6 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック (Static)] : IPv6 の管理 IP アドレスとプレフィックス長を手動で入力します。
  - [DHCP] : DHCPv6 を使用するインターフェイスを設定します (eth0 のみ)。
  - [ルータ割当て (Router Assigned)] : ステートレス自動設定を有効にします。
  - [無効 (Disabled)] : IPv6 を無効にします。IPv4 と IPv6 の両方を無効にしないでください。

**ステップ 3** [ルート (Routes)] エリアで、スタティックルートを編集アイコン (✎) をクリックして編集するか、またはルートを追加アイコン (+) をクリックして追加します。表示アイコン (🔍) をクリックして、ルートの統計を表示します。

(注) デフォルトルートでは、ゲートウェイ IP アドレスのみを変更できます。

次の設定をスタティック ルートに対して設定できます。

- [宛先 (Destination)] : ルートを作成する宛先ネットワークのアドレスを設定します。
- [ネットマスク (Netmask)] または [プレフィックス長 (Prefix Length)] : ネットワークのネットマスク (IPv4) またはプレフィックス長 (IPv6) を設定します。
- [インターフェイス (Interface)] : 出力管理インターフェイスを設定します。
- [ゲートウェイ (Gateway)] : ゲートウェイ IP アドレスを設定します。

**ステップ 4** [共有設定 (Shared Settings)] エリアで、すべてのインターフェイスで共有されているネットワーク パラメータを設定します。

(注) eth0 インターフェイスで [DHCP] を選択すると、DHCP サーバから取得する共有設定の一部を手動で指定することができなくなります。

以下の共有設定を行うことができます。

- [ホスト名 (Hostname)] : デバイスのホスト名を設定します。ホスト名を変更する場合、Syslog メッセージに新しいホスト名を反映させるには、デバイスをリブートします。再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。
- [ドメイン (Domains)] : カンマで区切ったデバイスの検索ドメインを設定します。これらのドメインは、コマンドで完全修飾ドメイン名を指定しないときに、ホスト名に ping system などとして加えられます。ping system ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。
- [プライマリ DNS サーバ (Primary DNS Server)]、[セカンダリ DNS サーバ (Secondary DNS Server)]、[テリタリ DNS サーバ (Tertiary DNS Server)] : DNS サーバが優先順で使用されるよう設定します。
- [リモート管理ポート (Remote Management Port)] : Management Center で通信のリモート管理ポートを設定します。Management Center および管理対象デバイスは、双方向の SSL 暗号化通信チャネル (デフォルトではポート 8305) を使用して通信します。

(注) Cisco は、リモート管理ポートをデフォルト設定のままにしておくことを強く推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要があるすべてのデバイスの管理ポートを変更する必要があります。

**ステップ 5** [LCD パネル (LCD Panel)] エリアで、[ネットワーク設定の再設定を許可 (Allow reconfiguration of network settings)] チェックボックスをオンにして、デバイスの LCD パネルを使用したネットワーク設定の変更を有効にします。

LCD パネルを使用して、デバイスの IP アドレスを編集できます。変更が管理 Firepower Management Center に反映されていることを確認します。状況によっては、Firepower Management Center でデータを手動で更新することが必要になります。

**注意** LCD パネルを使用した再構成を許可すると、セキュリティ リスクが発生する可能性があります。LCD パネルを使用してネットワーク設定を構成する場合は、物理アクセスだけが必要で、認証は必要ありません。このオプションを有効にするとセキュリティ上の問題が発生する可能性があることを示す警告が Web インターフェイスに表示されます。

**ステップ 6** [プロキシ (Proxy)] エリアで、HTTP プロキシ設定をします。

デバイスは、ポート TCP/443 (HTTPS) および TCP/80 (HTTP) でインターネットに直接接続するように設定されています。HTTP ダイジェスト経由で認証できるプロキシサーバを使用できます。

(注) NT LAN Manager (NTLM) 認証を使用するプロキシはサポートされません。

- a) [有効 (Enabled)] チェックボックスをオンにします。
- b) [HTTP プロキシ (HTTP Proxy)] フィールドに、プロキシサーバの IP アドレスまたは完全修飾ドメイン名を入力します。
- c) [ポート (Port)] フィールドに、ポート番号を入力します。
- d) [プロキシ認証の使用 (Use Proxy Authentication)] を選択してから [ユーザ名 (User Name)] と [パスワード (Password)] を入力して、認証資格情報を設定します。

**ステップ 7** [保存 (Save)] をクリックします。

## CLI でのデバイス管理インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Firepower Threat Defense 従来型 (Classic)	グローバルのみ	Admin

CLI を使用して、管理対象デバイスの管理インターフェイスの設定を変更します。これらの設定の多くは、初期セットアップ時に設定されたものです。この手順に従うことで、それらの設定を変更でき、さらに設定を追加できます (例: モデルでサポートされる場合にイベントインターフェイスを有効化する、スタティック ルートを追加する)。Firepower Threat Defense CLI については、『[Command Reference for Firepower Threat Defense](#)』を参照してください。クラシック デバイス CLI については、このガイドの[従来型デバイスのコマンドラインリファレンス \(2793 ページ\)](#)を参照してください。Firepower Threat Defense およびクラシック デバイスは、管理インターフェイス設定に同じコマンドを使用します。その他のコマンドは、プラットフォーム間で異なる可能性があります。



**注意**

SSH を使用する際は、慎重に管理インターフェイスに変更を加えてください。構成エラーで再接続できなくなると、デバイスのコンソールポートへのアクセスが必要になります。

**始める前に**

- [configure user add] コマンドを使用して、CLI にログインできるユーザアカウントを作成できます。 **configure user add**
- 7000 & 8000 シリーズ デバイスで、[ユーザアカウントの作成 \(86 ページ\)](#) の説明に従って、Web インターフェイスでユーザアカウントも作成できます。

## 手順

- ステップ 1** コンソールポートから、または SSH を使用して、デバイス CLI に接続します。  
[Firepower Threat Defense デバイスのコマンドライン インターフェイスへのログイン \(29 ページ\)](#) または [従来型デバイスでのコマンドライン インターフェイスへのログイン \(28 ページ\)](#) を参照してください。
- ステップ 2** 管理者のユーザ名とパスワードでログインします。
- ステップ 3** イベント オンリーのインターフェイスを有効にします (サポート モデルについては、[管理インターフェイスのサポート \(933 ページ\)](#) 参照)。

**configure network management-interface enable** *management\_interface*

**configure network management-interface disable-management-channel** *management\_interface*

例 :

これは Firepower 4100 または 9300 デバイスの例です。有効なインターフェイス名はデバイス タイプによって異なります。

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Preserve existing configuration- currently no IP addresses on eth1 to update (bootproto
  IPv4:,bootproto IPv6:
at /usr/local/sf/lib/perl/5.10.1/SF/NetworkConf/NetworkSettings.pm line 821.
Configuration updated successfully

>
```

管理チャンネルとイベントチャンネルの両方にデフォルト管理インターフェイスを使用することをお勧めします。その後、別個のイベント専用インターフェイスを有効にします。Firepower Management Center イベント専用インターフェイスは管理チャンネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャンネルを単に無効にしてください。

- ステップ 4** 管理インターフェイスまたはイベント インターフェイスのネットワーク設定をします。  
*management\_interface* 引数を指定しない場合は、デフォルト管理インターフェイスのネットワーク設定を変更します。イベント インターフェイスを設定する際には、必ず *management\_interface* 引数を指定してください。イベント インターフェイスは、管理インターフェイスの個別のネットワーク、または同じネットワークに配置できます。自分で設定するインターフェイスに接続すると、切断されます。新しい IP アドレスに再接続できます。

a) IPv4 アドレスを設定します。

- 手動設定

**configure network ipv4 manual** *ip\_address netmask gateway\_ip [management\_interface]*

例 :

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.
```

>

- DHCP (デフォルト管理インターフェイスのみでサポート)。

```
configure network ipv4 dhcp
```

b) IPv6 アドレスを設定します。

- ステートレス自動設定

```
configure network ipv6 router [management_interface]
```

例 :

```
> configure network ipv6 router management1
Setting IPv6 network configuration.
Network settings changed.
```

>

- 手動設定

```
configure network ipv6 manual ip6_address ip6_prefix_length [ip6_gateway_ip]
[management_interface]
```

例 :

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 2001:0DB8:BA98::3211
management1
Setting IPv6 network configuration.
Network settings changed.
```

>

- DHCPv6 (デフォルト管理インターフェイスのみでサポート)。

```
configure network ipv6 dhcp
```

**ステップ 5** スタティック ルートを追加します。

```
configure network static-routes {ipv4 | ipv6} add management_interface destination_ip netmask_or_prefix
gateway_ip
```

例 :

```
> configure network static-routes ipv4 add management0 10.89.89.0 255.255.255.0 10.10.1.1
Configuration updated successfully
```

```
> configure network static-routes ipv4 add management1 10.89.89.192.168.6.0 255.255.255.0
10.10.10.1
Configuration updated successfully
```

```
> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully
```

>

スタティック ルートを表示するには、**show network-static-routes** と入力します（デフォルト ルートは表示されません）。

```
> show network-static-routes
-----[ IPv4 Static Routes ]-----
Interface           : management0
Destination          : 10.89.89.0
Gateway              : 10.10.1.1
Netmask              : 255.255.255.0
[...]
```

#### ステップ 6 ホスト名の設定

**configure network hostname** 名前

例 :

```
> configure network hostname farscape1
```

再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。

#### ステップ 7 検索ドメインを設定します。

**configure network dns searchdomains** *domain\_list*

例 :

```
> configure network dns searchdomains example.com,cisco.com
```

カンマで区切ったデバイスの検索ドメインを設定します。これらのドメインは、コマンドで完全修飾ドメイン名を指定しないときに、ホスト名に ping system などとして加えられます。ping system ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。

#### ステップ 8 カンマで区切った 3 つの DNS サーバを設定します。

**configure network dns servers** *dns\_ip\_list*

例 :

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

#### ステップ 9 Management Center で通信のリモート管理ポートを設定します。

**configure network management-interface tcpport** *number*

例 :



```
> configure network management-interface tcpport 8555
```

Management Center および管理対象デバイスは、双方向の SSL 暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。

（注） Cisco は、リモート管理ポートをデフォルト設定のままにしておくことを強く推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要があるすべてのデバイスの管理ポートを変更する必要があります。

**ステップ 10** HTTP プロキシを設定します。デバイスは、ポート TCP/443 (HTTPS) および TCP/80 (HTTP) でインターネットに直接接続するように設定されています。HTTP ダイジェスト経由で認証できるプロキシサーバを使用できます。コマンド発行後に、HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかをユーザは尋ねられます。認証が必要な場合はプロキシのユーザ名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

```
configure network http-proxy
```

例：

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

## システムのシャットダウンと再起動

アプライアンス上のプロセスのシャットダウンおよび再起動を制御するには、Firepower システムの Web インターフェイスを使用します。アプライアンスのシャットダウンは、設定データを失うことなく、安全にシステムの電源を切って再起動する準備をします。

Firepower Management Center 上のプロセスを制御できる、以下のオプションがあります。

- システムのシャットダウン：Firepower システムのグレースフル シャットダウンを開始します。
- システムの再起動：システムを通常の方法でシャットダウンして再起動します。
- コンソールの再起動：通信、データベース、HTTP サーバのプロセスを再起動します。これは通常、トラブルシューティングの際に使用されます。

以上のオプションは、7000 および 8000 シリーズ 管理対象デバイスすべてで共通に使用できます。これらのデバイス上で Snort プロセスを再起動することもできます。



**注意** 電源ボタンを使用してアプライアンスを停止しないでください。データが失われる可能性があります。Web インターフェイスを使用して完全にアプライアンスをシャットダウンする必要があります。



**注意** Snort プロセスを再起動すると、一時的にトラフィック インспекションが中断されます。この中断中にトラフィックがドロップされるか、インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

Firepower 仮想管理対象デバイスの場合、VMware などの仮想インフラストラクチャーには一般的に、仮想マシンのシャットダウン方法、再起動方法、中断方法を定義する設定可能な電源オプションが用意されています。これらのオプションをどのように設定するかについては、使用している仮想プラットフォームのドキュメンテーションを参照してください。



(注) VMware 上で稼働する Firepower 仮想管理対象デバイスの場合、VMware ツールにカスタム電源オプションが含まれています。したがって、グレースフルシャットダウンを設定するには、仮想マシンに VMware ツールがインストールされている必要があります。

## システムのシャットダウンと再起動

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 7000 & 8000 シリーズ	グローバルだけ	Admin

### 手順

**ステップ 1** [システム (System)] > [設定 (Configuration)] を選択します。

**ステップ 2** [プロセス (Process)] を選択します。

**ステップ 3** アプライアンスをシャットダウンするには、以下を実行します。

- Management Center : [管理センターのシャットダウン (Shutdown Management Center)] の横にある [コマンドの実行 (Run Command)] をクリックします。

- 管理対象デバイス：[アプライアンスのシャットダウン (Shutdown Appliance)] の横にある [コマンドの実行 (Run Command)] をクリックします。

**ステップ 4** アプライアンスを再起動するには、以下を実行します。

- Management Center：[管理センターの再起動 (Reboot Management Center)] の横にある [コマンドの実行 (Run Command)] をクリックします。
- 管理対象デバイス：[アプライアンスの再起動 (Reboot Appliance)] の横にある [コマンドの実行 (Run Command)] をクリックします。

(注) Firepower Management Center または管理対象デバイスを再起動すると、アプライアンスからログアウトされます。システムはデータベースチェックを実行しますが、これは完了するのに 1 時間かかります。

**ステップ 5** アプライアンスを再起動するには、以下を実行します。

- Management Center：[管理センターの再起動 (Restart Management Center)] の横にある [コマンドの実行 (Run Command)] をクリックします。
- 管理対象デバイス：[アプライアンス コンソールの再起動 (Restart Appliance Console)] の横にある [コマンドの実行 (Run Command)] をクリックします。

(注) Firepower Management Center を再起動すると、ネットワーク マップ内に削除されたホストが再表示されることがあります。

**ステップ 6** 管理対象デバイスで Snort プロセスを再起動するには、[Snort の再起動 (Restart Snort)] の横にある [コマンドの実行 (Run Command)] をクリックします。

(注) このコマンドは、7000 および 8000 シリーズ デバイスのローカル Web インターフェイスでのみ使用できます。

**注意** Snort プロセスを再開すると、一時的にトラフィック検査が中断されます。この中断中にトラフィックがドロップするか、検査なしで通過するかどうかは、デバイスの設定方法によって異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

#### 関連トピック

[Snort® の再起動シナリオ \(354 ページ\)](#)

## リモートストレージ管理

Firepower Management Center では、バックアップおよびレポートのローカルストレージまたはリモートストレージとして、以下を使用することができます。

- ネットワーク ファイルシステム (NFS)
- サーバメッセージブロック (SMB) /Common Internet File System (CIFS)

- セキュア シェル (SSH)



(注) システムがサポートするバックアップおよびリモートストレージのサーバメッセージブロックプロトコルはバージョン1のみです。

1つのリモートシステムにバックアップを送信し、別のリモートシステムにレポートを送信することはできませんが、どちらかをリモートシステムに送信し、もう一方を Firepower Management Center に格納することは可能です。



ヒント リモートストレージを構成して選択した後は、接続データベースの制限を増やさなかった場合にのみ、ローカルストレージに戻すことができます。

## ローカルストレージの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	グローバルだけ	Admin

### 手順

- ステップ1 [システム (System)] > [設定 (Configuration)] を選択します。
- ステップ2 [リモートストレージデバイス (Remote Storage Device)] を選択します。
- ステップ3 [ストレージタイプ (Storage Type)] ドロップダウンリストから [ローカル (リモートストレージなし) (Local (No Remote Storage))] を選択します。
- ステップ4 [保存 (Save)] をクリックします。

## リモートストレージの NFS の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	グローバルだけ	Admin

始める前に

- 外部リモートストレージシステムが機能しており、Management Center からアクセスできることを確認します。

手順

**ステップ 1** [システム (System) ] > [設定 (Configuration) ] を選択します。

**ステップ 2** [リモートストレージデバイス (Remote Storage Device) ] をクリックします。

**ステップ 3** [ストレージタイプ (Storage Type) ] ドロップダウンリストから [NFS] を選択します。

**ステップ 4** 接続情報を追加します。

- [ホスト (Host) ] フィールドに、ストレージシステムの IPv4 アドレスまたはホスト名を入力します。
- [ディレクトリ (Directory) ] フィールドに、ストレージ領域へのパスを入力します。

**ステップ 5** 必要に応じて、[詳細オプションの使用 (Use Advanced Options) ] チェックボックスをオンにして、必要なコマンドライン オプションを入力します。 [リモートストレージの管理詳細設定オプション \(954 ページ\)](#) を参照してください。

**ステップ 6** [システムの使用方法 (System Usage) ] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用 (Use for Backups) ] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用 (Use for Reports) ] を選択します。
- リモート ストレージへのバックアップに関する [ディスク容量のしきい値 (Disk Space Threshold) ] を入力します。デフォルトは 90% です。

**ステップ 7** 設定をテストするには、[テスト (Test) ] をクリックします。

**ステップ 8** [保存 (Save) ] をクリックします。

## リモートストレージのSMBの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	グローバルだけ	Admin

### 始める前に

- 外部リモートストレージシステムが機能しており、Management Center からアクセスできることを確認します。

### 手順

**ステップ 1** [システム (System)] > [設定 (Configuration)] を選択します。

**ステップ 2** [リモートストレージデバイス (Remote Storage Device)] をクリックします。

**ステップ 3** [ストレージタイプ (Storage Type)] ドロップダウンリストから [SMB] を選択します。

**ステップ 4** 接続情報を追加します。

- [ホスト (Host)] フィールドに、ストレージシステムの IPv4 アドレスまたはホスト名を入力します。
- [共有 (Share)] フィールドに、ストレージ領域の共有を入力します。システムに認識されるのは、ファイルのフルパスではなく、最上位の共有だけであることに注意してください。指定した共有ディレクトリをリモートバックアップ先として使用するには、それを Windows システムで共有する必要があります。
- 必要に応じて、[ドメイン (Domain)] フィールドにリモートストレージシステムのドメイン名を入力します。
- [ユーザ名 (Username)] フィールドにストレージシステムのユーザ名を入力し、[パスワード (Password)] フィールドにそのユーザのパスワードを入力します。

**ステップ 5** 必要に応じて、[詳細オプションの使用 (Use Advanced Options)] チェックボックスをオンにして、必要なコマンドラインオプションを入力します。[リモートストレージの管理詳細設定オプション \(954 ページ\)](#) を参照してください。

**ステップ 6** [システムの使用方法 (System Usage)] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用 (Use for Backups)] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用 (Use for Reports)] を選択します。

**ステップ 7** 設定をテストするには、[テスト (Test)] をクリックします。

**ステップ 8** [保存 (Save)] をクリックします。

## リモートストレージの SSH の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	グローバルだけ	Admin

### 始める前に

- 外部リモートストレージシステムが機能しており、Firepower Management Center からアクセスできることを確認します。

### 手順

**ステップ 1** [システム (System) ] > [設定 (Configuration) ] を選択します。

**ステップ 2** [リモートストレージデバイス (Remote Storage Device) ] をクリックします。

**ステップ 3** [ストレージタイプ (Storage Type) ] ドロップダウンリストから [SSH] を選択します。

**ステップ 4** 接続情報を追加します。

- [ホスト (Host) ] フィールドに、ストレージシステムの IP アドレスまたはホスト名を入力します。
- [ディレクトリ (Directory) ] フィールドに、ストレージ領域へのパスを入力します。
- [ユーザ名 (Username) ] フィールドにストレージシステムのユーザ名を入力し、[パスワード (Password) ] フィールドにそのユーザのパスワードを入力します。接続ユーザ名の一部としてネットワーク ドメインを指定するには、ユーザ名の前にドメインを入力し、スラッシュ (/) で区切ります。
- SSH キーを使用するには、[SSH 公開キー (SSH Public Key) ] フィールドの内容をコピーして authorized\_keys ファイルに貼り付けます。

**ステップ 5** 必要に応じて、[詳細オプションの使用 (Use Advanced Options) ] チェックボックスをオンにして、必要なコマンドライン オプションを入力します。[リモートストレージの管理詳細設定オプション \(954 ページ\)](#) を参照してください。

**ステップ 6** [システムの使用方法 (System Usage) ] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用 (Use for Backups) ] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用 (Use for Reports) ] を選択します。

**ステップ 7** 設定をテストする場合は、[テスト (Test) ] をクリックする必要があります。

ステップ 8 [保存 (Save) ] をクリックします。

## リモートストレージの管理詳細設定オプション

セキュアコピー (SCP) を使用してレポートとバックアップを保存するためにネットワークファイルシステム (NFS) プロトコル、サーバメッセージブロック (SMB) プロトコル、または SSH を選択すると、NFS、SMB、SSH マウントのマニュアルページに記載されているいずれかのマウントバイナリ オプションを使用するために、[詳細設定オプションの使用] チェックボックスを選択できます。

SMB を選択すると、次の形式で [コマンドラインオプション (Command Line Options) ] フィールドにセキュリティモードを入力します。

```
sec=mode
```

mode は、リモートストレージで使用するセキュリティモードです。

表 69: SMB セキュリティモードの設定

[モード (Mode) ]	説明
なし	NULL ユーザ (名前なし) として接続します。
krb5	Kerberos バージョン 5 認証を使用します。
krb5i	Kerberos 認証とパケット署名を使用します。
ntlm	NTLM パスワードハッシュを使用します。 (デフォルト)
ntlmi	署名付きの NTLM パスワードハッシュを使用します (/proc/fs/cifs/PacketSigningEnabled がオンになっている場合またはサーバが署名を要求する場合はデフォルト)。
ntlmv2	NTLMv2 パスワードハッシュを使用します。
ntlmv2i	パケット署名付きの NTLMv2 パスワードハッシュを使用します。

## 変更調整

ユーザが行う変更をモニタし、変更が部門の推奨する標準に従っていることを確認するため、過去 24 時間に行われたシステム変更の詳細なレポートを電子メールで送信するようにシステムを構成できます。ユーザが変更をシステム構成に保存するたびに、変更のスナップショット



が取得されます。変更調整レポートは、これらのスナップショットを組み合わせて、最近のシステム変更の概要を提供します。

次の図は、変更調整レポートの[ユーザ (User) ]セクションの例を示しています。ここには、各構成の変更前の値と変更後の値の両方が一覧表示されています。ユーザが同じ構成に対して複数の変更を行った場合は、個々の変更の概要が最新のものから順に時系列でレポートに一覧表示されます。

過去 24 時間に行われた変更を参照できます。

## 変更調整の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 7000 & 8000 シリーズ	グローバルだけ	Admin

### 始める前に

- 24時間にシステムに行われた変更のメール送信されるレポートを受信する電子メールサーバを設定します。詳細については、[メールリレーホストおよび通知アドレスの設定 \(971 ページ\)](#) を参照してください。

### 手順

**ステップ 1** [システム (System) ] > [設定 (Configuration) ] を選択します。

**ステップ 2** [変更調整 (Change Reconciliation) ] をクリックします。

**ステップ 3** [有効 (Enable) ] チェックボックスをオンにします。

**ステップ 4** [実行する時間 (Time to Run) ] ドロップダウンリストから、システムが変更調整レポートを送信する時刻を選択します。

**ステップ 5** [メール宛先 (Email to) ] フィールドにメールアドレスを入力します。

**ヒント** 電子メールアドレスを追加したら、いつでも [最新のレポートの再送信 (Resend Last Report) ] をクリックして、最新の変更調整レポートのコピーを受信者に再送信できます。

**ステップ 6** ポリシーの変更を追加する場合は、[ポリシー設定を含める (Include Policy Configuration) ] チェックボックスをオンにします。

**ステップ 7** 過去 24 時間のすべての変更を含める場合は、[全変更履歴を表示 (Show Full Change History) ] チェックボックスをオンにします。

ステップ 8 [保存 (Save) ] をクリックします。

関連トピック

[監査ログを使って変更を調査する](#) (2775 ページ)

## 変更調整オプション

[ポリシー設定を含める (Include Policy Configuration) ] オプションは、ポリシーの変更のレコードを変更調整レポートに含めるかどうかを制御します。これには、アクセス制御、侵入、システム、ヘルス、およびネットワーク検出の各ポリシーの変更が含まれます。このオプションを選択しなかった場合は、ポリシーの変更はどれもレポートに表示されません。このオプションは Firepower Management Center のみで使用できます。

[すべての変更履歴を表示する (Show Full Change History) ] オプションは、過去 24 時間のすべての変更のレコードを変更調整レポートに含めるかどうかを制御します。このオプションを選択しなかった場合は、変更がカテゴリごとに統合された形でレポートに表示されます。

## ポリシー変更のコメント

ユーザがアクセス コントロール ポリシー、侵入ポリシー、またはネットワーク分析ポリシーを変更した場合、それらのポリシー関連の変更をコメント機能を使用してトラッキングするように Firepower システムを設定することができます。

ポリシー変更のコメントが有効にされていると、管理者はコメントにアクセスして、導入で重要なポリシーが変更された理由を素早く評価できます。オプションで、侵入ポリシーおよびネットワーク分析ポリシーに対する変更を監査ログに書き込むこともできます。

## ポリシーの変更を追跡するコメントの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	グローバルだけ	Admin

ユーザがアクセス コントロール ポリシー、侵入ポリシー、またはネットワーク分析ポリシーを変更する場合に、コメントの入力を要求するように Firepower システムを設定できます。コメントを使用して、ユーザのポリシーの変更の理由を追跡できます。ポリシーの変更に関するコメントを有効にした場合、コメントをオプションまたは必須に設定できます。システムは、ポリシーに対する新しい変更が保存されるたびに、ユーザにコメントを入力するようプロンプトを出します。

## 手順

**ステップ 1** [システム (System)] > [設定 (Configuration)] を選択します。

システム設定オプションは、左側のナビゲーション パネルに表示されます。

**ステップ 2** 次のいずれかのポリシー コメントの設定を行います□

- アクセス コントロール ポリシーのコメント設定には、[アクセス コントロールの設定 (Access Control Preferences)] をクリックします。
- 侵入ポリシーのコメント設定には、[侵入ポリシー設定 (Intrusion Policy Preferences)] をクリックします。
- ネットワーク分析ポリシーのコメント設定には、[ネットワーク分析ポリシー設定 (Network Analysis Policy Preferences)] をクリックします。

**ステップ 3** 各ポリシー タイプに次の選択肢があります。

- [無効化 (Disabled)] : 変更のコメントを無効にします。
- [オプション (Optional)] : コメントの変更について記述するオプションをユーザに提供します。
- [必須 (Required)] : 保存する前にコメントで変更について説明するようにユーザに要求します。

**ステップ 4** 侵入ポリシーまたはネットワーク分析ポリシーのコメントには、次のオプションがあります。

- 侵入ポリシーのすべての変更を監査ログに書き込むには、[侵入ポリシーの変更を監査ログに書き込む (Write changes in Intrusion Policy to audit log)] をオンにします。
- ネットワーク分析ポリシーのすべての変更を監査ログに書き込むには、[ネットワーク分析ポリシーの変更を監査ログに書き込む (Write changes in Network Analysis Policy to audit log)] をオンにします。

**ステップ 5** [保存 (Save)] をクリックします。

## アクセス リスト

Firepower Management Center およびクラシック管理対象デバイスでは、アクセスリストを使用して、IP アドレスとポートを基準にシステムへのアクセスを制限できます。デフォルトでは、任意の IP アドレスに対して以下のポートが有効化されています。

- 443 (HTTPS) : Web インターフェイス アクセスに使用されます。
- 22 (SSH) : コマンドラインアクセスに使用されます。

さらに、ポート 161 で SNMP 情報をポーリングするためのアクセスも追加できます。



**注意** デフォルトでは、アクセスは制限されていません。よりセキュアな環境で運用するために、特定の IP アドレスに対するアクセスを追加してから、デフォルトの **any** オプションを削除することを検討してください。

## システムのアクセス リストの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

このアクセス リストは、外部データベース アクセスを制御しないので注意してください。

### 手順

**ステップ 1** Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
- 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower ポリシーを作成または編集します。

**ステップ 2** [アクセス リスト (Access List)] をクリックします。

**ステップ 3** 現在の設定の 1 つを削除するために、削除アイコン (🗑️) をクリックすることもできます。

**注意** アプライアンスのインターフェイスへの接続に現在使用されている IP アドレスへのアクセスを削除し、IP=any port=443 のエントリが存在しない場合、ポリシーを展開した時点でシステムへのアクセスは失われます。

**ステップ 4** 1 つ以上の IP アドレスへのアクセスを追加するには、[ルールの追加 (Add Rules)] をクリックします。

- ステップ 5 [IP アドレス (IP Address) ] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、any を入力します。
- ステップ 6 [SSH]、[HTTPS]、[SNMP]、またはこれらのオプションの組み合わせを選択して、これらの IP アドレスで有効にするポートを指定します。
- ステップ 7 [追加 (Add) ] をクリックします。
- ステップ 8 [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## 監査ログ

Firepower Management Center および従来型管理対象デバイスは、ユーザアクティビティに関する読み取り専用の監査情報をログに記録します。Management Center および 7000 および 8000 シリーズの Web インターフェイスでは、監査ログ イベントは標準イベントビューに表示されます。標準イベントビューでは、監査ビューの任意の項目に基づいて監査ログメッセージの表示、並べ替え、フィルタ処理ができます。監査情報を簡単に削除したり、それに関するレポートを作成したりすることができ、ユーザが行った変更に関する詳細なレポートを表示することもできます。

監査ログメッセージを syslog に送信するよう、Firepower Management Center および従来型管理対象デバイスを設定することもできます。設定するには、syslog サーバ、およびメッセージに関連付ける重大度、ファシリティ、オプションタグを指定します。タグは、syslog の監査ログメッセージと一緒に表示されます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。syslog メッセージにはファシリティおよび重大度は含まれません。これらの値は syslog メッセージを受信するシステムにメッセージの分類方法を示す値です。

また、監査ログメッセージを HTTP サーバにストリーミングするよう、Firepower Management Center および従来型管理対象デバイスで設定することもできます。

監査ログストリーミング設定は、アプライアンスのタイプによって異なる設定の一部となっています。

- Firepower Management Center では、監査ログのストリーミングはシステム設定の一部です。
- クラシック管理対象デバイスでは、監査ログストリーミングは Firepower Management Center プラットフォーム設定ポリシーの一部です。

いずれの場合も、システム設定の変更を保存するか、共有プラットフォーム設定ポリシーを展開するまでは設定は有効になりません。

TLS 証明書を使用して TLS と相互認証を有効にすることで、監査ログストリーミング用のチャネルの安全性を確保できます。詳細については[カスタム監査ログクライアント証明書 \(963 ページ\)](#) を参照してください。



**注意** 外部 URL に監査情報を送信すると、システムパフォーマンスに影響を与える場合があります。

## syslog への監査ログメッセージの送信

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この機能を有効にすると、監査ログレコードは、syslog に次の形式で表示されます。

```
Date Time Host [Tag] Sender: User_Name@User_IP, Subsystem, Action
```

現地の日付、時刻、および発信元ホスト名の後に、角括弧で囲まれたオプションタグが続き、送信側デバイス名の後に監査ログメッセージが続きます。

たとえば、FROMMC のタグを指定した場合は、監査ログメッセージ例は次のように表示されます。

```
Mar 01 14:45:24 localhost [FROMMC] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring, Page View
```

TLS 証明書を使用して TLS および相互認証を有効にすることによって、監査ログストリーミングのチャネルを保護できます。詳細については、[カスタム監査ログクライアント証明書 \(963 ページ\)](#) を参照してください。

### 始める前に

- syslog サーバが機能しており、監査ログを送信するシステムからアクセスできることを確認します。

### 手順

**ステップ 1** Firepower Management Center または Classic 管理対象デバイスのいずれを設定しているかに応じて、以下を実行します。

- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
- 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択して、Firepower ポリシーを作成または編集します。

**ステップ 2** [監査ログ (Audit Log)] をクリックします。

**ステップ 3** [監査ログを Syslog に送信 (Send Audit Log to Syslog)] ドロップダウンメニューから、[有効 (Enabled)] を選択します。

**ステップ 4** [ホスト (Host)] フィールドにある syslog サーバの IP アドレスまたは完全修飾名を使用して、監査情報の宛先ホストを指定します。デフォルトポート (6514) が使用されます。

**注意** 監査ログを受け入れるように設定しているコンピュータが、リモートメッセージを受け入れるようにセットアップされていない場合、ホストは監査ログを受け入れません。

(注) このフィールドに無効な IPv4 アドレス (192.168.1.456 など) を入力した場合でも、システムは警告を表示しません。代わりに、システムは無効なアドレスをホスト名として扱います。

**ステップ 5** [Syslog アラート ファシリティ \(2345 ページ\)](#) で説明されているとおりに、[ファシリティ (Facility)] リストからファシリティを選択します。

**ステップ 6** [syslog 重大度レベル \(2346 ページ\)](#) で説明されているとおりに、[重大度 (Severity)] リストから重大度を選択します。

**ステップ 7** オプションで、[タグ (Tag)] フィールドに、syslog メッセージとともに表示するタグ名を入力します。たとえば、syslog に送信されるすべての監査ログレコードの先頭に「FROMMC」を付加したい場合に、このフィールドに「FROMMC」と入力します。

**ステップ 8** [保存 (Save)] をクリックします。

次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## HTTP サーバへの監査ログメッセージの送信

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この機能を有効にすると、アプライアンスは、HTTP サーバに次の形式で監査ログレコードを送信します。

*Date Time Host [Tag] Sender: User\_Name@User\_IP, Subsystem, Action*

現地の日付、時刻、および発信元ホスト名の後に、角括弧で囲まれたオプションタグが続き、送信側デバイス名の後に監査ログメッセージが続きます。

たとえば、FROMMC のタグを指定した場合は、監査ログメッセージ例は次のように表示されます。

```
Mar 01 14:45:24 localhost [FROMMC] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring, Page View
```

このストリームのチャンネルは、SSL 証明書を使用して TLS と相互認証を有効にすることで保護できます。詳細については、[カスタム監査ログクライアント証明書 \(963 ページ\)](#) を参照してください。

### 始める前に

- 外部ホストが機能していることと、監査ログを送信するシステムからアクセスできることを確認します。

### 手順

**ステップ 1** Firepower Management Center または従来型の管理対象デバイスのどちらを設定しているかに応じて、次の操作を実行します。

- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
- 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択して、Firepower ポリシーを作成または編集します。

**ステップ 2** [監査ログ (Audit Log)] をクリックします。

**ステップ 3** 必要に応じて、[タグ (Tag)] フィールドに、メッセージとともに表示するタグ名を入力します。たとえば、すべての監査ログレコードの前に FROMMC を付けるには、このフィールドに FROMMC を入力します。

**ステップ 4** [HTTP サーバへの監査ログの送信 (Send Audit Log to HTTP Server)] ドロップダウンリストから、[有効 (Enabled)] を選択します。

**ステップ 5** [監査情報を送信する URL (URL to Post Audit)] フィールドに、監査情報の送信先 URL を指定します。次にリストした HTTP POST 変数を要求するリスナープログラムに対応する URL を入力します。

- subsystem
- actor
- event\_type
- message
- action\_source\_ip
- action\_destination\_ip
- 結果
- 時刻
- tag (定義されている場合。手順 3 を参照)



**注意** 暗号化されたポストを許可するには、HTTPS URL を使用します。外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があります。

**ステップ 6** [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## カスタム監査ログクライアント証明書

HTTP サーバまたは syslog サーバに監査ログをストリーミングする場合、Transport Layer Security (TLS) 証明書を使ってアプライアンスとサーバ間のチャンネルを保護することができます。これにより、信頼されたサーバにシステム監査ログを安全にストリーミングすると同時に、ローカルアプライアンスの使用領域を節約することができます。

監査ログをアプライアンスから外部サーバに安全にストリーミングするには、2つの要件があります。

- アプライアンスの署名付きクライアント証明書をインポートします。システム情報と指定した ID 情報に基づいて、証明書要求を生成できます。生成された要求を認証局に送信して、クライアント証明書を要求します。認証局 (CA) から署名付き証明書を取得すると、その証明書をインポートできます。
- Transport Layer Security (TLS) を使用するサーバとの通信チャンネルを設定します。

サーバに署名付き証明書の提供を要求します。その証明書を確認するため、1つ以上の証明書失効リスト (CRL) をロードするようにアプライアンスを設定します。アプライアンスは、サーバ証明書を CRL に記載されている証明書に照らして比較します。サーバが提供した証明書が失効した証明書として CRL に記載されている場合、そのサーバには監査ログをストリーミングできません。



(注) CRL を使用した証明書の確認を選択すると、システムはクライアント ブラウザ証明書、監査ログ サーバ証明書の両方の検証に同じ CRL を使用します。

次の要件のいずれか1つを満たしていないクライアント証明書をインポートすると、監査ログのストリーミングは失敗となります。

- 証明書の署名が、サーバ証明書の署名と同じ CA による署名でない。
- 証明書が、証明書チェーンの中間証明書に署名したものと同一 CA によって署名されていない。

## 現在の監査ログクライアント証明書の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center7000 & 8000 シリーズ NGIPsv	グローバルのみ	Admin

ログインしているアプライアンスの監査ログクライアント証明書のみ表示できます。



(注) ASA FirePOWER デバイスの監査ログクライアント証明書を表示するには、**show audit\_cert** CLI コマンドを使用します。

### 手順

**ステップ 1** Firepower Management Center または従来型の管理対象デバイスのどちらに向けた監査ログのストリーミングを構成しているかに応じて、次のように操作します。

- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
- 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択して、Firepower ポリシーを作成または編集します。

**ステップ 2** [監査ログ証明書 (Audit Log Certificate)] をクリックします。

## 監査ログクライアントの証明書署名要求の生成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center7000 & 8000 シリーズ NGIPsv	グローバルのみ	Admin

この手順を使用して証明書要求を生成すると、単一のシステムにのみ対応する証明書を生成できます。セキュリティを確保するために、広く知られており、信頼できる CA によって署名された証明書を使用してください。

システムは、ベース 64 エンコードの PEM 形式で証明書要求のキーを生成します。



(注) ASA FirePOWER デバイスの場合は、キー ペアと証明書を手動で生成します。

## 手順

- 
- ステップ 1** Firepower Management Center または従来型の管理対象デバイスのどちらに向けた監査ログのストリーミングを構成しているかに応じて、次のように操作します。
- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
  - 管理対象デバイス : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択して、Firepower ポリシーを作成または編集します。
- ステップ 2** [監査ログ証明書 (Audit Log Certificate) ] をクリックします。
- ステップ 3** [新規 CSR の生成 (Generate New CSR) ] をクリックします。
- ステップ 4** [国名 (2 文字のコード) (Country Name (two-letter code)) ] フィールドに国番号を入力します。
- ステップ 5** [都道府県 (State or Province) ] フィールドに、都道府県名を入力します。
- ステップ 6** [市区町村 (Locality or City) ] を入力します。
- ステップ 7** [組織 (Organization) ] の名前を入力します。
- ステップ 8** [組織単位 (部署名) (Organizational Unit (Department)) ] の名前を入力します。
- ステップ 9** [共通名 (Common Name) ] フィールドに、証明書を要求するサーバの完全修飾ドメイン名を入力します。
- (注) 共通名と DNS ホスト名が一致しないと、監査ログのストリーミングは失敗します。
- ステップ 10** [生成 (Generate) ] をクリックします。
- ステップ 11** テキストエディタで、新しい空のファイルを開きます。
- ステップ 12** 証明書要求のテキストブロック全体 (BEGIN CERTIFICATE REQUEST 行と END CERTIFICATE REQUEST 行を含む) をコピーして、空のテキスト ファイルに貼り付けます。
- ステップ 13** このファイルを *clientname.csr* として保存します。 *clientname* は、証明書を使用する予定のアプライアンスの名前にします。
- ステップ 14** [閉じる (Close) ] をクリックします。
- 

## 次のタスク

- 証明機関に証明書要求を送信します。
- 署名された証明書を受信したら、その証明書を要求したアプライアンスにインポートします。 [監査ログクライアント証明書のインポート \(966 ページ\)](#) を参照してください。

## 監査ログクライアント証明書のインポート

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center7000 & 8000 シリーズ NGIPsv	グローバルのみ	Admin

証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、証明書チェーン（証明書パスとも呼ばれる）を提供します。

監査ログのストリーミングは、次に示す条件のいずれかを満たしていないクライアント証明書をインポートすると失敗します。

- 証明書が、サーバ証明書に署名したものと同一 CA によって署名されていない。
- 証明書が、証明書チェーンの中間証明書に署名したものと同一 CA によって署名されていない。



(注) ASA FirePOWER に監査ログクライアント証明書をインポートするには、CLI コマンド `configure audit_cert import` を使用します。

### 始める前に

- 証明書署名要求を生成します。[監査ログクライアントの証明書署名要求の生成 \(964 ページ\)](#) を参照してください。
- 証明書を要求する認証局に CSR ファイルをアップロードします。

### 手順

**ステップ 1** Firepower Management Center または従来型の管理対象デバイスのどちらに向けた監査ログのストリーミングを構成しているかに応じて、次のように操作します。

- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
- 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択して、Firepower ポリシーを作成または編集します。

**ステップ 2** [監査ログ証明書 (Audit Log Certificate)] をクリックします。

**ステップ 3** [監査クライアント証明書のインポート (Import Audit Client Certificate)] をクリックします。

**ステップ 4** テキストエディタでクライアント証明書を開いて、BEGIN CERTIFICATE の行と END CERTIFICATE の行を含むテキストのブロック全体をコピーします。このテキストを [クライアント証明書 (Client Certificate)] フィールドに貼り付けます。

- ステップ5** 秘密キーをアップロードするには、秘密キー ファイルを開いて、BEGIN RSA PRIVATE KEY の行と END RSA PRIVATE KEY の行を含むテキストのブロック全体をコピーします。このテキストを [秘密キー (Private Key) ] フィールドに貼り付けます。
- ステップ6** 必要な中間証明書をすべて開いて、それぞれのテキストのブロック全体をコピーして、[証明書チェーン (Certificate Chain) ] フィールドに貼り付けます。
- ステップ7** [保存 (Save) ] をクリックします。

## 有効な監査ログ サーバの証明書の強制

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center 従来型	グローバルのみ	Admin

システムは、識別符号化規則 (DER) 形式でインポートされている CRL を使用した、監査ログ サーバ証明書の検証をサポートしています。

CRL を使用する場合は、失効した証明書のリストを最新の状態に保つために、CRL を更新するスケジュールタスクを作成してください。システムは、最後に更新した CRL を表示します。



- (注) CRL を選択すると、システムは、同じ CRL を使用して、監査ログ証明書の検証と、アプライアンスと Web ブラウザの間の HTTP 接続を保護する証明書の検証の両方に同じ CRL を使用します。



- 注意** 有効なクライアント証明書をインポートせずに、相互認証を有効にすると、監査ログのストリーミングが失敗します。

### 始める前に

- 接続に使用するサーバ証明書に署名したものと同一 CA で署名されたクライアント証明書をインポートします。[監査ログクライアント証明書のインポート \(966 ページ\)](#) を参照してください。
- クライアント証明書チェーンをインポートします (必要な場合)。[監査ログクライアント証明書のインポート \(966 ページ\)](#) を参照してください。

## 手順

- 
- ステップ 1** Firepower Management Center または従来型の管理対象デバイスのどちらに向けた監査ログのストリーミングを構成しているかに応じて、次のように操作します。
- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
  - 管理対象デバイス : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択して、Firepower ポリシーを作成または編集します。
- ステップ 2** [監査ログ証明書 (Audit Log Certificate) ] をクリックします。
- ステップ 3** [TLS の有効化 (Enable TLS) ] を選択して、監査ログを外部サーバにストリーミングする際に Transport Layer Security を使用します。
- ステップ 4** [相互認証の有効化 (Enable Mutual Authentication) ] を選択します。
- ステップ 5** 次の 2 つの対処法があります。
- 1 つ以上の CRL を使用してサーバ証明書を検証する場合は、[CRL のフェッチの有効化 (Enable Fetching of CRL) ] を選択して、手順 6 に進みます。
  - 検証なしでサーバ証明書を承認する場合は、手順 9 に進みます。
- ステップ 6** 既存の CRL ファイルへの有効な URL を入力して、[CRL の追加 (Add CRL) ] をクリックします。最大 25 個まで CRL の追加を繰り返します。
- ステップ 7** [CRL の更新 (Refresh CRL) ] をクリックして現在の CRL をロードするか、指定した URL から CRL をロードします。
- (注) CRL のフェッチを有効にすると、定期的に CRL を更新するスケジュールタスクが作成されます。このタスクを編集して、更新の頻度を設定します。
- ステップ 8** クライアント証明書を作成したものと同一認証局によって生成された有効なクライアント証明書があることを確認します。
- ステップ 9** [保存 (Save) ] をクリックします。
- 

# ダッシュボード設定

ダッシュボードでは、ウィジェットを使用することにより、現在のシステムステータスが一目でわかります。ウィジェットは小さな自己完結型コンポーネントであり、Firepower システムのさまざまな側面に関するインサイトを提供します。Firepower システムには、事前定義された複数のダッシュボード ウィジェットが付属しています。

[カスタム分析 (Custom Analysis) ] ウィジェットがダッシュボードで有効になるように、Firepower Management Center を設定できます。

## 関連トピック

[ダッシュボードについて](#) (247 ページ)

## ダッシュボードのカスタム分析ウィジェットの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	グローバルだけ	Admin

[カスタム分析 (Custom Analysis) ]ダッシュボードウィジェットを使用して、柔軟でユーザによる構成が可能なクエリに基づいてイベントのビジュアル表現を作成します。

### 手順

- ステップ 1 [システム (System) ] > [設定 (Configuration) ] を選択します。
- ステップ 2 [ダッシュボード (Dashboard) ] をクリックします。
- ステップ 3 ユーザが [カスタム分析 (Custom Analysis) ] ウィジェットをダッシュボードに追加できるようにするには、[カスタム分析ウィジェットの有効化 (Enable Custom Analysis Widgets) ] チェックボックスをオンにします。
- ステップ 4 [保存 (Save) ] をクリックします。

## DNS キャッシュ

イベント表示ページで、IP アドレスを自動的に解決するようにシステムを設定できます。また、アプライアンスによって実行される DNS キャッシュの基本的なプロパティを設定できます。DNS キャッシングを設定すると、追加のルックアップを実行せずに、以前に解決した IP アドレスを識別できます。これにより、IP アドレスの解決が有効になっている場合に、ネットワーク上のトラフィックの量を減らし、イベントページの表示速度を速めることができます。

## DNS キャッシュ プロパティの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	グローバルだけ	Admin

DNS 解決のキャッシングは、以前に解決された DNS ルックアップのキャッシングを許可するシステム全体の設定です。

## 手順

- 
- ステップ 1** [システム (System) ] > [設定 (Configuration) ] を選択します。
- ステップ 2** [DNS キャッシュ (DNS Cache) ] を選択します。
- ステップ 3** [DNS 解決のキャッシング (DNS Resolution Caching) ] ドロップダウン リストから、次のいずれかを選択します。
- [有効化 (Enabled) ] : キャッシングを有効にします。
  - [無効化 (Disabled) ] : キャッシングを無効にします。
- ステップ 4** [DNS キャッシュ タイムアウト (分) (DNS Cache Timeout (in minutes) ) ] フィールドで、非アクティブのために削除されるまで DNS エントリがメモリ内にキャッシュされる時間 (分単位) を入力します。
- デフォルトは 300 分 (5 時間) です。
- ステップ 5** [保存 (Save) ] をクリックします。
- 

## 関連トピック

- [イベント ビュー設定の設定 \(37 ページ\)](#)
- [管理インターフェイス \(931 ページ\)](#)

# 電子メールの通知

次の処理を行う場合は、メール ホストを設定します。

- イベントベースのレポートの電子メール送信
- スケジュールされたタスクのステータス レポートの電子メール送信
- 変更調整レポートの電子メール送信
- データプルーニング通知の電子メール送信
- 検出イベント、インパクト フラグ、相関イベント アラート、侵入イベント アラート、およびヘルス イベント アラートでの電子メールの使用

電子メール通知を設定する場合、システムとメール リレー ホスト間の通信に使用する暗号化方式を選択し、必要に応じて、メールサーバの認証クレデンシャルを指定できます。設定した後、接続をテストできます。



## メールリレー ホストおよび通知アドレスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	グローバルだけ	Admin

### 手順

**ステップ 1** [システム (System) ] > [設定 (Configuration) ] を選択します。

**ステップ 2** [Email Notification] をクリックします。

**ステップ 3** [メールリレー ホスト (Mail Relay Host) ] フィールドで、使用するメール サーバのホスト名または IP アドレスを入力します。入力したメール ホストはアプライアンスからのアクセスを許可している **必要があります**。

**ステップ 4** [ポート番号 (Port Number) ] フィールドに、電子メール サーバで使用するポート番号を入力します。

一般的なポートには次のものがあります。

- 25。暗号化を使用しない場合
- 465。SSLv3 を使用する場合
- 587。TLS を使用する場合

**ステップ 5** [暗号化方式 (Encryption Method) ] を選択します。

- [TLS] : Transport Layer Security を使用して通信を暗号化します。
- [SSLv3] : セキュア ソケット レイヤを使用して通信を暗号化します。
- [なし (None) ] : 暗号化されていない通信を許可します。

(注) アプライアンスとメールサーバとの間の暗号化された通信では、証明書の検証は不要です。

**ステップ 6** [送信元アドレス (From Address) ] フィールドに、アプライアンスから送信されるメッセージの送信元電子メールアドレスとして使用する有効な電子メールアドレスを入力します。

**ステップ 7** 必要に応じて、メールサーバに接続する際にユーザ名とパスワードを指定するには、[認証を使用 (Use Authentication) ] を選択します。[ユーザ名 (Username) ] フィールドにユーザ名を入力します。パスワードを [パスワード (Password) ] フィールドに入力します。

**ステップ 8** 設定したメールサーバを使用してテストメールを送信するには、[テストメールのサーバ設定 (Test Mail Server Settings) ] をクリックします。  
テストの成功または失敗を示すメッセージがボタンの横に表示されます。

**ステップ 9** [保存 (Save) ] をクリックします。

## 言語の選択

[言語 (Language) ] ページを使用して、Web インターフェイス用に異なる言語を指定できます。

### 別の言語の指定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 7000 & 8000 シリーズ	任意 (Any)	Admin

この設定は、Firepower Management Center または 7000 および 8000 シリーズ 管理対象デバイスに適用されます。

- Firepower Management Center では、この設定はシステム設定の一部になります。
- 7000 および 8000 シリーズ 管理対象デバイスでは、この設定をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。



**注意** ここで指定した言語は、アプライアンスにログインしたすべてのユーザの Web インターフェイスに使用されます。

#### 手順

**ステップ 1** Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
- 管理対象デバイス : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower ポリシーを作成または編集します。

**ステップ 2** [言語 (Language) ] をクリックします。

**ステップ 3** 使用する言語を選択します。

**ステップ 4** [保存 (Save) ] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ログインバナー

[ログインバナー (Login Banner)] ページを使用して、セキュリティ アプライアンスまたは共有ポリシーのセッションバナー、ログインバナー、カスタム メッセージバナーを指定できます。

バナーのテキストにはスペースを使用できますが、タブは使用できません。バナーには複数行のテキストを指定できます。テキストに空の行が含まれている場合、バナーでは、その行が改行 (CR) として表示されます。使用できるのは、改行 (Enter キーを押す) を含む ASCII 文字だけです。改行は 2 文字としてカウントされます。

Telnet または SSH を介してセキュリティ アプライアンスにアクセスしたときに、バナー メッセージを処理するのに十分なシステム メモリがなかった場合や、バナー メッセージの表示を試行して TCP 書き込みエラーが発生した場合には、セッションが閉じます。

## カスタム ログインバナーの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

SSH または Web インターフェイスからログインするユーザに向けて表示するカスタム ログインバナーを作成できます。

この設定は、Firepower Management Center または従来型の管理対象デバイス (7000 および 8000 シリーズ、ASA FirePOWER および NGIPSv) に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

### 手順

- ステップ 1** Firepower Management Center または Classic 管理対象デバイスのいずれを設定しているかに応じて、以下を実行します。

- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
- 管理対象デバイスの場合 : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択するか、ファイアウォール ポリシーを作成、または編集します。

ステップ 2 [ログインバナー (Login Banner) ] を選択します。

ステップ 3 [カスタム ログインバナー (Custom Login Banner) ] フィールドに、使用するログインバナーテキストを入力します。

ステップ 4 [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## SNMP ポーリング

Firepower Management Center およびクラシック管理対象デバイスには、Simple Network Management Protocol (SNMP) ポーリングを有効にすることができます。SNMP 機能は、SNMP プロトコルのバージョン 1、2、3 をサポートします。

この機能を使用して、次の要素にアクセスできます。

- 標準 Management Information Base (MIB)。これには、連絡先、管理、場所、サービス情報、IP アドレッシングやルーティングの情報、トランスミッション プロトコルの使用状況の統計などのシステムの詳細が含まれます。
- 7000 および 8000 シリーズ 管理対象デバイスの追加の MIB。これには、物理インターフェイス、論理インターフェイス、仮想インターフェイス、ARP、NDP、仮想ブリッジ、仮想ルータを通して渡されるトラフィックの統計が含まれます。



(注) SNMP プロトコルの SNMP バージョンを選択する際は、SNMPv2 では読み取り専用コミュニティのみをサポートし、SNMPv3 では読み取り専用ユーザのみをサポートすることに注意してください。SNMPv3 は AES128 による暗号化もサポートします。

SNMP 機能を有効にすると、システムで SNMP トラップを送信できなくなり、MIB の情報はネットワーク管理システムによるポーリングでのみ使用可能になることに注意してください。

## SNMP ポーリングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。



- (注) システムをポーリングするには、使用する任意のコンピュータで SNMP アクセスを追加する必要があります。SNMP MIB には展開の攻撃に使用される可能性がある情報も含まれているので注意してください。SNMP アクセスのアクセスリストを MIB のポーリングに使用される特定のホストに制限することをお勧めします。SNMPv3 を使用し、ネットワーク管理アクセスには強力なパスワードを使用することもお勧めします。

SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

### 始める前に

- [システムのアクセスリストの設定 \(958 ページ\)](#) の説明に従って、使用するコンピュータごとに SNMP アクセスを追加し、システムをポーリングします。

### 手順

**ステップ 1** Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
- 管理対象デバイス : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower ポリシーを作成または編集します。

**ステップ 2** [SNMP] をクリックします。

- ステップ 3** [SNMP バージョン (SNMP Version)] ドロップダウン リストから、使用する SNMP バージョンを選択します。
- ステップ 4** 次の選択肢があります。
- [バージョン 1 (Version 1)] または [バージョン 2 (Version 2)] を選択した場合は、[コミュニティ スtring (Community String)] フィールドに SNMP コミュニティ名を入力します。手順 13 に進みます。
 

(注) SNMPv2 は、読み取り専用コミュニティのみをサポートしています。
  - [バージョン 3 (Version 3)] を選択した場合、[ユーザを追加 (Add User)] をクリックするとユーザ定義ページが表示されます。
 

(注) SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。
- ステップ 5** ユーザ名を入力します。
- ステップ 6** [認証プロトコル (Authentication Protocol)] ドロップダウン リストから、認証に使用するプロトコルを選択します。
- ステップ 7** [認証パスワード (Authentication Password)] フィールドに SNMP サーバの認証に必要なパスワードを入力します。
- ステップ 8** [パスワードの確認 (Verify Password)] フィールドに、認証パスワードを再度入力します。
- ステップ 9** 使用するプライバシー プロトコルを [プライバシー プロトコル (Privacy Protocol)] リストから選択するか、プライバシー プロトコルを使用しない場合は [なし (None)] を選択します。
- ステップ 10** [プライバシー パスワード (Privacy Password)] フィールドに SNMP サーバに必要な SNMP プライバシー キーを入力します。
- ステップ 11** [パスワードの確認 (Verify Password)] フィールドに、プライバシー パスワードを再度入力します。
- ステップ 12** [追加 (Add)] をクリックします。
- ステップ 13** [保存 (Save)] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## セキュリティ認定準拠の

お客様の組織が、米国防総省およびグローバル認定組織によって確立されたセキュリティ基準に従う機器とソフトウェアだけを使用することを求められる場合があります。Firepower システムでは、以下のセキュリティ認定標準規格へのコンプライアンスをサポートします。

- コモンクライテリア (CC) : 国際コモンクライテリア承認アレンジメントによって確立された、セキュリティ製品のプロパティを定義するグローバル標準規格
- Unified Capabilities Approved Products List (UCAPL) : 米国国防情報システム局 (DISA) によって確立された、セキュリティ要件を満たす製品のリスト



(注) 米国政府は、Unified Capabilities Approved Products List (UCAPL) の名称を Defense Information Network Approved Products List (DODIN APL) に変更しました。このドキュメントおよび Firepower Management Center Web インターフェイスでの UCAPL の参照は、DODIN APL への参照として解釈できます。

- 連邦情報処理標準 (FIPS) 140 : 暗号化モジュールの要件に関する規定

セキュリティ認定コンプライアンスは、CC モードまたは UCAPL モードで有効にすることができます。セキュリティ認定コンプライアンスを有効にしても、選択したセキュリティモードのすべての要件との厳密なコンプライアンスが保証されるわけではありません。強化手順についての詳細は、認定機関から提供されている本製品に関するガイドラインを参照してください。



**注意** この設定を有効にした場合、無効にすることはできません。設定を無効にする必要がある場合は、サポートに連絡して支援を求めてください。

## セキュリティ認定準拠特性

次の表は、CC または UCAPL モードを有効にしたときの動作の変更を示しています。(ログインアカウントの制約は、Web インターフェイスアクセスではなくコマンドラインまたはシェルアクセスを指します。)

システムの変更	CC モード	UCAPL モード
FIPS コンプライアンスは有効です。	○	○
バックアップまたはレポートについては、リモートストレージは利用できません。	○	○
追加のシステム監査デーモンが開始されます。	なし	○
システムブートローダは固定されています。	なし	○
追加のセキュリティがログインアカウントに適用されます。	なし	○
ログインアカウントセッションの自動ログアウトを実行します。	なし	○

システムの変更	CC モード	UCAPL モード
再起動キー シーケンスの Ctrl-Alt-Del を無効にします。	なし	○
最大 10 の同時ログイン セッションを実行します。	なし	○
次の場合、システムは、アプライアンスとの SSH セッションで自動的にキーを再生成します： <ul style="list-style-type: none"> <li>セッション アクティビティでキーが 1 時間使用された後</li> <li>キーを使用して接続で 1 GB のデータが伝送された後</li> </ul> これは、バージョン 6.1.0.4 またはそれ以降の 6.1.0.x パッチに当てはまります。	○	○
システムは、バージョン 6.1.0.6 の場合のみ、eStreamer を使用したイベント データのエクスポートをサポートします。	○	○
ログインアカウントの厳密なセーフガードを適用します。 <ul style="list-style-type: none"> <li>パスワードは、大文字および小文字を組み合わせて最大 15 の英数字として、1 つ以上の数字を含む必要があります。</li> <li>パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。</li> <li>3 回連続ログインに失敗した場合、そのユーザはロックアウトされます。この場合は、管理者がパスワードをリセットする必要があります。</li> <li>パスワード履歴を保存しています。</li> <li>ログインが成功した場合は、失敗したログインの履歴を表示します。</li> </ul>	なし	○

## セキュリティ認定準拠の推奨事項

セキュリティ認定コンプライアンスの使用が有効のときに、次のベストプラクティスを確認することをお勧めします。

- 展開時にセキュリティ認定準拠を有効にするには、最初に Firepower Management Center で有効にし、次に、管理対象のすべてのデバイスの同じモードで有効にします。



**注意** 両方が同じセキュリティ認定準拠モードで動作していない限り、Firepower Management Center は管理対象デバイスからイベントデータを受信しません。



- 次の機能を使用するようにシステムを設定できません。
  - 電子メールレポート、アラート、データのプルーニング通知。
  - Nmap Scan、Cisco IOS Null Route、Set Attribute Value、ISE EPS の修復。
  - バックアップまたはレポート用のリモートストレージ。
  - サードパーティクライアントのシステム データベースへのアクセス。
  - 電子メール、SNMP トラップ、syslog から送信される外部通知、アラート。
  - アプライアンスとサーバの間のチャンネルを保護するために、SSL 証明書を使用せずに、HTTP サーバまたは syslog サーバに送信された監査ログ メッセージ。
- バージョン 6.1.0.6 の場合のみ、eStreamer を使用してイベント データを外部クライアントにエクスポートするようにシステムを設定できます。
- CC モードを使用して展開中に SSO を有効にできません。
- CC モードを使用して展開中に CAC を有効にできません。
- CC または UCAPL モードを使用した展開では、Firepower REST API 経由で Firepower Management Center および管理対象デバイスへのアクセスを無効にします。
- UCAPL モードを使用して展開中に CAC を有効にします。



(注) Firepower システムは、以下に関する CC および UCAPL モードをサポートしていません。

- ハイ アベイラビリティ ペアの Firepower Management Center
- スタックまたはハイ アベイラビリティ ペアの従来型デバイス

## セキュリティ認定コンプライアンスの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来型の管理対象デバイス (7000 および 8000 シリーズ、ASA FirePOWER、NGIPSv) に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来型の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまでは、構成が有効になりません。



**注意** この設定を有効にした後は、無効にすることはできません。無効にする必要がある場合は、Cisco TAC にご連絡ください。

### 始める前に

- アプライアンスでセキュリティ認定コンプライアンスを有効にする前に、展開に組み込む予定のあるすべてのデバイスを Firepower Management Center に登録することをお勧めします。

### 手順

**ステップ 1** 設定するアプライアンスの種類に応じて、次のようにします。

- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
- 従来型管理対象デバイス : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower ポリシーを作成または編集します。

**ステップ 2** [UCAPL/CC コンプライアンス (UCAPL/CC Compliance) ] をクリックします。

- (注) UCAPL または CC コンプライアンスを有効にすると、アプライアンスがリブートします。Firepower Management Center は、システム設定を保存するとリブートし、管理対象デバイスは、設定の変更を展開するとリブートします。

**ステップ 3** アプライアンスのセキュリティ認定コンプライアンスを永続的に有効にするには、2つの選択肢があります。

- [コモンクライテリア (Common Criteria) ] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウンリストから [CC] を選択します。
- [Unified 機能承認製品リスト (Unified Capabilities Approved Products List) ] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウンリストから [UCAPL] を選択します。

**ステップ 4** [保存 (Save) ] をクリックします。

### 次のタスク

- まだ適用していない場合は、制御と防御のライセンスを、展開内のすべての従来型アプライアンスに適用します。
- アプライアンスがバージョン 5.2.0 より前のバージョンから更新された場合は、セキュリティ認定コンプライアンスを有効にすると、アプライアンス証明書が再生成されます。展

開全体でセキュリティ認定コンプライアンスを同じモードで有効にした後、管理対象デバイスを Firepower Management Center に再登録します。

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

## 時刻および時刻の同期

[時刻 (Time) ] ページを使用して、Firepower Management Center、あるいは 7000 または 8000 シリーズ デバイスのローカル Web インターフェイスから現在の時刻と時刻源を表示することができます。

時刻の設定は、アプライアンスの大半のページで、[タイムゾーン (Time Zone) ] ページで設定したタイムゾーン (デフォルトでは [アメリカ/ニューヨーク (America/New York) ]) を使用してローカル時間で表示されますが、アプライアンス自体には UTC 時間を使用して保存されます。また、現在の時刻は [時刻の同期 (Time Synchronization) ] ページの上部に UTC で表示されます (ローカル時間は [手動 (Manual) ] の時計設定オプションで表示されます (有効になっている場合) )。

時刻の同期は、[時刻の同期 (Time Synchronization) ] ページを使用して管理できます。時刻を同期する場合、以下の方法を選択できます。

- 手動で
- 1 つ以上の NTP サーバを使用 (推奨)

ハードウェアの Firepower Management Center を NTP サーバとして使用できますが、仮想 Firepower Management Center は NTP サーバとして使用しないでください。

リモートの NTP サーバを指定する場合、アプライアンスにそのサーバに対するネットワークアクセス権限が必要です。信頼できない NTP サーバを指定しないでください。NTP サーバへの接続では、構成されたプロキシ設定は使用されません。



- (注) 時刻の同期後に、Firepower Management Center と管理対象デバイスの時刻が一致するようにしてください。時刻が一致していない場合、管理対象デバイスが Firepower Management Center と通信する際に意図しない結果が生じるおそれがあります。

## 手動での時間指定

Firepower Management Center の時刻同期が [ローカル設定で手動 (Manually in Local Configuration) ] に設定されている場合、システムの時刻を手動で設定できます。

- Firepower Management Center が NTP を使用して時間を提供するようにするには、NTP を使用して時間を提供するように Firepower Management Center を設定する前に、時間を手動で変更する必要があります。

- Firepower Management Center を NTP サーバとして設定してから時刻を変更する必要がある場合、NTP オプションを無効にして、時間を手動で変更してから NTP オプションを再度有効にする必要があります。

システムの時間が NTP に基づいて同期されている場合、Firepower Management Center の Web インターフェイスおよび 7000 および 8000 シリーズ デバイスのローカル Web インターフェイスで以下の情報を含む NTP ステータスを表示できます。

表 70: NTP ステータス

カラム (Column)	説明
NTP サーバ	構成済みの NTP サーバの IP アドレスと名前。
ステータス	<p>NTP サーバの時間同期のステータス。</p> <ul style="list-style-type: none"> <li>• [使用中 (Being Used)] は、アプライアンスが NTP サーバと同期していることを示します。</li> <li>• [利用可能 (Available)] は、NTP サーバが使用可能であるものの、時間がまだ同期していないことを示します。</li> <li>• [使用不可 (Not Available)] は、NTP サーバが構成に含まれているものの、NTP デーモンがその NTP サーバを使用できないことを示します。</li> <li>• [待機中 (Pending)] は、NTP サーバが新しいか、または NTP デーモンが最近再起動されたことを示します。この値は、時間の経過とともに [使用中 (Being Used)]、[利用可能 (Available)]、または [使用不可 (Not Available)] に変わるはずです。</li> <li>• [不明 (Unknown)] は、NTP サーバのステータスが不明であることを示します。</li> </ul>
オフセット	アプライアンスと構成済みの NTP サーバ間の時間の差 (ミリ秒)。負の値はアプライアンスの時間が NTP サーバより遅れていることを示し、正の値は進んでいることを示します。

カラム (Column)	説明
最終更新	NTP サーバと最後に時間を同期してから経過した時間 (秒数)。NTP デーモンは、いくつかの条件に基づいて自動的に同期時間を調整します。たとえば、更新時間が大きい (300 秒など) 場合、それは時間が比較的安定しており、NTP デーモンが小さい更新増分値を使用する必要がないと判断したことを示します。

## 時刻の手動設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	任意 (Any)	Admin

Firepower Management Center または 7000 および 8000 シリーズ デバイスのローカル Web インターフェイスで [時間 (Time)] ページを使用して、現在の時刻と時刻源を表示できます。



- (注) NTP を使用して Firepower Management Center に時間を提供させる場合、時間を手動で変更してから Management Center が NTP を使用して時間を提供するように設定します。

### 手順

- ステップ 1 [システム (System)] > [設定 (Configuration)] を選択します。
- ステップ 2 [時間同期 (Time Synchronization)] をクリックします。
- ステップ 3 [NTP を使用して時間を提供 (Serve Time via NTP)] が [有効 (Enabled)] の場合、[無効 (Disable)] を選択します。
- ステップ 4 [保存 (Save)] をクリックします。
- ステップ 5 [ローカル設定で手動 (Manually in Local Configuration)] を選択します。
- ステップ 6 [保存 (Save)] をクリックします。
- ステップ 7 [時間 (Time)] をクリックします。
- ステップ 8 [時間の設定 (Set Time)] ドロップダウン リストを使用して時間を設定します。
- ステップ 9 [適用 (Apply)] をクリックします。

### 次のタスク

- NTP を使用して Firepower Management Center に時間を提供させるには、次の説明に従って続行します。 [Firepower Management Center からの時間の提供 \(984 ページ\)](#)

## Firepower Management Center からの時間の提供

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	グローバルだけ	Admin



- (注) NTP を使用して時刻を提供するように Management Center を設定してから、後でそれを無効にした場合、管理対象デバイスの NTP サービスは引き続き Management Center と時刻を同期しようとします。新しい時刻ソースを確立するには、すべての該当するプラットフォーム設定ポリシーを更新および再展開する必要があります。

### 始める前に

- 手動で時間を変更します。 [時刻の手動設定 \(983 ページ\)](#) を参照してください。

### 手順

- ステップ 1** [システム (System)] > [設定 (Configuration)] を選択します。
  - ステップ 2** [時刻同期 (Time Synchronization)] をクリックします。
  - ステップ 3** [NTP 経由で時刻を提供 (Serve Time via NTP)] ドロップダウンリストから、[有効 (Enabled)] を選択します。
  - ステップ 4** 管理対象デバイスの [自分のクロックの設定 (Set My Clock)] オプションについては、時刻の同期方法を指定するための次のオプションを選択できます。
    - [ローカル設定で手動 (Manually in Local Configuration)] を選択して、Firepower Management Center から NTP 経由で時刻を受信します。詳細については、 [時刻の手動設定 \(983 ページ\)](#) を参照してください。
    - [NTP 経由 (Via NTP from)] を選択して、さまざまなサーバから NTP 経由で時刻を受信します。テキストボックスで、NTP サーバの IP アドレスのカンマ区切りリストを入力するか、DNS が有効になっている場合は、完全修飾ホスト名およびドメイン名を入力します。
- 注意** アプライアンスがリブートされ、ここで指定したものと異なる NTP サーバレコードを DHCP サーバが設定した場合、DHCP 提供の NTP サーバが代わりに使用されます。この状況を回避するには、同じ NTP サーバを設定するように DHCP サーバを設定します。

ステップ5 [保存 (Save) ]をクリックします。

(注) Management Center を管理対象デバイスと同期するには、数分かかる場合があります。

## 時間の同期

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス (7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv) に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

### 手順

ステップ1 Firepower Management Center または Classic 管理対象デバイスのいずれを設定しているかに応じて、以下を実行します。

- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
- 管理対象デバイス : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower ポリシーを作成または編集します。

ステップ2 [時間同期 (Time Synchronization) ]をクリックします。

ステップ3 管理対象デバイスで時刻を同期する方法を指定する次のオプションがあります。

- NTP を介して Management Center から時刻を受信するには、[NTP 経由で管理センターから (Via NTP from Management Center) ] を選択します。詳細については、[Firepower Management Center からの時間の提供 \(984 ページ\)](#) を参照してください。
- [NTP 経由 (Via NTP from) ] を選択して、さまざまなサーバから NTP 経由で時刻を受信します。テキスト ボックスで、NTP サーバの IP アドレスのカンマ区切りリストを入力するか、DNS が有効になっている場合は、完全修飾ホスト名およびドメイン名を入力します。

ステップ4 [保存 (Save) ]をクリックします。

(注) 設定された NTP サーバと管理対象デバイスを同期するには、数分かかる場合があります。さらに、管理対象デバイスを NTP サーバとして設定されている Management Center と同期する場合、Management Center 自体が NTP サーバを使用するように設定されていると、時刻を同期するのにいくらか時間がかかることがあります。これは、管理対象デバイスに時刻を提供するために、Management Center は設定された NTP サーバとまず同期する必要があるためです。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。
- Management Center と管理対象デバイスの時刻が一致していることを確認します。

## セッションタイムアウト

Firepower システムの Web インターフェイスまたは補助コマンドライン インターフェイスの無人ログインセッションは、セキュリティ上のリスクを生じさせる場合があります。ユーザのログインセッションが非アクティブになったためにタイムアウトするまでのアイドル時間を分単位で設定できます。シェル (コマンドライン) セッションでも同様のタイムアウトを設定できます。

長期にわたり Web インターフェイスをパッシブかつセキュアにモニタする予定のユーザが、導入内に存在する可能性があります。ユーザ設定オプションで Web インターフェイスのセッションタイムアウトからユーザを除外することができます。メニュー オプションへの完全なアクセス権がある管理者ロールのユーザは、侵害が生じる場合、余分のリスクを生じさせますが、セッションタイムアウトから除外することはできません。

## セッションタイムアウトの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス (7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv) に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。



いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

システムへのシェルアクセスを制限する必要がある場合、追加オプションによって補助コマンドライン インターフェイスの `expert` コマンドを永続的に無効にすることができます。アプライアンスでエキスパートモードを無効にすると、構成シェルアクセスを持つユーザでも、シェルのエキスパートモードに入ることができなくなります。ユーザが補助コマンドライン インターフェイスのエキスパートモードに入ると、ユーザはシェルに応じた任意の Linux コマンドを実行できます。エキスパートモードに入っていない場合は、コマンドラインユーザはコマンドライン インターフェイスが提供するコマンドだけを実行できます。

## 手順

**ステップ 1** Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
- 管理対象デバイス : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower ポリシーを作成または編集します。

**ステップ 2** [シェルタイムアウト (Shell Timeout) ] をクリックします。

**ステップ 3** 次の選択肢があります。

- Web インターフェイスのセッションタイムアウトを設定するには、[ブラウザセッションタイムアウト (分) (Browser Session Timeout (Minutes)) ] フィールドに数値 (分数) を入力します。デフォルト値は 60 で、最大値は 1440 (24 時間) です。このセッションタイムアウトからユーザを除外する方法については、[ユーザアカウントログインオプション \(89 ページ\)](#) を参照してください。
- コマンドライン インターフェイスのセッションタイムアウトを設定するには、[シェルタイムアウト (分) (Shell Timeout (Minutes)) ] フィールドに数値 (分数) を入力します。デフォルト値は 0 で、最大値は 1440 (24 時間) です。
- 補助コマンドライン インターフェイスで `expert` コマンドを永続的に無効にするには、[`expert` コマンドを永続的に無効化 (Permanently Disable Expert Access) ] チェックボックスを選択します。

**注意** エキスパートモードが無効になった状態でポリシーをアプライアンスに展開した場合、Web インターフェイスまたは補助コマンドライン インターフェイスを介してエキスパートモードにアクセスする機能を復元することはできません。エキスパートモード機能を復元するには、サポートに問い合わせる必要があります。

**ステップ 4** [保存 (Save) ] をクリックします。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 脆弱性マッピング

サーバのディスカバリ イベント データベースにアプリケーション ID が含まれており、トラフィックの packets ヘッダーにベンダーおよびバージョンが含まれる場合、Firepower システムは、そのアドレスから送受信されるすべてのアプリケーション プロトコル トラフィックについて、脆弱性をホスト IP アドレスに自動的にマップします。

パケットにベンダー情報もバージョン情報も含まれないサーバすべてに対して、システムでこれらのベンダーとバージョンレスのサーバのサーバトラフィックと脆弱性を関連付けるかどうかを設定できます。

たとえば、ホストがヘッダーにベンダーまたはバージョンが含まれていない SMTP トラフィックを提供しているとします。システム設定の [脆弱性マッピング (Vulnerability Mapping)] ページで SMTP サーバを有効にしてから、そのトラフィックを検出するデバイスを管理する Firepower Management Center にその設定を保存した場合、SMTP サーバと関連付けられているすべての脆弱性がそのホストのホストプロファイルに追加されます。

ディテクタがサーバ情報を収集して、それをホストプロファイルに追加しますが、アプリケーション プロトコル ディテクタは脆弱性のマッピングに使用されません。これは、カスタム アプリケーション プロトコル ディテクタにベンダーまたはバージョンを指定できず、また脆弱性マッピング用のサーバを選択できないためです。

## サーバの脆弱性のマッピング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Protection	Management Center	グローバルのみ	Admin

### 手順

**ステップ 1** [システム (System)] > [設定 (Configuration)] を選択します。

**ステップ 2** [脆弱性マッピング (Vulnerability Mapping)] を選択します。

**ステップ 3** 次の選択肢があります。

- ベンダーまたはバージョンの情報が含まれていないアプリケーション プロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされないようにするには、そのサーバのチェックボックスをオフにします。
- ベンダーまたはバージョンの情報が含まれていないアプリケーション プロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされるようにするには、そのサーバのチェックボックスをオフにします。

**ヒント** [有効 (Enabled)] の横にあるチェックボックスを使用すると、すべてのチェックボックスを一度にオンまたはオフにできます。

ステップ4 [保存 (Save) ]をクリックします。

## リモート コンソールのアクセス管理

サポート対象システム上でリモートアクセスを行うため、VGA ポート (デフォルト) または物理アプライアンス上のシリアルポートを介してLinux システムのコンソールを使用できます。組織のCisco 導入の物理レイアウトに最も適したオプションを選択してください。

サポートされている物理ハードウェアベースのFirepower システムでは、Serial Over LAN (SOL) 接続のデフォルト管理インターフェイス (eth0) でLights-Out 管理 (LOM) を使用すると、システムの管理インターフェイスにログインすることなく、リモートでシステムをモニタまたは管理できます。アウトオブバンド管理接続のコマンドラインインターフェイスを使用すると、シャーシのシリアル番号の表示や状態 (ファン速度や温度など) のモニタなどの、限定タスクを実行できます。

LOM は、システムとシステムを管理するユーザの両方で有効にする必要があります。システムとユーザを有効にした後、サードパーティ製の Intelligent Platform Management Interface (IPMI) ユーティリティを使用し、システムにアクセスして管理します。

## システム上のリモート コンソール設定の構成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center および 7000 & 8000 シリーズ	グローバルだけ	LOM アクセス権限のある Admin

### 始める前に

- デバイスの管理インターフェイスに接続されたサードパーティスイッチング装置で、スパニング ツリー プロトコル (STP) を無効にします。

### 手順

ステップ1 [システム (System) ] > [設定 (Configuration) ] を選択します。

ステップ2 [コンソール構成 (Console Configuration) ] をクリックします。

ステップ3 リモート コンソール アクセスのオプションを選択します。

- アプライアンスのVGA ポートを使用するには、[VGA] を選択します。

- アプライアンスのシリアル ポートを使用するか、Firepower Management Center、Firepower 7050、または 8000 シリーズ デバイス上で LOM/SOL を使用する場合には、[物理シリアルポート (Physical Serial Port)] を選択します。
- 7000 シリーズ デバイス (Firepower 7050 以外) で LOM/SOL を使用する場合は、[Lights-Out Management] を選択します。これらのデバイスでは、SOL と通常のシリアル接続を同時に使用することはできません。

(注) リモート コンソールを [物理シリアルポート (Physical Serial Port)] から [Lights-Out Management] に変更した場合や、70xx ファミリのデバイス (Firepower 7050 以外) で [Lights-Out Management] から [物理シリアルポート (Physical Serial Port)] に変更した場合は、アプライアンスを 2 回リブートしないと、期待どおりのブートプロンプトが表示されないことがあります。

**ステップ 4** SOL 経由で LOM を設定するには、必要な IPv4 設定を入力します。

- システムのアドレス構成 ([DHCP] または [Manual (手動)]) を選択します。
- LOM に使用する IP アドレスを入力します。

(注) LOM IP アドレスは、システムの管理インターフェイスの IP アドレスとは異なる必要があります。

- システムのネットマスクを入力します。
- システムのデフォルト ゲートウェイを入力します。

**ステップ 5** [保存 (Save)] をクリックします。

#### 次のタスク

- Lights-Out Management を設定した場合は、Lights-Out Management ユーザを有効にします。[Lights-Out 管理のユーザ アクセス設定 \(990 ページ\)](#) を参照してください。

## Lights-Out 管理のユーザ アクセス設定

Lights-Out 管理機能を使用するユーザに対して、この機能の権限を明示的に付与する必要があります。LOM ユーザには、次のような制約もあります。

- ユーザに Administrator ロールを割り当てる必要があります。
- ユーザ名に使用できるのは最大 16 個の英数字です。LOM ユーザに対し、ハイフンやそれより長いユーザ名はサポートされていません。
- 71xx ファミリ デバイスへの設定を除き、パスワードには最大 20 文字の英数字を使用できます。Firepower 7110、7115、7120、または 7125 デバイスで LOM が有効になっている場合、パスワードには最大 16 文字の英数字を使用できます。20 または 16 文字よりも長いパスワードは、LOM ユーザに対してサポートされません。ユーザの LOM パスワードは、そ

のユーザのシステムパスワードと同じです。辞書に載っていない複雑な最大長のパスワードをアプライアンスに対して使用し、それを3か月ごとに変更することを推奨します。

- 物理 Firepower Management Center および 8000 シリーズ デバイスには、最大 13 人の LOM ユーザを設定できます。8000 シリーズ デバイスには、最大 8 人の LOM ユーザを設定できます。

あるロールを持つユーザのログイン中に LOM でそのロールを非アクティブ化してから再アクティブ化した場合や、ユーザのログインセッション中にそのユーザまたはユーザロールをバックアップから復元した場合、そのユーザは IPMItool コマンドへのアクセスを回復するために Web インターフェイスにログインし直す必要があります。

## Lights-Out 管理ユーザ アクセスの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center および 7000 & 8000 シリーズ	グローバルだけ	LOM アクセス権限のある Admin

各システムのローカル Web インターフェイスを使用して、システムごとに LOM と LOM ユーザを設定します。つまり、Firepower Management Center を使用して管理対象デバイスで LOM を設定することはできません。同様に、ユーザはアプライアンスごとに個別に管理されるため、Firepower Management Center で LOM 対応ユーザを有効化または作成しても、管理対象デバイスのユーザにはその機能は転送されません。

### 手順

**ステップ 1** [システム (System) ] > [設定 (Configuration) ] を選択します。

**ステップ 2** [コンソール構成 (Console Configuration) ] をクリックします。

**ステップ 3** [Lights Out 管理 (Lights Out Management) ] をクリックします。

**ステップ 4** 次の選択肢があります。

- 既存のユーザに LOM ユーザアクセスを許可するには、リスト内のユーザ名の横にある編集アイコン (✎) をクリックします。
- 新しいユーザに LOM ユーザアクセスを許可するには、[ユーザの作成 (Create User) ] をクリックします。

**ステップ 5** [ユーザの設定 (User Configuration) ] で、Administrator ロールを有効にします。

**ステップ 6** [Lights-Out 管理アクセスの許可 (Allow Lights-Out Management Access) ] チェックボックスをオンにします。

**ステップ 7** [保存 (Save) ] をクリックします。

## Serial over LAN 接続の設定

アプライアンスへの Serial over LAN 接続を作成するには、コンピュータ上でサードパーティ製の IPMI ユーティリティを使用します。Linux 系環境または Mac 環境を使用するコンピュータでは IPMITool を使用し、Windows 環境では IPMIutil を使用します。



(注) シスコでは、IPMITool バージョン 1.8.12 以降の使用を推奨しています。

### Linux

多くのディストリビューションで IPMITool が標準となっており、使用可能です。

### Mac

Mac では、IPMITool をインストールする必要があります。最初に、Mac に Apple の XCode Apple Developer Tools がインストールされていることを確認します。これにより、コマンドライン開発用のオプションコンポーネント（新しいバージョンでは UNIX Development and System Tools、古いバージョンでは Command Line Support）がインストールされていることを確認できます。次に、MacPorts と IPMITool をインストールします。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

<https://developer.apple.com/technologies/tools/>  
<http://www.macports.org/>

### Windows

Windows では、IPMIutil をコンパイルする必要があります。コンパイラにアクセスできない場合は、IPMIutil 自体を使用してコンパイルできます。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

<http://ipmiutil.sourceforge.net/>

### IPMI ユーティリティのコマンドについて

IPMI ユーティリティで使用するコマンドは、次の IPMITool の例に示したセグメントで構成されます。

```
ipmitool -I lanplus -H IP_address -U user_name command
```

引数の説明

- ipmitool はユーティリティを起動します
- -I lanplus はセッションの暗号化を有効にします
- -H IP\_address はアクセスするアプライアンスの IP アドレスを示します
- -U user\_name は権限を持つユーザの名前です

- - command は指定するコマンドの名前です



(注) シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Windows 用の同等のコマンドは次のとおりです。

```
ipmiutil command -V 4 -J 3 -N IP_address -User_name
```

このコマンドは、アプライアンスのコマンドラインにユーザを接続します。これによって、ユーザは物理的にそのアプライアンスの近くにいるときと同じようにログインできます。場合によっては、パスワードの入力を求められます。

## IPMItool を使用した Serial Over LAN の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Centerおよび7000 & 8000 シリーズ	任意 (Any)	LOM アクセス権限のある Admin

### 手順

IPMItool を使用して、次のコマンドと、プロンプトが表示されたらパスワードを入力します:

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

## IPMIutil を使用した Serial Over LAN の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Centerおよび7000 & 8000 シリーズ	任意 (Any)	LOM アクセス権限のある Admin

### 手順

IPMIutil を使用して、次のコマンドと、プロンプトが表示されたらパスワードを入力します。

```
ipmiutil -J 3 -H IP_address -U username sol -a
```

## Lights-Out 管理の概要

Lights-Out 管理 (LOM) では、システムにログインすることなく、デフォルトの管理インターフェイス (eth0) から SOL 接続を介して一連の限定操作を実行できます。SOL 接続を作成するコマンドに続いて、次のいずれかの LOM コマンドを使用します。コマンドが完了すると、接続は終了します。電源制御コマンドの中には、70xx Family デバイスに対して有効でないものもあります。



- (注) Firepower 71xx、Firepower 82xx、または Firepower 83xx デバイスのベースボード管理コントローラ (BMC) は、ホストの電源がオンのときのみ 1 Gbps のリンク速度でアクセスできます。デバイスの電源がオフの場合、BMC は 10/100 Mbps でのみイーサネットリンクを確立できます。したがって、デバイスにリモートから電源供給するために LOM を使用している場合は、10/100 Mbps のリンク速度だけを使用してデバイスをネットワークに接続してください。



- 注意** まれに、コンピュータがシステムの管理インターフェイスとは異なるサブネットにあり、そのシステムに DHCP が構成されている場合は、LOM 機能にアクセスしようとすると失敗することがあります。この場合は、システムの LOM を無効にして再び有効にするか、または同じサブネット上のコンピュータをシステムとして使用して、その管理インターフェイスを ping することができます。その後、LOM を使用できるようになるはずですが。



- 注意** シスコでは、Intelligent Platform Management Interface (IPMI) 標準 (CVE-2013-4786) に内在する脆弱性を認識しています。システムの Lights-Out 管理 (LOM) を有効にすると、この脆弱性にさらされます。この脆弱性を軽減するために、信頼済みユーザだけがアクセス可能なセキュアな管理ネットワークにシステムを展開し、辞書に載っていない複雑な最大長のパスワードをシステムに対して使用し、それを 3 か月ごとに変更してください。この脆弱性のリスクを回避するには、LOM を有効にしないでください。

システムへのアクセス試行がすべて失敗した場合は、LOM を使用してリモートでシステムを再起動できます。SOL 接続がアクティブなときにシステムが再起動すると、LOM セッションが切断されるか、またはタイムアウトする可能性があります。



- 注意** システムが別の再起動の試行に応答している間は、システムを再起動しないでください。リモートでシステムを再起動すると、通常の方法でシステムがリブートしないため、データが失われる可能性があります。



表 71: Lights-Out 管理のコマンド

IPMItool	IPMIutil	説明
(適用なし)	-V 4	IPMI セッションの管理者権限を有効にします。
-I lanplus	-J 3	IPMI セッションの暗号化を有効にします。
-H	-N	リモートアプライアンスの IP アドレスを指定します。
-U	-U	認可された LOM アカウントのユーザ名を指定します。
sol activate	sol -a	SOL セッションを開始します。
sol deactivate	sol -d	SOL セッションを終了します。
chassis power cycle	power -c	アプライアンスを再起動します (70xx Family デバイスでは無効)。
chassis power on	power -u	アプライアンスの電源を投入します。
chassis power off	power -d	アプライアンスの電源をオフにします (70xx Family デバイスでは無効)。
sdr	センサー	アプライアンスの情報 (ファン速度や温度など) を表示します。

たとえば、アプライアンスの情報のリストを表示する IPMItool のコマンドは、次のとおりです。

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```



(注) シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

IPMIutil ユーティリティの同等のコマンドは次のとおりです。

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

## IPMItool による Lights-Out Management の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Centerおよび7000 & 8000 シリーズ	任意 (Any)	LOM アクセス権限のある Admin

### 手順

プロンプトが表示されたら、IPMItool の次のコマンドとパスワードを入力します。

```
ipmitool -I lanplus -H IP_address -U user_name command
```

## IPMIutil による Lights-Out Management の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Centerおよび7000 & 8000 シリーズ	任意 (Any)	LOM アクセス権限のある Admin

### 手順

プロンプトが表示されたら、IPMIutil の次のコマンドとパスワードを入力します。

```
ipmiutil -J 3 -H IP_address -U username command
```

## REST API 設定

Firepower の REST API は、サードパーティ アプリケーションで REST クライアントおよび標準 HTTP メソッドを使用してアプライアンス設定を表示および管理するための軽量なインターフェイスを提供します。Firepower の REST API の詳細については、『*Firepower REST API Quick Start Guide*』を参照してください。

デフォルトでは、Firepower Management Center はアプリケーションからの REST API を使用した要求を許可します。このアクセスをブロックするように Firepower Management Center を設定できます。

## REST API アクセスの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center	任意 (Any)	Admin



(注) Firepower Management Center ハイ アベイラビリティを使用する展開では、この機能は、アクティブな Firepower Management Center でだけ使用できます。

### 手順

- ステップ 1 [システム (System) ] > [設定 (Configuration) ] を選択します。
- ステップ 2 [REST API 設定 (REST API Preferences) ] をクリックします。
- ステップ 3 Firepower Management Center への REST API アクセスを有効または無効にするには、[REST API の有効化 (Enable REST API) ] チェックボックスをオンまたはオフにします。
- ステップ 4 [保存 (Save) ] をクリックします。

## VMware Tools と仮想システム

VMware Tools は、仮想マシン向けのパフォーマンスを向上させるためのユーティリティスイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をフルに活用できます。VMware で実行されている Firepower 仮想アプライアンスは、次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup

サポートされるすべてのバージョンの ESXi で VMware Tools を有効にすることもできます。サポートされているバージョンの一覧については、『Cisco Firepower NGIPSv for VMware クイックスタートガイド』を参照してください。VMware Tools のすべての機能については、VMware の Web サイト (<http://www.vmware.com/>) を参照してください。

## VMware 向け Firepower Management Center での VMware ツールの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Firepower Management Center	グローバルだけ	Admin

NGIPSv には Web インターフェイスがないため、そのプラットフォームで VMware ツールを有効にするには CLI を使用する必要があります (Cisco Firepower NGIPSv for VMware クイック スタート ガイドを参照)。

### 手順

- 
- ステップ 1 [システム (System) ] > [設定 (Configuration) ] を選択します。
  - ステップ 2 [VMware ツール (VMware Tools) ] をクリックします。
  - ステップ 3 [VMware ツールの有効化 (Enable VMware Tools) ] をクリックします。
  - ステップ 4 [保存 (Save) ] をクリックします。
-



## 第 42 章

# 管理対象デバイス用のプラットフォーム設定ポリシー

以下のトピックでは、プラットフォーム設定ポリシーについて、および管理対象デバイスにそれらを導入する方法について説明します。

- [プラットフォーム設定の概要 \(999 ページ\)](#)
- [プラットフォーム設定ポリシーの管理 \(1000 ページ\)](#)
- [プラットフォーム設定ポリシーの作成 \(1001 ページ\)](#)
- [プラットフォーム設定ポリシーのターゲットデバイスの設定 \(1002 ページ\)](#)

## プラットフォーム設定の概要

プラットフォーム設定ポリシーは、時刻の設定や外部認証など、展開内の他の管理対象デバイスと同様になる可能性の高い、管理対象デバイスの側面を定義する共有の機能またはパラメータのセットです。

共有ポリシーによって同時に複数の管理対象デバイスを設定することができ、これによって展開に一貫性をもたらし、管理の手間を合理化することができます。プラットフォーム設定ポリシーへの変更は、ポリシーを適用したすべての管理対象デバイスに影響します。デバイスごとに異なる設定を使用する場合でも、共有ポリシーを作成して目的のデバイスに適用する必要があります。

たとえば、組織のセキュリティポリシーではユーザのログイン時にアプライアンスに「無断使用禁止」のメッセージを表示する必要があるとします。プラットフォーム設定を使えば、プラットフォーム設定ポリシー内で一度ログインバナーを設定するだけで完了します。

また、Firepower Management Center で複数のプラットフォーム設定ポリシーを活用することもできます。たとえば、さまざまな状況で別々のメールリレーホストを使用する場合や、さまざまなアクセスリストをテストする場合は、単一のポリシーを編集するのではなく、いくつかのプラットフォーム設定ポリシーを作成し、それらを切り替えることができます。

### 関連トピック

- [Firepower プラットフォームの設定 \(1004 ページ\)](#)
- [システム設定 \(917 ページ\)](#)

## プラットフォーム設定ポリシーの管理




スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

[プラットフォームの設定 (Platform Settings)] ページ ([デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)]) を使用して、プラットフォーム設定ポリシーを管理します。このページには、各ポリシーのデバイスのタイプが示されます。[ステータス (Status)] 列で、ポリシーのデバイス ターゲットが示されます。

### 手順

**ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択します。

**ステップ 2** プラットフォーム設定ポリシーを管理します。

- **作成**：新しいプラットフォーム設定ポリシーを作成するには、[新規ポリシー (New Policy)] をクリックします。[プラットフォーム設定ポリシーの作成 \(1001 ページ\)](#) を参照してください。
- **コピー**：プラットフォーム設定ポリシーをコピーするには、コピー アイコン () をクリックします。
- **編集**：既存のプラットフォーム設定ポリシーの設定を変更するには、編集 アイコン () をクリックします。
- **削除**：使用されていないポリシーを削除するには、削除 アイコン () をクリックして、選択内容を確認します。

**注意** どのターゲットデバイスでも、最後に展開したポリシーは期限切れであっても削除しないでください。ポリシーを完全に削除する前に、それらのターゲットに別のポリシーを展開するようにしてください。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## プラットフォーム設定ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

新しいプラットフォーム設定ポリシーを作成する場合は、少なくとも、クラシック管理対象デバイスまたは Firepower Threat Defense のどちらかのデバイス タイプを選択する必要があります。



(注) Firepower Threat Defense デバイスのプラットフォーム設定は、クラシック管理対象デバイスのプラットフォーム設定とは異なります。

### 手順

**ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択します。

**ステップ 2** [新しいポリシー (New Policy) ] をクリックします。

**ステップ 3** ドロップダウン リストから、デバイス タイプを選択します。

- クラシック管理対象デバイス用の共有ポリシーを作成する場合は、[Firepower 設定 (Firepower Settings) ] を選択します。
- Firepower Threat Defense 管理対象デバイス用の共有ポリシーを作成する場合は、[脅威に対する防御設定 (Threat Defense Settings) ] を選択します。

**ステップ 4** 新しいポリシーの [名前 (Name) ]、および必要に応じて [説明 (Description) ] を入力します。

**ステップ 5** 必要に応じて、ポリシーを適用する [使用可能なデバイス (Available Devices) ] を選択し、[ポリシーに追加 (Add to Policy) ] をクリック (またはドラッグ アンド ドロップ) して、選択したデバイスを追加します。[検索 (Search) ] フィールドに検索文字列を入力して、デバイスのリストを絞り込むことができます。

**ステップ 6** [保存 (Save) ] をクリックします。

システムにより、ポリシーが作成され、編集のために開かれます。

**ステップ 7** デバイス プラットフォーム タイプに基づいて、プラットフォーム設定を行います。

- Firepower 設定については、[Firepower プラットフォーム設定の概要 \(1003 ページ\)](#) を参照してください。
- 脅威に対する防御設定については、[Firepower Threat Defense のプラットフォーム設定 \(1033 ページ\)](#) を参照してください。

ステップ 8 [保存 (Save) ] をクリックします。

次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## プラットフォーム設定ポリシーのターゲットデバイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

新しいポリシーを作成すると同時にターゲットデバイスを追加したり、後で変更したりできます。

手順

ステップ 1 [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択します。

ステップ 2 編集するプラットフォーム設定ポリシーの横にある編集アイコン (✎) をクリックします。

ステップ 3 [ポリシーの割り当て (Policy Assignment) ] をクリックします。

ステップ 4 次のいずれかを実行します。

- デバイス、スタック、高可用性ペア、またはデバイスグループをポリシーに割り当てるには、[使用可能なデバイス (Available Devices) ] リストで選択し、[ポリシーに追加 (Add to Policy) ] をクリックします。ドラッグアンドドロップを使用することもできます。
- デバイスの割り当てを削除するには、[選択されたデバイス (Selected Device) ] リストのデバイス、スタック、高可用性ペア、またはデバイスグループの横にある削除アイコン (🗑) をクリックします。

ステップ 5 [OK] をクリック

次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。





## 第 43 章

# 従来型デバイス用の Firepower プラットフォーム設定

次のトピックでは、Firepower プラットフォーム設定について、および従来型デバイスでそれを設定する方法について説明します。

- [Firepower プラットフォーム設定の概要 \(1003 ページ\)](#)
- [Firepower プラットフォームの設定 \(1004 ページ\)](#)
- [アクセスリスト \(1005 ページ\)](#)
- [監査ログ \(1006 ページ\)](#)
- [カスタム監査ログクライアント証明書 \(1010 ページ\)](#)
- [外部認証の設定 \(1016 ページ\)](#)
- [言語の選択 \(1018 ページ\)](#)
- [ログインバナー \(1019 ページ\)](#)
- [セッションタイムアウト \(1021 ページ\)](#)
- [SNMP ポーリング \(1022 ページ\)](#)
- [セキュリティ認定準拠の \(1025 ページ\)](#)
- [時刻および時刻同期 \(1029 ページ\)](#)

## Firepower プラットフォーム設定の概要

Firepower クラシック管理対象デバイス向けのプラットフォーム設定は無関係な機能の範囲を指定しますが、その値は複数のデバイス間で共有できます。この場合は、7000 および 8000 シリーズ、ASA FirePOWER モジュールや NGIPSv デバイスです。デバイスごとに異なる設定を使用する場合でも、共有ポリシーを作成して目的のデバイスに適用する必要があります。

### 関連トピック

- [管理対象デバイス用のプラットフォーム設定ポリシー \(999 ページ\)](#)
- [システム設定 \(917 ページ\)](#)

# Firepower プラットフォームの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	従来型 (Classic)	任意 (Any)	Admin

プラットフォームを設定するには、既存のプラットフォーム設定ポリシーを編集するか、新しいポリシーを作成します。デバイスに現在展開されているプラットフォーム設定ポリシーを編集する場合、変更を保存した後にポリシーを再展開してください。

## 手順

**ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択します。

既存のシステムポリシーのリストを含む、[プラットフォーム設定 (Platform Settings)] ページが表示されます。

**ステップ 2** 新しいポリシーを作成するか、既存のポリシーを編集します。

- 新しいポリシーを作成するには、[プラットフォーム設定ポリシーの作成 \(1001 ページ\)](#) を参照してください。
- 既存のポリシーを編集するには、そのポリシーの横にある編集アイコン (✎) をクリックします。

[ポリシーの編集 (Edit Policy)] ページが表示されます。ポリシー名とポリシーの説明を変更できます。プラットフォーム設定ポリシーのそれぞれの側面の設定については、次の項のいずれかを参照してください。

- [システムのアクセス リストの設定 \(958 ページ\)](#)
- [syslog への監査ログ メッセージの送信 \(960 ページ\)](#)
- [HTTP サーバへの監査ログ メッセージの送信 \(961 ページ\)](#)
- [外部認証の有効化 \(1017 ページ\)](#)
- [別の言語の指定 \(972 ページ\)](#)
- [カスタム ログイン バナーの追加 \(973 ページ\)](#)
- [セッション タイムアウトの設定 \(986 ページ\)](#)
- [SNMP ポーリングの設定 \(975 ページ\)](#)
- [syslog への監査ログ メッセージの送信 \(960 ページ\)](#)
- [Firepower Management Center からの時間の提供 \(984 ページ\)](#)

**ステップ 3** (オプション) [ポリシー割り当て (Policy Assignment)] をクリックして、ポリシーを展開する利用可能なデバイスを選択します。[ポリシーに追加 (Add to Policy)] をクリックして (またはドラッグ アンド ドロップして)、選択したデバイスを追加します。

[検索 (Search)] フィールドに検索文字列を入力して、デバイスのリストを絞り込むことができます。

**ステップ 4** [保存 (Save)] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## アクセス リスト

Firepower Management Center およびクラシック管理対象デバイスでは、アクセス リストを使用して、IP アドレスとポートを基準にシステムへのアクセスを制限できます。デフォルトでは、任意の IP アドレスに対して以下のポートが有効化されています。

- 443 (HTTPS) : Web インターフェイス アクセスに使用されます。
- 22 (SSH) : コマンドライン アクセスに使用されます。

さらに、ポート 161 で SNMP 情報をポーリングするためのアクセスも追加できます。



**注意** デフォルトでは、アクセスは制限されていません。よりセキュアな環境で運用するために、特定の IP アドレスに対するアクセスを追加してから、デフォルトの **any** オプションを削除することを検討してください。

## システムのアクセス リストの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス (7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv) に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

このアクセス リストは、外部データベース アクセスを制御しないので注意してください。

### 手順

**ステップ 1** Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
- 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower ポリシーを作成または編集します。

**ステップ 2** [アクセス リスト (Access List)] をクリックします。

**ステップ 3** 現在の設定の 1 つを削除するために、削除アイコン (🗑️) をクリックすることもできます。

**注意** アプライアンスのインターフェイスへの接続に現在使用されている IP アドレスへのアクセスを削除し、IP=any port=443 のエントリが存在しない場合、ポリシーを展開した時点でシステムへのアクセスは失われます。

**ステップ 4** 1 つ以上の IP アドレスへのアクセスを追加するには、[ルールの追加 (Add Rules)] をクリックします。

**ステップ 5** [IP アドレス (IP Address)] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、any を入力します。

**ステップ 6** [SSH]、[HTTPS]、[SNMP]、またはこれらのオプションの組み合わせを選択して、これらの IP アドレスで有効にするポートを指定します。

**ステップ 7** [追加 (Add)] をクリックします。

**ステップ 8** [保存 (Save)] をクリックします。

### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## 監査ログ

Firepower Management Center および従来型管理対象デバイスは、ユーザアクティビティに関する読み取り専用の監査情報をログに記録します。Management Center および 7000 および 8000 シリーズの Web インターフェイスでは、監査ログ イベントは標準イベントビューに表示されます。標準イベントビューでは、監査ビューの任意の項目に基づいて監査ログ メッセージの表示、並べ替え、フィルタ処理ができます。監査情報を簡単に削除したり、それに関するレ

ポートを作成したりすることができ、ユーザが行った変更に関する詳細なレポートを表示することもできます。

監査ログメッセージを syslog に送信するよう、Firepower Management Center および従来型管理対象デバイスを設定することもできます。設定するには、syslog サーバ、およびメッセージに関連付ける重大度、ファシリティ、オプションタグを指定します。タグは、syslog の監査ログメッセージと一緒に表示されます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。syslog メッセージにはファシリティおよび重大度は含まれません。これらの値は syslog メッセージを受信するシステムにメッセージの分類方法を示す値です。

また、監査ログメッセージを HTTP サーバにストリーミングするよう、Firepower Management Center および従来型管理対象デバイスで設定することもできます。

監査ログストリーミング設定は、アプライアンスのタイプによって異なる設定の一部となっています。

- Firepower Management Center では、監査ログのストリーミングはシステム設定の一部です。
- クラシック管理対象デバイスでは、監査ログストリーミングは Firepower Management Center プラットフォーム設定ポリシーの一部です。

いずれの場合も、システム設定の変更を保存するか、共有プラットフォーム設定ポリシーを展開するまでは設定は有効になりません。

TLS 証明書を使用して TLS と相互認証を有効にすることで、監査ログストリーミング用のチャネルの安全性を確保できます。詳細については [カスタム監査ログ クライアント証明書 \(963 ページ\)](#) を参照してください。



**注意** 外部 URL に監査情報を送信すると、システムパフォーマンスに影響を与える場合があります。

## 監査ログメッセージを Syslog に送信する

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この機能を有効にすると、監査ログレコードは、syslog に次の形式で表示されます。

*Date Time Host [Tag] Sender: User\_Name@User\_IP, Subsystem, Action*

現地の日付、時刻、および発信元ホスト名の後に、角括弧で囲まれたオプションタグが続き、送信側デバイス名の後に監査ログメッセージが続きます。

たとえば、FROMMC のタグを指定した場合は、監査ログメッセージ例は次のように表示されます。

```
Mar 01 14:45:24 localhost [FROMMC] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring,
Page View
```

TLS 証明書を使用して TLS および相互認証を有効にすることによって、監査ログ ストリーミングのチャンネルを保護できます。詳細については、[カスタム監査ログ クライアント証明書 \(963 ページ\)](#) を参照してください。

### 始める前に

- syslog サーバが機能しており、監査ログを送信するシステムからアクセスできることを確認します。

### 手順

**ステップ 1** Firepower Management Center または Classic 管理対象デバイスのいずれを設定しているかに応じて、以下を実行します。

- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
- 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択して、Firepower ポリシーを作成または編集します。

**ステップ 2** [監査ログ (Audit Log)] をクリックします。

**ステップ 3** [監査ログを Syslog に送信 (Send Audit Log to Syslog)] ドロップダウンメニューから、[有効 (Enabled)] を選択します。

**ステップ 4** [ホスト (Host)] フィールドにある syslog サーバの IP アドレスまたは完全修飾名を使用して、監査情報の宛先ホストを指定します。デフォルト ポート (6514) が使用されます。

**注意** 監査ログを受け入れるように設定しているコンピュータが、リモートメッセージを受け入れるようにセットアップされていない場合、ホストは監査ログを受け入れません。

(注) このフィールドに無効な IPv4 アドレス (192.168.1.456 など) を入力した場合でも、システムは警告を表示しません。代わりに、システムは無効なアドレスをホスト名として扱います。

**ステップ 5** [Syslog アラート ファシリティ \(2345 ページ\)](#) で説明されているとおりに、[ファシリティ (Facility)] リストからファシリティを選択します。

**ステップ 6** [syslog 重大度レベル \(2346 ページ\)](#) で説明されているとおりに、[重大度 (Severity)] リストから重大度を選択します。

**ステップ 7** オプションで、[タグ (Tag)] フィールドに、syslog メッセージとともに表示するタグ名を入力します。たとえば、syslog に送信されるすべての監査ログ レコードの先頭に「FROMMC」を付加したい場合に、このフィールドに「FROMMC」と入力します。

ステップ 8 [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

## 監査ログメッセージを HTTP サーバに送信する

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この機能を有効にすると、アプライアンスは、HTTP サーバに次の形式で監査ログレコードを送信します。

```
Date Time Host [Tag] Sender: User_Name@User_IP, Subsystem, Action
```

現地の日付、時刻、および発信元ホスト名の後に、角括弧で囲まれたオプションタグが続き、送信側デバイス名の後に監査ログメッセージが続きます。

たとえば、FROMMC のタグを指定した場合は、監査ログメッセージ例は次のように表示されます。

```
Mar 01 14:45:24 localhost [FROMMC] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring, Page View
```

このストリームのチャンネルは、SSL 証明書を使用して TLS と相互認証を有効にすることで保護できます。詳細については、[カスタム監査ログクライアント証明書 \(963 ページ\)](#) を参照してください。

#### 始める前に

- 外部ホストが機能していることと、監査ログを送信するシステムからアクセスできることを確認します。

#### 手順

ステップ 1 Firepower Management Center または従来型の管理対象デバイスのどちらを設定しているかに応じて、次の操作を実行します。

- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
- 管理対象デバイス : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択して、Firepower ポリシーを作成または編集します。

**ステップ 2** [監査ログ (Audit Log)] をクリックします。

**ステップ 3** 必要に応じて、[タグ (Tag)] フィールドに、メッセージとともに表示するタグ名を入力します。たとえば、すべての監査ログレコードの前に FROMMC を付けるには、このフィールドに FROMMC を入力します。

**ステップ 4** [HTTP サーバへの監査ログの送信 (Send Audit Log to HTTP Server)] ドロップダウンリストから、[有効 (Enabled)] を選択します。

**ステップ 5** [監査情報を送信する URL (URL to Post Audit)] フィールドに、監査情報の送信先 URL を指定します。次にリストした HTTP POST 変数を要求するリスナー プログラムに対応する URL を入力します。

- subsystem
- actor
- event\_type
- message
- action\_source\_ip
- action\_destination\_ip
- 結果
- 時刻
- tag (定義されている場合。手順 3 を参照)

**注意** 暗号化されたポストを許可するには、HTTPS URL を使用します。外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があります。

**ステップ 6** [保存 (Save)] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## カスタム監査ログクライアント証明書

HTTP サーバまたは syslog サーバに監査ログをストリーミングする場合、Transport Layer Security (TLS) 証明書を使ってアプライアンスとサーバ間のチャンネルを保護することができます。これにより、信頼されたサーバにシステム監査ログを安全にストリーミングすると同時に、ローカルアプライアンスの使用領域を節約することができます。

監査ログをアプライアンスから外部サーバに安全にストリーミングするには、2 つの要件があります。



- アプライアンスの署名付きクライアント証明書をインポートします。システム情報と指定した ID 情報に基づいて、証明書要求を生成できます。生成された要求を認証局に送信して、クライアント証明書を要求します。認証局 (CA) から署名付き証明書を取得すると、その証明書をインポートできます。
- Transport Layer Security (TLS) を使用するサーバとの通信チャネルを設定します。

サーバに署名付き証明書の提供を要求します。その証明書を確認するため、1 つ以上の証明書失効リスト (CRL) をロードするようにアプライアンスを設定します。アプライアンスは、サーバ証明書を CRL に記載されている証明書に照らして比較します。サーバが提供した証明書が失効した証明書として CRL に記載されている場合、そのサーバには監査ログをストリーミングできません。



(注) CRL を使用した証明書の確認を選択すると、システムはクライアント ブラウザ証明書、監査ログ サーバ証明書の両方の検証に同じ CRL を使用します。

次の要件のいずれか1つを満たしていないクライアント証明書をインポートすると、監査ログのストリーミングは失敗となります。

- 証明書の署名が、サーバ証明書の署名と同じ CA による署名でない。
- 証明書が、証明書チェーンの中間証明書に署名したのと同じ CA によって署名されていない。

## 現在の監査ログクライアント証明書の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center7000 & 8000 シリーズ NGIPsv	グローバルのみ	Admin

ログインしているアプライアンスの監査ログクライアント証明書のみ表示できます。



(注) ASA FirePOWER デバイスの監査ログクライアント証明書を表示するには、**show audit\_cert** CLI コマンドを使用します。

### 手順

- ステップ 1** Firepower Management Center または従来型の管理対象デバイスのどちらに向けた監査ログのストリーミングを構成しているかに応じて、次のように操作します。

- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
- 管理対象デバイス : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択して、Firepower ポリシーを作成または編集します。

ステップ 2 [監査ログ証明書 (Audit Log Certificate) ] をクリックします。

## 監査ログクライアント証明書の署名要求の生成

スマート ライセ ンス	従来のライセンス	サポートされるデ バイス	サポートされるド メイン	アクセス (Access)
該当なし	任意 (Any)	Management Center7000 & 8000 シリーズ NGIPsv	グローバルのみ	Admin

この手順を使用して証明書要求を生成すると、単一のシステムにのみ対応する証明書を生成できます。セキュリティを確保するために、広く知られており、信頼できる CA によって署名された証明書を使用してください。

システムは、ベース 64 エンコードの PEM 形式で証明書要求のキーを生成します。



(注) ASA FirePOWER デバイスの場合は、キー ペアと証明書を手動で生成します。

### 手順

- ステップ 1 Firepower Management Center または従来型の管理対象デバイスのどちらに向けた監査ログのストリーミングを構成しているかに応じて、次のように操作します。
- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
  - 管理対象デバイス : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択して、Firepower ポリシーを作成または編集します。
- ステップ 2 [監査ログ証明書 (Audit Log Certificate) ] をクリックします。
- ステップ 3 [新規 CSR の生成 (Generate New CSR) ] をクリックします。
- ステップ 4 [国名 (2 文字のコード) (Country Name (two-letter code)) ] フィールドに国番号を入力します。
- ステップ 5 [都道府県 (State or Province) ] フィールドに、都道府県名を入力します。
- ステップ 6 [市区町村 (Locality or City) ] を入力します。
- ステップ 7 [組織 (Organization) ] の名前を入力します。
- ステップ 8 [組織単位 (部署名) (Organizational Unit (Department)) ] の名前を入力します。
- ステップ 9 [共通名 (Common Name) ] フィールドに、証明書を要求するサーバの完全修飾ドメイン名を入力します。

(注) 共通名と DNS ホスト名が一致しないと、監査ログのストリーミングは失敗します。

- ステップ 10 [生成 (Generate) ] をクリックします。
- ステップ 11 テキスト エディタで、新しい空のファイルを開きます。
- ステップ 12 証明書要求のテキストブロック全体 (BEGIN CERTIFICATE REQUEST 行と END CERTIFICATE REQUEST 行を含む) をコピーして、空のテキスト ファイルに貼り付けます。
- ステップ 13 このファイルを *clientname.csr* として保存します。 *clientname* は、証明書を使用する予定のアプライアンスの名前にします。
- ステップ 14 [閉じる (Close) ] をクリックします。

次のタスク

- 証明機関に証明書要求を送信します。
- 署名された証明書を受信したら、その証明書を要求したアプライアンスにインポートします。 [監査ログクライアント証明書のインポート \(966 ページ\)](#) を参照してください。

## 監査ログクライアント証明書のインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center7000 & 8000 シリーズ NGIPSv	グローバルのみ	Admin

証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、証明書チェーン (証明書パスとも呼ばれる) を提供します。

監査ログのストリーミングは、次に示す条件のいずれかを満たしていないクライアント証明書をインポートすると失敗します。

- 証明書が、サーバ証明書に署名したものと同一 CA によって署名されていない。
- 証明書が、証明書チェーンの中間証明書に署名したものと同一 CA によって署名されていない。



(注) ASA FirePOWER に監査ログクライアント証明書をインポートするには、CLI コマンド **configure audit\_cert import** を使用します。

### 始める前に

- 証明書署名要求を生成します。 [監査ログクライアントの証明書署名要求の生成 \(964ページ\)](#) を参照してください。
- 証明書を要求する認証局に CSR ファイルをアップロードします。

### 手順

- 
- ステップ 1** Firepower Management Center または従来型の管理対象デバイスのどちらに向けた監査ログのストリーミングを構成しているかに応じて、次のように操作します。
- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
  - 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択して、Firepower ポリシーを作成または編集します。
- ステップ 2** [監査ログ証明書 (Audit Log Certificate)] をクリックします。
- ステップ 3** [監査クライアント証明書のインポート (Import Audit Client Certificate)] をクリックします。
- ステップ 4** テキストエディタでクライアント証明書を開いて、BEGIN CERTIFICATE の行と END CERTIFICATE の行を含むテキストのブロック全体をコピーします。このテキストを [クライアント証明書 (Client Certificate)] フィールドに貼り付けます。
- ステップ 5** 秘密キーをアップロードするには、秘密キー ファイルを開いて、BEGIN RSA PRIVATE KEY の行と END RSA PRIVATE KEY の行を含むテキストのブロック全体をコピーします。このテキストを [秘密キー (Private Key)] フィールドに貼り付けます。
- ステップ 6** 必要な中間証明書をすべて開いて、それぞれのテキストのブロック全体をコピーして、[証明書チェーン (Certificate Chain)] フィールドに貼り付けます。
- ステップ 7** [保存 (Save)] をクリックします。
- 

## 有効な監査ログ サーバ証明書の要求

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center 従来型	グローバルのみ	Admin

システムは、識別符号化規則 (DER) 形式でインポートされている CRL を使用した、監査ログ サーバ証明書の検証をサポートしています。

CRL を使用する場合は、失効した証明書のリストを最新の状態に保つために、CRL を更新するスケジュールタスクを作成してください。システムは、最後に更新した CRL を表示します。



- (注) CRL を選択すると、システムは、同じ CRL を使用して、監査ログ証明書の検証と、アプライアンスと Web ブラウザの間の HTTP 接続を保護する証明書の検証の両方に同じ CRL を使用します。



- 注意 有効なクライアント証明書をインポートせずに、相互認証を有効にすると、監査ログのストリーミングが失敗します。

### 始める前に

- 接続に使用するサーバ証明書に署名したものと同一 CA で署名されたクライアント証明書をインポートします。[監査ログクライアント証明書のインポート \(966 ページ\)](#) を参照してください。
- クライアント証明書チェーンをインポートします (必要な場合)。[監査ログクライアント証明書のインポート \(966 ページ\)](#) を参照してください。

### 手順

- ステップ 1** Firepower Management Center または従来型の管理対象デバイスのどちらに向けた監査ログのストリーミングを構成しているかに応じて、次のように操作します。
- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
  - 管理対象デバイス : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択して、Firepower ポリシーを作成または編集します。
- ステップ 2** [監査ログ証明書 (Audit Log Certificate) ] をクリックします。
- ステップ 3** [TLS の有効化 (Enable TLS) ] を選択して、監査ログを外部サーバにストリーミングする際に Transport Layer Security を使用します。
- ステップ 4** [相互認証の有効化 (Enable Mutual Authentication) ] を選択します。
- ステップ 5** 次の 2 つの対処法があります。
- 1 つ以上の CRL を使用してサーバ証明書を検証する場合は、[CRL のフェッチの有効化 (Enable Fetching of CRL) ] を選択して、手順 6 に進みます。
  - 検証なしでサーバ証明書を承認する場合は、手順 9 に進みます。
- ステップ 6** 既存の CRL ファイルへの有効な URL を入力して、[CRL の追加 (Add CRL) ] をクリックします。最大 25 個まで CRL の追加を繰り返します。
- ステップ 7** [CRL の更新 (Refresh CRL) ] をクリックして現在の CRL をロードするか、指定した URL から CRL をロードします。

(注) CRL のフェッチを有効にすると、定期的に CRL を更新するスケジュール タスクが作成されます。このタスクを編集して、更新の頻度を設定します。

**ステップ 8** クライアント証明書を作成したものと同一認証局によって生成された有効なクライアント証明書があることを確認します。

**ステップ 9** [保存 (Save) ] をクリックします。

## 外部認証の設定

外部認証サーバを参照する認証オブジェクトを作成する場合、外部認証を有効にすることにより、ローカルデータベースを使用せずに、管理対象デバイスにログインしているユーザをそのサーバに認証させることができます。

外部認証を有効にすると、システムでは LDAP または RADIUS サーバのユーザのユーザ クレデンシャルが確認されます。さらに、ユーザがローカルの内部認証を有効にしており、ユーザ クレデンシャルが内部データベースにない場合、システムは一致するクレデンシャルのセットがないか外部サーバを検査します。ユーザが複数のシステムで同じユーザ名を持っている場合、すべてのサーバですべてのパスワードが動作します。ただし、使用可能な外部認証サーバで認証が失敗した場合、システムはローカルデータベースの検査に戻らないので注意してください。

外部認証を有効にすると、アカウントが外部で認証されている任意のユーザのデフォルトのユーザ ロールを設定できます。これらのロールを組み合わせることができる場合は、複数のロールを選択できます。たとえば、自社の [ネットワーク セキュリティ (Network Security) ] グループのユーザのみを取得する外部認証を有効にした場合、デフォルトのユーザ ロールを設定して [セキュリティ アナリスト (Security Analyst) ] ロールを組み込み、ユーザが自分で追加のユーザ設定を行わなくても収集されたイベントデータにアクセスできるようにすることが可能です。ただし、外部認証がセキュリティグループに加えて他のユーザのレコードを取得する場合、デフォルトのロールを未選択のままにしておきたい場合もあります。

アクセスロールが選択されていない場合、ユーザはログインできますが、どの機能にもアクセスできません。ユーザがログインを試行すると、アカウントがユーザ管理ページ ([システム (System) ] > [ユーザ (Users) ]) に表示されます。ここで、追加の権限を付与するアカウント設定を編集できます。



**ヒント** 1つのユーザ ロールを使用するようにシステムを設定してそのポリシーを適用し、後で設定を変更して別のデフォルトのユーザ ロールを使用する場合、アカウントを変更するか、削除して再作成するまで、変更前に作成されたユーザ アカウントはすべて、最初のユーザ ロールを保持します。

シェル アクセスまたは CAC 認証および承認のために LDAP サーバに対して認証できる一連のユーザを指定する場合は、それぞれに個別の認証オブジェクトを作成し、オブジェクトを個別に有効にする必要があります。

内部認証によってユーザがログインしようとする時、システムは最初にそのユーザがローカルユーザデータベースに存在するかどうかを検査します。ユーザが存在する場合、システムは次にユーザ名とパスワードをローカルデータベースに対して検査します。一致が検出されると、ユーザは正常にログインします。ただし、ログインが失敗し、外部認証が有効になっている場合、システムはそれぞれの外部認証サーバに対して、ユーザを設定に表示される認証順序で検査します。ユーザ名およびパスワードが外部サーバからの結果と一致した場合、システムはユーザを、その認証オブジェクトに対してデフォルトの権限を持つ外部ユーザに変更します。

外部ユーザがログインしようとする時、システムは外部認証サーバに対してユーザ名およびパスワードを検査します。一致が検出されると、ユーザは正常にログインします。ログインが失敗した場合、ユーザのログイン試行は拒否されます。外部ユーザは、ローカルデータベース内のユーザリストに対して認証できません。ユーザが新しい外部ユーザの場合、外部認証オブジェクトのデフォルト権限を持つ外部ユーザアカウントがローカルデータベースに作成されます。

関連トピック

[ユーザアカウント](#) (84 ページ)

## 外部認証の有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center、従来型	任意 (Any)	Admin

始める前に

- [外部認証 \(External Authentication\)](#) (96 ページ) の説明に従って外部認証オブジェクトを設定します。

手順

- ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower ポリシーを作成または編集します。
- ステップ 2** [外部認証 (External Authentication) ] をクリックします。
- ステップ 3** [ステータス (Status) ] ドロップダウンリストから [有効 (Enabled) ] を選択します。
- ステップ 4** [デフォルトユーザロール (Default User Role) ] ドロップダウンリストから、ユーザロールを選択して、外部認証済みユーザに付与するデフォルト権限を定義します。
- ステップ 5** 外部サーバを使用して CLI またはシェル アクセス アカウントを認証する場合、[シェル認証 (Shell Authentication) ] ドロップダウンリストから [有効 (Enabled) ] を選択します。
- ステップ 6** CAC 認証および認可を有効にする場合は、[CAC 認証 (CAC Authentication) ] ドロップダウンリストから使用可能な CAC 認証オブジェクトを選択します。CAC 認証および認可の設定の詳細については、[CAC 認証](#) (99 ページ) を参照してください。

**ステップ 7** 事前設定された認証オブジェクトの使用を有効にするには、オブジェクトの横にあるチェックボックスをオンにします。外部認証を有効にするには、少なくとも1つの認証オブジェクトを指定する**必要があります**。

シェル認証を有効にした場合、CLIまたはシェルアクセスを許可するよう設定された認証オブジェクトを選択する**必要があります**。

同じシステム設定でCLIまたはシェルアクセスと、CAC認証を制御するためには異なる認証オブジェクトを使用します。[CAC 認証 \(99 ページ\)](#) および[LDAP シェルアクセスのフィールド \(119 ページ\)](#) を参照してください。

**ステップ 8** 必要に応じて、上矢印および下矢印を使用して、認証要求が行われたときに認証サーバがアクセスされる順序を変更できます。

CLIまたはシェルアクセスのユーザは、認証オブジェクトがプロファイルの順序で最も高いサーバに対して**のみ**認証できることに注意してください。

**ステップ 9** [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 言語の選択

[言語 (Language) ] ページを使用して、Web インターフェイス用に異なる言語を指定できます。

### 別の言語の指定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 7000 & 8000 シリーズ	任意 (Any)	Admin

この設定は、Firepower Management Center または 7000 および 8000 シリーズ 管理対象デバイスに適用されます。

- Firepower Management Center では、この設定はシステム設定の一部になります。
- 7000 および 8000 シリーズ 管理対象デバイスでは、この設定をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。



いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。



**注意** ここで指定した言語は、アプライアンスにログインしたすべてのユーザの Web インターフェイスに使用されます。

### 手順

**ステップ 1** Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
- 管理対象デバイス : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower ポリシーを作成または編集します。

**ステップ 2** [言語 (Language) ] をクリックします。

**ステップ 3** 使用する言語を選択します。

**ステップ 4** [保存 (Save) ] をクリックします。

### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## ログインバナー

[ログインバナー (Login Banner) ] ページを使用して、セキュリティアプライアンスまたは共有ポリシーのセッションバナー、ログインバナー、カスタムメッセージバナーを指定できます。

バナーのテキストにはスペースを使用できますが、タブは使用できません。バナーには複数行のテキストを指定できます。テキストに空の行が含まれている場合、バナーでは、その行が改行 (CR) として表示されます。使用できるのは、改行 (Enter キーを押す) を含む ASCII 文字だけです。改行は 2 文字としてカウントされます。

Telnet または SSH を介してセキュリティアプライアンスにアクセスしたときに、バナーメッセージを処理するのに十分なシステムメモリがなかった場合や、バナーメッセージの表示を試行して TCP 書き込みエラーが発生した場合には、セッションが閉じます。

## カスタム ログインバナーの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

SSH または Web インターフェイスからログインするユーザに向けて表示するカスタム ログインバナーを作成できます。

この設定は、Firepower Management Center または従来型の管理対象デバイス (7000 および 8000 シリーズ、ASA FirePOWER および NGIPSv) に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

### 手順

**ステップ 1** Firepower Management Center または Classic 管理対象デバイスのいずれを設定しているかに応じて、以下を実行します。

- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
- 管理対象デバイスの場合 : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択するか、ファイアウォールポリシーを作成、または編集します。

**ステップ 2** [ログインバナー (Login Banner)] を選択します。

**ステップ 3** [カスタム ログインバナー (Custom Login Banner)] フィールドに、使用するログインバナーテキストを入力します。

**ステップ 4** [保存 (Save)] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

# セッションタイムアウト

Firepower システムの Web インターフェイスまたは補助コマンドライン インターフェイスの無人ログインセッションは、セキュリティ上のリスクを生じさせる場合があります。ユーザのログインセッションが非アクティブになったためにタイムアウトするまでのアイドル時間を分単位で設定できます。シェル（コマンドライン）セッションでも同様のタイムアウトを設定できます。

長期にわたり Web インターフェイスをパッシブかつセキュアにモニタする予定のユーザが、導入内に存在する可能性があります。ユーザ設定オプションで Web インターフェイスのセッションタイムアウトからユーザを除外することができます。メニュー オプションへの完全なアクセス権がある管理者ロールのユーザは、侵害が生じる場合、余分のリスクを生じさせますが、セッションタイムアウトから除外することはできません。

## セッションタイムアウトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

システムへのシェルアクセスを制限する必要がある場合、追加オプションによって補助コマンドライン インターフェイスの expert コマンドを永続的に無効にすることができます。アプライアンスでエキスパートモードを無効にすると、構成シェルアクセスを持つユーザでも、シェルのエキスパートモードに入ることができなくなります。ユーザが補助コマンドライン インターフェイスのエキスパートモードに入ると、ユーザはシェルに応じた任意の Linux コマンドを実行できます。エキスパートモードに入っていない場合は、コマンドラインユーザはコマンドライン インターフェイスが提供するコマンドだけを実行できます。

## 手順

**ステップ 1** Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
- 管理対象デバイス : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower ポリシーを作成または編集します。

**ステップ 2** [シェル タイムアウト (Shell Timeout) ] をクリックします。

**ステップ 3** 次の選択肢があります。

- Web インターフェイスのセッションタイムアウトを設定するには、[ブラウザセッションタイムアウト (分) (Browser Session Timeout (Minutes)) ] フィールドに数値 (分数) を入力します。デフォルト値は 60 で、最大値は 1440 (24 時間) です。このセッションタイムアウトからユーザを除外する方法については、[ユーザアカウントログインオプション \(89 ページ\)](#) を参照してください。
- コマンドラインインターフェイスのセッションタイムアウトを設定するには、[シェルタイムアウト (分) (Shell Timeout (Minutes)) ] フィールドに数値 (分数) を入力します。デフォルト値は 0 で、最大値は 1440 (24 時間) です。
- 補助コマンドラインインターフェイスで expert コマンドを永続的に無効にするには、[expert コマンドを永続的に無効化 (Permanently Disable Expert Access) ] チェックボックスを選択します。

**注意** エキスパート モードが無効になった状態でポリシーをアプライアンスに展開した場合、Web インターフェイスまたは補助コマンドラインインターフェイスを介してエキスパート モードにアクセスする機能を復元することはできません。エキスパート モード機能を復元するには、サポートに問い合わせる必要があります。

**ステップ 4** [保存 (Save) ] をクリックします。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

# SNMP ポーリング

Firepower Management Center およびクラシック管理対象デバイスには、Simple Network Management Protocol (SNMP) ポーリングを有効にすることができます。SNMP 機能は、SNMP プロトコルのバージョン 1、2、3 をサポートします。

この機能を使用して、次の要素にアクセスできます。

- 標準 Management Information Base (MIB)。これには、連絡先、管理、場所、サービス情報、IP アドレッシングやルーティングの情報、トランスミッション プロトコルの使用状況の統計などのシステムの詳細が含まれます。
- 7000 および 8000 シリーズ 管理対象デバイスの追加の MIB。これには、物理インターフェイス、論理インターフェイス、仮想インターフェイス、ARP、NDP、仮想ブリッジ、仮想ルータを通して渡されるトラフィックの統計が含まれます。



(注) SNMP プロトコルの SNMP バージョンを選択する際は、SNMPv2 では読み取り専用コミュニティのみをサポートし、SNMPv3 では読み取り専用ユーザのみをサポートすることに注意してください。SNMPv3 は AES128 による暗号化もサポートします。

SNMP 機能を有効にすると、システムで SNMP トラップを送信できなくなり、MIB の情報はネットワーク管理システムによるポーリングでのみ使用可能になることに注意してください。

## SNMP ポーリングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス (7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv) に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。



(注) システムをポーリングするには、使用する任意のコンピュータで SNMP アクセスを追加する必要があります。SNMP MIB には展開の攻撃に使用される可能性がある情報も含まれているので注意してください。SNMP アクセスのアクセス リストを MIB のポーリングに使用される特定のホストに制限することをお勧めします。SNMPv3 を使用し、ネットワーク管理アクセスには強力なパスワードを使用することをお勧めします。

SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

## 始める前に

- [システムのアクセスリストの設定 \(958 ページ\)](#) の説明に従って、使用するコンピュータごとに SNMP アクセスを追加し、システムをポーリングします。

## 手順

- ステップ 1** Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。
- Management Center : [システム (System) ] > [設定 (Configuration) ] を選択します。
  - 管理対象デバイス : [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower ポリシーを作成または編集します。
- ステップ 2** [SNMP] をクリックします。
- ステップ 3** [SNMP バージョン (SNMP Version) ] ドロップダウン リストから、使用する SNMP バージョンを選択します。
- ステップ 4** 次の選択肢があります。
- [バージョン 1 (Version 1) ] または [バージョン 2 (Version 2) ] を選択した場合は、[コミュニティストリング (Community String) ] フィールドに SNMP コミュニティ名を入力します。手順 13 に進みます。
 

(注) SNMPv2 は、読み取り専用コミュニティのみをサポートしています。
  - [バージョン 3 (Version 3) ] を選択した場合、[ユーザを追加 (Add User) ] をクリックするとユーザ定義ページが表示されます。
 

(注) SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。
- ステップ 5** ユーザ名を入力します。
- ステップ 6** [認証プロトコル (Authentication Protocol) ] ドロップダウン リストから、認証に使用するプロトコルを選択します。
- ステップ 7** [認証パスワード (Authentication Password) ] フィールドに SNMP サーバの認証に必要なパスワードを入力します。
- ステップ 8** [パスワードの確認 (Verify Password) ] フィールドに、認証パスワードを再度入力します。
- ステップ 9** 使用するプライバシー プロトコルを [プライバシー プロトコル (Privacy Protocol) ] リストから選択するか、プライバシー プロトコルを使用しない場合は [なし (None) ] を選択します。
- ステップ 10** [プライバシー パスワード (Privacy Password) ] フィールドに SNMP サーバに必要な SNMP プライバシー キーを入力します。
- ステップ 11** [パスワードの確認 (Verify Password) ] フィールドに、プライバシー パスワードを再度入力します。
- ステップ 12** [追加 (Add) ] をクリックします。

ステップ 13 [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## セキュリティ認定準拠の

お客様の組織が、米国防総省およびグローバル認定組織によって確立されたセキュリティ基準に従う機器とソフトウェアだけを使用することを求められる場合があります。Firepower システムでは、以下のセキュリティ認定標準規格へのコンプライアンスをサポートします。

- コモンクライテリア (CC) : 国際コモンクライテリア承認アレンジメントによって確立された、セキュリティ製品のプロパティを定義するグローバル標準規格
- Unified Capabilities Approved Products List (UCAPL) : 米国防情報システム局 (DISA) によって確立された、セキュリティ要件を満たす製品のリスト



(注) 米国政府は、Unified Capabilities Approved Products List (UCAPL) の名称を Defense Information Network Approved Products List (DODIN APL) に変更しました。このドキュメントおよび Firepower Management Center Web インターフェイスでの UCAPL の参照は、DODIN APL への参照として解釈できます。

- 連邦情報処理標準 (FIPS) 140 : 暗号化モジュールの要件に関する規定

セキュリティ認定コンプライアンスは、CC モードまたは UCAPL モードで有効にすることができます。セキュリティ認定コンプライアンスを有効にしても、選択したセキュリティモードのすべての要件との厳密なコンプライアンスが保証されるわけではありません。強化手順についての詳細は、認定機関から提供されている本製品に関するガイドラインを参照してください。



**注意** この設定を有効にした場合、無効にすることはできません。設定を無効にする必要がある場合は、サポートに連絡して支援を求めてください。

## セキュリティ認定準拠特性

次の表は、CC または UCAPL モードを有効にしたときの動作の変更を示しています。(ログインアカウントの制約は、Web インターフェイスアクセスではなくコマンドラインまたはシェルアクセスを指します。)

システムの変更	CC モード	UCAPL モード
FIPS コンプライアンスは有効です。	○	○
バックアップまたはレポートについては、リモートストレージは利用できません。	○	○
追加のシステム監査デーモンが開始されます。	なし	○
システム ブートローダは固定されています。	なし	○
追加のセキュリティがログインアカウントに適用されます。	なし	○
ログインアカウントセッションの自動ログアウトを実行します。	なし	○
再起動キー シーケンスの Ctrl-Alt-Del を無効にします。	なし	○
最大 10 の同時ログインセッションを実行します。	なし	○
次の場合、システムは、アプライアンスとの SSH セッションで自動的にキーを再生成します： <ul style="list-style-type: none"> <li>セッション アクティビティでキーが 1 時間使用された後</li> <li>キーを使用して接続で 1 GB のデータが伝送された後</li> </ul> <p>これは、バージョン 6.1.0.4 またはそれ以降の 6.1.0.x パッチに当てはまります。</p>	○	○
システムは、バージョン 6.1.0.6 の場合のみ、eStreamer を使用したイベント データのエクスポートをサポートします。	○	○
ログインアカウントの厳密なセーフガードを適用します。 <ul style="list-style-type: none"> <li>パスワードは、大文字および小文字を組み合わせ最大 15 の英数字として、1 つ以上の数字を含む必要があります。</li> <li>パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。</li> <li>3 回連続ログインに失敗した場合、そのユーザはロックアウトされます。この場合は、管理者がパスワードをリセットする必要があります。</li> <li>パスワード履歴を保存しています。</li> <li>ログインが成功した場合は、失敗したログインの履歴を表示します。</li> </ul>	なし	○



## セキュリティ認定準拠の推奨事項

セキュリティ認定コンプライアンスの使用が有効のときに、次のベストプラクティスを確認することをお勧めします。

- 展開時にセキュリティ認定準拠を有効にするには、最初に Firepower Management Center で有効にし、次に、管理対象のすべてのデバイスの同じモードで有効にします。



**注意** 両方が同じセキュリティ認定準拠モードで動作していない限り、Firepower Management Center は管理対象デバイスからイベントデータを受信しません。

- 次の機能を使用するようにシステムを設定できません。
  - 電子メールレポート、アラート、データのプルーニング通知。
  - Nmap Scan、Cisco IOS Null Route、Set Attribute Value、ISE EPS の修復。
  - バックアップまたはレポート用のリモートストレージ。
  - サードパーティクライアントのシステムデータベースへのアクセス。
  - 電子メール、SNMP トラップ、syslog から送信される外部通知、アラート。
  - アプライアンスとサーバの間のチャンネルを保護するために、SSL 証明書を使用せずに、HTTP サーバまたは syslog サーバに送信された監査ログメッセージ。
- バージョン 6.1.0.6 の場合のみ、eStreamer を使用してイベントデータを外部クライアントにエクスポートするようにシステムを設定できます。
- CC モードを使用して展開中に SSO を有効にできません。
- CC モードを使用して展開中に CAC を有効にできません。
- CC または UCAPL モードを使用した展開では、Firepower REST API 経由で Firepower Management Center および管理対象デバイスへのアクセスを無効にします。
- UCAPL モードを使用して展開中に CAC を有効にします。



(注) Firepower システムは、以下に関する CC および UCAPL モードをサポートしていません。

- ハイ アベイラビリティ ペアの Firepower Management Center
- スタックまたはハイ アベイラビリティ ペアの従来型デバイス

## セキュリティ認定コンプライアンスの有効化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来型の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来型の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまでは、構成が有効になりません。



**注意** この設定を有効にした後は、無効にすることはできません。無効にする必要がある場合は、Cisco TAC にご連絡ください。

### 始める前に

- アプライアンスでセキュリティ認定コンプライアンスを有効にする前に、展開に組み込む予定のあるすべてのデバイスを Firepower Management Center に登録することをお勧めします。

### 手順

**ステップ 1** 設定するアプライアンスの種類に応じて、次のようにします。

- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
- 従来型管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower ポリシーを作成または編集します。

**ステップ 2** [UCAPL/CC コンプライアンス (UCAPL/CC Compliance)] をクリックします。

(注) UCAPL または CC コンプライアンスを有効にすると、アプライアンスがリブートします。Firepower Management Center は、システム設定を保存するとリブートし、管理対象デバイスは、設定の変更を展開するとリブートします。

**ステップ 3** アプライアンスのセキュリティ認定コンプライアンスを永続的に有効にするには、2つの選択肢があります。

- [コモンクライテリア (Common Criteria) ]モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウンリストから [CC] を選択します。
- [Unified 機能承認製品リスト (Unified Capabilities Approved Products List) ]モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウンリストから [UCAPL] を選択します。

ステップ 4 [保存 (Save) ] をクリックします。

#### 次のタスク

- まだ適用していない場合は、制御と防御のライセンスを、展開内のすべての従来型アプライアンスに適用します。
- アプライアンスがバージョン 5.2.0 より前のバージョンから更新された場合は、セキュリティ認定コンプライアンスを有効にすると、アプライアンス証明書が再生成されます。展開全体でセキュリティ認定コンプライアンスを同じモードで有効にした後、管理対象デバイスを Firepower Management Center に再登録します。
- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

## 時刻および時刻同期

[時刻 (Time) ] ページを使用して、Firepower Management Center、あるいは 7000 または 8000 シリーズデバイスのローカル Web インターフェイスから現在の時刻と時刻源を表示することができます。

時刻の設定は、アプライアンスの大半のページで、[タイムゾーン (Time Zone) ] ページで設定したタイムゾーン (デフォルトでは [アメリカ/ニューヨーク (America/New York) ]) を使用してローカル時間で表示されますが、アプライアンス自体には UTC 時間を使用して保存されます。また、現在の時刻は [時刻の同期 (Time Synchronization) ] ページの上部に UTC で表示されます (ローカル時間は [手動 (Manual) ] の時計設定オプションで表示されます (有効になっている場合) )。

時刻の同期は、[時刻の同期 (Time Synchronization) ] ページを使用して管理できます。時刻を同期する場合、以下の方法を選択できます。

- 手動で
- 1 つ以上の NTP サーバを使用 (推奨)

ハードウェアの Firepower Management Center を NTP サーバとして使用できますが、仮想 Firepower Management Center は NTP サーバとして使用しないでください。

リモートの NTP サーバを指定する場合、アプライアンスにそのサーバに対するネットワークアクセス権限が必要です。信頼できない NTP サーバを指定しないでください。NTP サーバへの接続では、構成されたプロキシ設定は使用されません。



(注) 時刻の同期後に、Firepower Management Center と管理対象デバイスの時刻が一致するようにしてください。時刻が一致していない場合、管理対象デバイスが Firepower Management Center と通信する際に意図しない結果が生じるおそれがあります。

## 時刻の同期

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

### 手順

**ステップ 1** Firepower Management Center または Classic 管理対象デバイスのいずれを設定しているかに応じて、以下を実行します。

- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
- 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower ポリシーを作成または編集します。

**ステップ 2** [時間同期 (Time Synchronization)] をクリックします。

**ステップ 3** 管理対象デバイスで時刻を同期する方法を指定する次のオプションがあります。

- NTP を介して Management Center から時刻を受信するには、[NTP 経由で管理センターから (Via NTP from Management Center)] を選択します。詳細については、[Firepower Management Center からの時間の提供 \(984 ページ\)](#) を参照してください。
- [NTP 経由 (Via NTP from)] を選択して、さまざまなサーバから NTP 経由で時刻を受信します。テキストボックスで、NTP サーバの IP アドレスのカンマ区切りリストを入力するか、DNS が有効になっている場合は、完全修飾ホスト名およびドメイン名を入力します。

**ステップ 4** [保存 (Save)] をクリックします。

(注) 設定された NTP サーバと管理対象デバイスを同期するには、数分かかる場合があります。さらに、管理対象デバイスを NTP サーバとして設定されている Management Center と同期する場合、Management Center 自体が NTP サーバを使用するように設定されていると、時刻を同期するのにいくらか時間がかかることがあります。これは、管理対象デバイスに時刻を提供するために、Management Center は設定された NTP サーバとまず同期する必要があるためです。

---

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。
- Management Center と管理対象デバイスの時刻が一致していることを確認します。





## 第 44 章

# Firepower Threat Defense のプラットフォーム設定

Firepower Threat Defense デバイス用のプラットフォーム設定では、互いに関連しないさまざまな機能を設定して、いくつかのデバイス間でその値を共有できます。デバイスごとに異なる設定が必要な場合でも、共有ポリシーを作成し、該当するデバイスにそれを適用する必要があります。

- [ARP インспекションの設定 \(1033 ページ\)](#)
- [バナー設定 \(1035 ページ\)](#)
- [フラグメントの処理の設定 \(1036 ページ\)](#)
- [HTTP の設定 \(1037 ページ\)](#)
- [ICMP アクセス ルールの設定 \(1039 ページ\)](#)
- [セキュア シェルの設定 \(1041 ページ\)](#)
- [SMTP の設定 \(1043 ページ\)](#)
- [SNMP の脅威に対する防御の設定 \(1043 ページ\)](#)
- [Syslog の設定 \(1050 ページ\)](#)
- [グローバル タイムアウトの設定 \(1064 ページ\)](#)
- [脅威に対する防御のための NTP 時刻同期の設定 \(1066 ページ\)](#)

## ARP インспекションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

デフォルトでは、ブリッジグループのメンバーの間ですべての ARP パケットが許可されます。ARP パケットのフローを制御するには、ARP インспекションを有効にします。

ARP インспекションによって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホストトラフィックを代行受信してルータに転送できるようになります。

ARP インспекションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

ARP インспекションをイネーブルにすると、Firepower Threat Defense デバイスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、Firepower Threat Defense デバイスはパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするように Firepower Threat Defense デバイスを設定できます。



(注) 専用の診断インターフェイスは、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

## 手順

**ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

**ステップ 2** [ARP インспекション (ARP Inspection)] を選択します。

**ステップ 3** ARP インспекション テーブルにエントリを追加します。

- a) [追加 (Add)] をクリックして新しいエントリを作成するか、エントリがすでにある場合は、[編集 (Edit)] アイコンをクリックします。
- b) 任意のオプションを選択します。
  - [インспекション有効 (Inspect Enabled)] : 選択されているインターフェイスとゾーンの ARP インспекションを実行します。
  - [フラッディング有効 (Flood Enabled)] : 静的 ARP エントリに一致しない ARP 要求を元のインターフェイスまたは専門の管理インターフェイス以外のすべてのインターフェイスにフラッディングします。これはデフォルトの動作です。



ARP 要求のフラグディングを選択しない場合、静的 ARP エントリに一致する要求のみが許可されます。

- [セキュリティゾーン (Security Zones) ]: 選択されているアクションを実行するインターフェイスを含むゾーンを追加します。ゾーンはスイッチドゾーンにする必要があります。ゾーンにないインターフェイスでは、選択されたセキュリティゾーンのリストの下のフィールドにインターフェイス名を入力し、[追加 (Add) ]をクリックします。これらのルールは、デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ適用されます。

c) [OK] をクリックします。

**ステップ 4** [スタティック ARP エントリの追加 \(689 ページ\)](#) に従って、静的 ARP エントリを追加します。

**ステップ 5** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## バナー設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

デバイスの CLI (コマンドラインインターフェイス) に接続するユーザを表示するよう、メッセージを設定できます。

### 手順

**ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

**ステップ 2** [バナー (Banner) ] を選択します。

**ステップ 3** バナーを設定します。

以下は、バナーのコツと要件です。

- 使用できる文字は ASCII 文字のみです。回線返品 (Enter を押します) を使用できますが、タブを使用できません。
- デバイスのホスト名またはドメイン名は、**\$(hostname)** 変数と **\$(domain)** 変数を組み込むことによってダイナミックに追加できます。

- バナーに長さの制限はありませんが、バナー メッセージの処理に十分なシステム メモリがない場合、Telnet または SSH セッションは閉じます。
- セキュリティの観点から、バナーで不正アクセスを防止することが重要です。侵入者を招き入れる可能性があるため、「ようこそ」や「お願いします」などの言葉は使用しないでください。次のバナーは、不正アクセスに対する適切な基調を定めます。

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk criminal charges.
```

**ステップ 4** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## フラグメントの処理の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

デフォルトでは、Firepower Threat Defense デバイスは 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。NFS over UDP など、アプリケーションが日常的にパケットをフラグメント化する場合は、ネットワークでフラグメント化を許可する必要があります。ただし、トラフィックをフラグメント化するアプリケーションがない場合は、[チェーン (Chain) ] を 1 に設定してフラグメントを許可しないようにすることをお勧めします。フラグメント化されたパケットは、サービス妨害 (DoS) 攻撃によく使われます。



(注) これらの設定は、このポリシーが割り当てられたデバイスのデフォルトになります。インターフェイス構成で [デフォルトフラグメント設定のオーバーライド (Override Default Fragment Setting) ] を選択することで、デバイスの特定のインターフェイスでこれらの設定をオーバーライドできます。インターフェイスを編集する際、[詳細 (Advanced) ] > [セキュリティ設定 (Security Configuration) ] タブでオプションを確認できます。> [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択して、Firepower Threat Defense デバイスを編集し、[インターフェイス (Interfaces) ] タブを選択して、インターフェイスのプロパティを編集します。>

手順

**ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

**ステップ 2** [フラグメント (Fragment) ] を選択します。

**ステップ 3** 次のオプションを設定します。デフォルト設定を使用する場合は、[デフォルトにリセット (Reset to Defaults) ] をクリックします。

- [サイズ (ブロック (Size (Block) ) ] : リアセンブルを待機可能な、すべての集成的な接続からのパケットフラグメントの最大数。デフォルトは 200 フラグメントです。
- [チェーン (フラグメント) (Chain (Fragment) ) ] : 1 つの完全な IP パケットにフラグメント化できる最大パケット数を指定します。デフォルトは 24 パケットです。フラグメントを許可しない場合は、このオプションを 1 に設定します。
- [タイムアウト (秒) (Timeout (Sec) ) ] : フラグメント化されたパケット全体の到着を待機する最大秒数を設定します。デフォルトは 5 秒です。すべてのフラグメントがこの時間内に受信されなかった場合、すべてのフラグメントが破棄されます。

**ステップ 4** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## HTTP の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

HTTPS 接続を Firepower Threat Defense デバイスの複数のインターフェイスに対して許可するには、HTTPS 設定を行います。トラブルシューティングでパケットキャプチャをダウンロードするために、HTTPS を使用できます。

### 始める前に

- HTTPS の使用で、ホスト IP アドレスを許可するアクセスルールは必要ありません。このセクションの手順に従って、HTTPS アクセスを設定する必要があるだけです。
- 到達可能なインターフェイスにのみ HTTPS を使用できます。HTTPS ホストが外部インターフェイスにある場合は、外部インターフェイスへの直接的な管理接続のみ開始できます。

- デバイスでは、最大 5 つの HTTPS 接続を同時にできます。
- デバイスへの HTTPS 接続に許可するホストまたはネットワークを定義するネットワーク オブジェクトが必要です。オブジェクトをプロシージャの一部として追加できますが、IP アドレスのグループを特定するためにオブジェクトグループを使用する場合は、ルールに必要なグループがすでに存在することを確認します。[オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択してオブジェクトを設定します。
- 物理管理インターフェイスは、診断論理インターフェイスと管理論理インターフェイスの間で共有されます。この設定は、診断論理インターフェイスを使用すると、こちらにのみ適用されます。管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。Firepower Management Center にデバイスを設定し、登録するために使用されます。これには、個別の IP アドレスとスタティック ルーティングがあります。

## 手順

**ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

**ステップ 2** [HTTP] を選択します。

**ステップ 3** [HTTP サーバを有効にする (Enable HTTP server) ] をクリックして、HTTPS サーバを有効にします。

**ステップ 4** (任意) HTTPS ポートを変更します。デフォルトは 443 です。

**ステップ 5** HTTPS 接続を許可する IP アドレスとインターフェイスを指定します。

このテーブルを使用して、HTTPS 接続および HTTPS 接続が許可されているクライアントの IP アドレスを承認するインターフェイスを制限します。個々の IP アドレスではなく、ネットワーク アドレスを使用することができます。

- [追加 (Add) ] をクリックして新しいルールを追加するか、[編集 (Edit) ] アイコンをクリックして既存のルールを編集します。
- ルールのプロパティを設定します。
  - [IP アドレス (IP Address) ] : HTTPS 接続を許可するホストまたはネットワークを識別するネットワーク オブジェクト。ドロップダウン メニューからオブジェクトを選択するか、または + ボタンをクリックして新しいネットワーク オブジェクトを追加します。
  - [セキュリティゾーン (Security Zones) ] : HTTPS 接続を許可するインターフェイスを含むゾーンを追加します。ゾーンにないインターフェイスでは、選択されたセキュリティゾーンのリストの下のフィールドにインターフェイス名を入力し、[追加 (Add) ] をクリックします。これらのルールは、デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ適用されます。

c) [OK] をクリックします。

**ステップ 6** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## ICMP アクセス ルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

デフォルトでは、IPv4 または IPv6 を使用して任意のインターフェイスに ICMP パケットを送信できます。ただし、次の例外があります。

- Firepower Threat Defense デバイスは、ブロードキャストアドレス宛ての ICMP エコー要求に応答しません。
- Firepower Threat Defense デバイスは、トラフィックが着信するインターフェイス宛ての ICMP トラフィックにのみ応答します。ICMP トラフィックは、インターフェイス経由で離れたインターフェイスに送信できません。

デバイスを攻撃から保護するために、ICMP ルールを使用して、インターフェイスへの ICMP アクセスを特定のホスト、ネットワーク、または ICMP タイプに限定できます。ICMP ルールにはアクセスルールと同様に順序があり、パケットに最初に一致したルールのアクションが適用されます。

インターフェイスに対していずれかの ICMP ルールを設定すると、ICMP ルールのリストの最後に暗黙の deny ICMP ルールが追加され、デフォルトの動作が変更されます。そのため、一部のメッセージタイプだけを拒否する場合は、残りのメッセージタイプを許可するように ICMP ルールのリストの最後に permit any ルールを含める必要があります。

ICMP 到達不能メッセージタイプ (タイプ 3) には常にアクセス許可を付与することを推奨します。ICMP 到達不能メッセージを拒否すると、ICMP パス MTU ディスカバリが無効化され、IPsec および PPTP トラフィックが停止することがあります。また、IPv6 の ICMP パケットは、IPv6 のネイバー探索プロセスに使用されます。

### 始める前に

ルールに必要なオブジェクトがすでに存在していることを確認します。[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、オブジェクトを設定します。> 任意のホストまたはネットワークを定義するネットワークオブジェクトまたはグループ、あるいは制御する ICMP メッセージタイプを定義するポート オブジェクトが必要です。

## 手順

**ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

**ステップ 2** [ICMP] を選択します。

**ステップ 3** ICMP ルールを設定します。

- a) [追加 (Add) ] をクリックして新しいルールを追加するか、[編集 (Edit) ] アイコンをクリックして既存のルールを編集します。
- b) ルールのプロパティを設定します。
  - [アクション (Action) ] : 一致するトラフィックを許可または拒否 (ドロップ) するかどうかを指定します。
  - [ICMP サービス (ICMP Service) ] : ICMP メッセージタイプを識別するポート オブジェクト。
  - [ネットワーク (Network) ] : アクセスを制御しているホストまたはネットワークを識別するネットワーク オブジェクトまたはグループ。
  - [セキュリティゾーン (Security Zones) ] : 保護しているインターフェイスを含むゾーンを追加します。ゾーンにないインターフェイスでは、選択されたセキュリティゾーンのリストの下のフィールドにインターフェイス名を入力し、[追加 (Add) ] をクリックします。これらのルールは、デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ適用されます。
- c) [OK] をクリックします。

**ステップ 4** (オプション) ICMPv4 到達不能メッセージをレート制限します。

- [レート制限 (Rate Limit) ] : 到達不能メッセージのレート制限を、1 秒あたり 1 ~ 100 の範囲で設定します。デフォルトは、1 秒あたり 1 メッセージです。
- [バースト サイズ (Burst Size) ] : バースト レートを 1 ~ 10 の範囲で設定します。現在、この値はシステムによって使用されていません。

**ステップ 5** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

# セキュア シェルの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

Firepower Threat Defense デバイスの 1 つ以上のインターフェイスへの SSH 接続を許可するには、セキュア シェル設定を行います。

## 始める前に

- SSH は診断インターフェイスに対してサポートされていません。
- SSH ローカルユーザは、**configure user add** コマンドを使用して CLI でのみ設定できます。デフォルトでは、初期設定時にパスワードを設定した **Admin** ユーザが存在します。
- SSH トラフィックでは、設定または CLI で設定されたスタティック ルートではなく、通常のルーティング設定が使用されます。
- SSH を使用するには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、SSH アクセスを設定する必要があるだけです。
- SSH は、到達可能なインターフェイスにのみ使用できます。SSH ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。
- デバイスでは、最大 5 つの同時 SSH 接続を許可できます。
- デバイスへの SSH 接続を許可するホストまたはネットワークを定義するネットワーク オブジェクトが必要です。手順の一部としてオブジェクトを追加できますが、IP アドレスのグループを特定するためにオブジェクト グループを使用する場合は、ルールに必要なグループがすでに存在することを確認します。[オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択してオブジェクトを設定します。



(注) システムが提供する **any** ネットワーク オブジェクトは使用できません。代わりに、**any-ipv4** または **any-ipv6** を使用します。

## 手順

- ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2** [セキュア シェル (Secure Shell) ] を選択します。

**ステップ 3** (オプション) SSH アクセスの制限を変更します。

- [SSH バージョン (SSH Version) ] : デフォルトでは、ユーザは SSH バージョン 1 および 2 を使用して接続できます。これらのバージョンの 1 つのみにアクセスを制限できます。たとえば SSH バージョン 2 のみをサポートする場合は、**2** を選択します。
- [タイムアウト (Timeout) ] : システムがセッションを切断するまでに SSH セッションがアイドル状態を維持する時間の長さ。タイムアウトは 1 ~ 60 分に設定します。デフォルトは 5 分です。
- [セキュア コピーを有効にする (Enable Secure Copy) ] : デバイスのセキュア コピー (SCP) サーバを有効にするかどうか。これにより、デバイスはデバイスとの間でファイルを転送するための SCP サーバとして機能できます。SSH を使用したセキュリティ アプライアンスへのアクセスを許可されるクライアントだけが、セキュア コピー接続を確立できます。SCP には、SSH バージョン 2 が必要です。

**ステップ 4** SSH 接続を許可するインターフェイスと IP アドレスを指定します。

この表を使用して、SSH 接続を受け入れるインターフェイス、およびそれらの接続を許可されるクライアントの IP アドレスを制限します。個々の IP アドレスはなく、ネットワークアドレスを使用できます。

- a) [追加 (Add) ] をクリックして新しいルールを追加するか、[編集 (Edit) ] アイコンをクリックして既存のルールを編集します。
- b) 次のルールプロパティを設定します。
  - [IP アドレス (IP Address) ] : SSH 接続を許可するホストまたはネットワークを特定するネットワーク オブジェクト。オブジェクトをドロップダウンメニューから選択するか、または + ボタンをクリックして新しいネットワーク オブジェクトを追加します。
  - [セキュリティゾーン (Security Zones) ] : SSH 接続を許可するインターフェイスを含むゾーンを追加します。ゾーンに存在しないインターフェイスの場合は、[選択されたセキュリティゾーン (Selected Security Zone) ] リストの下のフィールドにインターフェイス名を入力し、[追加 (Add) ] をクリックします。これらのルールは、デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ適用されます。
- c) [OK] をクリックします。

**ステップ 5** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。



## SMTP の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

Syslog 設定で電子メール アラートを設定する場合は、SMTP サーバを指定する必要があります。Syslog で設定する送信元電子メールアドレスは、SMTP サーバの有効なアカウントである必要があります。

### 始める前に

プライマリおよびセカンダリ SMTP サーバのホストアドレスを定義するネットワーク オブジェクトが存在することを確認します。[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択してオブジェクトを定義します。または、ポリシーの編集時にオブジェクトを作成することもできます。

### 手順

- ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2 [SMTP サーバ (SMTP Server)] をクリックします。
- ステップ 3 [プライマリ サーバの IP アドレス (Primary Server IP Address)]、およびオプションで、[セカンダリ サーバの IP アドレス (Secondary Server IP Address)] を特定するネットワーク オブジェクトを選択します。
- ステップ 4 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## SNMP の脅威に対する防御の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

簡易ネットワーク管理プロトコル (SNMP) は、PC またはワークステーションで実行されているネットワーク管理ステーションが、スイッチ、ルータ、セキュリティアプライアンスなどのさまざまなタイプのデバイスのヘルスとステータスをモニタするための標準的な方法を定義します。[SNMP] ページを使用して、SNMP 管理ステーションによってモニタされるようにファイアウォール デバイスを設定できます。

簡易ネットワーク管理プロトコル (SNMP) は、集中管理する場所からのネットワークデバイスのモニタリングをイネーブルにします。Cisco セキュリティアプライアンスでは、SNMP バージョン 1、2c、および 3 を使用したネットワークモニタリングに加えて、トラップおよび SNMP 読み取りアクセスがサポートされます。SNMP 書き込みアクセスはサポートされません。

SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。



(注) 外部 SNMP サーバでアラートを作成するには、[ポリシー (Policies)] > [アクション (Action)] > [アラート (Alerts)] にアクセスします。 > >

#### 手順

**ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

**ステップ 2** [SNMP] を選択します。

**ステップ 3** SNMP を有効にし、基本オプションを設定します。

- [SNMP サーバを有効にする (Enable SNMP Servers)] : 設定された SNMP ホストに SNMP 情報を提供するかどうかを指定します。このオプションの選択を解除すると、設定情報を保持したまま、SNMP モニタリングをディセーブルにできます。
- [コミュニティストリングの表示 (Read Community String)]、[確認 (Confirm)] : SNMP 管理ステーションが Firepower Threat Defense デバイスに要求を送信する際に使用するパスワードを入力します。SNMP コミュニティストリングは、SNMP 管理ステーションと管理対象のネットワーク ノード間の共有秘密キーです。セキュリティ デバイスでは、このパスワードを使用して、着信 SNMP 要求が有効かどうかを判断します。パスワードは大文字小文字が区別される、最大 32 文字の英数字の文字列です。スペースは使用できません。
- [システム管理者名 (System Administrator Name)] : デバイス管理者またはその他の担当者の名前を入力します。この文字列は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。
- [場所 (Location)] : このセキュリティ デバイスの場所を入力します (Building 42, Sector 54 など)。この文字列は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。
- [ポート (Port)] : 着信要求が受け入れられる UDP ポートを入力します。デフォルトは 161 です。

**ステップ 4** (SNMPv3 のみ) [SNMPv3 ユーザの追加 \(1045 ページ\)](#)。

**ステップ 5** [SNMP ホストの追加 \(1047 ページ\)](#)。

ステップ6 **SNMP トラップの設定 (1048 ページ)**。

ステップ7 [保存 (Save) ]をクリックします。

これで、[展開 (Deploy) ]をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## SNMPv3 ユーザの追加



(注) SNMPv3 でのみユーザを作成できます。以下の手順は、SNMPv1 または SNMPv2c には適用されません。

SNMPv3 は読み取り専用ユーザのみをサポートすることに注意してください。

SNMP ユーザには、ユーザ名、認証パスワード、暗号化パスワードおよび使用する認証アルゴリズムと暗号化アルゴリズムが指定されています。認証アルゴリズムのオプションは MD5 と SHA です。暗号化アルゴリズムのオプションは DES、3DES と AES128 です。

### 手順

- ステップ1 [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ2 目次の [SNMP] をクリックして、[ユーザ (User) ] タブをクリックします。
- ステップ3 [追加 (Add) ] をクリックします。
- ステップ4 [セキュリティ レベル (Security Level) ] ドロップダウン リストからユーザに適したセキュリティ レベルを選択します。
- **Auth** : 認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
  - **No Auth** : 認証もプライバシーもありません。メッセージにどのようなセキュリティも適用されないことを意味します。
  - **Priv** : 認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。
- ステップ5 [ユーザ名 (Username) ] フィールドに SNMP ユーザの名前を入力します。このユーザ名は 32 文字以下であることが必要です。
- ステップ6 [暗号化パスワードタイプ (Encryption Password Type) ] ドロップダウン リストから使用するパスワードのタイプを選択します。
- **Clear text** : Firepower Threat Defense デバイスは、デバイスへの導入時を待ってパスワードを暗号化します。

- **Encrypted** : Firepower Threat Defense デバイスは、暗号化を済ませたパスワードを直接展開します。

**ステップ 7** [認証アルゴリズム タイプ (Auth Algorithm Type) ] ドロップダウン リストから MD5 または SHA のうち、使用する認証タイプを選択します。

**ステップ 8** 認証に使用するパスワードを、[認証パスワード (Authentication Password) ] フィールドに入力します。暗号化パスワードタイプに [暗号化 (Encrypted) ] を選択した場合、パスワードは xx:xx:xx... という形式にフォーマットされます。ここで、xx は 16 進数の値です。

(注) パスワードの長さは、選択した認証アルゴリズムによって異なります。すべてのパスワードの長さを 256 文字以下とする必要があります。

暗号化パスワードタイプに [クリアテキスト (Clear Text) ] を選択した場合、[確認 (Confirm) ] フィールドにパスワードをもう一度入力してください。

**ステップ 9** [暗号化タイプ (Encryption Type) ] ドロップダウン リストで、AES128、AES192、AES256、3DES、DES の中から使用する暗号化タイプを選択します。

(注) AES または 3DES 暗号化を使用するには、デバイスに適切なライセンスをインストールしておく必要があります。

**ステップ 10** [暗号化パスワード (Encryption Password) ] フィールドに暗号化で使用するパスワードを入力します。暗号化パスワードタイプに [暗号化 (Encrypted) ] を選択した場合、パスワードは xx:xx:xx... という形式にフォーマットされます。ここで、xx は 16 進数の値です。暗号化を行う場合のパスワードの長さは選択された暗号化のタイプにより異なります。パスワードの長さは次のとおりです (各 xx は 1 つのオクテットを示します) 。

- AES 128 では 16 オクテットとする必要があります
- AES 192 では 24 オクテットとする必要があります
- AES 256 では 32 オクテットとする必要があります
- 3DES では 32 オクテットとする必要があります
- DES の長さはさまざまです。

(注) すべてのパスワードの長さを 256 文字以下とする必要があります。

暗号化パスワードタイプに [クリアテキスト (Clear Text) ] を選択した場合、[確認 (Confirm) ] フィールドにパスワードをもう一度入力してください。

**ステップ 11** [OK] をクリックします。

**ステップ 12** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## SNMP ホストの追加

[ホスト (Host) ] タブを使用して、[SNMP] ページにある [SNMP ホスト (SNMP Hosts) ] テーブルのエントリを追加または編集します。これらのエントリは、Firepower Threat Defense デバイスへのアクセスが許可されている SNMP 管理ステーションを示します。

### 始める前に

SNMP 管理ステーションを定義するネットワーク オブジェクトが存在することを確認します。[デバイス (Device) ] > [オブジェクト管理 (Object Management) ] を選択し、ネットワーク オブジェクトを設定します。 >



(注) サポートされているのは IPv4 アドレスだけです。

### 手順

- ステップ 1 [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2 目次の [SNMP] をクリックして、[ホスト (Hosts) ] タブをクリックします。
- ステップ 3 [追加 (Add) ] をクリックします。
- ステップ 4 [IP アドレス (IP Address) ] フィールドで、SNMP 管理ステーションのホストアドレスを決定するネットワークオブジェクトを選択します。
- ステップ 5 [SNMP バージョン (SNMP Version) ] ドロップダウン リストから、適切な SNMP バージョンを選択します。
- ステップ 6 (SNMPv3 のみ) [ユーザ名 (User Name) ] ドロップダウン リストから設定した SNMP ユーザのユーザ名を選択します。  
(注) SNMP ホストごとに 23 人までの SNMP ユーザを関連付けることができます。
- ステップ 7 (SNMPv1、2c のみ) [Read コミュニティストリング (Read Community String) ] フィールドに、デバイスの読み取りアクセスのためにすでに設定してあるコミュニティストリングを入力します。確認のためにこの文字列を再入力します。  
(注) この文字列は、この SNMP ステーションで使用されている文字列が [SNMP サーバを有効にする (Enable SNMP Server) ] セクションに定義済みのものと異なる場合のみ必須です。
- ステップ 8 デバイスと SNMP 管理ステーションの間の通信タイプを選択します。両方のタイプを選択できます。
  - [ポーリング (Poll) ] : 管理ステーションは定期的にデバイスに情報を要求します。
  - [トラップ (Trap) ] : デバイスは、イベント発生時にこれをトラップし、管理ステーションに送信します。

- ステップ 9** [ポート (Port) ]フィールドに、SNMPホストのUDPポート番号を入力します。デフォルト値は162です。有効な範囲は1～65535です。
- ステップ 10** [追加 (Add) ]をクリックし、このSNMP管理ステーションがデバイスにアクセスするインターフェイスを入力または選択します。
- ステップ 11** [ゾーン/インターフェイス (Zones/Interfaces) ]リストに、デバイスが管理ステーションとの通信を行うインターフェイスが含まれたゾーンを追加します。ゾーン内にはないインターフェイスの場合は、[選択したゾーン/インターフェイス (Selected Zone/Interface) ]リストの下のフィールドにインターフェイス名を入力し、[追加 (Add) ]をクリックします。デバイスに選択されたインターフェイスやゾーンが含まれる場合のみデバイスにホストが設定されます。
- ステップ 12** [OK] をクリックします。
- ステップ 13** [保存 (Save) ] をクリックします。
- これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## SNMP トラップの設定

[SNMP トラップ] タブを使用して、Firepower Threat Defense デバイスの SNMP トラップ (イベント通知) を設定します。トラップは参照とは異なります。トラップは、生成されるリンクアップイベント、リンクダウンイベント、Syslog イベントなど、特定のイベントに対する Firepower Threat Defense デバイスから管理ステーションへの割り込み「コメント」です。デバイスの SNMP オブジェクト ID (OID) は、デバイスから送信される SNMP イベントトラップに表示されます。

一部のトラップは、特定のハードウェアモデルに適用できません。これらのトラップは、これらのモデルの1つのポリシーを適用すると無視されます。たとえば、すべてのモデルに現場交換可能ユニットがあるわけではありません。そのため、[現場交換可能ユニット挿入/削除 (Field Replaceable Unit Insert/Delete) ] トラップはこれらのモデルで設定されません。

### 手順

- ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2** 目次の [SNMP] をクリックし、[SNMP トラップ (SNMP Traps) ] タブをクリックして、Firepower Threat Defense デバイスの SNMP トラップ (イベント通知) を設定します。
- ステップ 3** 適切な [Enable Traps] オプションを選択します。いずれかまたは両方のオプションを選択できます。
- [すべての SNMP トラップを有効にする (Enable All SNMP Traps) ] にマークを付けて、連続する 4 セクションですべてのトラップを素早く選択します。
  - [すべての Syslog トラップを有効にする (Enable All Syslog Traps) ] にマークを付けて、トラップ関連の Syslog メッセージの伝送を有効にします。

**ステップ 4** [標準 (Standard) ]セクションのイベント通知トラップは、既存のポリシーでは、デフォルトで有効になっています。

- [認証 (Authentication) ] : 未認可の SNMP アクセス。この認証エラーは、間違ったコミュニティ スtring が付いたパケットによって発生します。
- [リンクアップ (Link Up) ] : 通知に示されているとおり、デバイスの通信リンクの1つが使用可能になりました。
- [リンクダウン (Link Down) ] : 通知に示されているとおり、デバイスの通信リンクの1つにエラーが発生しました。
- [コールドスタート (Cold Start) ] : デバイスが自動で再初期化しているときに、その設定またはプロトコル エンティティの実装が変更されることがあります。
- [ウォームスタート (Warm Start) ] : デバイスが自動で再初期化しているときに、その設定またはプロトコル エンティティの実装が変更されることはありません。

**ステップ 5** [エンティティ MIB (Entity MIB) ]セクションで好きなイベント通知トラップを選択します。

- [現場交換可能ユニット挿入 (Field Replaceable Unit Insert) ] : 示されているとおり、現場交換可能ユニット (FRU) が挿入されました (FRU には電源装置、ファン、プロセッサモジュール、インターフェイス モジュールなどの組み立て部品が含まれます) 。
- [現場交換可能ユニット除外 (Field Replaceable Unit Remove) ] : 通知に示されているとおり、現場交換可能ユニット (FRU) が取り外されました。
- [設定変更 (Configuration Change) ] : 通知に示されているとおり、ハードウェアに変更がありました。

**ステップ 6** [リソース (Resource) ]セクションで好きなイベント通知トラップを選択します。

- [接続制限到達 (Connection Limit Reached) ] : このトラップは、設定した接続制限に達したため、接続試行が拒否されたことを示します。

**ステップ 7** [その他 (Other) ]セクションで好きなイベント通知トラップを選択します。

- [NAT パケット破棄 (NAT Packet Discard) ] : IP パケットが NAT 機能により廃棄されると、この通知が生成されます。ネットワーク アドレス変換の使用可能なアドレスまたはポートが、設定したしきい値を下回りました。

**ステップ 8** [保存 (Save) ]をクリックします。

これで、[展開 (Deploy) ]をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

# Syslog の設定

Firepower Threat Defense デバイスのシステム ロギング (syslog) を有効にすることができます。情報をロギングすることで、ネットワークの問題またはデバイス設定の問題を特定して分離できます。ここでは、ロギングとその設定方法について説明します。

## Syslog について

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央 syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。シスコ デバイスでは、これらのログ メッセージを UNIX スタイルの syslog サービスに送信できます。syslog サービスは、簡単なコンフィギュレーションファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、ログ用の保護された長期ストレージを提供します。ログは、ルーチンのトラブルシューティングおよびインシデント処理の両方で役立ちます。

Firepower Threat Defense では、syslog を 2 つの場所で構成できます。

- [プラットフォーム設定 (Platform Settings) ]: この syslog 設定では、データプレーン上で実行されている機能、つまり **show running-config** コマンドで表示できる CLI 設定で定義されている機能に関するメッセージが生成されます。これには、ルーティング、VPN、データ インターフェイス、DHCP サーバ、NAT などの機能が含まれます。データプレーンの syslog メッセージには番号が付けられており、ASA ソフトウェアを実行しているデバイスで生成されるものと同じです。しかし、Firepower Threat Defense は、必ずしも ASA ソフトウェアで使用可能なすべてのメッセージタイプを生成するとは限りません。これらのメッセージの詳細については、『[Cisco ASA Series Syslog Messages](#)』を参照してください。この構成については、次のトピックで説明します。
- [アラート応答 (Alert Responses) ]: この syslog 設定では、[アラート応答のサポート設定 \(2342 ページ\)](#) で説明されているように、アクセス制御ルール、侵入ルール、およびその他のアドバンスドサービスに関するアラートが生成されます。これらのメッセージには番号が付けられていません。このタイプの syslog の設定については、[Syslog アラート応答の作成 \(2344 ページ\)](#) を参照してください。

複数の syslog サーバを設定し、各サーバに送信されるメッセージとイベントを制御できます。また、コンソール、電子メール、内部バッファなどの異なる宛先を構成することもできます。

## 重大度

次の表に、syslog メッセージの重大度の一覧を示します。



表 72: syslog メッセージの重大度

レベル番号	重大度	説明
[0]	緊急	システムが使用不可能な状態です。
1	アラート	すぐに措置する必要があります。
2	重大	深刻な状況です。
3	error	エラー状態です。
4	警告	警告状態です。
5	通知	正常ですが、注意を必要とする状況です。
[6]	情報	情報メッセージです。
7	デバッグ	デバッグ メッセージです。



(注) Firepower Threat Defense は、重大度 0 (緊急) の syslog メッセージを生成しません。

## syslog メッセージ フィルタリング

生成される syslog メッセージは、特定の syslog メッセージだけが特定の出力先に送信されるようにフィルタリングできます。たとえば、Firepower Threat Defense デバイスを設定して、すべての syslog メッセージを 1 つの出力先に送信し、それらの syslog メッセージのサブセットを別の出力先に送信することができます。

具体的には、syslog メッセージが次の基準に従って出力先に転送されるようにできます。

- syslog メッセージの ID 番号
- syslog メッセージの重大度
- syslog メッセージクラス (機能エリアと同等)

これらの基準は、出力先を設定するときに指定可能なメッセージリストを作成して、カスタマイズできます。あるいは、メッセージリストとは無関係に、特定のメッセージクラスを各タイプの出力先に送信するように Firepower Threat Defense デバイスを設定することもできます。

## syslog メッセージクラス

syslog メッセージのクラスは次の 2 つの方法で使用できます。

- syslog メッセージのカテゴリ全体の出力場所を指定します。
- メッセージクラスを指定するメッセージリストを作成します。

syslog メッセージクラスは、デバイスの特徴または機能と同等のタイプによって syslog メッセージを分類する方法を提供します。たとえば、RIP クラスは RIP ルーティングを示します。

特定のクラスに属する syslog メッセージの ID 番号はすべて、最初の 3 桁が同じです。たとえば、611 で始まるすべての syslog メッセージ ID は、vpnc (VPN クライアント) クラスに関連付けられています。VPN クライアント機能に関連付けられている syslog メッセージの範囲は、611101 ~ 611323 です。

また、ほとんどの ISAKMP syslog メッセージには先頭に付加されたオブジェクトの共通セットが含まれているため、トンネルを識別するのに役立ちます。これらのオブジェクトは、使用可能なときに、syslog メッセージの説明テキストの前に付加されます。syslog メッセージ生成時にオブジェクトが不明な場合、特定の heading = value の組み合わせは表示されません。

オブジェクトは次のように先頭に付加されます。

Group = *groupname*, Username = *user*, IP = *IP\_address*

Group はトンネルグループ、Username はローカルデータベースまたは AAA サーバから取得したユーザ名、IP アドレスはリモートアクセスクライアントまたはレイヤ 2 ピアのパブリック IP アドレスです。

次の表に、メッセージクラスと各クラスのメッセージ ID の範囲をリストします。

表 73: セージクラスおよび関連するメッセージ ID 番号

クラス	定義 (Definition)	メッセージ ID 番号
auth	ユーザ認証	109、113
ブリッジ	トランスペアレント ファイアウォール	110、220
ca	PKI 証明機関	717
config	コマンドインターフェイス	111、112、208、308
電子メール (e-mail)	電子メール プロキシ	719
ha	フェールオーバー (ハイ アベイラビリティ)	101、102、103、104、105、210、311、709
ids	侵入検知システム	400、401、415
ip	IP スタック	209、215、313、317、408
np	ネットワークプロセッサ	319
ospf	OSPF ルーティング	318、409、503、613

クラス	定義 (Definition)	メッセージ ID 番号
rip	RIP ルーティング	107、312
rm	Resource Manager	321
session	ユーザ セッション	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
webvpn	Web ベースの VPN	716

## ロギングのガイドライン

この項では、ロギングを設定する前に確認する必要のある制限事項とガイドラインについて説明します。

### IPv6 のガイドライン

IPv6 はサポートされません。

### その他のガイドライン

- syslog サーバでは、syslogd というサーバプログラムを実行する必要があります。Windows では、オペレーティング システムの一部として syslog サーバを提供しています。
- Firepower Threat Defense デバイスが生成したログを表示するには、ロギングの出力先を指定する必要があります。ロギングの出力先を指定せずにロギングをイネーブルにすると、Firepower Threat Defense デバイスはメッセージを生成しますが、それらのメッセージは後で表示できる場所に保存されません。各ロギングの出力先は個別に指定する必要があります。

- 2つの異なるリストまたはクラスを異なる syslog サーバまたは同じ場所に割り当てることはできません。
- 最大 16 台の syslog サーバを設定できます。
- syslog サーバは、Firepower Threat Defense デバイス 経由で到達できなければなりません。syslog サーバが到達できるインターフェイス上で、デバイスが ICMP 到達不能メッセージを拒否し、同じサーバに syslog を送信するように設定する必要があります。すべての重大度に対してロギングがイネーブルであることを確認します。syslog サーバがクラッシュしないようにするため、syslog 313001、313004、および 313005 の生成を抑制します。
- syslog の UDP 接続の数は、ハードウェアプラットフォームの CPU の数と、設定する syslog サーバの数に直接関連しています。可能な UDP syslog 接続の数は常に、CPU の数と設定する syslog サーバの数を乗算した値と同じになります。たとえば各 syslog サーバでは次のようになります。
  - Firepower 4110 では最大 22 の UDP syslog 接続が可能です。
  - Firepower 4120 では最大 46 の UDP syslog 接続が可能です。

これは予期されている動作です。グローバル UDP 接続アイドル タイムアウトはこれらのセッションに適用され、デフォルトは2分であることを注意してください。これらのセッションをこれよりも短い時間で閉じる場合にはこの設定を調整できますが、タイムアウトは syslog だけでなくすべての UDP 接続に適用されます。

- Firepower Threat Defense デバイス が TCP 経由で syslog を送信すると、syslogd サービスの再起動後、接続の開始に約 1 分かかります。

## Syslog 設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

Syslog の設定を行うには、以下の手順を実行します。

### 手順

- ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2** 目次の [Syslog] をクリックします。

- ステップ 3** [ロギング設定 (Logging Setup)] タブをクリックしてロギングを有効にし、FTP サーバの設定を指定し、フラッシュの使用を指定します。詳細については、次を参照してください。 [ロギングの有効化および基本設定の構成 \(1055 ページ\)](#)
- ステップ 4** [ロギング接続先 (Logging Destinations)] タブをクリックして、特定の接続先へのロギングを有効にし、メッセージ重要度、イベント クラスまたはカスタム イベント リストでフィルタリングを指定します。詳細については、次を参照してください。 [ロギング接続先の有効化 \(1057 ページ\)](#)
- ロギング接続先を有効にして、その接続先でメッセージを表示可能にする必要があります。
- ステップ 5** [電子メール設定 (E-mail Setup)] タブをクリックして、Syslog メッセージを電子メールとして送信する際に、その送信元アドレスとして使用する電子メールアドレスを指定します。詳細については、次を参照してください。 [電子メールアドレスへの syslog メッセージの送信 \(1058 ページ\)](#)
- ステップ 6** [イベントリスト (Events List)] タブをクリックして、イベントクラス、重要度、イベント ID を含むカスタム イベント リストを定義します。詳細については、次を参照してください。 [カスタム イベント リストの作成 \(1059 ページ\)](#)
- ステップ 7** [レート制限 (Rate Limit)] タブをクリックして、設定されているすべての宛先に送信されるメッセージの量を指定し、レート制限を割り当てるメッセージの重大度を定義します。詳細については、次を参照してください。 [Syslog メッセージの生成レートの制限 \(1060 ページ\)](#)
- ステップ 8** [Syslog 設定 (Syslog Settings)] タブをクリックして、サーバを Syslog 接続先として設定するために、ロギング機能を指定し、タイムスタンプの包含を有効にし、他の設定を有効にします。詳細については、次を参照してください。 [Syslog 設定 \(1061 ページ\)](#)
- ステップ 9** [Syslog サーバ (Syslog Servers)] タブをクリックして、ロギング接続先として指定される Syslog サーバの IP アドレス、使用されているプロトコル、形式、およびセキュリティ ゾーンを指定します。詳細については、次を参照してください。 [Syslog サーバの設定 \(1063 ページ\)](#)

## ロギングの有効化および基本設定の構成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

データ プレーン イベントの syslog メッセージを生成するには、システムでロギングを有効にする必要があります。

また、ローカル バッファがいっぱいになると、フラッシュまたは FTP サーバ上のアーカイブを保存場所として設定することもできます。ログ データは保存後に操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたときに特別なアクションが実行されるように指定したり、ログからデータを抽出してレポート用の別のファイルにその記録を保存したり、サイト固有のスクリプトを使用して統計情報を追跡したりできます。

次の手順では、基本的な syslog 設定の一部について説明します。

## 手順

**ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

**ステップ 2** [syslog] > [ロギングの設定 (Logging Setup)] を選択します。

**ステップ 3** ロギングを有効にし、基本のロギング設定を構成します。

- [ロギングの有効化 (Enable Logging)] : Firepower Threat Defense デバイスのデータ プレーン システム ロギングをオンにします。
- フェールオーバー スタンバイ ユニットでのロギングの有効化 (Enable Logging on the Failover Standby Unit) : Firepower Threat Defense デバイスのスタンバイのロギングをオンにします。
- EMBLEM 形式での syslog の送信 (Send syslogs in EMBLEM format) : すべてのロギング宛先に対して、EMBLEM形式のロギングを有効にします。EMBLEMを有効にする場合は、UDPプロトコルを使用して syslog メッセージをパブリッシュする必要があります。EMBLEM は TCP と互換性がありません。
- デバッグ メッセージを syslog として送信 (Send debug messages as syslogs) : すべてのデバッグ トレース出力を syslog にリダイレクトします。このオプションが有効になっている場合、syslog メッセージはコンソールに表示されません。したがって、デバッグ メッセージを表示するには、コンソールでロギングを有効にし、デバッグ syslog メッセージ番号とログ レベルの宛先として設定する必要があります。使用される syslog メッセージ番号は 711011 です。この syslog のデフォルト ログ レベルは [デバッグ (debug)] です。
- 内部バッファのメモリ サイズ (Memory Size of Internal Buffer) : ロギング バッファが有効の場合に syslog メッセージが保存される内部バッファのサイズを指定します。バッファが一杯になった場合は上書きされます。デフォルトは 4096 バイトです。指定できる範囲は 4096 ~ 52428800 です。

**ステップ 4** (オプション) バッファが上書きされる前に、サーバにログバッファの内容を保存するには、FTP サーバを設定します。FTP サーバ情報を指定します。

- FTP サーバ バッファ ラップ (FTP Server Buffer Wrap) : バッファの内容が上書きされる前に FTP サーバに保存するには、このボックスをオンにし、次のフィールドに必要な宛先情報を入力します。FTP 設定を削除するには、このオプションを選択解除します。
- IP アドレス (IP Address) : FTP サーバの IP アドレスを含むホスト ネットワーク オブジェクトを選択します。
- ユーザ名 (User Name) : FTP サーバに接続するときに使用するユーザ名を入力します。
- パス (Path) : バッファの内容を保存するパスを FTP ルートからの相対で入力します。
- パスワードの確認 (Password Confirm) : FTP サーバへのユーザ名の認証に使用されるパスワードを入力および確認します。

**ステップ 5** (オプション) バッファが上書きされる前に、サーバにログバッファの内容を保存するには、フラッシュ サイズを指定します。

- フラッシュ (Flash) : バッファの内容が上書きされる前にフラッシュ メモリに保存するには、このチェックボックスをオンにします。
- ロギングに使用する最大フラッシュ (KB) (Maximum flash to be used by logging (KB)) : フラッシュ メモリ内でロギングに使用される最大領域を指定します (KB)。範囲は、4 ~ 8044176 バイトです。
- 保持する最小空き領域 (KB) (Minimum free space to be preserved (KB)) : フラッシュ メモリに保持する最小空き領域を指定します (KB)。範囲は、0 ~ 8044176 バイトです。

ステップ 6 [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## ロギング接続先の有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ロギング接続先を有効にして、その接続先でメッセージを表示可能にする必要があります。接続先を有効にするとき、その接続先に適用するメッセージフィルタも指定する必要があります。

### 手順

- ステップ 1 [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2 [Syslog] > [ロギング接続先 (Logging Destinations) ] を選択します。 >
- ステップ 3 接続先を有効にし、ロギング フィルタを適用するか、または既存の接続先を編集するには、[追加 (Add) ] をクリックします。
- ステップ 4 [ロギング接続先 (Logging Destinations) ] ダイアログボックスで、接続先を選択し、接続先で使用するフィルタを設定します。
  - a) [ロギング接続先 (Logging Destination) ] ドロップダウンリストで、有効にする接続先を選択します。コンソール、メール、内部バッファ、SNMPトラップ、SSHセッション、Syslog サーバのそれぞれの接続先に各自のフィルタを作成できます。
 

(注) コンソールおよび SSH セッション ロギングは、診断 CLI でのみ機能します。  
**system support diagnostic-cli** を入力します。
  - b) [イベントクラス (Event Class) ] で、テーブルに表示されていないすべてのクラスに適用するフィルタを選択します。

次のフィルタを設定できます。

- [重大度によるフィルタ (Filter on severity) ] : 重大度のレベルを選択します。設定したレベル以上のメッセージが接続先に送られます。
- [イベントリスト使用 (Use Event List) ] : フィルタを定義するイベントリストを選択します。このイベントリストは [イベントリスト (Event Lists) ] タブで作成します。
- [ロギング無効 (Disable Logging) ] : この接続先へのメッセージ送信を停止します。

c) イベントクラスごとのフィルタを作成するには、[追加 (Add) ] をクリックして新しいフィルタを作成するか、既存のフィルタを編集し、そのクラスでのメッセージを制限するイベントクラスと重大度レベルを選択します。[OK] をクリックして、フィルタを保存します。

イベントクラスの説明については、[syslog メッセージクラス \(1051 ページ\)](#) を参照してください。

d) [OK] をクリックします。

**ステップ 5** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## 電子メールアドレスへの **syslog** メッセージの送信

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

電子メールとして送信される syslog メッセージの受信者リストを設定できます。

### 始める前に

- SMTP サーバのプラットフォーム設定ページで SMTP サーバを設定します
- [ロギングの有効化および基本設定の構成 \(1055 ページ\)](#)
- [ロギング接続先の有効化](#)

### 手順

**ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

**ステップ 2** [Syslog] > [電子メールの設定 (Email Setup) ] を選択します。



- ステップ 3** 電子メール メッセージとして送信される syslog メッセージの送信元アドレスとして使用する電子メール アドレスを指定します。
- ステップ 4** [追加 (Add) ] をクリックして、指定した syslog メッセージの受信者の新しい電子メール アドレスを入力します。
- ステップ 5** その受信者に送信する syslog メッセージの重大度レベルを、ドロップダウンリストから選択します。
- 宛先の電子メール アドレスに対して適用される syslog メッセージの重大度フィルタにより、指定された重大度レベル以上のメッセージが送信されます。レベルについては、[重大度 \(1050 ページ\)](#) を参照してください。
- ステップ 6** [OK] をクリックします。
- ステップ 7** [保存 (Save) ] をクリックします。
- これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## カスタム イベント リストの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

イベントリストは、ロギング接続先に適用して接続先に送信するメッセージを制御できるカスタムフィルタです。通常、重大度のみに基づいて接続先へのメッセージをフィルタリングしますが、イベントリストを使用して、イベントクラス、重大度、およびメッセージ識別子 (ID) の組み合わせに基づいて送信されるメッセージを微調整できます。

カスタム イベント リストの作成は、2 段階のプロセスです。[イベントリスト (Event Lists) ] タブでカスタム リストを作成し、イベントリストを使用して、[宛先のロギング (Logging Destinations) ] タブで各種宛先のロギング フィルタを定義します。

### 手順

- ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2** [Syslog] > [イベントリスト (Events List) ] を選択します。
- ステップ 3** イベントリストを設定します。
- a) [追加 (Add) ] をクリックして新規リストを追加したり、既存のリストを編集したりします。

- b) [名前 (Name) ]フィールドにイベントリストの名前を入力します。スペースは使用できません。
- c) 重大度またはイベントクラスに基づいてメッセージを識別するには、[重大度/イベントクラス (Severity/Event Class) ]タブを選択して、項目を追加または編集します。

使用可能なクラスの詳細については、[syslog メッセージクラス \(1051 ページ\)](#) を参照してください。

レベルについては、[重大度 \(1050 ページ\)](#) を参照してください。

特定のイベントクラスは、トランスペアレント モードのデバイスには適用されません。そのようなオプションが設定された場合、オプションは無視され、展開されません。

- d) メッセージ ID を指定してメッセージを識別するには、[メッセージ ID (Message ID) ]タブを選択し、ID を追加または編集します。

ハイフンを使用して ID 範囲を入力できます (たとえば、100000-200000)。ID は 6 桁の数字です。最初の 3 桁が機能にどのようにマップされるかについては、[syslog メッセージクラス \(1051 ページ\)](#) を参照してください。

特定のメッセージ番号については、『[Cisco ASA Series Syslog Messages](#)』を参照してください。

- e) [OK] をクリックして、イベントリストを保存します。

**ステップ 4** [ロギング接続先 (Logging Destinations) ]タブをクリックし、フィルタを使用する必要がある接続先を追加または編集します。

[ロギング接続先の有効化 \(1057 ページ\)](#) を参照してください。

**ステップ 5** [保存 (Save) ]をクリックします。

これで、[展開 (Deploy) ]をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## Syslog メッセージの生成レートの制限

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

syslog メッセージの生成レートは、重大度レベルまたはメッセージ ID によって制限できます。ロギング レベルごと、および Syslog メッセージ ID ごとに個別の制限を指定できます。設定が競合する場合は、Syslog メッセージ ID の制限が優先されます。

手順

- ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2** [Syslog] > [レート制限 (Rate Limit) ] を選択します。
- ステップ 3** 重大度レベルによりメッセージの生成を制限するには、[ログレベル (Logging Level) ] タブで [追加 (Add) ] をクリックして、次のオプションを設定します。
- ログレベル (Logging Level) : レートを制限する重大度レベル。レベルについては、[重大度 \(1050 ページ\)](#) を参照してください。
  - メッセージ数 (Number of messages) : 指定した時間内に許容される指定したタイプのメッセージの最大数。
  - 間隔 (Interval) : レート制限カウンタがリセットされるまでの秒数。
- ステップ 4** [OK] をクリックします。
- ステップ 5** syslog のメッセージ ID によりメッセージの生成を制限するには、[Syslog レベル (Syslog Level) ] タブで [追加 (Add) ] をクリックし、次のオプションを設定します。
- [Syslog ID] : レートを制限する syslog のメッセージ ID。特定のメッセージ番号については、『[Cisco ASA Series Syslog Messages](#)』を参照してください。
  - メッセージ数 (Number of messages) : 指定した時間内に許容される指定したタイプのメッセージの最大数。
  - 間隔 (Interval) : レート制限カウンタがリセットされるまでの秒数。
- ステップ 6** [OK] をクリックします。
- ステップ 7** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## Syslog 設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

一般的な Syslog 設定を設定して、Syslog サーバに送信される Syslog メッセージに含めるファシリティコードの設定、各メッセージにタイムスタンプが含まれるかどうかの指定、メッセージに含めるデバイス ID の指定、メッセージの重大度レベルの表示と変更、および特定のメッセージの生成のディセーブル化を行うことができます。

手順

- 
- ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2** [Syslog] > [Syslog 設定 (Syslog Settings) ] を選択します。 >
- ステップ 3** ファイルメッセージのベースとして使用する Syslog サーバのシステム ログ機能を、[ファシリティ (Facility) ] ドロップダウンリストから選択します。
- デフォルトは LOCAL4(20) です。これは UNIX システムで最も可能性の高いコードです。ただし、ネットワーク デバイス間では使用可能なファシリティが共有されているため、システム ログではこの値を変更しなければならない場合があります。
- ステップ 4** [タイムスタンプを各 Syslog メッセージで有効にする (Enable timestamp on each syslog message) ] チェックボックスをオンにして、メッセージ生成日時を Syslog メッセージに含めます。
- ステップ 5** デバイス識別子を Syslog メッセージに追加する場合は (これはメッセージの先頭に配置されます) 、[Syslog デバイス ID を有効にする (Enable Syslog Device ID) ] チェックボックスをオンにし、ID のタイプを選択します。
- [インターフェイス (Interface) ] : アプライアンスがメッセージの送信に使用するインターフェイスに関係なく、選択されたインターフェイスの IP アドレスを使用します。インターフェイスを識別するセキュリティゾーンを選択します。ゾーンは、単一のインターフェイスにマッピングされる必要があります。
  - [ユーザー定義 ID (User Defined ID) ] : 選択したテキスト文字列を使用します (最大 16 文字) 。
  - [ホスト名 (Host Name) ] : デバイスのホスト名を使用します。
- ステップ 6** [Syslog Message] テーブルを使用して、特定の Syslog メッセージのデフォルト設定を変更します。デフォルト設定を変更する場合にだけ、このテーブルでルールを設定する必要があります。メッセージに割り当てられている重大度を変更したり、メッセージの生成を無効にしたりできます。
- デフォルトでは、NetFlow が有効になり、エントリはテーブルに表示されます。
- a) NetFlow が原因で冗長している Syslog メッセージを抑制するには、[ネットワーク同等 Syslog (Netflow Equivalent Syslogs) ] を選択します。
- これにより、メッセージが抑止されたメッセージとしてテーブルに追加されます。
- (注) これらの同等の Syslog メッセージがすでにテーブルにある場合、既存のルールは上書きされません。
- b) ルールを追加するには、[追加 (Add) ] ボタンをクリックします。
- c) 設定変更するメッセージ番号を [Syslog ID] ドロップダウンリストから選択し、新しい重大度を [ロギング レベル (Logging Level) ] ドロップダウンリストから選択するか、または [抑制 (Suppressed) ] を選択してメッセージの生成を無効にします。通常は、重大度レベルの変更やメッセージのディセーブル化は行いませんが、必要に応じて両方のフィールドを変更できます。

d) [OK] をクリックしてテーブルにルールを追加します。

**ステップ 7** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## Syslog サーバの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

データ プレーンから生成されたメッセージを処理するように syslog サーバを設定するには、次の手順を実行します。

アクセス コントロールルールなど、接続やその他のイベントのために syslog サーバを設定するには、[Syslog アラート応答の作成 \(2344 ページ\)](#) を参照してください。

### 手順

- ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2** [Syslog] > [Syslog サーバ (Syslog Server) ] > を選択します。
- ステップ 3** [TCP syslog サーバのダウン時ユーザトラフィックの通過を許可 (Allow user traffic to pass when TCP syslog server is down) ] チェックボックスをオンにして、TCP プロトコルを使用する Syslog サーバがダウンしている場合にトラフィックを許可するようにします。
- ステップ 4** [メッセージキュー サイズ (メッセージ) (Message queue size (messages)) ] フィールドに、Syslog サーバが取り込み中の場合に、Syslog メッセージをセキュリティアプライアンスに保存するキューのサイズを入力します。最小件数は 1 件です。デフォルトは 512 です。無制限の数のメッセージをキューに入れる場合は、0 を指定します (使用可能なブロックメモリによって制限されます) 。
- ステップ 5** [追加 (Add) ] をクリックして、新しい Syslog サーバを追加します。
- [IP アドレス (IP Address) ] ドロップダウンリストで、Syslog サーバの IP アドレスを含むネットワーク ホストオブジェクトを選択します。
  - プロトコル (TCP または UDP) を選択し、Firepower Threat Defense デバイスと Syslog サーバの間の通信のポート番号を入力します。

UDP のデフォルト ポートは 514、TCP のデフォルト ポートは 1470 です。有効な非デフォルトのポート値は、どちらのプロトコルでも 1025 ~ 65535 です。

- c) [Cisco EMBLEM 形式でのログ メッセージ (UDP のみ) (Log messages in Cisco EMBLEM format (UDP only))] チェックボックスをオンにして、Cisco の EMBLEM 形式でメッセージをログに記録するかどうかを指定します (プロトコルとして UDP が選択されている場合に限る)。
- d) Syslog サーバとの通信に使用するインターフェイスを含むゾーンを追加します。ゾーンにないインターフェイスでは、[選択されたゾーン/インターフェイス (Selected Zones/Interface)] リストの下のフィールドにインターフェイス名を入力し、[追加 (Add)] をクリックします。選択されているインターフェイスまたはゾーンがデバイスに含まれているときにのみ、これらのルールがデバイスに適用されます。

(注) Syslog サーバが物理管理インターフェイスに接続されたネットワーク上にある場合は、そのインターフェイスの名前を [選択したセキュリティ ゾーン (Selected Security Zones)] リストの下の [インターフェイス名 (Interface Name)] フィールドに入力し、[追加 (Add)] をクリックする必要があります。また、診断インターフェイスにこの名前 (まだ設定されていない場合) と IP アドレスを設定する必要があります ([デバイス管理 (Device Management)] ページからデバイスを編集し、[インターフェイス (Interfaces)] タブを選択します)。管理/診断インターフェイスの詳細については、[診断インターフェイス \(650 ページ\)](#) を参照してください。

- e) [OK] をクリックします。

**ステップ 6** [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## グローバル タイムアウトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

さまざまなプロトコルの接続スロットと変換スロットのグローバルアイドルタイムアウト期間を設定できます。指定したアイドル時間の間スロットが使用されなかった場合、リソースはフリープールに戻されます。

また、デバイスのコンソールセッションでタイムアウトを設定できます。

## 手順

**ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

**ステップ 2** [タイムアウト (Timeouts) ] を選択します。

**ステップ 3** 変更するタイムアウトを設定します。

任意の設定で、[カスタム (Custom) ] を選択して自分の値を定義し、[デフォルト (Default) ] を選択してシステムのデフォルト値に戻します。ほとんどの場合、最大タイムアウトは 1193 時間です。

[無効 (Disable) ] を選択して、タイムアウトを無効にできます。

- [コンソールタイムアウト (Console Timeout) ] : コンソールへの接続が閉じられるまでのアイドル時間。範囲は 0 ~ 60、分です。デフォルトは 0 で、セッションがタイムアウトしないことを示します。値を変更すると、既存のコンソールセッションで古いタイムアウト値が使用されます。新しい値は新しい接続にのみ適用されます。
- [変換スロット (Translation Slot (xlate)) ] : NAT 変換スロットが解放されるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 3 時間です。
- [接続 (Connection (Conn)) ] : 接続スロットが解放されるまでのアイドル時間。この期間は 5 分以上にする必要があります。デフォルトは 1 時間です。
- [ハーフクローズ (Half-Closed) ] : TCP ハーフクローズ接続を閉じるまでのアイドル時間。最小値は 30 秒です。デフォルト値は 10 分です。
- [UDP] : UDP 接続を閉じるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 2 分です。
- [ICMP] : 全般的な ICMP 状態が終了するまでのアイドル時間。デフォルト (かつ最小値) は 2 秒です。
- [RPC/SunRPC] : SunRPC スロットが解放されるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルト値は 10 分です。
- [H.225] : H.225 シグナリング接続を閉じるまでのアイドル時間。デフォルトは 1 時間です。すべての呼び出しがクリアされた後に接続をすぐにクローズするには、タイムアウト値を 1 秒 (0:0:1) にすることを推奨します。
- [H.323] : H.245 (TCP) および H.323 (UDP) メディア接続が終了するまでのアイドル時間。デフォルト (かつ最小値) は 5 分です。H.245 と H.323 のいずれのメディア接続にも同じ接続フラグが設定されているため、H.245 (TCP) 接続は H.323 (RTP および RTCP) メディア接続とアイドルタイムアウトを共有します。
- [SIP] : SIP シグナリングポート接続を閉じるまでのアイドル時間。この期間は 5 分以上にする必要があります。デフォルトは 30 分です。
- [SIP メディア (SIP Media) ] : SIP メディアポート接続を閉じるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 2 分です。SIP メディアタイマー

は、SIP UDP メディア パケットを使用する SIP RTP/RTCP で、UDP 非アクティブ タイムアウトの代わりに使用されます。

- [SIP 接続解除 (SIP Disconnect) ] : CANCEL メッセージまたは BYE メッセージで 200 OK を受信しなかった場合に、SIP セッションを削除するまでのアイドル時間を 0:0:1 ~ 0:10:0 の範囲で指定します。デフォルトは、2 分 (0:2:0) です。
- [SIP インバイト (SIP Invite) ] : 暫定応答のピンホールとメディア xlate を閉じるまでのアイドル時間 (0:1:0 ~ 00:30:0) 。デフォルトは、3 分 (0:3:0) です。
- [SIP 暫定メディア (SIP Provisional Media) ] : SIP 暫定メディア接続のタイムアウト値 (1 ~ 30 分) 。デフォルトは 2 分です。
- [フローティング接続 (Floating Connection) ] : 同じネットワークへの複数のルートが存在しており、それぞれメトリックが異なる場合、ASA は接続確立時点でメトリックが最良のルートを使用します。より適切なルートが使用可能になった場合は、このタイムアウトによって接続が閉じられるので、その適切なルートを使用して接続を再確立できます。デフォルトは 0 です (接続はタイムアウトしません) 。より良いルートを使用できるようにするには、タイムアウト値を 0:0:30 ~ 1193:0:0 の間で設定します。
- [ARP タイムアウト (ARP Timeout) ] : (トランスペアレントモードのみ) 。ARP テーブルを再構築する間隔の秒数 (60 ~ 4294967) 。デフォルトは 14,400 秒 (4 時間) です。

ステップ 4 [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## 脅威に対する防御のための NTP 時刻同期の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

Network Time Protocol (NTP) を使用して、デバイスのクロック設定を同期します。デフォルトでは、デバイスは Firepower Management Center サーバを NTP サーバとして使用しますが、別の NTP サーバを設定することができます。



## 手順

**ステップ 1** [デバイス (Devices) ] > [プラットフォーム設定 (Platform Settings) ] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

**ステップ 2** [時間の同期化 (Time Synchronization) ] を選択します。

**ステップ 3** 次のいずれかのクロック オプションを設定します。

- [デフェンスセンターの NTP 使用 (Via NTP from Defense Center) ] : Firepower Management Center サーバを NTP サーバとして使用します。これがデフォルトです。
- [その他の NTP 使用 (Via NTP from) ] : 別の NTP サーバの完全修飾 DNS 名 (ntp.example.com など) または IP アドレスを入力します。複数のアドレスを入力する場合は、各アドレスをカンマで区切ります (例 : ntp1.example.com, ntp2.example.com) 。

**ステップ 4** [保存 (Save) ] をクリックします。

これで、[展開 (Deploy) ] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。





## 第 **XIII** 部

# ネットワーク アドレス変換 (NAT)

- [NAT ポリシー管理 \(1071 ページ\)](#)
- [7000 および 8000 シリーズ デバイス用の NAT \(1079 ページ\)](#)
- [Firepower Threat Defense 用のネットワーク アドレス変換 \(NAT\) \(1101 ページ\)](#)





## 第 45 章

# NAT ポリシー管理

以下のトピックでは、Firepower システム用の NAT ポリシーを管理する方法について説明します。

- [NAT ポリシーの管理 \(1071 ページ\)](#)
- [NAT ポリシーの作成 \(1072 ページ\)](#)
- [NAT ポリシーの設定 \(1074 ページ\)](#)
- [NAT ポリシーの対象の設定 \(1075 ページ\)](#)
- [NAT ポリシーのコピー \(1076 ページ\)](#)

## NAT ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin





マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカル ポリシーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

### 手順

ステップ 1 [デバイス (Devices)] > [NAT] を選択します。

ステップ2 NAT ポリシーを管理します。

- コピー：コピーするポリシーの横にあるコピーアイコン () をクリックします。 [NAT ポリシーのコピー \(1076 ページ\)](#) を参照してください。
  - 作成：[新規ポリシー (New Policy)] をクリックします。 [NAT ポリシーの作成 \(1072 ページ\)](#) を参照してください。
  - 削除：削除するポリシーの横にある削除アイコン () をクリックして、[OK] をクリックします。続行するかどうかを尋ねるプロンプトで、ポリシー内に別のユーザの未保存の変更が存在するかどうかも通知されます。
- 注意** 管理対象デバイスに NAT ポリシーを展開した後は、デバイスからそのポリシーを削除できません。その代わりに、ルールを持たない NAT ポリシーを展開して、すでに管理対象デバイスに存在する NAT ルールを削除する必要があります。また、どのターゲットデバイスでも、最後に展開したポリシーは期限切れであっても削除できません。ポリシーを完全に削除する前に、それらのターゲットに異なるポリシーを展開する必要があります。
- 展開：[展開 (Deploy)] をクリックします ([設定変更の導入 \(350 ページ\)](#) を参照)。
  - 編集：編集アイコン () をクリックします。 [NAT ポリシーの設定 \(1074 ページ\)](#) を参照してください。
  - [レポート (Report)]：レポートアイコン () をクリックします ([現在のポリシー レポートの生成 \(363 ページ\)](#) を参照)。

## NAT ポリシーの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

新しい NAT ポリシーを作成する場合、少なくとも一意の名前を付ける必要があります。ポリシーの作成時にポリシー ターゲットを特定する必要はありませんが、ポリシーを展開する前に、この手順を実行する必要があります。ルールを持たない NAT ポリシーをデバイスに適用すると、そのデバイスからすべての NAT ルールが削除されます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカル ポリシーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

## 手順

**ステップ 1** [デバイス (Devices) ] > [NAT] を選択します。

**ステップ 2** [新しいポリシー (New Policy) ] ドロップダウン リストで、以下のいずれかを選択します。


- 7000 & 8000 シリーズ デバイスの場合は [Firepower NAT]。
- Firepower Threat Defense デバイスの場合は [脅威に対する防御 NAT (Threat Defense NAT) ]。

**ステップ 3** [名前 (Name) ] に一意の名前を入力します。

マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

**ステップ 4** 必要に応じて、[説明 (Description) ] を入力します。

**ステップ 5** ポリシーを展開するデバイスを選択します。

- [使用可能なデバイス (Available Devices) ] リストでデバイスを選択し、[ポリシーに追加 (Add to Policy) ] をクリックします。
- [使用可能なデバイス (Available Devices) ] リストから [選択されたデバイス (Selected Devices) ] リストに、デバイスをクリックしてドラッグします。
- デバイスの横にある削除アイコン (  ) をクリックして、[選択されたデバイス (Selected Devices) ] リストからデバイスを削除します。

**ステップ 6** [保存 (Save) ] をクリックします。

## 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## NAT ポリシーの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカルポリシーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

インターフェイスのタイプを、そのインターフェイスがあるデバイスを対象とする NAT ポリシーでの使用が無効なタイプに変更した場合、ポリシーはそのインターフェイスに削除済みのラベルを付けます。NAT ポリシーの [保存 (Save)] をクリックすると、インターフェイスはポリシーから自動的に削除されます。



- (注) ルール属性は NAT ポリシー タイプによって異なります。ルールを追加または編集する場合、詳細については、ダイアログボックスで [?] をクリックするか、関連する章 [Firepower Threat Defense 用のネットワーク アドレス変換 \(NAT\) \(1101 ページ\)](#) または [7000 および 8000 シリーズ デバイス用の NAT \(1079 ページ\)](#) を参照してください。

### 手順

**ステップ 1** [デバイス (Devices)] > [NAT] を選択します。

**ステップ 2** 変更する NAT ポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** NAT ポリシーを設定します。

- ポリシー名や説明を変更するには、[名前 (Name)] または [説明 (Description)] フィールドをクリックし、必要に応じて文字を削除し、新しい名前または説明を入力します。マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システ



ムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

- ポリシーの対象を管理するには、[NAT ポリシーの対象の設定 \(1075 ページ\)](#) を参照してください。
- ポリシーの変更を保存するには、[保存 (Save)] をクリックします。
- ポリシーにルールを追加するには、[ルールの追加 (Add Rule)] をクリックします。
- 既存のルールを編集するには、ルールの横にある編集アイコン (✎) をクリックします。
- ルールを削除するには、ルールの横にある削除アイコン (🗑) をクリックし、[OK] をクリックします。
- 既存のルールを有効または無効にするには、ルールを右クリックして [状態 (State)] を選択し、[無効化 (Disable)] または [有効化 (Enable)] を選択します。
- (Firepower NAT のみ。) 特定のルール属性の設定ページを表示するには、ルールの行にある条件の列で名前、値、またはアイコンをクリックします。たとえば、[送信元ネットワーク (Source Networks)] 列の名前または値をクリックすると、選択したルールの [送信元ネットワーク (Source Networks)] ページが表示されます。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## NAT ポリシーの対象の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ポリシーを適用する管理対象デバイスは、ポリシーを作成または編集する際に特定できます。使用可能なデバイス、7000 または 8000 シリーズ スタック、および高可用性ペアのリストを検索して、選択したデバイスのリストに追加できます。

異なるバージョンの Firepower システムを実行中のスタック構成デバイスを対象にすることはできません (たとえば、デバイスのいずれかでアップグレードが失敗した場合)。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカル ポリ

シーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

## 手順

**ステップ 1** [デバイス (Devices) ] > [NAT] を選択します。

**ステップ 2** 変更する NAT ポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** [ポリシー割り当て (Policy Assignments) ] をクリックします。

**ステップ 4** 次のいずれかを実行します。

- デバイス、スタック、高可用性ペア、またはデバイスグループをポリシーに割り当てるには、[使用可能なデバイス (Available Devices) ] リストで選択し、[ポリシーに追加 (Add to Policy) ] をクリックします。ドラッグアンドドロップを使用することもできます。
- デバイスの割り当てを削除するには、[選択されたデバイス (Selected Device) ] リストのデバイス、スタック、高可用性ペア、またはデバイスグループの横にある削除アイコン (🗑) をクリックします。

**ステップ 5** [OK] をクリック

## 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

# NAT ポリシーのコピー

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin


NAT ポリシーのコピーを作成できます。コピーには、ポリシーのすべてのルールと設定が含まれます。

マルチドメイン導入では、現在のドメインおよび先祖ドメインからポリシーをコピーできます。

## 手順

---

**ステップ 1** [デバイス (Devices) ] > [NAT] を選択します。

**ステップ 2** コピーする NAT ポリシーの横にあるコピー アイコン () をクリックします。

**ステップ 3** [名前 (Name) ] に、ポリシーの一意の名前を入力します。

マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

**ステップ 4** [OK] をクリックします。

---





## 第 46 章

# 7000 および 8000 シリーズ デバイス用の NAT

以下のトピックでは、7000 および 8000 シリーズ デバイス用に NAT を設定する方法を示します。

- [NAT ポリシーの設定 \(1079 ページ\)](#)
- [NAT ポリシー内のルール編成 \(1081 ページ\)](#)
- [NAT ルールの編成 \(1082 ページ\)](#)
- [NAT ポリシー規則のオプション \(1083 ページ\)](#)

## NAT ポリシーの設定

特定のネットワーク ニーズを管理するためにさまざまな方法で NAT ポリシーを設定できます。次の操作を実行できます。

- 外部ネットワークに内部サーバを公開します。

この設定では、外部 IP アドレスから内部 IP アドレスへのスタティック変換を定義するため、システムはネットワーク外部から内部サーバにアクセスできます。サーバに送信されるトラフィックは、外部 IP アドレスまたは IP アドレスとポートを対象とし、内部 IP アドレスまたは IP アドレスとポートに変換されます。サーバからのリターントラフィックは、外部アドレスに再度変換されます。

- 内部ホスト/サーバが外部アプリケーションに接続できるようにします。

この設定では、内部アドレスから外部アドレスへのスタティック変換を定義します。この定義により、内部ホストまたはサーバは、内部ホストまたはサーバが特定の IP アドレスおよびポートを持っていると予期する外部アプリケーションへの接続を開始できます。したがって、システムは内部ホストまたはサーバのアドレスを動的に割り当てることはできません。

- 外部ネットワークに対してプライベート ネットワーク アドレスを隠します。

以下のいずれかの設定を使用して、内部ネットワークアドレスをわかりにくくすることができます。

- 内部ネットワークの必要に十分対応できるだけの数の外部 IP アドレスがある場合は、IP アドレスのブロックを使用できます。この設定では、すべての発信トラフィックの

送信元 IP アドレスを、外部に面する IP アドレスのうち未使用の IP アドレスに自動的に変換するダイナミック変換を作成します。

- 内部ネットワークの必要に対応できるだけの数の外部 IP アドレスがない場合は、限定した数の IP アドレスのブロックとポート変換を使用できます。この設定では、発信トラフィックの送信元 IP アドレスとポートを、外部に面する IP アドレスのうち未使用の IP アドレスとポートに自動的に変換するダイナミック変換を作成します。



**注意** 7000 または 8000 シリーズ デバイスの高可用性ペアでは、NAT 変換により影響を受けるすべてのネットワークがプライベートの場合、ペアを構成するデバイス上でのスタティック NAT ルールに対して個別のピア インターフェイスのみを選択します。パブリック ネットワークとプライベート ネットワーク間のトラフィックに影響するスタティック NAT ルールには、この設定を使用しないでください。

## NAT ポリシーの設定ガイドライン

NAT ポリシーを設定するには、ポリシーに一意の名前を付け、ポリシーを展開するデバイスつまりターゲットを特定する必要があります。また、NAT ルールを追加、編集、削除、有効化、および無効化することができます。NAT ポリシーを作成または変更した後、ターゲットデバイスのすべてまたは一部にポリシーを展開できます。

スタンドアロンデバイスと同様に、NAT ポリシーをペアリングされたスタックを含む 7000 または 8000 シリーズ デバイス高可用性ペアに展開できます。ただし、個別のペアリングされたデバイスまたは高可用性ペア全体でインターフェイスのスタティック NAT ルールを定義し、送信元ゾーン内でインターフェイスを使用できます。ダイナミックルールの場合、送信元ゾーンまたは宛先ゾーンで高可用性ペア全体のインターフェイスのみを使用できます。



**注意** 7000 または 8000 シリーズ デバイス高可用性ペアで、NAT 変換により影響を受けるすべてのネットワークがプライベートの場合、ペアリングされたデバイスのスタティック NAT ルールに対して、個別のピア インターフェイスのみを選択します。パブリック ネットワークとプライベート ネットワーク間のトラフィックに影響するスタティック NAT ルールに対してこの設定を使用しないでください。

HA リンク インターフェイスが確立されていないデバイス高可用性ペアでダイナミック NAT を設定した場合、両方のペアリングされたデバイスは別々にダイナミック NAT エントリを割り当て、システムはデバイス間でエントリを同期できません。

スタンドアロン デバイスと同様に、NAT ポリシーをデバイス スタックに展開できます。NAT ポリシーに含まれ、スタックのメンバーであるセカンダリデバイスのインターフェイスに関連付けられているルールを持ったデバイスからデバイス スタックを確立した場合、セカンダリデバイスのインターフェイスは NAT ポリシーに残ります。インターフェイスを持つポリシーを保存および展開できますが、ルールは変換を実現しません。

先祖ドメインのマルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。管理者は、NAT ポリシーのターゲットを子孫ドメインのデバイスに設定できます。こうすることで、子孫ドメインではカスタマイズされたローカルポリシーを使用または置き換えることができます。

## NAT ポリシー内のルール編成

NAT ポリシーの編集ページにはスタティックな NAT ルールとダイナミックな NAT ルールが別々に表示されます。このシステムでは、スタティックルールは名前のアルファベット順に並べ替えられ、表示順序を変更できません。同一の照合値を持つスタティックルールは作成できません。システムの照合では、ダイナミック変換を検査する前に、スタティック変換を検査します。

ダイナミックルールは番号順に処理されます。各ダイナミックルールの番号位置は、ページ左側のルールの横に表示されます。ダイナミックルールは移動または挿入したり、ルールの順序を変更したりすることができます。たとえば、ダイナミックルール 10 をダイナミックルール 3 の下に移動した場合、ルール 10 がルール 4 になり、後に続くすべての番号が順次繰り上がります。

このシステムでは、ポリシーの編集ページ上のルールの番号順にパケットとダイナミックルールを比較するので、ダイナミックルールの位置は重要です。パケットがダイナミックルールのすべての条件を満たすと、システムはパケットにそのルール条件を適用し、そのパケットに対する後続のルールはすべて無視します。

ダイナミックルールを追加または編集する際、ダイナミックルールの番号の位置を指定できます。新しいダイナミックルールを追加する前にダイナミックルールを強調表示して、強調表示したルールの下に新しいルールを挿入することもできます。

ルールの行内の空白部分をクリックすることにより、1つ以上のダイナミックルールを選択できます。選択したダイナミックルールを新しい場所にドラッグアンドドロップできます。これにより、移動したルールと後続のすべてのルールの位置が変更されます。

選択したルールを既存のルールの上または下にカット アンドペーストできます。スタティックルールはスタティック変換リストにのみ、ダイナミックルールはダイナミック変換リストにのみ貼り付けることができます。また、選択したルールを削除したり、既存のルールリスト内の任意の場所に新しいルールを挿入したりすることもできます。

先行ルールが優先して適用されるために決して一致することがないルールを示す、説明的な警告を表示することもできます。

展開にアクセスコントロールポリシーが存在する場合、このシステムではアクセス制御を通過するまでトラフィックを変換することはありません。

## NAT ルールの編成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

### 手順

**ステップ 1** [デバイス (Devices)] > [NAT] を選択します。

**ステップ 2** 変更する NAT ポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** NAT ルールを編成します。

- ルールを選択するには、ルールのある行の空白部分をクリックします。
- ルールの選択をクリアするには、ページの右下にあるリロードアイコン (🔄) をクリックします。個別のルールをクリアするには、Ctrl キーを押しながら各ルールの行内の空白部分をクリックします。
- 選択したルールを切り取りまたはコピーするには、選択したルールのある行の空白部分を右クリックして、[切り取り (Cut)] または [コピー (Copy)] を選択します。
- 切り取ったルールまたはコピーしたルールをルールリストに貼り付けるには、選択したルールを貼り付けるルールのある行の空白部分を右クリックして、[上に貼り付け (Paste above)] または [下に貼り付け (Paste below)] を選択します。
- 選択したルールを移動するには、選択したルールを新しい位置の下にドラッグアンドドロップします。この移動先の位置は、ドラッグ時にポインタの上に表示される青い横線で示されます。
- ルールを削除するには、ルールのある横にある削除アイコン (🗑️) をクリックして、[OK] をクリックします。
- 警告を表示するには、[警告の表示 (Show Warnings)] をクリックします。

## NAT ルールの警告とエラー

NAT ルールの条件が後続のルールによるトラフィックの照合をプリエンブション処理する場合があります。どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。



あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールは回避されます。いずれかの条件が異なっていた場合、後続のルールはブリエンプション処理されません。

NAT ポリシーの展開失敗の原因となるルールを作成した場合、ルールの横にエラー アイコン (❗) が表示されます。スタティック ルールに矛盾がある場合、または現時点で無効となるポリシーで使用されるネットワーク オブジェクトを編集した場合、エラーが発生します。たとえば、IPv6 アドレスのみを使用するようにネットワーク オブジェクトを変更した結果、少なくとも1つのネットワークが必要な状況で、そのオブジェクトを使用するルールに有効なネットワークがなくなると、エラーが発生します。エラー アイコンは自動的に表示されます。[警告を表示 (Show Warnings)] をクリックする必要はありません。

## NAT ルール警告の表示と非表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

### 手順

**ステップ 1** [デバイス (Devices)] > [NAT] を選択します。

**ステップ 2** 変更する NAT ポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔔) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** 警告を表示するには、[警告を表示 (Show Warnings)] をクリックします。

ページが更新され、ブリエンプション処理された各ルールの横に警告アイコン (⚠) が表示されます。

**ステップ 4** ルールの警告を表示するには、ルールの横にある警告アイコン (⚠) の上にポインタを合わせます。

ルールをブリエンプション処理するルールを示すメッセージが表示されます。

**ステップ 5** 警告をクリアするには、[警告を非表示 (Hide Warnings)] をクリックします。

ページが更新され、警告が消えます。

## NAT ポリシー規則のオプション

NAT ルールは次の働きを持つ設定および条件のセットです。

- ネットワーク トラフィックを限定する

- 条件に一致するトラフィックの変換方法を指定する

既存の NAT ポリシーから NAT ルールを作成および編集します。各ルールは 1 つのポリシーにのみ属します。

ルールの追加と編集は同様の Web インターフェイスで行います。ページの上でルールの名前、状態、タイプ、および位置 (ダイナミックの場合) を指定します。ページの左側のタブを使用して、条件を構築します。条件タイプごとに独自のタブがあります。

次のリストは、NAT ルールの設定可能なコンポーネントを示しています。

### [名前 (Name)]

各ルールに一意の名前を付けます。スタティック NAT ルールでは、最大 22 文字を使用します。ダイナミック NAT ルールでは、最大 30 文字を使用します。印刷可能文字を使用できません。スペースや特殊文字を含めることができますが、コロン (:) は使用できません。

### ルール状態 (Rule State)

デフォルトでは、ルールは有効になっています。ルールを無効にすると、変換用のネットワークトラフィックの評価に使用されません。NAT ポリシーのルールリストを表示すると、無効なルールはグレー表示されますが、変更は可能です。

### タイプ (Type)

ルールのタイプによって、ルールの条件に一致するトラフィックの処理方法が決まります。NAT ルールを作成および編集する際、設定可能なコンポーネントはルールタイプによって異なります。

### 位置 (Position) (ダイナミック ルールのみ)

NAT ポリシーのダイナミックルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、NAT ルールを上から順にトラフィックと照合します。

ルールをポリシーに追加する際、参照ポイントとしてルール番号を使用し、特定のルールの上または下に配置することによって位置を指定します。既存のルールを編集するときには、同様の方法でルールを移動できます。

### 条件 (Conditions)

ルール条件は変換する特定のトラフィックを識別します。条件はセキュリティゾーン、ネットワーク、および転送プロトコルのポートなど、複数の属性を任意に組み合わせてトラフィックと照合できます。

### 関連トピック

[NAT ルールの作成および編集 \(1085 ページ\)](#)

## NAT ルールの作成および編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

マルチドメイン導入では、現在のドメインで作成されたポリシーとルールが表示されます。これは編集できます。先祖ドメインで作成されたポリシーとルールも表示されますが、これは編集できません。下位のドメインで作成されたルールを表示および編集するには、そのドメインに切り替えます。

### 手順

**ステップ 1** [デバイス (Devices) ] > [NAT] を選択します。

**ステップ 2** ルールを追加する NAT ポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** 新しいルールを追加するか、既存のルールを編集します。

- 新しいルールを追加するには、[ルールの追加 (Add Rule) ] をクリックします。
- 既存のルールを編集するには、そのルールの横にある編集アイコン (✎) をクリックします。

**ステップ 4** [名前 (Name) ] に一意のルール名を入力します。

**ステップ 5** 次のルール コンポーネントを設定します。

- ルールを**有効**にするかどうかを指定します。
- [タイプ (Type) ] で、ルール タイプを指定します。
- ルールの位置 (ダイナミック ルールのみ) を指定します。
- ルールの条件を設定します。

(注) スタティック ルールは元の宛先ネットワークを含む必要があります。ダイナミック ルールは変換された送信元ネットワークを含む必要があります。

**ステップ 6** [追加 (Add) ] をクリックします。

**ステップ 7** [保存 (Save) ] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## NAT ルールのタイプ

すべての NAT ルールには次の働きを持つタイプが関連付けられています。

- ネットワーク トラフィックを限定する
- 条件に一致するトラフィックの変換方法を指定する

次に、NAT ルール タイプの概要を示します。

### 静的

スタティックルールは宛先ネットワークと任意選択のポートおよびプロトコルで1対1の変換を提供します。スタティック変換を設定する場合、送信元ゾーン、宛先ネットワーク、および宛先ポートを設定できます。宛先ゾーンまたは送信元ネットワークを設定できません。

元の宛先ネットワークを指定する**必要**があります。宛先ネットワークでは、単一の IP アドレスを含むネットワーク オブジェクトおよびグループを選択するか、または単一の IP アドレスを表すリテラル IP アドレスを入力することのみが可能です。元の宛先ネットワークと変換後の宛先ネットワークはそれぞれ1つのみ指定できます。



- (注) システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

元の宛先ポートと変換後の宛先ポートをそれぞれ1つ指定できます。元の宛先ポートを指定するには、その前に、元の宛先ネットワークを指定する必要があります。さらに、元の宛先ポートを指定しない場合は、変換後の宛先ポートを指定できません。また、変換後の値は、元の値のプロトコルと一致する必要があります。



- 注意** 高可用性ペアとして構成されている 7000 または 8000 シリーズ デバイスのスタティック NAT ルールについては、NAT 変換で影響を受けるすべてのネットワークがプライベートの場合、個別のピアインターフェイスのみを選択します。パブリックネットワークとプライベートネットワーク間のトラフィックに影響するスタティック NAT ルールに対してこの設定を使用しないでください。

### ダイナミック IP 専用

ダイナミック IP 専用ルールは多対多の送信元ネットワークを変換しますが、ポートおよびプロトコルを維持します。ダイナミック IP 専用変換を設定する場合、ゾーン、送信元ネットワーク、元の宛先ネットワーク、および元の宛先ポートを設定できます。変換後の宛先ネットワークまたは変換後の宛先ポートは設定できません。

変換後の送信元ネットワークを少なくとも1つ指定する**必要**があります。変換後の送信元ネットワーク値の数が元の送信元ネットワークの数よりも小さい場合、元のアドレスがすべて照合される前に変換後のアドレスが不足する可能性があるという警告がルールに表示されます。

同じパケットに一致する条件を持つルールが複数個ある場合、優先度の低いルールはデッドルールとなり、トリガーされなくなります。デッドルールにも警告が表示されます。ツールチップを表示して、デッドルールに代わるルールを判別できます。



- (注) デッドルールを持つポリシーを保存し、展開することは可能ですが、ルールは変換を実現できません。

場合によっては、範囲の広いルールよりも優先される、範囲が限定されたルールを作成することをお勧めします。次に例を示します。

```
Rule 1: Match on address A and port A/Translate to address B
Rule 2: Match on address A/Translate to Address C
```

この例で、ルール1はルール2にも一致するいくつかのパケットに一致します。したがって、ルール2は完全に無効ではありません。

元の宛先ポートだけを指定した場合、変換後の宛先ポートを指定することはできません。

#### ダイナミック IP およびポート

ダイナミック IP およびポート ルールは多対1または多対多の送信元ネットワークとポートおよびプロトコルを変換します。ダイナミック IP およびポート変換を設定する場合、ゾーン、送信元ネットワーク、元の宛先ネットワーク、および元の宛先ポートを設定できます。変換後の宛先ネットワークまたは変換後の宛先ポートは設定できません。

変換後の送信元ネットワークを少なくとも1つ指定する**必要**があります。同じパケットに一致する条件を持つルールが複数個ある場合、優先度の低いルールはデッドルールとなり、トリガーされなくなります。デッドルールにも警告が表示されます。ツールチップを表示して、デッドルールに代わるルールを判別できます。



- (注) デッドルールを持つポリシーを保存し、展開することは可能ですが、ルールは変換を実現できません。

元の宛先ポートだけを指定した場合、変換後の宛先ポートを指定することはできません。



- (注) ダイナミック IP およびポート ルールを作成し、システムがポートを使用しないトラフィックを渡す場合、そのトラフィックに対して変換は発生しません。たとえば、送信元ネットワークに一致する IP アドレスからの ping (ICMP) は、ICMP がポートを使用しないため、マッピングされません。

## NAT ルールの条件タイプ

次の表に、指定された NAT ルール タイプに基づいて設定可能な NAT ルールの条件タイプをまとめています。

表 74: NAT ルール タイプごとに使用可能な NAT ルールの条件タイプ

条件	静的	ダイナミック (IP 専用または IP およびポート)
送信元ゾーン (Source Zones)	オプション	オプション
宛先ゾーン (Destination Zones)	不可	オプション
元の送信元ネットワーク	不可	オプション
変換後の送信元ネットワーク	不可	必須 (Required)
元の宛先ネットワーク	必須 (Required)	オプション
変換後の宛先ネットワーク	任意。単一アドレスのみ	不可
元の宛先ポート	任意。単一ポートでのみ、元の宛先ネットワークを定義する場合のみ可能	オプション
変換後の宛先ポート	任意。単一ポートでのみ、元の宛先ポートを定義する場合のみ可能	不可

## NAT ルールの条件と条件の仕組み

ルールに一致するトラフィックのタイプを識別するために NAT ルールに条件を追加できます。それぞれの条件タイプごとに、使用可能条件リストから、ルールに追加する条件を選択します。条件フィルタを適用できる場合は、条件フィルタを使って使用可能な条件を限定できます。使用可能な条件リスト、および選択した条件リストは、1 つの条件だけを含む場合も、数ページに及ぶ場合もあります。使用可能な条件は検索することができ、名前や値を入力するとそれに一致する条件だけが表示され、入力していくにつれてそのリストが更新されます。

条件のタイプに応じて、使用可能条件リストには、Cisco から直接提供された条件と、他の Firepower システム機能を使って設定された条件が一緒に含まれることがあります。その中には、オブジェクト マネージャ ([**オブジェクト (Objects)**] > [**オブジェクト管理 (Object Management)**]) を使って作成されたオブジェクト、個別の条件ページから直接作成されたオブジェクト、およびリテラル条件が含まれます。

## NAT ルールの条件

次の表で説明されている条件のいずれかを満たすトラフィックを照合するための NAT ルールを設定できます。

表 75: NAT ルールの条件タイプ

条件	説明
ゾーン	NAT ポリシーを展開できる 1 つ以上のルーテッドインターフェイスの設定。ゾーンは、送信元インターフェイスと宛先インターフェイスでトラフィックを分類するメカニズムであり、ルールに送信元のゾーン条件と宛先のゾーン条件を追加することができます。
ネットワーク	明示的に指定した、またはネットワーク オブジェクトとグループを使用した、個々の IP アドレス、CIDR ブロック、およびプレフィックス長の組み合わせ。NAT ルールに送信元ネットワーク条件と宛先ネットワーク条件を追加できます。
宛先ポート	トランスポート プロトコルに基づいて作成される、個別のポート オブジェクトとグループポート オブジェクトを含むトランスポート プロトコル ポート。

## NAT ルールへの条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

NAT ルールへの条件の追加は基本的にどの条件のタイプでも同じです。左側の使用可能な条件のリストから選択して、右側で選択した条件の 1 つまたは 2 つのリストに、選択した条件を追加します。

すべての条件タイプで、使用可能な個々の条件を 1 つまたは複数クリックすると、それが強調表示され、選択状態になります。2 つのタイプのリスト間にあるボタンをクリックして選択した使用可能な条件を選択した条件のリストに追加するか、または選択した使用可能な条件を選択した条件のリストにドラッグ アンド ドロップします。

選択済み条件リストには、タイプごとに最大 50 個までの条件を追加できます。たとえばアプライアンスの上限に達するまで、最大 50 個の送信元ゾーン条件、最大 50 個の宛先ゾーン条件、最大 50 個の送信元ネットワーク条件などを追加できます。

### 手順

**ステップ 1** [デバイス (Devices) ] > [NAT] を選択します。

**ステップ 2** 変更する NAT ポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** [ルールへの追加 (Add Rule)] をクリックします。

**ステップ 4** ルールの [名前 (Name)] を入力します。

**ステップ 5** ルールの [タイプ (Type)] を指定します。

**ステップ 6** ルールに追加する条件タイプに対応したタブをクリックします。

**ステップ 7** 次のいずれかの操作を行います。

- 表示されている条件を、すでに選択済みの条件のリストに追加するには、表示されている条件をクリックします。
- 表示されている条件をすべて選択するには、条件のいずれかの行を右クリックし、[すべて選択 (Select All)] をクリックします。
- 表示されている条件の一部またはフィルタされた条件を選択するには、[検索 (Search)] フィールド内をクリックし、検索のための文字列を入力します。入力していくと、リストが更新されて一致する項目が表示されます。

オブジェクト名およびオブジェクトに設定されている値を検索対象にできます。たとえば Texas Office という名前の個別ネットワーク オブジェクトがあり、192.168.3.0/24 という値が設定されていて、US Offices というグループ オブジェクトに含まれる場合、Tex などの部分的または完全な検索文字列を入力するか、または 3 などの値を入力することにより、両方のオブジェクトを表示できます。

- 表示されている条件を検索中、またはフィルタ中に検索文字列をクリアするには、検索フィールドの上のリロードアイコン (🔄) または検索フィールド内のクリアアイコン (✕) をクリックします。
- 表示されている条件リストからゾーンの条件を選択し、選択済みの送信元または宛先の条件リストに追加するには、[送信元に追加 (Add to Source)] または [宛先に追加 (Add to Destination)] をクリックします。
- 表示されている条件リストからネットワークとポートの条件を選択し、選択済みの元または変換済みの条件リストに追加するには、[元に追加 (Add to Original)] または [変換済みに追加 (Add to Translated)] をクリックします。
- 表示されている条件を選択済み条件のリストにドラッグアンドドロップするには、選択済み条件をクリックし、選択済み条件のリストにドラッグアンドドロップします。
- リテラルフィールドを使用し、選択済み条件のリストにリテラル条件を追加するには、クリックしてリテラルフィールドからのプロンプトを削除し、リテラル条件を入力し、[追加 (Add)] をクリックします。ネットワーク条件は、リテラル条件を追加するためのフィールドを提供します。
- ドロップダウンリストを使用し、選択済み条件のリストにリテラル条件を追加するには、ドロップダウンリストから条件を選択し、[追加 (Add)] をクリックします。ポート条件には、リテラル条件を追加するためのドロップダウンリストがあります。
- 個々のオブジェクトまたは条件フィルタを追加して、条件リストからそれを選択できるように表示させるには、追加アイコン (+) をクリックします。



- 選択済み条件のリストから条件を 1 つだけ削除するには、条件の横にある削除アイコン (🗑️) をクリックします。
- 選択済み条件のリストから条件を削除するには、選択済み条件のリストの行を右クリックして強調表示し、[削除 (Delete)] をクリックします。

**ステップ 8** 設定を保存するには、[追加 (Add)] をクリックします。

## NAT ルールのリテラル条件

次の条件タイプについて、元のおよび変換後の条件のリストにリテラル値を追加できます。

- ネットワーク
- ポート

ネットワーク条件の場合、元または変換後の条件リストの下にある設定フィールドにリテラル値を入力します。

ポート条件では、ドロップダウンリストからプロトコルを選択します。プロトコルが All、または TCP または UDP である場合、設定フィールドにポート番号を入力します。

該当するそれぞれの条件ページには、リテラル値を追加するために必要なコントロールがあります。設定フィールドに入力した値が無効である場合や、まだ有効と認識されていない場合は、赤いテキストとして表示されます。入力時に有効と認識された値は青色に変わります。有効な値が認識されると、グレー表示の [追加 (Add)] ボタンがアクティブになります。追加したリテラル値は、選択済み条件リストにただちに表示されます。



- (注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

## NAT ルールの条件のオブジェクト

オブジェクト マネージャ ([オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]) で作成されたオブジェクトは、使用可能な NAT ルール条件の関連リストからすぐに選択可能になります。

NAT ポリシーから直接オブジェクトを作成することもできます。該当する条件ページ上のコントロールでは、オブジェクト マネージャでの設定コントロールと同じ機能を利用できます。

直接作成された個別のオブジェクトは使用可能なオブジェクトのリストにすぐに表示されます。それらを現在のルールと他の既存および将来のルールに追加できます。該当する条件ページとポリシー編集ページで、ポインタを 1 つの個別オブジェクトの上に置くとそのオブジェク

トの内容が表示され、グループオブジェクトの上に置くと、グループ内の個々のオブジェクトの数が表示されます。

## NAT ルール内のゾーン条件

システムのセキュリティゾーンは、管理対象デバイス上のインターフェイスから構成されています。NAT ルールに追加するゾーンは、それらのゾーン内にルーテッドインターフェイスまたはハイブリッドインターフェイスを持つ、ネットワーク上のデバイスにそのルールをターゲットします。NAT ルールの条件として、ルーテッドインターフェイスまたはハイブリッドインターフェイスを持つセキュリティゾーンのみを追加できます。

現在仮想ルータに割り当てられているゾーンまたはスタンドアロンインターフェイスのどちらかを NAT ルールに追加できます。デバイス設定が展開されていないデバイスがある場合、[ゾーン (Zones)] ページの使用可能なゾーン リストの上に警告アイコン (⚠) が表示され、展開済みのゾーンとインターフェイスだけが表示されることが示されます。ゾーンの横にある矢印アイコン (▾) をクリックして、ゾーンを縮小または展開し、そのインターフェイスを非表示または表示することができます。

インターフェイスがハイアベイラビリティペアの 7000 または 8000 シリーズデバイス上にある場合、使用可能なゾーンのリストに、そのインターフェイスからの追加のブランチが表示されると共に、そのハイアベイラビリティペアの他のインターフェイスがそのハイアベイラビリティペアのアクティブデバイスのプライマリインターフェイスの子として表示されます。矢印アイコン (▾) をクリックして、ペアになったデバイスインターフェイスを縮小または展開し、そのインターフェイスを非表示または表示することもできます。



- (注) 無効にされたインターフェイスを持つポリシーを保存して展開できますが、ルールではそれらのインターフェイスが有効になるまで変換を提供できません。

右側の 2 つのリストは、NAT ルールによって照合目的に使用される送信元ゾーンと宛先ゾーンです。すでにルールに値が設定されている場合、ルールを編集する際、これらのリストには既存の値が表示されます。送信元ゾーンのリストが空の場合、ルールは任意のゾーンまたはインターフェイスからのトラフィックを照合します。宛先ゾーンのリストが空の場合、ルールは任意のゾーンまたはインターフェイス宛てのトラフィックを照合します。

対象のデバイスでトリガーされることがないゾーンの組み合わせを持つルールに対しては警告が表示されます。



- (注) これらのゾーンの組み合わせを持つポリシーを保存して展開できますが、ルールでは変換を提供しません。

ゾーン内の項目を選択するか、またはスタンドアロンインターフェイスを選択することによって、個別のインターフェイスを追加できます。ゾーン内のインターフェイスを追加できるのは、それらのインターフェイスが割り当てられるゾーンがまだ送信元ゾーンまたは宛先ゾーン

のリストに追加されていない場合のみです。これらの個別に選択されたインターフェイスは、それらのインターフェイスを削除して別のゾーンに追加した場合でも、各ゾーンに対する変更の影響を受けません。インターフェイスがハイアベイラビリティペアのプライマリメンバーで、ダイナミックルールを設定する場合、そのプライマリインターフェイスだけを送信元ゾーンまたは宛先ゾーンのリストに追加できます。スタティックルールの場合、個別のハイアベイラビリティペアのメンバーインターフェイスを送信元ゾーンのリストに追加できます。ハイアベイラビリティペアのプライマリインターフェイスは、その子がまったく追加されていない場合にだけ、リストに追加できます。また、個別のハイアベイラビリティペアのインターフェイスは、プライマリが追加されていない場合にだけ追加できます。

ゾーンを追加すると、ルールではそのゾーンに関連付けられているすべてのインターフェイスを使用します。ゾーンに対してインターフェイスを追加または削除すると、インターフェイスが存在するデバイスにデバイス設定が再度展開されるまで、ルールでは更新されたバージョンのゾーンを使用しません。



(注) スタティック NAT ルールでは、送信元ゾーンのみを追加できます。ダイナミック NAT ルールでは、送信元ゾーンと宛先ゾーンの両方を追加できます。

## NAT ルールへのゾーン条件の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

### 手順

- ステップ 1 [デバイス (Devices) ] > [NAT] を選択します。
- ステップ 2 変更する NAT ポリシーの横にある編集アイコン (✎) をクリックします。  
代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3 [ルールの追加 (Add Rule) ] をクリックします。
- ステップ 4 ルールの [名前 (Name) ] を入力します。
- ステップ 5 ルールの [タイプ (Type) ] を指定します。
- ステップ 6 [ゾーン (Zones) ] タブをクリックします。
- ステップ 7 [使用可能なゾーン (Available Zones) ] リスト内のゾーンまたはインターフェイスをクリックします。
- ステップ 8 次の選択肢があります。

- 送信元ゾーンによりトラフィックを照合するには、[送信元に追加 (Add to Source)] をクリックします。
- 宛先ゾーンによりトラフィックを照合するには、[宛先に追加 (Add to Destination)] をクリックします。

(注) スタティック NAT ルールには送信元ゾーンのみを追加できます。さらに、無効になっているインターフェイスを NAT ルールに追加できますが、ルールは変換を実現しません。

**ステップ 9** [追加 (Add)] をクリックして新しいルールを保存します。

**ステップ 10** [保存 (Save)] をクリックして、変更したポリシーを保存します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ダイナミック NAT ルールの送信元ネットワーク条件

パケットの送信元 IP アドレスの照合値と変換値を設定します。元の送信元ネットワークが設定されていない場合、すべての送信元 IP アドレスがダイナミック NAT ルールに一致します。スタティック NAT ルールの送信元ネットワークは設定できないことに注意してください。パケットが NAT ルールに一致すると、システムは変換後の送信元ネットワークの値を使用して、送信元 IP アドレスの新しい値を割り当てます。ダイナミック ルール用に少なくとも 1 つの値を持つ変換後の送信元ネットワークを設定する必要があります。



**注意** ネットワーク オブジェクトまたはオブジェクト グループが NAT ルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

ダイナミック NAT ルールに、次の種類の送信元ネットワーク条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのネットワーク オブジェクト
- 送信元ネットワーク条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のネットワーク オブジェクト
- リテラル、単一 IP アドレス、範囲、またはアドレス ブロック



- (注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン 展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

## ネットワーク条件のダイナミック NAT ルールへの追加

スマート ライセ ンス	従来のライセンス	サポートされるデ バイス	サポートされるド メイン	アクセス (Access)
該当なし	Control	7000 & 8000 シ リーズ	任意 (Any)	Admin/Network Admin

展開されているポリシーで使用中のダイナミックルールのネットワーク条件を更新すると、既存の変換済みアドレス プールを使用しているネットワーク セッションがドロップされます。

### 手順

- ステップ 1 [デバイス (Devices)] > [NAT] を選択します。
- ステップ 2 変更する NAT ポリシーの横にある編集アイコン (✎) をクリックします。  
代わりに表示アイコン (👁) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3 [ルールの追加 (Add Rule)] をクリックします。
- ステップ 4 ルールの [名前 (Name)] を入力します。
- ステップ 5 ルールのダイナミック [タイプ (Type)] を指定します。
  - ダイナミック IP 専用
  - ダイナミック IP およびポート
- ステップ 6 [送信元ネットワーク (Source Network)] タブをクリックします。
- ステップ 7 必要に応じて、リストの上にある追加アイコン (+) をクリックし、[使用可能なネットワー  
ク (Available Networks)] リストへ個々のネットワーク オブジェクトを追加します。  
各ネットワーク オブジェクトに複数の IP アドレス、CIDR ブロック、およびプレフィクス長  
を追加できます。
- ステップ 8 [使用可能なネットワーク (Available Networks)] リスト内の条件をクリックします。
- ステップ 9 次の選択肢があります。
  - 元の送信元ネットワークによりトラフィックを照合するには、[元に追加 (Add to Original)] をクリックします。

- 変換後の送信元ネットワークと照合するトラフィックの変換値を指定するには、[変換後に追加 (Add to Translated) ] をクリックします。

**ステップ 10** リテラル IP アドレス、範囲、アドレスブロックを追加するには、

- [元の送信元ネットワーク (Original Source Network) ] または [変換後の送信元ネットワーク (Translated Source Network) ] リストの下にある [IP アドレス入力 (Enter an IP address) ] プロンプトをクリックします。
- IP アドレス、範囲、アドレスブロックを入力します。

範囲は、下位の IP アドレス - 上位の IP アドレスの形式で追加します。たとえば、179.13.1.1-179.13.1.10 です。

(注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

- 入力した値の横にある [追加 (Add) ] をクリックします。

**ステップ 11** [追加 (Add) ] をクリックしてルールを保存します。

**ステップ 12** [保存 (Save) ] をクリックして、変更したポリシーを保存します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## NAT ルールの宛先ネットワーク条件

パケットの宛先 IP アドレスの照合値と変換値を設定します。ダイナミック NAT ルールでは変換済み宛先ネットワークは設定できないことに注意してください。

スタティック NAT ルールは 1 対 1 変換であるため、[利用可能なネットワーク (Available Networks) ] リストには単一の IP アドレスのみを含むネットワーク オブジェクトおよびグループのみが含まれます。スタティック変換では、[元の宛先ネットワーク (Original Destination Network) ] リストと [変換済み宛先ネットワーク (Translated Destination Network) ] リストにそれぞれ追加できるオブジェクトまたはリテラル値は 1 つのみです。



**注意** ネットワーク オブジェクトまたはオブジェクトグループが NAT ルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

NAT ルールに、次の種類の宛先ネットワーク条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのネットワーク オブジェクト
- [宛先ネットワーク (Destination Network) ]条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のネットワーク オブジェクト
- リテラル、単一 IP アドレス、範囲、またはアドレス ブロック

スタティック NAT ルールでは、リストにまだ値がない場合に限り、CIDR とサブネット マスク /32 のみを追加できます。



- (注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン 展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

## NAT ルールへの宛先ネットワーク条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

展開されているポリシーで使用中のダイナミックルールのネットワーク条件を更新すると、既存の変換済みアドレス プールを使用しているネットワーク セッションがドロップされます。

### 手順

- ステップ 1** [デバイス (Devices) ] > [NAT] を選択します。
- ステップ 2** 変更する NAT ポリシーの横にある編集アイコン (✎) をクリックします。  
代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3** [ルールの追加 (Add Rule) ] をクリックします。
- ステップ 4** ルールの [名前 (Name) ] を入力します。
- ステップ 5** ルールの [タイプ (Type) ] を指定します。
- ステップ 6** [宛先ネットワーク (Destination Network) ] タブをクリックします。
- ステップ 7** 必要に応じて、リストの上にある追加アイコン (+) をクリックし、[使用可能なネットワーク (Available Networks) ] リストへ個々のネットワーク オブジェクトを追加します。

ダイナミックルールの場合、各ネットワークオブジェクトに複数の IP アドレス、CIDR ブロック、およびプレフィクス長を追加できます。スタティックルールの場合、単一の IP アドレスのみを追加できます。

- ステップ 8** [使用可能なネットワーク (Available Networks) ] リスト内の条件またはオブジェクトをクリックします。
- ステップ 9** 次の選択肢があります。
- 元の宛先ネットワークによりトラフィックを照合するには、[元に追加 (Add to Original) ] をクリックします。
  - 変換後の宛先ネットワークと照合するトラフィックの変換値を指定するには、[変換後に追加 (Add to Translated) ] をクリックします。
- ステップ 10** オプションで、[元の宛先ネットワーク (Original Destination Network) ] リストまたは [変換後の宛先ネットワーク (Translated Destination Network) ] リストの下の [IP アドレス入力 (Enter an IP address) ] プロンプトをクリックし、次に、IP アドレスまたはアドレスブロックを入力して、[追加 (Add) ] をクリックします。
- ステップ 11** [追加 (Add) ] をクリックします。
- ステップ 12** [保存 (Save) ] をクリックし、ポリシーの変更内容を保存します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## NAT ルールでのポート条件

ルールにポート条件を追加することで、元の宛先ポートと変換後の宛先ポートおよび変換用の転送プロトコルに基づいてネットワークトラフィックを照合できます。元のポートが設定されていない場合、すべての宛先ポートがルールと照合されます。パケットを NAT ルールと照合し変換後の宛先ポートが設定されていた場合、システムはその値にポートを変換します。ダイナミックルールでは元の宛先ポートのみを指定できることに注意してください。スタティックルールの場合、変換後の宛先ポートを定義できますが、元の宛先ポートオブジェクトまたはリテラル値と同じプロトコルを持つオブジェクトでのみ可能です。

システムは宛先ポートを、スタティックルールの元の宛先ポートリスト内のポートオブジェクトまたはリテラルポートの値、またはダイナミックルールの複数の値と照合します。

スタティック NAT ルールは 1 対 1 変換であるため、[利用可能なポート (Available Ports) ] リストには単一のポートのみを含むポートオブジェクトおよびグループのみが含まれます。スタティック変換では、単一のオブジェクトまたはリテラル値のみを [元のポート (Original Port) ] リストと [変換済みポート (Translated Port) ] リストの両方に追加できます。

ダイナミックルールの場合、ポートの範囲を追加できます。たとえば、元の宛先ポートを指定する場合、リテラル値として 1000-1100 を追加できます。



**注意**

ポート オブジェクトまたはオブジェクトグループが NAT ルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

NAT ルールには、次の種類のポート条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのポート オブジェクト
- 宛先ポート条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のポート オブジェクト
- TCP、UDP、またはすべて (TCP および UDP) の転送プロトコルとポートから構成されるリテラルポート値

**NAT ルールへのポートの条件の追加**

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	Control	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

**手順**

**ステップ 1** [デバイス (Devices) ] > [NAT] を選択します。

**ステップ 2** 変更する NAT ポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** [ルールの追加 (Add Rule) ] をクリックします。

**ステップ 4** ルールの [名前 (Name) ] を入力します。

**ステップ 5** ルールの [タイプ (Type) ] を指定します。

**ステップ 6** [宛先ポート (Destination Port) ] タブをクリックします。

**ステップ 7** 必要に応じて、[使用可能なポート (Available Ports) ] リストの上にある追加アイコン (+) をクリックし、リストに個別のポートオブジェクトを追加します。

追加する各ポート オブジェクトの 1 つのポートまたはポート範囲を指定できます。その後、ルールの条件として追加するオブジェクトを選択できます。スタティックルールの場合、単一のポートを持つポート オブジェクトのみを使用できます。

**ステップ 8** [使用可能なポート (Available Ports) ] リスト内の条件をクリックします。

**ステップ 9** 次の選択肢があります。

- [元に追加 (Add to Original) ] をクリックします。

- [変換後に追加 (Add to Translated) ] をクリックします。
- 使用可能なポートをリストにドラッグ アンド ドロップします。

**ステップ 10** リテラルポートを追加するには、次の手順を実行します。

- a) [元のポート (Original Port) ] または [変換後のポート (Translated Port) ] リストの下にある [プロトコル (Protocol) ] ドロップダウンリストからエントリを選択します。
- b) ポートを入力します。
- c) [追加 (Add) ] をクリックします。

ダイナミック ルールの場合、単一のポートまたは範囲を指定できます。

**ステップ 11** [追加 (Add) ] をクリックします。

**ステップ 12** [保存 (Save) ] をクリックし、ポリシーの変更内容を保存します。

---

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。



## 第 47 章

# Firepower Threat Defense 用のネットワーク アドレス変換 (NAT)

ここでは、ネットワーク アドレス変換 (NAT) について、および Firepower Threat Defense デバイスでそれを設定する方法について説明します。

- [NAT を使用する理由 \(1101 ページ\)](#)
- [NAT の基本 \(1102 ページ\)](#)
- [NAT のガイドライン \(1111 ページ\)](#)
- [脅威に対する防御のための NAT の設定 \(1117 ページ\)](#)
- [IPv6 ネットワークの変換 \(1162 ページ\)](#)
- [NAT のモニタリング \(1173 ページ\)](#)
- [NAT の例 \(1173 ページ\)](#)

## NAT を使用する理由

IP ネットワーク内の各コンピュータおよびデバイスには、ホストを識別する固有の IP アドレスが割り当てられています。パブリック IPv4 アドレスが不足しているため、これらの IP アドレスの大部分はプライベートであり、プライベートの企業ネットワークの外部にルーティングできません。RFC 1918 では、アドバタイズされない、内部で使用できるプライベート IP アドレスが次のように定義されています。

- 10.0.0.0 ~ 10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0 ~ 192.168.255.255

NAT の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。NAT は、プライベート IP アドレスをパブリック IP に置き換え、内部プライベート ネットワーク内のプライベートアドレスをパブリック インターネットで使用可能な正式の、ルーティング可能なアドレスに変換します。このようにして、NAT はパブリックアドレスを節約します。これは、ネットワーク全体に対して 1 つのパブリックアドレスだけを外部に最小限にアドバタイズするように NAT を設定できるからです。

NAT の他の機能は、次のとおりです。

- セキュリティ：内部アドレスを隠蔽し、直接攻撃を防止します。
- IP ルーティング ソリューション：NAT を使用する際は、重複 IP アドレスが問題になりません。
- 柔軟性：外部で使用可能なパブリック アドレスに影響を与えずに、内部 IP アドレッシング スキームを変更できます。たとえば、インターネットにアクセス可能なサーバの場合、インターネット用に固定 IP アドレスを維持できますが、内部的にはサーバのアドレスを変更できます。
- IPv4 と IPv6 (ルーテッドモードのみ) の間の変換：IPv4 ネットワークに IPv6 ネットワークを接続する場合は、NAT を使用すると、2つのタイプのアドレス間で変換を行うことができます。



---

(注) NAT は必須ではありません。特定のトラフィック セットに NAT を設定しない場合、そのトラフィックは変換されませんが、セキュリティ ポリシーはすべて通常通りに適用されます。

---

## NAT の基本

ここでは、NAT の基本について説明します。

## NAT の用語

このマニュアルでは、次の用語を使用しています。

- 実際のアドレス/ホスト/ネットワーク/インターフェイス：実際のアドレスとは、ホストで定義されている、変換前のアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、内部ネットワークが「実際の」ネットワークになります。内部ネットワークだけでなく、デバイスに接続されている任意のネットワークに変換できることに注意してください。したがって、外部アドレスを変換するように NAT を設定した場合、「実際の」は、外部ネットワークが内部ネットワークにアクセスしたときの外部ネットワークを指します。
- マッピングアドレス/ホスト/ネットワーク/インターフェイス：マッピングアドレスとは、実際のアドレスが変換されるアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、外部ネットワークが「マッピング」ネットワークになります。



---

(注) アドレスの変換中、デバイス インターフェイスに設定された IP アドレスは変換されません。

---

- 双方向の開始：スタティック NAT では、双方向に接続を開始できます。つまり、ホストへの接続とホストからの接続の両方を開始できます。
- 送信元および宛先の NAT：任意のパケットについて、送信元 IP アドレスと宛先 IP アドレスの両方を NAT ルールと比較し、1 つまたは両方を変換する、または変換しないことができます。スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。

## NAT タイプ

NAT は、次の方法を使用して実装できます。

- **ダイナミック NAT**：実際の IP アドレスのグループが、（通常は、より小さい）マッピング IP アドレスのグループに先着順でマッピングされます。実際のホストだけがトラフィックを開始できます。[ダイナミック NAT \(1122 ページ\)](#) を参照してください。
- **ダイナミック ポートアドレス変換 (PAT)**：実際の IP アドレスのグループが、1 つの IP アドレスにマッピングされます。この IP アドレスの一意の送信元ポートが使用されます。[ダイナミック PAT \(1128 ページ\)](#) を参照してください。
- **スタティック NAT**：実際の IP アドレスとマッピング IP アドレスとの間での一貫したマッピング。双方向にトラフィックを開始できます。[スタティック NAT \(1138 ページ\)](#) を参照してください。
- **アイデンティティ NAT**：実際のアドレスが同一アドレスにスタティックに変換され、基本的に NAT をバイパスします。大規模なアドレスのグループを変換するものの、小さいアドレスのサブセットは免除する場合は、NAT をこの方法で設定できます。[アイデンティティ NAT \(1149 ページ\)](#) を参照してください。

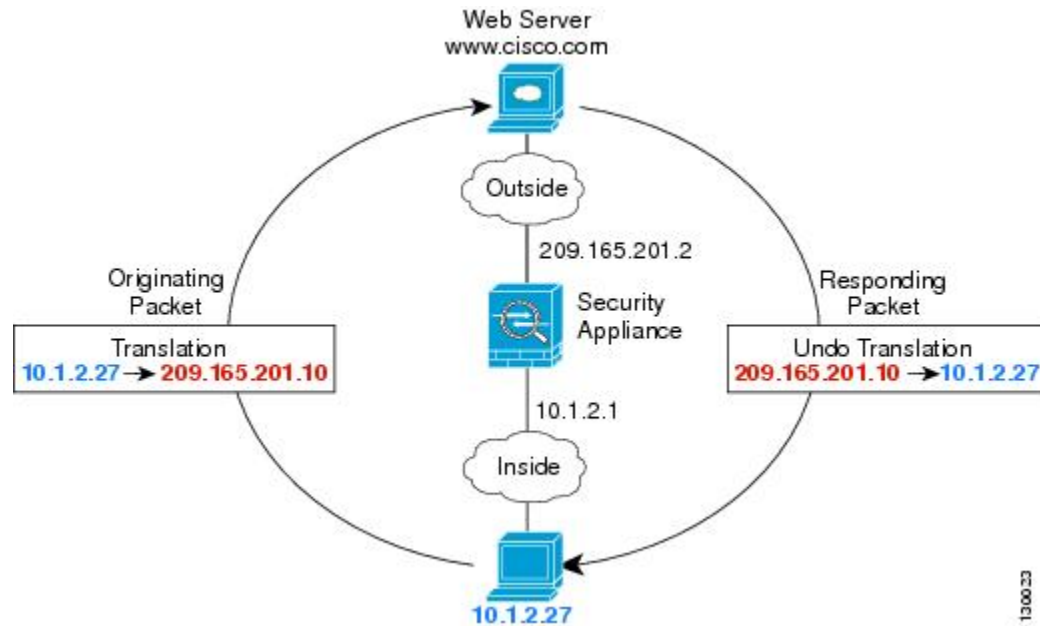
## ルーテッドモードとトランスペアレントモードの NAT

NAT は、ルーテッドモードおよびトランスペアレントファイアウォールモードの両方に設定できます。インライン、インラインタップ、またはパッシブモードで動作するインターフェイスに対しては NAT を設定できません。次の項では、各ファイアウォールモードの一般的な使用方法について説明します。

### ルーテッドモードの NAT

次の図は、内部にプライベートネットワークを持つ、ルーテッドモードの一般的な NAT の例を示しています。

図 20: NAT の例 : ルーテッドモード



1. 内部ホスト 10.1.2.27 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.2.27 はマッピングアドレス 209.165.201.10 に変換されます。
2. サーバが応答すると、マッピングアドレス 209.165.201.10 に応答を送信し、Firepower Threat Defense デバイスがそのパケットを受信します。これは、Firepower Threat Defense デバイスがプロキシ ARP を実行してパケットを要求するためです。
3. Firepower Threat Defense デバイスはその後、パケットをホストに送信する前に、マッピングアドレス 209.165.201.10 を変換し、実際のアドレス 10.1.2.27 に戻します。

## トランスパレントモードの NAT

NAT をトランスパレントモードで使用すると、ネットワークで NAT を実行するためのアップストリーム ルータまたはダウンストリーム ルータがなくなります。

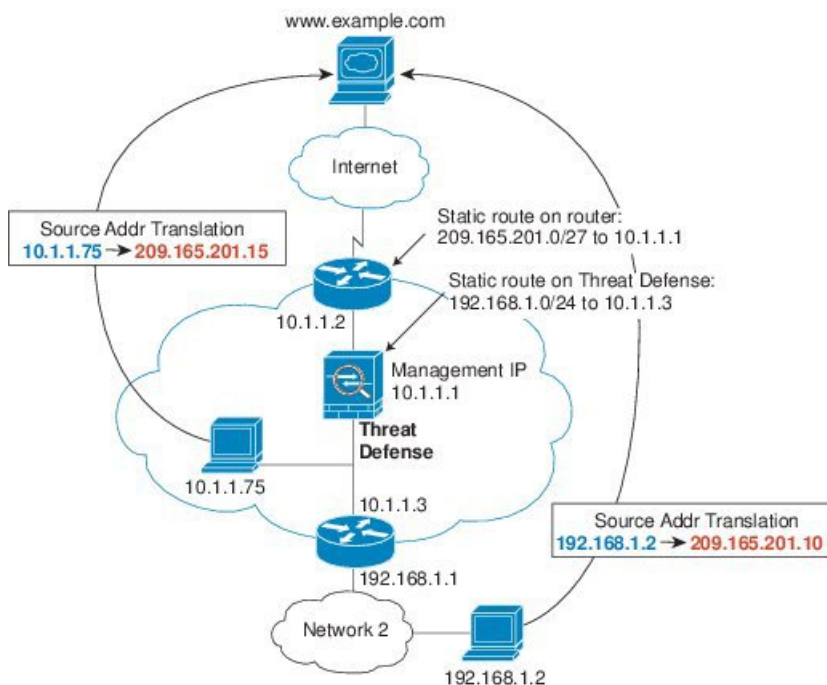
トランスパレントモードの NAT には、以下の要件および制限があります。

- インターフェイスに接続されている IP アドレスがないため、マッピングされたアドレスがブリッジグループメンバーのインターフェイスである場合、インターフェイス PAT を設定することはできません。
- ARP インспекションはサポートされていません。さらに、何らかの理由で Firepower Threat Defense デバイスの片側にあるホストから Firepower Threat Defense デバイスのもう片側にあるホストに ARP 要求が送信され、送信側ホストの実アドレスが同じサブネット上の別のアドレスにマップされている場合、その実アドレスは ARP 要求で表示されたままになります。

- IPv4 および IPv6 ネットワークの間の変換はサポートされていません。2つの IPv6 ネットワーク間、または2つの IPv4 ネットワーク間の変換がサポートされます。

次の図に、インターフェイス内部と外部に同じネットワークを持つ、トランスペアレントモードの一般的な NAT のシナリオを示します。このシナリオのトランスペアレントファイアウォールは NAT サービスを実行しているため、アップストリーム ルータは NAT を実行する必要がありません。

図 21: NAT の例 : トランスペアレントモード



1. 内部ホスト 10.1.1.75 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.1.75 はマッピングアドレス 209.165.201.15 に変更されます。
2. サーバが応答すると、マッピングアドレス 209.165.201.15 に応答を送信し、Firepower Threat Defense デバイス がそのパケットを受信します。これは、アップストリーム ルータには、Firepower Threat Defense デバイス の管理 IP アドレスに転送されるスタティック ルートのこのマッピング ネットワークが含まれるためです。
3. その後、Firepower Threat Defense デバイス はマッピングアドレス 209.165.201.15 を変換して実際のアドレス 10.1.1.75 に戻します。実際のアドレスは直接接続されているため、Firepower Threat Defense デバイス はそのアドレスを直接ホストに送信します。
4. ホスト 192.168.1.2 の場合も、リターントラフィックを除き、同じプロセスが発生します。Firepower Threat Defense デバイス はルーティングテーブルでルートを検索し、192.168.1.0/24 の Firepower Threat Defense デバイス スタティック ルートに基づいてパケットを 10.1.1.3 にあるダウンストリーム ルータに送信します。

## 自動 NAT および手動 NAT

自動 NAT および手動 NAT という 2 種類の方法でアドレス変換を実装できます。

手動 NAT の追加機能を必要としない場合は、自動 NAT を使用することをお勧めします。自動 NAT の設定が容易で、Voice over IP (VoIP) などのアプリケーションでは信頼性が高い場合があります (VoIP では、ルールで使用されているオブジェクトのいずれにも属さない間接アドレスの変換が失敗することがあります)。

### 自動 NAT

ネットワーク オブジェクトのパラメータとして設定されているすべての NAT ルールは、自動 NAT ルールと見なされます。これは、ネットワーク オブジェクトに NAT を設定するための迅速かつ簡単な方法です。しかし、グループオブジェクトに対してこれらのルールを作成することはできません。

これらのルールはオブジェクト自体の一部として設定されますが、オブジェクトマネージャを通してオブジェクト定義内の NAT 設定を確認することはできません。

パケットがインターフェイスに入ると、送信元 IP アドレスと宛先 IP アドレスの両方が自動 NAT ルールと照合されます。個別の照合が行われる場合、パケット内の送信元アドレスと宛先アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはないため、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定することはできません。この種の機能には、手動 NAT を使用することで、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます。

### 手動 NAT

手動 NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定できます。



- (注) スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。たとえば、ポートアドレス変換を使用するスタティック NAT を設定し、送信元アドレスを Telnet サーバとして指定する場合に、Telnet サーバに向かうすべてのトラフィックのポートを 2323 から 23 に変換するには、変換する送信元ポート (実際: 23、マッピング: 2323) を指定する必要があります。Telnet サーバアドレスを送信元アドレスとして指定しているため、その送信元ポートを指定します。

宛先アドレスはオプションです。宛先アドレスを指定する場合、宛先アドレスを自身にマッピングするか (アイデンティティ NAT)、別のアドレスにマッピングできます。宛先マッピングは、常にスタティック マッピングです。



## 自動 NAT と手動 NAT の比較

自動 NAT と手動 NAT の主な違いは、次のとおりです。

- 実アドレスの定義方法。
  - 自動 NAT : NAT ルールがネットワーク オブジェクトのパラメータとなります。ネットワーク オブジェクトの IP アドレスは、元の (実) アドレスとして機能します。
  - 手動 NAT : 実アドレスおよびマッピングアドレスの両方に対し、ネットワーク オブジェクトまたはネットワーク オブジェクト グループを特定します。この場合、NAT はネットワーク オブジェクトのパラメータではありません。ネットワーク オブジェクトまたはグループが、NAT 設定のパラメータとなります。実際のアドレスのネットワーク オブジェクト グループを使用できることは、手動 NAT がよりスケーラブルであることを意味します。
- 送信元および宛先 NAT の実装方法。
  - 自動 NAT : 個々のルールは、パケットの送信元または宛先のどちらかに適用されます。このため、送信元 IP アドレス、宛先 IP アドレスにそれぞれ 1 つずつ、計 2 つのルールが使用される場合もあります。このような 2 つのルールを 1 つに結合し、送信元/宛先ペアに対して特定の変換を強制することはできません。
  - 手動 NAT : 単一のルールが送信元と宛先の両方を変換します。1 つのパケットは 1 つのルールにしか一致せず、以降のルールはチェックされません。オプションの宛先アドレスを設定していない場合でも、パケットは 1 つの手動 NAT ルールのみ的一致します。送信元および宛先は相互に結び付けられるため、送信元と宛先の組み合わせに応じて、異なる変換を適用できます。たとえば、送信元 A/宛先 A のペアには、送信元 A/宛先 B のペアとは異なる変換を適用できます。
- NAT ルールの順序。
  - 自動 NAT : NAT テーブル内で自動的に順序が決まります。
  - 手動 NAT : NAT テーブル内で手動で順序が決められます (自動 NAT ルールの前または後)。

## NAT ルールの順序

自動 NAT および手動 NAT ルールは、3 つのセクションに分割された 1 つのテーブルに格納されます。最初にセクション 1 のルール、次にセクション 2、最後にセクション 3 というように、一致が見つかるまで順番に適用されます。たとえば、セクション 1 で一致が見つかった場合、セクション 2 とセクション 3 は評価されません。次の表に、各セクション内のルールの順序を示します。

表 76: NAT ルール テーブル

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 1	手動 NAT	設定に登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、固有のルールを期待どおりに適用できない可能性があります。デフォルトでは、手動 NAT ルールはセクション 1 に追加されます。
セクション 2	自動 NAT	<p>セクション 1 で一致が見つからない場合、セクション 2 のルールが次の順序で適用されます。</p> <ol style="list-style-type: none"> <li>1. スタティック ルール</li> <li>2. ダイナミック ルール</li> </ol> <p>各ルールタイプでは、次の順序ガイドラインが使用されます。</p> <ol style="list-style-type: none"> <li>1. 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。</li> <li>2. 数量が同じ場合には、IP アドレス番号（最小から最大まで）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。</li> <li>3. 同じ IP アドレスが使用される場合、ネットワーク オブジェクトの名前がアルファベット順で使用されます。たとえば、abracadabra は catwoman よりも先に評価されます。</li> </ol>
セクション 3	手動 NAT	まだ一致が見つからない場合、セクション 3 のルールがコンフィギュレーションに登場する順に、最初の一致ベースで適用されます。このセクションには、最も一般的なルールを含める必要があります。このセクションにおいても、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、一般的なルールが適用されます。

たとえばセクション 2 のルールでは、ネットワーク オブジェクト内に定義されている次の IP アドレスがあるとします。

- 192.168.1.0/24 (スタティック)
- 192.168.1.0/24 (ダイナミック)

- 10.1.1.0/24 (スタティック)
- 192.168.1.1/32 (スタティック)
- 172.16.1.0/24 (ダイナミック) (オブジェクト def)
- 172.16.1.0/24 (ダイナミック) (オブジェクト abc)

この結果、使用される順序は次のとおりです。

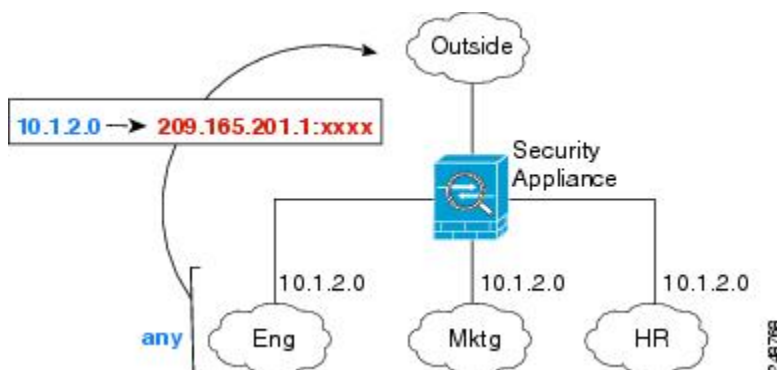
- 192.168.1.1/32 (スタティック)
- 10.1.1.0/24 (スタティック)
- 192.168.1.0/24 (スタティック)
- 172.16.1.0/24 (ダイナミック) (オブジェクト abc)
- 172.16.1.0/24 (ダイナミック) (オブジェクト def)
- 192.168.1.0/24 (ダイナミック)

## NAT インターフェイス

ブリッジグループメンバー インターフェイスを除き、任意のインターフェイス（つまり、すべてのインターフェイス）に適用される NAT ルールを設定したり、特定の実際のインターフェイスとマッピング インターフェイスを識別したりできます。実際のアドレスには任意のインターフェイスを指定できます。マッピング インターフェイスには特定のインターフェイスを指定できます。または、その逆も可能です。

たとえば、複数のインターフェイスで同じプライベートアドレスを使用し、外部へのアクセス時にはすべてのインターフェイスを同じグローバルプールに変換する場合、実際のアドレスに任意のインターフェイスを指定し、マッピング アドレスには **outside** インターフェイスを指定します。

図 22: 任意のインターフェイスの指定





- (注) インライン、インライン タップ、またはパッシブ モードで動作するインターフェイスに対しては NAT を設定できません。インターフェイスの指定は、インターフェイスを含むインターフェイス オブジェクトを選択することによって間接的に行います。

## NAT のルーティング設定

Firepower Threat Defense デバイスは、変換された (マッピング) アドレスに送信されるパケットの宛先である必要があります。

パケットを送信する際の出カインターフェイスの決定に、指定した場合はその宛先インターフェイスが使用され、指定していない場合はルーティング テーブル ルックアップが使用されます。アイデンティティ NAT では、宛先インターフェイスを指定していてもルート ルックアップを使用するオプションがあります。

必要なルート設定のタイプは、次のトピックで説明するように、マッピングアドレスのタイプによって異なります。

### マッピング インターフェイスと同じネットワーク上のアドレス

宛先 (マッピング) インターフェイスと同じネットワーク上のアドレスを使用する場合、Firepower Threat Defense デバイスはプロキシ ARP を使用してマッピングアドレスの ARP 要求に応答し、マッピングアドレス宛てのトラフィックを代行受信します。この方法では、Firepower Threat Defense デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。このソリューションは、外部ネットワークに十分な数のフリーアドレスが含まれている場合に最も適しており、ダイナミック NAT またはスタティック NAT などの 1:1 変換を使用している場合は考慮が必要です。ダイナミック PAT ではアドレス数が少なくても使用できる変換の数が大幅に拡張されるため、外部ネットワークで使用できるアドレスが少ししかない場合でも、この方法を使用できます。PAT では、マッピング インターフェイスの IP アドレスも使用できます。



- (注) マッピング インターフェイスを任意のインターフェイスとして設定し、マッピング インターフェイスの 1 つとして同じネットワーク上のマッピングアドレスを指定すると、そのマッピングアドレスの ARP 要求を別のインターフェイスで受信する場合、入力インターフェイスでそのネットワークの ARP エントリを手動で設定し、その MAC アドレスを指定する必要があります。通常、マッピング インターフェイスに任意のインターフェイスを指定して、マッピングアドレスの固有のネットワークを使用すると、この状況は発生しません。入力インターフェイスの [詳細 (Advanced)] 設定で ARP テーブルを設定します。

### 固有のネットワーク上のアドレス

宛先 (マッピング) インターフェイスのネットワーク上で使用可能な数より多くのアドレスが必要な場合は、別のサブネット上でアドレスを指定できます。アップストリームルータには、

Firepower Threat Defense デバイスを指しているマッピング アドレスのスタティック ルートが必要です。

また、ルーテッドモードの場合、宛先ネットワーク上の IP アドレスをゲートウェイとして使用して、マッピングアドレスの Firepower Threat Defense デバイスにスタティック ルートを設定し、ルーティングプロトコルを使用してルートを再配布することができます。たとえば、内部ネットワーク (10.1.1.0/24) には NAT を使用して、マッピング IP アドレス 209.165.201.5 を使用する場合、209.165.201.5 255.255.255.255 (ホストアドレス) に対して、10.1.1.99 ゲートウェイへのスタティック ルートを設定し、これを再配布できます。

トランスペアレントモードでは、実際のホストが直接接続されている場合は、Firepower Threat Defense デバイスをポイントするように、上流に位置するルータのスタティック ルートを設定します。ブリッジグループの IP アドレスを指定します。トランスペアレントモードのリモートホストの場合は、上流に位置するルータのスタティック ルートで、代わりに下流ルータの IP アドレスを指定できます。

## 実際のアドレスと同じアドレス (アイデンティティ NAT)

アイデンティティ NAT のデフォルト動作で、プロキシ ARP は有効になっており、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP を無効にすることができます。必要に応じて標準スタティック NAT のプロキシ ARP を無効にできます。その場合は、アップストリーム ルータに適切なルートがあることを確認する必要があります。

アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。たとえば、「任意」の IP アドレスの広範なアイデンティティ NAT ルールを設定した場合、プロキシ ARP を有効のままにしておくと、マッピング インターフェイスに直接接続されたネットワーク上のホストの問題を引き起こすことがあります。この場合、マッピング ネットワークのホストが同じネットワークの他のホストと通信すると、ARP 要求内のアドレスは (「任意」のアドレスと一致する) NAT ルールと一致します。次に、Firepower Threat Defense デバイスは、パケットが実際に Firepower Threat Defense デバイス宛てでなくても、アドレスの ARP をプロキシします。(この問題は、手動 NAT ルールが設定されている場合にも発生します。NAT ルールは送信元と宛先のアドレス両方に一致する必要がありますが、プロキシ ARP 判定は「送信元」アドレスに対してのみ行われます)。Firepower Threat Defense デバイスの ARP 応答が実際のホストの ARP 応答の前に受信された場合、トラフィックは誤って Firepower Threat Defense デバイスに送信されます。

## NAT のガイドライン

ここでは、NAT を実装するためのガイドラインについて詳細に説明します。

## NAT のファイアウォールモードのガイドライン

NAT は、ルーテッドモードとトランスペアレントファイアウォールモードでサポートされています。

ただし、ブリッジグループメンバーのインターフェイス（ブリッジグループ仮想インターフェイスの一部であるインターフェイス、BVI）での NAT 設定には次の制限があります。

- ブリッジグループのメンバーに NAT を設定するには、メンバーインターフェイスを指定します。NAT をブリッジグループインターフェイス（BVI）自体に設定することはできません。
- ブリッジグループメンバーのインターフェイス間で NAT を実行するときには、実際のおよびマッピングされたアドレスを指定する必要があります。インターフェイスとして「任意」を指定することはできません。
- インターフェイスに接続されている IP アドレスがないため、マッピングされたアドレスがブリッジグループメンバーのインターフェイスである場合、インターフェイス PAT を設定することはできません。
- 送信元インターフェイスと宛先インターフェイスが同じブリッジグループのメンバーである場合、IPv4 ネットワークと IPv6 ネットワーク（NAT64/46）同士を変換することはできません。スタティック NAT/PAT 44/66、ダイナミック NAT44/66、およびダイナミック PAT44 のみが許可されている方法であり、ダイナミック PAT66 はサポートされません。



(注) インライン、インライン タップ、またはパッシブ モードで動作するインターフェイスに対しては NAT を設定できません。

## IPv6 NAT のガイドライン

NAT では、IPv6 のサポートに次のガイドラインと制限が伴います。

- 標準のルーテッドモードのインターフェイスの場合は、IPv4 と IPv6 との間でも変換できます。
- 同じブリッジグループのメンバーであるインターフェイスでは、IPv4 と IPv6 の間の変換はできません。2つの IPv6 ネットワーク間または2つの IPv4 ネットワーク間でのみ変換できます。
- 同じブリッジグループ内のインターフェイス間で変換する場合は、IPv6 対応のダイナミック PAT（NAT66）は使用できません。
- スタティック NAT の場合は、/64 までの IPv6 サブネットを指定できます。これよりも大きいサブネットはサポートされません。
- FTP を NAT46 とともに使用する場合は、IPv4 FTP クライアントが IPv6 FTP サーバに接続するときに、クライアントは拡張パッシブモード（EPSV）または拡張ポートモード（EPRT）を使用する必要があります。PASV コマンドおよび PORT コマンドは IPv6 ではサポートされません。

## IPv6 NAT の推奨事項

NAT を使用すると、IPv6 ネットワーク間、さらに IPv4 および IPv6 ネットワークの間で変換できます (ルーテッドモードのみ)。次のベストプラクティスを推奨します。

- NAT66 (IPv6-to-IPv6) : スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます (手動 NAT のみ)。
- NAT46 (IPv4-to-IPv6) : スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいため、容易にスタティック変換に対応できます。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます (手動 NAT のみ)。IPv6 サブネットに変換する場合 (/96 以下)、結果のマッピングアドレスはデフォルトで IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます (混合表記で表示)。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。また、任意で、ネット間のアドレスを変換できます。この場合、最初の IPv6 アドレスに最初の IPv4 アドレス、2 番目 IPv6 アドレスに 2 番目の IPv4 アドレス、のようにマッピングします。
- NAT64 (IPv6-to-IPv4) : IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

## インスペクション対象プロトコルに対する NAT サポート

セカンダリ接続を開くアプリケーション層プロトコルの一部、またはパケットに IP アドレスを埋め込んだアプリケーション層プロトコルの一部は、次のサービスを提供するためにインスペクションが実行されます。

- ピンホールの作成 : 一部のアプリケーションプロトコルは、標準ポートまたはネゴシエートされたポートでセカンダリ TCP または UDP 接続を開きます。インスペクションでは、これらのセカンダリポートのピンホールが開くため、ユーザはそれらを許可するアクセスコントロールルールを作成する必要はありません。
- NAT の書き換え : プロトコルの一部としてのパケットデータ内のセカンダリ接続用の FTP 埋め込み型 IP アドレスおよびポートなどのプロトコル。エンドポイントのいずれかに関与する NAT 変換がある場合、インスペクションエンジンは、埋め込まれたアドレスおよびポートの NAT 変換を反映するようにパケットデータを書き換えます。セカンダリ接続は NAT の書き換えがないと動作しません。
- プロトコルの強制 : 一部のインスペクションでは、インスペクション対象プロトコルにある程度の RFC への準拠が強制されます。

次の表に、NAT の書き換えと NAT の制限事項を適用するインスペクション対象プロトコルを示します。これらのプロトコルを含む NAT ルールの作成時は、これらの制限事項に留意してください。ここに記載されていないインスペクション対象プロトコルは NAT の書き換えを適用しません。これらのインスペクションには、GTP、HTTP、IMAP、POP、SMTP、SSH、および SSL が含まれます。



- (注) NAT の書き換えは、リストされているポートでのみサポートされます。これらのプロトコルの一部では、ネットワーク解析ポリシーを使用してインスペクションを他のポートに拡張できますが、NAT の書き換えはこれらのポートに拡張されません。これには、DCERPC、DNS、FTP、および Sun RPC のインスペクションが含まれます。非標準ポートでこれらのプロトコルを使用する場合は、接続で NAT を使用しないでください。

表 77: NAT のサポート対象アプリケーション インスペクション

Application	インスペクション対象 プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
DCERPC	TCP/135	NAT64 なし。	○
DNS over UDP	UDP/53	NAT サポートは、WINS 経由の名前解決では使用できません。	なし
ESMTP	TCP/25	NAT64 なし。	なし
FTP	TCP/21	制限なし。 (クラスタリング) スタティック PAT なし。	○
H.323 H.225 (コール シグナリング) H.323 RAS	TCP/1720 UDP/1718 RAS の場合、 UDP/1718 ~ 1719	(クラスタリング) スタティック PAT なし。 拡張 PAT なし。 NAT64 なし。	○
ICMP ICMP エラー	ICMP (デバイス インター フェイスに送信される ICMP トラフィックの インスペクションは実 行されません。)	制限なし。	なし
IP オプション	RSVP	NAT64 なし。	なし
NetBIOS Name Server over IP	UDP/137、138 (送信元 ポート)	拡張 PAT なし。 NAT64 なし。	なし



Application	インスペクション対象 プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
RSH	TCP/514	PAT なし。 NAT64 なし。 (クラスタリング) スタティック PAT なし。	○
RTSP	TCP/554 (HTTP クローキング は処理しません。)	拡張 PAT なし。 NAT64 なし。 (クラスタリング) スタティック PAT なし。	○
SIP	TCP/5060 UDP/5060	拡張 PAT なし。 NAT64 または NAT46 なし。 (クラスタリング) スタティック PAT なし。	○
Skinny (SCCP)	TCP/2000	拡張 PAT なし。 NAT64、NAT46、または NAT66 なし。 (クラスタリング) スタティック PAT なし。	○
SQL*Net (バージョン 1、2)	TCP/1521	拡張 PAT なし。 NAT64 なし。 (クラスタリング) スタティック PAT なし。	○
Sun RPC	TCP/111 UDP/111	拡張 PAT なし。 NAT64 なし。	○
TFTP	UDP/69	NAT64 なし。 (クラスタリング) スタティック PAT なし。 ペイロード IP アドレスは変換されません。	○
XDMCP	UDP/177	拡張 PAT なし。 NAT64 なし。 (クラスタリング) スタティック PAT なし。	○

## NAT のその他のガイドライン

- (自動 NAT のみ) 特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。オブジェクトに対して複数の NAT ルールを設定する場合は、同じ IP アドレスを指定する異なる名前の複数のオブジェクトを作成する必要があります。

- インターフェイスで VPN が定義されている場合、そのインターフェイスの着信 ESP トラフィックには NAT ルールは適用されません。システムは、確立済みの VPN トンネルに対してのみ ESP トラフィックを許可し、既存のトンネルに関連付けられていないトラフィックはドロップされます。この制約は、ESP および UDP のポート 500 と 4500 に適用されません。
- NAT 設定を変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT 設定が使用されるようにするには、デバイスの CLI で **clear xlate** コマンドを使用して変換テーブルを消去できます。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。



(注) ダイナミック NAT または PAT ルールを削除し、次に削除したルールに含まれるアドレスと重複するマッピングアドレスを含む新しいルールを追加すると、新しいルールは、削除されたルールに関連付けられたすべての接続がタイムアウトするか、**clear xlate** コマンドを使用してクリアされるまで使用されません。この予防手段のおかげで、同じアドレスが複数のホストに割り当てられないようにすることができます。

- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを含めることはできません。オブジェクトグループには、1 つのタイプのアドレスのみを含める必要があります。
- (手動 NAT のみ) NAT ルールで送信元アドレスとして **any** を使用する場合、「any」トラフィックの定義 (IPv4 と IPv6) はルールによって異なります。Firepower Threat Defense デバイスがパケットに対して NAT を実行する前に、パケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件では、Firepower Threat Defense デバイスが、NAT ルールの **any** の値を決定できます。たとえば、「any」から IPv6 サーバへのルールを設定しており、このサーバが IPv4 アドレスからマップされている場合、**any** は「任意の IPv6 トラフィック」を意味します。「any」から「any」へのルールを設定しており、送信元をインターフェイス IPv4 アドレスにマッピングする場合、マッピングされたインターフェイス アドレスによって宛先も IPv4 であることが示されるため、**any** は「任意の IPv4 トラフィック」を意味します。
- 同じマッピング オブジェクトやグループを複数の NAT ルールで使用できます。
- マッピング IP アドレス プールに、次のアドレスを含めることはできません。
  - マッピング インターフェイスの IP アドレス。ルールに "any" インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT (ルーテッドモードのみ) の場合は、インターフェイスアドレスの代わりにインターフェイス名を指定します。
  - フェールオーバー インターフェイスの IP アドレス。
  - (トランスペアレント モード) 管理 IP アドレス。

- (ダイナミック NAT) VPN が有効な場合は、スタンバイ インターフェイスの IP アドレス。
- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- ルールで宛先インターフェイスを指定すると、ルーティングテーブルでルートが検索されるのではなく、そのインターフェイスが出力インターフェイスとして使用されます。ただし、アイデンティティ NAT の場合は、代わりにルート ルックアップを使用するオプションがあります。

## 脅威に対する防御のための NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ネットワークアドレス変換は非常に複雑な場合があります。変換の問題やトラブルシューティングが困難な状況を避けるため、ルールはできるだけシンプルにすることを推奨します。NAT を実装する前に注意深く計画することが重要です。次の手順では、基本的なアプローチを示します。

NAT ポリシーは、共有ポリシーです。同様の NAT ルールを持つべきデバイスに、ポリシーを割り当てます。

割り当てられたデバイスにポリシーの特定のルールが適用されるかどうかは、ルールで使用されるインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) によって決定されます。インターフェイスオブジェクトにデバイスのインターフェイスが1つ以上含まれている場合、ルールがデバイスに導入されます。したがって、注意深くインターフェイスオブジェクトを設計することで、単一の共有ポリシー内のデバイスのサブセットに適用されるルールを設定できます。「任意」のインターフェイスオブジェクトに適用されるルールは、すべてのデバイスに導入されます。

デバイスのグループにさまざまなルールが必要な場合は、複数の NAT ポリシーを設定できます。

### 手順

**ステップ 1** [デバイス (Devices) ] > [NAT] を選択します。

- 新しいポリシーを作成するには、**[新しいポリシー (New Policy)]** > **[脅威防御 NAT (Threat Defense NAT)]** をクリックします。ポリシーに名前を付け、オプションでデバイスを割り当て、**[保存 (Save)]** をクリックします。

デバイスの割り当てを後で変更するには、ポリシーを編集して、**[ポリシー割り当て (Policy Assignments)]** リンクをクリックします。

- 既存の脅威防御 NAT ポリシーを編集するには、編集アイコン (✎) をクリックします。このページには、Firepower Threat Defense では使用されない Firepower NAT ポリシーも表示されます。

## ステップ 2 必要なルールを決定します。

ダイナミック NAT ルール、ダイナミック PAT ルール、スタティック NAT ルール、およびアイデンティティ NAT ルールを作成できます。概要については、[NAT タイプ \(1103 ページ\)](#) を参照してください。

## ステップ 3 手動 NAT または自動 NAT として実装するルールを決定します。

これらの2つの実装オプションの比較については、[自動 NAT および手動 NAT \(1106 ページ\)](#) を参照してください。

## ステップ 4 デバイスごとにカスタマイズするルールを決定します。

複数のデバイスに1つの NAT ポリシーを割り当てることができるため、多くのデバイスに1つのルールを設定できます。ただし、各デバイスによって異なる解釈が必要なルールや、デバイスのサブセットにのみ適用すべきルールの場合もあります。

インターフェイスオブジェクトを使用して、ルールを設定するデバイスを制御します。次に、ネットワークオブジェクトでオブジェクトのオーバーライドを使用して、デバイスごとに使用されるアドレスをカスタマイズします。

詳細については、[複数のデバイスの NAT ルールのカスタマイズ \(1119 ページ\)](#) を参照してください。

## ステップ 5 次の項で説明するルールを作成します。

- [ダイナミック NAT \(1122 ページ\)](#)
- [ダイナミック PAT \(1128 ページ\)](#)
- [スタティック NAT \(1138 ページ\)](#)
- [アイデンティティ NAT \(1149 ページ\)](#)

## ステップ 6 NAT ポリシーとルールを管理します。

ポリシーとそのルールを管理するには、次のことを行います。

- ポリシーの名前または説明を編集するには、これらのフィールドをクリックし、変更を入力して、フィールドの外側をクリックします。

- 特定のデバイスに適用されるルールのみを表示するには、[デバイスによるフィルタ (Filter by Device)] をクリックし、目的のデバイスを選択します。ルールがデバイスのインターフェイスを含むインターフェイスオブジェクトを使用している場合、そのデバイスにルールが適用されます。
- ポリシーが割り当てられているデバイスを変更するには、[ポリシー割り当て (Policy Assignments)] リンクをクリックし、必要に応じて選択したデバイスリストを変更します。
- ルールが有効であるか、または無効であるかを変更するには、ルールを右クリックし、[状態 (State)] コマンドから目的のオプションを選択します。これらのコントロールを使用して、ルールを削除しないで一時的に無効にすることができます。
- ルールを編集するには、ルールの編集アイコン (✎) をクリックします。
- ルールを削除するには、ルールの削除アイコン (🗑) をクリックします。

**ステップ 7** [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

## 複数のデバイスの NAT ルールのカスタマイズ

NAT ポリシーは共有されるため、複数のデバイスに特定のポリシーを割り当てることができます。ただし、指定したオブジェクトに設定できる自動 NAT ルールは 1 つまでです。そのため、変換を実行する特定のデバイスに基づいてオブジェクトにさまざまな変換を設定する場合は、インターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) を注意深く設定し、変換済みアドレスのネットワークオブジェクトのオーバーライドを定義する必要があります。

インターフェイスオブジェクトでは、ルールを設定するデバイスを決定します。ネットワークオブジェクトのオーバーライドでは、そのオブジェクトの特定のデバイスで使用する IP アドレスを決定します。

次のような例が考えられます。

- FTD-A と FTD-B に、「inside」という名前のインターフェイスに接続される内部ネットワーク 192.168.1.0/24 があります。
- FTD-A では、「外部」インターフェイスに移動するときに、すべての 192.168.1.0/24 アドレスを 10.100.10.10 ~ 10.100.10.200 の範囲の NAT プールに変換する必要があります。
- FTD-B では、「外部」インターフェイスに移動するときに、すべての 192.168.1.0/24 アドレスを 10.200.10.10 ~ 10.200.10.200 の範囲の NAT プールに変換する必要があります。

このように変換するには、次の手順を実行します。この例のルールはダイナミック自動 NAT 用ですが、任意のタイプの NAT ルールにこのテクニックを一般化できます。

## 手順

**ステップ 1** 内部インターフェイスと外部インターフェイスのセキュリティ ゾーンを作成します。

- a) [オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択します。
- b) コンテンツのテーブルから [インターフェイス オブジェクト (Interface Objects) ] を選択し、[追加 (Add) ] > [セキュリティ ゾーン (Security Zone) ] をクリックします。(ゾーンの代わりにインターフェイス グループを使用できます)。
- c) 内部ゾーンのプロパティを設定します。
  - [名前 (Name) ] : **inside-zone** などの名前を入力します。
  - [タイプ (Type) ] : ルーテッドモードのデバイスの場合は [ルーテッド (Routed) ]、トランスペアレントモードの場合は [スイッチド (Switched) ] を選択します。
  - [選択したインターフェイス (Selected Interfaces) ] : 選択済みリストに FTD-A/内部および FTD-B/内部インターフェイスを追加します。
- d) [保存 (Save) ] をクリックします。
- e) [追加 (Add) ] > [セキュリティ ゾーン (Security Zone) ] をクリックし、外部ゾーンのプロパティを定義します。
  - [名前 (Name) ] : **outside-zone** などの名前を入力します。
  - [タイプ (Type) ] : ルーテッドモードのデバイスの場合は [ルーテッド (Routed) ]、トランスペアレントモードの場合は [スイッチド (Switched) ] を選択します。
  - [選択したインターフェイス (Selected Interfaces) ] : 選択済みリストに FTD-A/外部および FTD-B/外部インターフェイスを追加します。
- f) [保存 (Save) ] をクリックします。

**ステップ 2** [オブジェクト管理 (Object Management) ] ページで、元の内部ネットワーク内のネットワーク オブジェクトを作成します。

- a) コンテンツのテーブルから [ネットワーク (Network) ] を選択し、[ネットワークの追加 (Add Network) ] > [Add Object (オブジェクトの追加) ] をクリックします。
- b) 内部ネットワークのプロパティを設定します。
  - [名前 (Name) ] : **inside-network** などの名前を入力します。
  - [ネットワーク (Network) ] : **192.168.1.0/24** などのネットワーク アドレスを入力します。
- c) [保存 (Save) ] をクリックします。

**ステップ 3** 変換済み NAT プールのネットワーク オブジェクトを作成し、オーバーライドを定義します。

- a) [ネットワークの追加 (Add Network)] > [Add Object (オブジェクトの追加)] をクリックします。
- b) FTD-A の NAT プールのプロパティを設定します。
  - [名前 (Name)] : **NAT-pool** などの名前を入力します。
  - [ネットワーク (Network)] : **10.100.10.10-10.100.10.200** などの FTD-A のプールに含めるアドレスの範囲を入力します。
- c) [オーバーライドを許可 (Allow Overrides)] を選択します。
- d) [オーバーライド (Override)] の見出しをクリックして、オブジェクト オーバーライドのリストを開きます。
- e) [追加 (Add)] をクリックして、[オブジェクト オーバーライドの追加 (Add Object Override)] ダイアログボックスを開きます。
- f) FTD-B を選択し、[選択されたデバイス (Selected Devices)] リストに追加します。
- g) [オーバーライド (Override)] タブをクリックし、[ネットワーク (Network)] を [10.200.10.10-10.200.10.200] に変更します。
- h) [追加 (Add)] をクリックして、オーバーライドをデバイスに追加します。

FTD-B のオーバーライドを定義すると、FTD-B のこのオブジェクトが設定されるたびに、元のオブジェクトに定義されている値の代わりにオーバーライド値が使用されます。
- i) [保存 (Save)] をクリックします。

#### ステップ 4 NAT ルールを設定します。

- a) [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule)] をクリックします。
- c) 次のプロパティを設定します。
  - [NAT ルール (NAT Rule)] = 自動 NAT ルール。
  - [タイプ (Type)] = Dynamic。
- d) [インターフェイス オブジェクト (Interface Objects)] タブで、次の項目を設定します。
  - [送信元インターフェイス オブジェクト (Source Interface Objects)] : inside-zone。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects)] : outside-zone。

(注) インターフェイス オブジェクトはルールが設定されるデバイスを制御します。この例ではゾーンに FTD-A と FTD-B のインターフェイスのみが含まれているため、NAT ポリシーが追加のデバイスに割り当てられた場合でも、ルールはこれらの 2 つのデバイスにのみ展開されます。
- e) [変換 (Translation)] タブで、次の項目を設定します。
  - [元の送信元 (Original Source)] : inside-network オブジェクト。

- [変換済み送信元 (Translated Source) ] > [アドレス (Address) ] : NAT-pool オブジェクト。

f) [保存 (Save) ] をクリックします。

各ファイアウォールによって保護される内部ネットワークに固有の変換を指定して、1つのルールを FTD-A と FTD-B で異なるように解釈できるようになりました。

## ダイナミック NAT

ここでは、ダイナミック NAT とその設定方法について説明します。

### ダイナミック NAT について

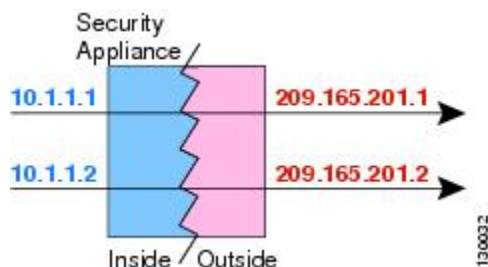
ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピングアドレスのプールに変換されます。マッピングされたプールにあるアドレスは、通常、実際のグループより少なくなります。変換対象のホストが宛先ネットワークにアクセスすると、NAT は、マッピングされたプールから IP アドレスをそのホストに割り当てます。変換は、実際のホストが接続を開始したときにだけ作成されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセスルールでその接続が許可されている場合でも、宛先ネットワークのユーザは、ダイナミック NAT を使用するホストへの確実な接続を開始できません。



- (注) 変換が継続している間、アクセスルールで許可されていれば、リモートホストは変換済みホストへの接続を開始できます。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセスルールのセキュリティに依存できます。

次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

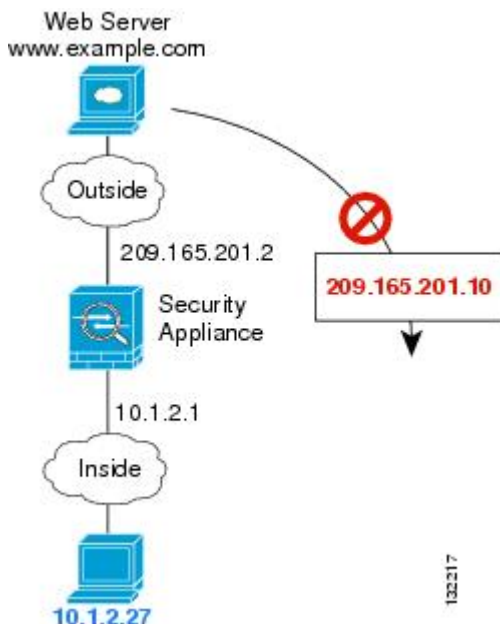
図 23: ダイナミック NAT



次の図に、マッピングアドレスへの接続開始を試みているリモートホストを示します。このアドレスは、現時点では変換テーブルにないため、パケットはドロップされます。



図 24: マッピングアドレスへの接続開始を試みているリモートホスト



## ダイナミック NAT の欠点と利点

ダイナミック NAT には、次の欠点があります。

- マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。

PAT では、1つのアドレスのポートを使用して 64,000 を超える変換を処理できるため、このイベントが頻繁に発生する場合は、PAT または PAT のフォールバック方式を使用します。

- マッピングプールではルーティング可能なアドレスを多数使用する必要があるのに、ルーティング可能なアドレスは多数用意できない場合があります。

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、PAT は次の場合は機能しません。

- GRE バージョン 0 などのように、オーバーロードするためのポートがない IP プロトコルでは機能しません。
- 一部のマルチメディアアプリケーションなどのように、1つのポート上にデータストリームを持ち、別のポート上に制御パスを持ち、公開規格ではないアプリケーションでも機能しません。

## ダイナミック自動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ダイナミック自動 NAT ルールを使用して、宛先ネットワーク上でルーティング可能な別の IP アドレスにアドレスを変換します。

### 始める前に

[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元の送信元 (Original Source)] : これはネットワーク オブジェクト (グループではない) でなければならず、ホスト、範囲、またはサブネットも可能です。
- [変換済み送信元 (Translated Source)] : ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1つのタイプだけ含める必要があります。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。

### 手順

**ステップ 1** [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。

**ステップ 2** 次のいずれかを実行します。

- [ルールの追加 (Add Rule)] ボタンをクリックして、新しいルールを作成します。
- 編集アイコン (✎) をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

**ステップ 3** 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule)] : [自動 NAT ルール (Auto NAT Rule)] を選択します。
- [タイプ (Type)] : [動的 (Dynamic)] を選択します。

**ステップ 4** [インターフェイス オブジェクト (Interface Objects)] タブで、次のフィールドを設定します。

- [送信元インターフェイスオブジェクト (Source Interface Objects) ]、[宛先インターフェイスオブジェクト (Destination Interface Objects) ]: (ブリッジグループメンバーインターフェイスの場合に必要な) **DestinationSource**

**ステップ 5** [一般 (General) ] [変換 (Translation) ] タブで、次のオプションを設定します。

- [元の送信元 (Original Source) ]: 変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元 (Translated Source) ]: マッピングアドレスを含むネットワーク オブジェクトまたはグループ。

**ステップ 6** (オプション) [詳細 (Advanced) ] タブで、必要なオプションを選択します。

- [このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule) ]: DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングインターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、[NAT を使用した DNS クエリと応答の書き換え \(1203 ページ\)](#) を参照してください。
- [インターフェイス PAT へのフォールスルー (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface) ) ]: その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6]: インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。

**ステップ 7** [保存 (Save) ] をクリックしてルールを追加します。

**ステップ 8** NAT ページで [保存 (Save) ] をクリックして変更を保存します。

## ダイナミック手動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

自動 NAT では要件を満たせない場合は、ダイナミック手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。ダイナミック NAT は、宛先ネットワーク上でルーティング可能な別の IP アドレスにアドレスを変換します。

### 始める前に

[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元 (Original Source)] : これはネットワーク オブジェクトまたはグループで、ホストまたはサブネットを含むことができます。すべての元のトラフィックを変換する場合、この手順をスキップし、ルールで [すべて (Any)] を指定します。
- [変換済み送信元 (Translated Source)] : ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。

ルールで各アドレスのスタティック変換を設定すると、[元の宛先 (Original Destination)] および [変換済み宛先 (Translated Destination)] のネットワーク オブジェクトを作成できます。

ダイナミック NAT の場合、宛先でポート変換を実行することもできます。オブジェクト マネージャで、[元の宛先ポート (Original Destination Port)] と [変換済み宛先ポート (Translated Destination Port)] に使用できるポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

### 手順

**ステップ 1** [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。

**ステップ 2** 次のいずれかを実行します。

- [ルール の追加 (Add Rule)] ボタンをクリックして、新しいルールを作成します。
- 編集アイコン (✎) をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

**ステップ 3** 基本ルールのオプションを設定します。

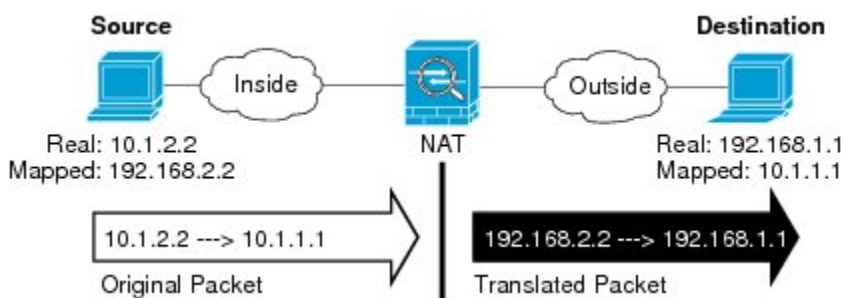
- [NAT ルール (NAT Rule)] : [手動 NAT ルール (Manual NAT Rule)] を選択します。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。
- [有効にする (Enable)] : ルールをアクティブにするかどうかを指定します。ルール ページの右クリック メニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。
- [挿入 (Insert)] : ルールを追加する場所を指定します。ルールは、カテゴリ (自動 NAT ルールの前か後)、または指定したルール番号の上か下に挿入できます。

**ステップ 4** [インターフェイス オブジェクト (Interface Objects)] タブで、次のフィールドを設定します。

- [送信元インターフェイスオブジェクト (Source Interface Objects) ]、[宛先インターフェイスオブジェクト (Destination Interface Objects) ]: (共有ポリシーのみ)。[送信元ゾーン (Source Zone) ]、[宛先ゾーン (Destination Zone) ]: (トランスペアレントファイアウォールモードの場合に必要)。この NAT ルールが適用されるインターフェイスを識別するセキュリティゾーン。[送信元 (Source) ]は、デバイスに入るトラフィックが通過する実際のインターフェイスを含むゾーン。[宛先 (Destination) ]は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含むゾーン。デフォルトでは、すべてのインターフェイスにルールが適用されます ([すべて (Any) ])。(ブリッジグループメンバーインターフェイスの場合に必要) **Source ZoneDestination ZoneSourceDestinationAny**

**ステップ 5** ([変換 (Translation) ]タブで次を実行します。) 元の packet アドレス (IPv4 または IPv6)、つまり、元の packet に表示される packet アドレスを特定します。

元の packet と変換済み packet の例については、次の図を参照してください。



- [元の送信元アドレス (Original Source Address) ]: 変換しているアドレスを含むネットワークオブジェクトまたはグループ。
- [元の宛先アドレス (Original Destination Address) ]: (オプション) 宛先アドレスを含むネットワークオブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用することができます。

**[送信元インターフェイス IP (Source Interface IP) ]** を選択して、送信元インターフェイスの元の宛先 ([すべて (Any) ]は選択不可) をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスに対して、ポート変換を設定したスタティックインターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポートオブジェクトも選択します。

**ステップ 6** 変換された packet アドレス (IPv4 または IPv6)、すなわちそれが宛先インターフェイスネットワーク上に現れるときの packet アドレスを識別します。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元 (Translated Source) ]: マッピングアドレスを含むネットワークオブジェクトまたはグループ。
- [変換済み宛先 (Translated Destination) ]: (オプション)。変換された packet で使用される宛先アドレスを含むネットワークオブジェクトまたはグループ。[元の宛先 (Original Destination) ]を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT (つまり変換なし) を設定できます。

**ステップ 7** (オプション) サービス変換の宛先サービスポートを特定します。[元の宛先ポート (Original Destination Port)]、[変換済み宛先ポート (Translated Destination Port)]。

ダイナミック NAT はポート変換をサポートしていないため、[元の送信元ポート (Original Source Port)] フィールドと [変換済み送信元ポート (Translated Source Port)] フィールドは空白のままにする必要があります。ただし、宛先変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします (両方とも TCP または両方とも UDP)。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

**ステップ 8** (オプション) [詳細 (Advanced)] タブで、必要なオプションを選択します。

- (送信元変換の場合のみ) [このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule)] : DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、[NAT を使用した DNS クエリと応答の書き換え \(1203 ページ\)](#) を参照してください。
- [インターフェイス PAT へのフォールスルー (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface))] : その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合のみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6] : [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。 **IPv6**

**ステップ 9** [保存 (Save)] をクリックしてルールを追加します。

**ステップ 10** NAT ページで [保存 (Save)] をクリックして変更を保存します。

## ダイナミック PAT

次のトピックでは、ダイナミック PAT について説明します。

### ダイナミック PAT について

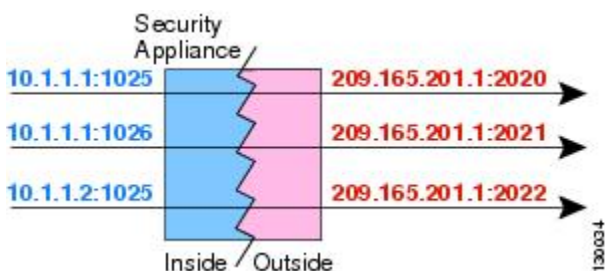
ダイナミック PAT では、実際のアドレスおよび送信元ポートが 1 つのマッピング アドレスおよび固有のポートに変換されることによって、複数の実際のアドレスが 1 つのマッピング IP

アドレスに変換されます。使用できる場合、実際の送信元ポート番号がマッピングポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピングポートは実際のポート番号と同じポート範囲 (0 ~ 511、512 ~ 1023、および 1024 ~ 65535) から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。下位ポート範囲を使用するトラフィックが数多くある場合は、サイズが異なる3つの層の代わりにフラットなポート範囲を使用するように指定できます。

送信元ポートが接続ごとに異なるため、各接続には別の変換セッションが必要です。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

次の図に、一般的なダイナミック PAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。マッピングアドレスはどの変換でも同じですが、ポートがダイナミックに割り当てられます。

図 25: ダイナミック PAT



変換が継続している間、アクセスルールで許可されていれば、宛先ネットワーク上のリモートホストは変換済みホストへの接続を開始できます。実際のポートアドレスおよびマッピングポートアドレスはどちらも予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセスルールのセキュリティに依存できます。

接続の有効期限が切れると、ポート変換も有効期限切れになります。

## ダイナミック PAT の欠点と利点

ダイナミック PAT を使用すると、単一のマッピングアドレスを使用できるため、ルーティング可能なアドレスを節約できます。さらに、Firepower Threat Defense デバイス インターフェイスの IP アドレスを PAT アドレスとして使用できます。

同じブリッジグループ内のインターフェイス間で変換する場合は、IPv6 対応のダイナミック PAT (NAT66) は使用できません。

ダイナミック PAT は、制御パスとは異なるデータ ストリームを持つ一部のマルチメディア アプリケーションでは機能しません。詳細については、[インスペクション対象プロトコルに対する NAT サポート \(1113 ページ\)](#) を参照してください。

ダイナミック PAT によって、単一の IP アドレスから送信されたように見える数多くの接続が作成されることがあります。この場合、このトラフィックはサーバで DoS 攻撃として解釈される可能性があります。アドレスの PAT プールを設定し、PAT アドレスのラウンドロビン割り当てを使用することで、この状況を軽減することができます。

## PAT プールオブジェクトのガイドライン

PAT プールのネットワーク オブジェクトを作成する場合は、次のガイドラインに従ってください。

### PAT プールの場合

- 使用できる場合、実際の送信元ポート番号がマッピングポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピングポートは実際のポート番号と同じポート範囲 (0 ~ 511、512 ~ 1023、および 1024 ~ 65535) から選択されます。そのため、1024 よりも下のポートでは、小さいPATプールのみを使用できます。下位ポート範囲を使用するトラフィックが数多くある場合は、サイズが異なる3つの層の代わりにフラットなポート範囲を使用するように指定できます。1024 ~ 65535 または 1 ~ 65535 です。
- 同じ PAT プールオブジェクトを2つの異なるルールの中で使用する場合は、必ず同じオプションを各ルールに指定してください。たとえば、1つのルールで拡張 PAT およびフラットな範囲が指定される場合は、もう一方のルールでも拡張 PAT およびフラットな範囲が指定される必要があります。

### PAT プールの拡張 PAT の場合

- 多くのアプリケーション インспекションでは、拡張 PAT はサポートされていません。
- ダイナミック PAT ルールに対して拡張 PAT をイネーブルにする場合、PAT プールのアドレスを、ポート トランスレーションルールを持つ別のスタティック NAT の PAT アドレスとしても使用することはできません。たとえば、PAT プールに 10.1.1.1 が含まれている場合、PAT アドレスとして 10.1.1.1 を使用する、ポート トランスレーションルールを持つスタティック NAT は作成できません。
- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。
- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。

### PAT プールのラウンド ロビン方式の場合

- ホストに既存の接続がある場合は、そのホストからの以降の接続は同じ PAT IP アドレスを使用します (ポートが使用可能である場合)。ただし、この「粘着性」は、フェールオーバーが発生すると失われます。デバイスがフェールオーバーすると、ホストからの後続の接続では最初の IP アドレスが使用されない場合があります。
- ラウンドロビンでは、特に拡張 PAT と組み合わせた場合に、大量のメモリが消費されます。NAT プールはマッピングされるプロトコル/IP アドレス/ポート範囲ごとに作成されるため、ラウンドロビンでは数多くの同時 NAT プールが作成され、メモリが使用されます。拡張 PAT では、さらに多くの同時 NAT プールが作成されます。



## ダイナミック自動 PAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ダイナミック自動 PAT ルールを使用して、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。1つのアドレス（宛先インターフェイスまたは他のアドレスのいずれか）に変換するか、またはたくさんの有効な変換を提供するために、アドレスの PAT プールを使用します。

### 始める前に

[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。 > または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元の送信元 (Original Source)] : これはネットワーク オブジェクト（グループではない）でなければならず、ホスト、範囲、またはサブネットも可能です。
- [変換済み送信元 (Translated Source)] : PAT アドレスを指定するオプションは次のとおりです。
  - [宛先インターフェイス (Destination Interface)] : 宛先インターフェイスのアドレスを使用するには、ネットワーク オブジェクトは必要ありません。
  - [単一 PAT アドレス (Single PAT address)] : 単一のホストを含むネットワーク オブジェクトを作成します。
  - [PAT プール (PAT pool)] : 範囲を含むネットワーク オブジェクトを作成するか、またはホスト、範囲あるいはその両方を含むネットワーク オブジェクトグループを作成します。サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1つのタイプだけ含める必要があります。

### 手順

**ステップ 1** [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。

**ステップ 2** 次のいずれかを実行します。

- [ルールの追加 (Add Rule)] ボタンをクリックして、新しいルールを作成します。
- 編集アイコン (✎) をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

**ステップ 3** 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule) ] : [自動 NAT ルール (Auto NAT Rule) ] を選択します。
- [タイプ (Type) ] : [ダイナミック (Dynamic) ] を選択します。

**ステップ 4** [インターフェイス オブジェクト (Interface Objects) ] タブで、以下のオプションを設定します。

- [送信元インターフェイス オブジェクト (Source Interface Objects) ]、[宛先インターフェイス オブジェクト (Destination Interface Objects) ] : (ブリッジグループ メンバー インターフェイスの場合に必要な) **DestinationSource**

**ステップ 5** [一般 (General) ] [変換 (Translation) ] タブで、次のオプションを設定します。

- [元の送信元 (Original Source) ] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元 (Translated Source) ] : 以下のいずれかになります。
  - (インターフェイス PAT) 。宛先のアドレスのインターフェイスを使用するには、[インターフェイス (Interface) ] > [宛先インターフェイス IP (Destination Interface IP) ] を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced) ] タブで [IPv6] オプションを選択する必要もあります。PAT プールの設定ステップを飛ばします。
  - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールの設定ステップを飛ばします。
  - PAT プールを使用するには、[変換済み送信元 (Translated Source) ] を空にしておきます。

**ステップ 6** PAT プールを使用している場合は、[PAT プール (PAT Pool) ] タブを選択して、次の手順を実行します。

- a) [PAT プールの有効化 (Enable PAT pool) ] を選択します。
- b) [PAT] > [アドレス (Address) ] フィールドで、プールのアドレスを保持するネットワーク オブジェクト グループを選択します。

または、インターフェイス PAT を実装するもう 1 つの方法として、[インターフェイス (Interface) ] [宛先インターフェイス IP (Destination Interface IP) ] を選択します。

- c) (オプション) 必要に応じて、次のオプションを選択します。
  - [ラウンドロビン割り当てを使用 (Use Round Robin Allocation) ] : アドレスとポートをラウンドロビン形式で割り当てます。デフォルトではラウンドロビンを使用されず、1 つの PAT アドレスのポートがすべて割り当てられてから次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレ

スとポートが割り当てられると、また最初のアドレスに戻り、次に 2 番目のアドレスという順に使用されます。

- [拡張 PAT テーブル (Extended PAT Table) ] : 拡張 PAT を使用します。拡張 PAT では、変換情報に宛先アドレスとポートを含めることで、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。このオプションは、インターフェイス PAT またはインターフェイス PAT フォールバックで使用することはできません。
- [フラットなポート範囲 (Flat Port Range) ]、[予約済みポートを含む (Include Reserved Ports) ] : TCP/UDP ポートを割り当てる際に、ポート範囲 (1024 ~ 65535) を単一のフラットな範囲として使用します。変換用のマッピングポート番号を選択する場合、PAT によって、実際の送信元ポート番号が使用されます (使用可能な場合)。ただし、このオプションを設定しないと、実際のポートが使用できない場合、デフォルトでは、実際のポート番号と同じポート範囲 (1 ~ 511、512 ~ 1023、および 1024 ~ 65535) からマッピングポートが選択されます。下位の範囲でポートが不足するのを回避するには、この設定を行います。1 ~ 65535 の範囲全体を使用するには、[予約済みポートを含む (Include Reserved Ports) ] オプションも選択します。

**ステップ 7** (オプション) [詳細 (Advanced) ] タブで、必要なオプションを選択します。

- [インターフェイス PAT へのフォールスルー (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface)) ] : [インターフェイス PAT へのフォールスルー (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface)) ] : (ルーテッドモードのみ)。その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションを選択します。インターフェイス PAT を変換済みアドレスまたは PAT プールとしてすでに設定している場合、このオプションは選択できません。その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6] : [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。

**ステップ 8** [保存 (Save) ] をクリックしてルールを追加します。

**ステップ 9** NAT ページで [保存 (Save) ] をクリックして変更を保存します。

## ダイナミック手動 PAT の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

自動 PAT がお客様のニーズを満たしていない場合は、ダイナミック手動 PAT ルールを使用します。たとえば、宛先に基づいて別の変換を行いたい場合に使用します。ダイナミック PAT は、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。1つのアドレス（宛先インターフェイスまたは他のアドレスのいずれか）に変換するか、またはたくさんの有効な変換を提供するために、アドレスの PAT プールを使用します。

### 始める前に

[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。> IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

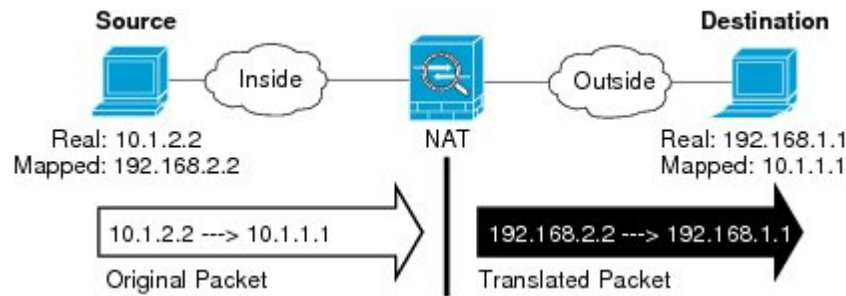
- [元の送信元 (Original Source)] : これはネットワーク オブジェクトまたはグループで、ホスト、範囲、またはサブネットを含むことができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて (Any)] を指定します。
- [変換済み送信元 (Translated Source)] : PAT アドレスを指定するオプションは次のとおりです。
  - [宛先インターフェイス (Destination Interface)] : 宛先インターフェイスのアドレスを使用するには、ネットワーク オブジェクトは必要ありません。
  - [単一 PAT アドレス (Single PAT address)] : 単一のホストを含むネットワーク オブジェクトを作成します。
  - [PAT プール (PAT pool)] : 範囲を含むネットワーク オブジェクトを作成するか、またはホスト、範囲あるいはその両方を含むネットワーク オブジェクトグループを作成します。サブネットを含めることはできません。

ルールで各アドレスの静的変換を設定すると、[元の宛先 (Original Destination)] および [変換済み宛先 (Translated Destination)] のネットワーク オブジェクトを作成できます。

ダイナミック NAT の場合、宛先でポート変換を実行することもできます。オブジェクトマネージャで、[元の宛先ポート (Original Destination Port)] と [変換済み宛先ポート (Translated Destination Port)] に使用できるポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

## 手順

- ステップ 1** [デバイス (Devices) ] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- ステップ 2** 次のいずれかを実行します。
- [ルールの追加 (Add Rule) ] ボタンをクリックして、新しいルールを作成します。
  - 編集アイコン (✎) をクリックして、既存のルールを編集します。
- メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。
- ステップ 3** 基本ルールのオプションを設定します。
- [NAT ルール (NAT Rule) ] : [手動 NAT ルール (Manual NAT Rule) ] を選択します。
  - [タイプ (Type) ] : [ダイナミック (Dynamic) ] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。
  - [有効にする (Enable) ] : ルールをアクティブにするかどうかを指定します。ルールページの右クリックメニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。
  - [挿入 (Insert) ] : ルールを追加する場所を指定します。ルールは、カテゴリ (自動 NAT ルールの前か後) 、または指定したルール番号の上か下に挿入できます。
- ステップ 4** [インターフェイス オブジェクト (Interface Objects) ] タブで、以下のオプションを設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects) ]、[宛先インターフェイス オブジェクト (Destination Interface Objects) ] : (共有ポリシーのみ) 。[送信元ゾーン (Source Zone) ]、[宛先ゾーン (Destination Zone) ] : (トランスペアレントファイアウォールモードの場合に必要) 。この NAT ルールが適用されるインターフェイスを識別するセキュリティゾーン。[送信元 (Source) ] は、デバイスに入るトラフィックが通過する実際のインターフェイスを含むゾーン。[宛先 (Destination) ] は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含むゾーン。デフォルトでは、すべてのインターフェイスにルールが適用されます ([すべて (Any) ]) 。(ブリッジグループメンバーインターフェイスの場合に必要) **Source ZoneDestination ZoneSourceDestinationAny**
- ステップ 5** ([変換 (Translation) ] タブで次を実行します。) 元のパケットアドレス (IPv4 または IPv6) 、つまり、元のパケットに表示されるパケットアドレスを特定します。
- 元のパケットと変換済みパケットの例については、次の図を参照してください。



- [元の送信元アドレス (Original Source Address) ] : 変換しているアドレスを含むネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス (Original Destination Address) ] : (オプション) 宛先アドレスを含むネットワークオブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用することができます。

[送信元インターフェイス IP (Source Interface IP) ] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any) ] は選択不可) をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスに対して、ポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポートオブジェクトも選択します。

**ステップ 6** 変換されたパケットアドレス (IPv4 または IPv6) 、すなわちそれが宛先インターフェイスネットワーク上に現れるときのパケットアドレスを識別します。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元 (Translated Source) ] : 以下のいずれかになります。
  - (インターフェイス PAT) 。宛先のアドレスのインターフェイスを使用するには、[インターフェイス (Interface) ] > [宛先インターフェイス IP (Destination Interface IP) ] を選択します。また特定の宛先インターフェイスオブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced) ] タブで [IPv6] オプションを選択する必要もあります。PAT プールの設定ステップを飛ばします。
  - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールの設定ステップを飛ばします。
  - PAT プールを使用するには、[変換済み送信元 (Translated Source) ] を空にしておきます。
- [変換済み宛先 (Translated Destination) ] : (オプション) 。変換されたパケットで使用される宛先アドレスを含むネットワークオブジェクトまたはグループ。[元の宛先 (Original Destination) ] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT (つまり変換なし) を設定できます。

**ステップ 7** (オプション) サービス変換の宛先サービスポートを特定します。[元の宛先ポート (Original Destination Port) ]、[変換済み宛先ポート (Translated Destination Port) ]。

ダイナミック NAT はポート変換をサポートしていないため、[元の送信元ポート (Original Source Port) ] フィールドと [変換済み送信元ポート (Translated Source Port) ] フィールドは空白のままにする必要があります。ただし、宛先変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします (両方とも TCP または両方とも UDP)。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

**ステップ 8** PAT プールを使用している場合は、[PAT プール (PAT Pool) ] タブを選択して、次の手順を実行します。

- a) [PAT プールの有効化 (Enable PAT pool) ] を選択します。
- b) [PAT] > [アドレス (Address) ] フィールドで、プールのアドレスを保持するネットワーク オブジェクト グループを選択します。

または、インターフェイス PAT を実装するもう 1 つの方法として、[インターフェイス (Interface) ] [宛先インターフェイス IP (Destination Interface IP) ] を選択します。

- c) (オプション) 必要に応じて、次のオプションを選択します。
  - [ラウンドロビン割り当てを使用 (Use Round Robin Allocation) ] : アドレスとポートをラウンドロビン形式で割り当てます。デフォルトではラウンドロビンは使用されず、1 つの PAT アドレスのポートがすべて割り当てられてから次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレスとポートが割り当てられると、また最初アドレスに戻り、次に 2 番目のアドレスという順に使用されます。
  - [拡張 PAT テーブル (Extended PAT Table) ] : 拡張 PAT を使用します。拡張 PAT では、変換情報に宛先アドレスとポートを含めることで、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。このオプションは、インターフェイス PAT またはインターフェイス PAT フォールバックで使用することはできません。
  - [フラットなポート範囲 (Flat Port Range) ]、[予約済みポートを含む (Include Reserved Ports) ] : TCP/UDP ポートを割り当てる際に、ポート範囲 (1024 ~ 65535) を単一のフラットな範囲として使用します。変換用のマッピングポート番号を選択する場合、PAT によって、実際の送信元ポート番号が使用されます (使用可能な場合)。ただし、このオプションを設定しないと、実際のポートが使用できない場合、デフォルトでは、実際のポート番号と同じポート範囲 (1 ~ 511、512 ~ 1023、および 1024 ~ 65535) からマッピングポートが選択されます。下位の範囲でポートが不足するのを回避するには、この設定を行います。1 ~ 65535 の範囲全体を使用するには、[予約済みポートを含む (Include Reserved Ports) ] オプションも選択します。

**ステップ 9** (オプション) [詳細 (Advanced)] タブで、必要なオプションを選択します。

- [インターフェイス PAT へのフォールスルー (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface))] : その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6] : [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。 **IPv6**

**ステップ 10** [保存 (Save)] をクリックしてルールを追加します。

**ステップ 11** NAT ページで [保存 (Save)] をクリックして変更を保存します。

## スタティック NAT

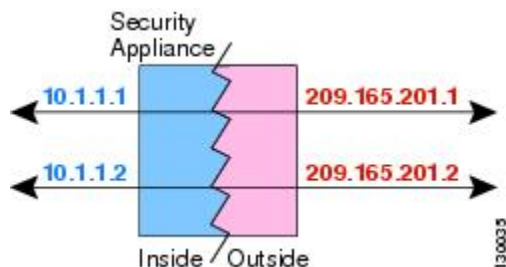
ここでは、スタティック NAT とその実装方法について説明します。

### スタティック NAT について

スタティック NAT では、実際のアドレスからマッピングアドレスへの固定変換が作成されます。マッピングアドレスは連続する各接続で同じであるため、スタティック NAT では、双方向の接続 (ホストへの接続とホストから接続の両方) を開始できます (接続を許可するアクセスルールが存在する場合)。一方、ダイナミック NAT および PAT では、各ホストが以降の各変換に対して異なるアドレスまたはポートを使用するため、双方向の開始はサポートされません。

次の図は、スタティック NAT の一般的なシナリオを示します。この変換は常にアクティブであるため、実際のホストとリモートホストの両方が接続を開始できます。

図 26: スタティック NAT



(注) 必要に応じて、双方向接続を無効にできます。



## ポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT では、実際のプロトコルおよびポートとマッピングされたプロトコルおよびポートを指定できます。

スタティック NAT を使用してポートを指定する場合、ポートまたは IP アドレスを同じ値にマッピングするか、別の値にマッピングするかを選択できます。

次の図に、ポート変換が設定された一般的なスタティック NAT のシナリオを示します。自身にマッピングしたポートと、別の値にマッピングしたポートの両方を示しています。いずれのケースでも、IP アドレスは別の値にマッピングされています。この変換は常にアクティブであるため、変換されたホストとリモートホストの両方が接続を開始できます。

図 27: ポート変換を設定したスタティック NAT の一般的なシナリオ



(注) セカンダリチャネルのアプリケーションインスペクションが必要なアプリケーション (FTP、VoIP など) を使用する場合は、NAT が自動的にセカンダリポートを変換します。

次に、ポート変換を設定したスタティック NAT のその他の使用例の一部を示します。

### アイデンティティ ポート変換を設定したスタティック NAT

内部リソースへの外部アクセスを簡素化できます。たとえば、異なるポートでサービスを提供する3つの個別のサーバ (FTP、HTTP、SMTP など) がある場合は、それらのサービスにアクセスするための単一の IP アドレスを外部ユーザに提供できます。その後、アイデンティティ ポート変換を設定したスタティック NAT を設定し、アクセスしようとしているポートに基づいて、単一の外部 IP アドレスを実サーバの正しい IP アドレスにマッピングすることができます。サーバは標準のポート (それぞれ 21、80、および 25) を使用しているため、ポートを変更する必要はありません。

### 標準以外のポートのポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT を使用すると、予約済みポートから標準以外のポートへの変換や、その逆の変換も実行できます。たとえば、内部 Web サーバがポート 8080 を使用する場合、ポート 80 に接続することを外部ユーザに許可し、その後、変換を元のポート 8080 に戻すことができます。同様に、セキュリティをさらに高めるには、Web ユーザに標準以外のポート 6785 に接続するように指示し、その後、変換をポート 80 に戻すことができます。

### ポート変換を設定したスタティック インターフェイス NAT

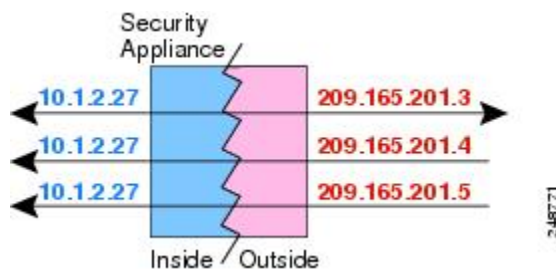
スタティック NAT は、実際のアドレスをインターフェイス アドレスとポートの組み合わせにマッピングするように設定できます。たとえば、デバイスの外部インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を外部インターフェイス アドレス/ポート 23 にマッピングできます。

### 一対多のスタティック NAT

通常、スタティック NAT は 1 対 1 のマッピングで設定します。しかし、場合によっては、1 つの実際のアドレスを複数のマッピング アドレスに設定することがあります (1 対多)。1 対多のスタティック NAT を設定する場合、実際のホストがトラフィックを開始すると、常に最初のマッピング アドレスが使用されます。しかし、ホストに向けて開始されたトラフィックの場合、任意のマッピング アドレスへのトラフィックを開始でき、1 つの実際のアドレスには変換されません。

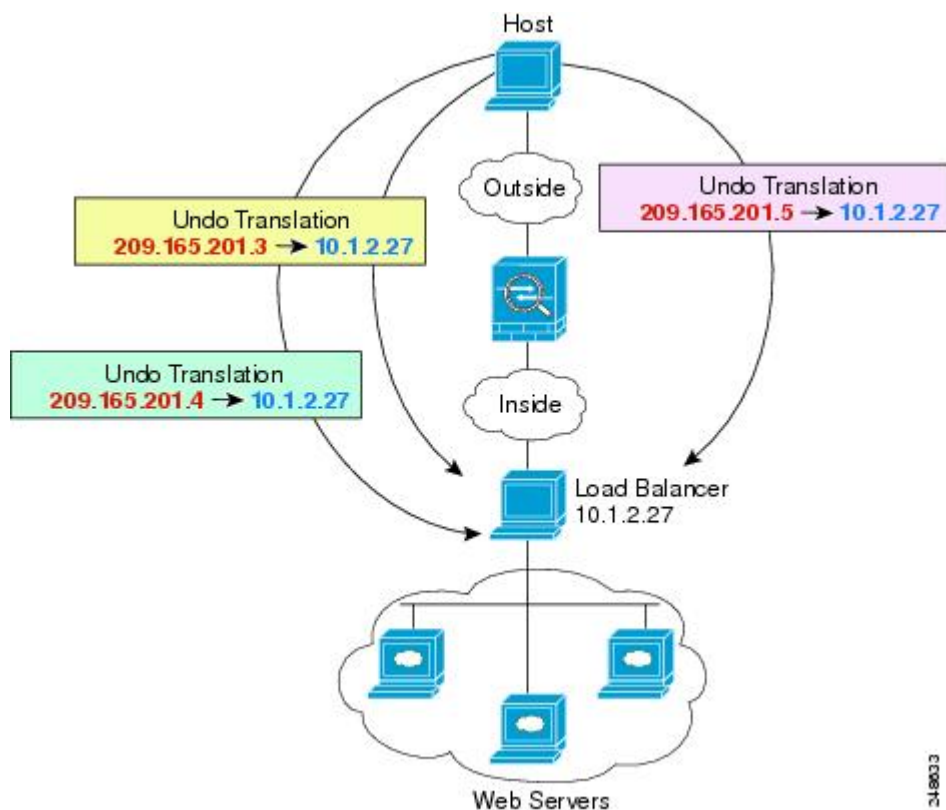
次の図に、一般的な一対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピング アドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 28: 一対多のスタティック NAT



たとえば、10.1.2.27 にロード バランサが存在するとします。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。

図 29: 一対多のスタティック NAT の例



### 他のマッピング シナリオ (非推奨)

NATには、1対1、1対多だけでなく、少対多、多対少、多対1など任意の種類のスタティックマッピングシナリオを使用できるという柔軟性があります。1対1マッピングまたは1対多マッピングだけを使用することをお勧めします。これらの他のマッピングオプションは、予期しない結果が発生する可能性があります。

機能的には、少対多は1対多と同じです。ただし、設定が複雑になり、実際のマッピングがひと目で明らかにならない可能性があるため、必要とする実際の各アドレスに対して1対多の設定を作成することをお勧めします。たとえば、少対多のシナリオでは、少数の実際のアドレスが多数のマッピングアドレスに順番にマッピングされます (Aは1、Bは2、Cは3)。すべての実際のアドレスがマッピングされたら、次のマッピングアドレスが最初の実際のアドレスにマッピングされ、すべてのマッピングアドレスがマッピングされるまで続行されます (Aは4、Bは5、Cは6)。この結果、実際の各アドレスに対して複数のマッピングアドレスが存在することになります。1対多の設定のように、最初のマッピングだけが双方向であり、以降のマッピングでは、実際のホストへのトラフィックを開始できますが、実際のホストからのすべてのトラフィックは、送信元の最初のマッピングアドレスだけを使用できます。

次の図に、一般的な少対多のスタティック NAT シナリオを示します。

図 30: 少対多のスタティック NAT



多対少または多対1の設定では、マッピングアドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足するよりも前に、マッピングアドレスが不足します。双方向の開始を実現できるのは、最下位の実際の IP アドレスとマッピング プールの間でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターントラフィックは、接続の固有の5つの要素（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。



- (注) 多対少または多対1の NAT は PAT ではありません。2つの実際のホストが同じ送信元ポート番号を使用して同じ外部サーバおよび同じ TCP 宛先ポートにアクセスする場合は、両方のホストが同じ IP アドレスに変換されると、アドレスの競合がある（5つのタプルが一意でない）ため、両方の接続がリセットされます。

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 31: 多対少のスタティック NAT



このようにスタティックルールを使用するのではなく、双方向の開始を必要とするトラフィックに1対1のルールを作成し、残りのアドレスにダイナミックルールを作成することをお勧めします。

## スタティック自動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

スタティック 自動 NAT ルールを使用して、アドレスを宛先ネットワーク上でルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールでポートの変換もできます。

### 始める前に

[**オブジェクト (Objects)**] > [**オブジェクト管理 (Object Management)**] を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元の送信元 (Original Source) ]: これはネットワーク オブジェクト (グループではない) でなければならず、ホスト、範囲、またはサブネットも可能です。
- [変換済み送信元 (Translated Source) ]: 変換済みアドレスを指定するには、次のオプションがあります。
  - [宛先インターフェイス (Destination Interface) ]: 宛先インターフェイス アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
  - [アドレス (Address) ]: ホスト、範囲、またはサブネットを含むネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

### 手順

**ステップ 1** [**デバイス (Devices)**] > [**NAT**] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。

**ステップ 2** 次のいずれかを実行します。

- [ルール の追加 (Add Rule) ] ボタンをクリックして、新しいルールを作成します。
- 編集アイコン (✎) をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

**ステップ 3** 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule) ] : [自動 NAT ルール (Auto NAT Rule) ] を選択します。
- [タイプ (Type) ] : [スタティック (Static) ] を選択します。

**ステップ 4** [インターフェイス オブジェクト (Interface Objects) ] タブで、以下のオプションを設定します。

- [送信元インターフェイス オブジェクト (Source Interface Objects) ]、[宛先インターフェイス オブジェクト (Destination Interface Objects) ] : (ブリッジグループ メンバー インターフェイスの場合に必要な) **DestinationSource**

**ステップ 5** [一般 (General) ] [変換 (Translation) ] タブで、次のオプションを設定します。

- [元の送信元 (Original Source) ] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元 (Translated Source) ] : 次のいずれかになります。
  - アドレスの設定グループを使用するには、[アドレス (Address) ] およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1対1のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - (ポート変換を設定したスタティック インターフェイス NAT) 。宛先のアドレスのインターフェイスを使用するには、[インターフェイス (Interface) ] [宛先インターフェイス IP (Destination Interface IP) ] を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced) ] タブで [IPv6] オプションを選択する必要もあります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
- (オプション) [元のポート (Original Port) ]、[変換済みポート (Translated Port) ] : TCP または UDP ポートを変換する必要がある場合は、[元のポート (Original Port) ] でプロトコルを選択し、元のポート番号と変換済みポート番号を入力します。たとえば、必要に応じて TCP/80 を 8080 に変換できます。

**ステップ 6** (オプション) [詳細 (Advanced) ] タブで、必要なオプションを選択します。

- [このルールに一致する DNS 応答を変換する (Translate DNS replies that match this rule) ] : DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、[NAT を使用した DNS クエリと応](#)

答の書き換え (1203 ページ) を参照してください。ポート変換を実行する場合、このオプションは使用できません。

- [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。
- [ネット間マッピング (Net to Net Mapping) ] : NAT 46 の場合、このオプションを選択して、最初の IPv4 アドレスを最初の IPv6 アドレスに変換し、2 番目を 2 番目に変換という順序で変換します。このオプションを選択しない場合、IPv4 埋め込み方式が使用されません。1 対 1 の変換の場合は、このオプションを使用する必要があります。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface) ] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

ステップ 7 [保存 (Save) ] をクリックしてルールを追加します。

ステップ 8 NAT ページで [保存 (Save) ] をクリックして変更を保存します。

## スタティック手動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

自動 NAT がニーズを満たさない場合、スタティック手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。スタティック NAT は、アドレスを宛先ネットワーク上でルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールでポートの変換もできます。

### 始める前に

[オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元 (Original Source) ]: これはネットワーク オブジェクトまたはグループで、ホスト、範囲、またはサブネットを含むことができます。すべての元のトラフィックを変換する場合、この手順をスキップし、ルールで [すべて (Any) ] を指定します。
- [変換済み送信元 (Translated Source) ]: 変換済みアドレスを指定するには、次のオプションがあります。
  - [宛先インターフェイス (Destination Interface) ]: 宛先インターフェイス アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
  - [アドレス (Address) ]: ホスト、範囲、またはサブネットを含むネットワーク オブジェクトまたはグループを作成します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数不一致の場合もあります。

ルールで各アドレスのスタティック変換を設定すると、[元の宛先 (Original Destination) ] および [変換済み宛先 (Translated Destination) ] のネットワーク オブジェクトを作成できます。ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピングアドレスに対するオブジェクトの追加をスキップでき、ルールでインターフェイスを指定します。

また送信元、宛先、またはその両方のポート変換も実行できます。Object Manager では、元のポートと変換されたポートで使用できるポート オブジェクトがあることを確認します。

## 手順

- 
- ステップ 1** [デバイス (Devices) ] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- ステップ 2** 次のいずれかを実行します。
- [ルールの追加 (Add Rule) ] ボタンをクリックして、新しいルールを作成します。
  - 編集アイコン (✎) をクリックして、既存のルールを編集します。
- メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。
- ステップ 3** 基本ルールのオプションを設定します。
- [NAT ルール (NAT Rule) ]: [手動 NAT ルール (Manual NAT Rule) ] を選択します。
  - [タイプ (Type) ]: [スタティック (Static) ] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。
  - [有効にする (Enable) ]: ルールをアクティブにするかどうかを指定します。ルール ページの右クリックメニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。



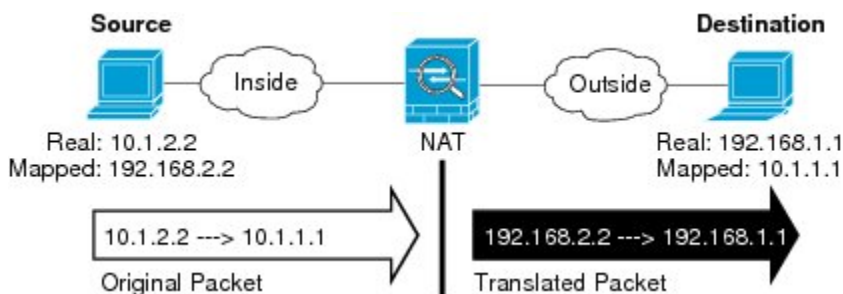
- [挿入 (Insert) ]: ルールを追加する場所を指定します。ルールは、カテゴリ (自動 NAT ルールの前か後)、または指定したルール番号の上か下に挿入できます。

**ステップ 4** [インターフェイスオブジェクト (Interface Objects) ] タブで、以下のオプションを設定します。

- [送信元インターフェイスオブジェクト (Source Interface Objects) ]、[宛先インターフェイスオブジェクト (Destination Interface Objects) ]: (共有ポリシーのみ)。[送信元ゾーン (Source Zone) ]、[宛先ゾーン (Destination Zone) ]: (トランスペアレントファイアウォールモードの場合に必要)。この NAT ルールが適用されるインターフェイスを識別するセキュリティゾーン。[送信元 (Source) ]は、デバイスに入るトラフィックが通過する実際のインターフェイスを含むゾーン。[宛先 (Destination) ]は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含むゾーン。デフォルトでは、すべてのインターフェイスにルールが適用されます ([すべて (Any) ])。(ブリッジグループメンバーインターフェイスの場合に必要) **Source Zone Destination Zone Source Destination Any**

**ステップ 5** ([変換 (Translation) ] タブで次を実行します。) 元の packets アドレス (IPv4 または IPv6)、つまり、元の packets に表示される packets アドレスを特定します。

元の packets と変換済み packets の例については、次の図を参照してください。



- [元の送信元アドレス (Original Source Address) ]: 変換しているアドレスを含むネットワークオブジェクトまたはグループ。
- [元の宛先アドレス (Original Destination Address) ]: (オプション) 宛先アドレスを含むネットワークオブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用することができます。

[送信元インターフェイス IP (Source Interface IP) ] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any) ] は選択不可) をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスに対して、ポート変換を設定したスタティックインターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポートオブジェクトも選択します。

**ステップ 6** 変換された packets アドレス (IPv4 または IPv6)、すなわちそれが宛先インターフェイスネットワーク上に現れるときの packets アドレスを識別します。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元 (Translated Source) ]: 次のいずれかになります。

- アドレスの設定グループを使用するには、[アドレス (Address)] およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
- (ポート変換を設定したスタティック インターフェイス NAT)。宛先のアドレスのインターフェイスを使用するには、[インターフェイス (Interface)] [宛先インターフェイス IP (Destination Interface IP)] を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced)] タブで [IPv6] オプションを選択する必要もあります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
- [変換済み宛先 (Translated Destination)] : (オプション)。変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先 (Original Destination)] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT (つまり変換なし) を設定できます。

**ステップ 7** (オプション) サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。

ポート変換を設定したスタティック NAT を設定した場合、送信元、宛先、またはその両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 間を変換できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします (両方とも TCP または両方とも UDP)。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

- [元の送信元ポート (Original Source Port)]、[変換済み送信元ポート (Translated Source Port)] : 送信元アドレスのポート変換を定義します。
- [元の宛先ポート (Original Destination Port)]、[変換済み宛先ポート (Translated Destination Port)] : 宛先アドレスのポート変換を定義します。

**ステップ 8** (オプション) [詳細 (Advanced)] タブで、必要なオプションを選択します。

- [このルールに一致する DNS 応答を変換する (Translate DNS replies that match this rule)] : DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、[NAT を使用した DNS クエリと応答の書き換え \(1203 ページ\)](#) を参照してください。ポート変換を実行する場合、このオプションは使用できません。

- [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。
- [ネット間マッピング (Net to Net Mapping) ] : NAT 46 の場合、このオプションを選択して、最初の IPv4 アドレスを最初の IPv6 アドレスに変換し、2 番目を 2 番目に変換という順序で変換します。このオプションを選択しない場合、IPv4 埋め込み方式が使用されます。1 対 1 の変換の場合は、このオプションを使用する必要があります。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface) ] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。
- [単方向 (Unidirectional) ] : 宛先アドレスから送信元アドレスへのトラフィックの送信開始を防ぐには、このオプションを選択します。

**ステップ 9** [保存 (Save) ] をクリックしてルールを追加します。

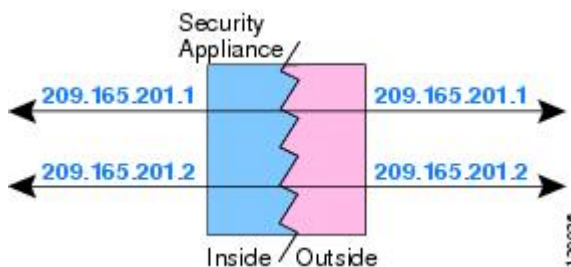
**ステップ 10** NAT ページで [保存 (Save) ] をクリックして変更を保存します。

## アイデンティティ NAT

IP アドレスを自身に変換する必要がある NAT コンフィギュレーションを設定できます。たとえば、NAT を各ネットワークに適するものの、1 つのネットワークを NAT から除外するという広範なルールを作成する場合、スタティック NAT ルールを作成して、アドレスを自身に変換することができます。

次の図に、一般的なアイデンティティ NAT のシナリオを示します。

図 32: アイデンティティ NAT



ここでは、アイデンティティ NAT の設定方法について説明します。

## アイデンティティ自動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

スタティック アイデンティティ自動 NAT ルールを使用して、アドレスの変換を防止します。つまり、自身のアドレスに変換します。

### 始める前に

[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元の送信元 (Original Source)] : これはネットワーク オブジェクト (グループではない) でなければならず、ホスト、範囲、またはサブネットも可能です。
- [変換済み送信元 (Translated Source)] : 元の送信元オブジェクトとコンテンツが全く同一のネットワーク オブジェクトまたはグループ。同じオブジェクトを使用できます。

### 手順

**ステップ 1** [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。

**ステップ 2** 次のいずれかを実行します。

- [ルール の追加 (Add Rule)] ボタンをクリックして、新しいルールを作成します。
- 編集アイコン (✎) をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

**ステップ 3** 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule)] : [自動 NAT ルール (Auto NAT Rule)] を選択します。
- [タイプ (Type)] : [スタティック (Static)] を選択します。

**ステップ 4** [インターフェイス オブジェクト (Interface Objects)] タブで、以下のオプションを設定します。

- [送信元インターフェイス オブジェクト (Source Interface Objects)]、[宛先インターフェイス オブジェクト (Destination Interface Objects)] : (ブリッジグループ メンバー インターフェイスの場合に必要な) **DestinationSource**

**ステップ 5** [一般 (General)] [変換 (Translation)] タブで、次のオプションを設定します。

- [元の送信元 (Original Source)] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元 (Translated Source)] : 元の送信元と同じオブジェクト。オプションで、内容がまったく同じ別のオブジェクトを選択できます。

アイデンティティ NAT には、[元のポート (Original Port)] オプションと [変換済みポート (Translated Port)] オプションを設定しないでください。

**ステップ 6** (オプション) [詳細 (Advanced)] タブで、必要なオプションを選択します。

- [このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule)] : アイデンティティ NAT には、このオプションを設定しないでください。
- [IPv6] : アイデンティティ NAT にこのオプションを設定しないでください。
- [ネット マッピングへのネット (Net to Net Mapping)] : アイデンティティ NAT にこのオプションを設定しないでください。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface)] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。
- [宛先インターフェイスのルート ルックアップを実行 (Perform Route Lookup for Destination Interface)] : 元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択していて、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代わりに、ルーティングテーブルに基づいて宛先インターフェイスを決めさせることができます。

**ステップ 7** [保存 (Save)] をクリックしてルールを追加します。

**ステップ 8** NAT ページで [保存 (Save)] をクリックして変更を保存します。

## アイデンティティ手動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

自動 NAT がお客様のニーズを満たしていない場合は、スタティック アイデンティティ手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。スタティック アイデンティティ NAT ルールを使用して、アドレスの変換を防止します。つまり、自身のアドレスに変換します。

### 始める前に

[オブジェクト (Objects) ]>[オブジェクト管理 (Object Management) ]を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。> IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元 (Original Source) ]: これはネットワーク オブジェクトまたはグループで、ホスト、範囲、またはサブネットを含むことができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて (Any) ] を指定します。
- [変換済み送信元 (Translated Source) ]: 元の送信元と同じオブジェクト。オプションで、内容がまったく同じ別のオブジェクトを選択できます。

ルールで各アドレスの静的変換を設定すると、[元の宛先 (Original Destination) ]および [変換済み宛先 (Translated Destination) ]のネットワーク オブジェクトを作成できます。ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピングアドレスに対するオブジェクトの追加をスキップでき、ルールでインターフェイスを指定します。

また送信元、宛先、またはその両方のポート変換も実行できます。オブジェクトマネージャでは、元のポートと変換されたポートで使用できるポート オブジェクトがあることを確認します。アイデンティティ NAT には同じオブジェクトを使用できます。

### 手順

**ステップ 1** [デバイス (Devices) ]> [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。

**ステップ 2** 次のいずれかを実行します。

- [ルールの追加 (Add Rule) ] ボタンをクリックして、新しいルールを作成します。
- 編集アイコン (✎) をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

**ステップ 3** 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule) ]: [手動 NAT ルール (Manual NAT Rule) ] を選択します。
- [タイプ (Type) ]: [スタティック (Static) ] を選択します。この設定は送信元アドレスのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われず。

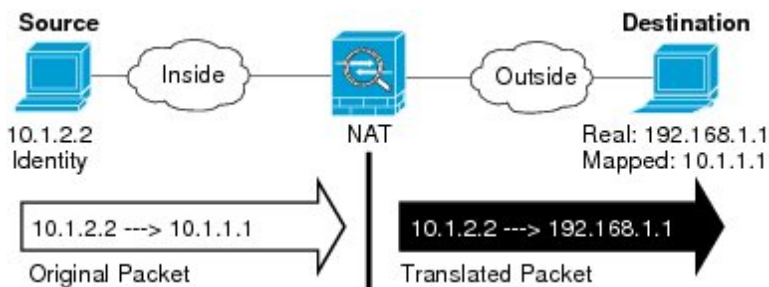
- [有効にする (Enable) ]: ルールをアクティブにするかどうかを指定します。ルールページの右クリックメニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。
- [挿入 (Insert) ]: ルールを追加する場所を指定します。ルールは、カテゴリ (自動 NAT ルールの前か後)、または指定したルール番号の上か下に挿入できます。

**ステップ 4** [インターフェイス オブジェクト (Interface Objects) ] タブで、以下のオプションを設定します。

- [送信元インターフェイス オブジェクト (Source Interface Objects) ]、[宛先インターフェイス オブジェクト (Destination Interface Objects) ]: (共有ポリシーのみ)。[送信元ゾーン (Source Zone) ]、[宛先ゾーン (Destination Zone) ]: (トランスペアレントファイアウォールモードの場合に必要)。NAT ルールが適用されるインターフェイスを識別するセキュリティゾーン。[送信元 (Source) ]は、デバイスに入るトラフィックが通過する実際のインターフェイスを含むゾーン。[宛先 (Destination) ]は、デバイスから出るトラフィックが通過するマッピング インターフェイスを含むゾーン。デフォルトでは、すべてのインターフェイスにルールが適用されます ([すべて (Any) ])。(ブリッジグループメンバー インターフェイスの場合に必要)

**ステップ 5** 元の packets アドレス (IPv4 または IPv6)、つまり、元の packets に表示される packets アドレスを特定します。

元の packets と変換済み packets の例については、次の図を参照してください。ここでは、内部ホストでアイデンティティ NAT を実行しますが、外部ホストを変換します。



- [元の送信元 (Original Source) ]: 変換しているアドレスを含むネットワーク オブジェクトまたはグループ。
- [元の宛先 (Original Destination) ]: (オプション)。宛先のアドレスを含むネットワーク オブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用することができます。

[インターフェイス (Interface) ]>[インターフェイス オブジェクト (Interface Object) ] を選択し、送信元インターフェイスの元の宛先 ([Any] は選択不可) をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスに対して、ポート変換を設定したスタティックインターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

**ステップ 6** 変換済みパケットアドレス（つまり、IPv4 または IPv6）を特定します。パケットアドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元 (Translated Source) ] : 元の送信元と同じオブジェクト。オプションで、内容がまったく同じ別のオブジェクトを選択できます。
- [変換済み宛先 (Translated Destination) ] : (オプション) 。変換されたパケットで使用される宛先アドレスを含むネットワークオブジェクトまたはグループ。[元の宛先 (Original Destination) ] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT（つまり変換なし）を設定できます。

**ステップ 7** (オプション) サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。

ポート変換を設定したスタティック NAT を設定した場合、送信元、宛先、またはその両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 間を変換できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービスオブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

- [元の送信元ポート (Original Source Port) ]、[変換済み送信元ポート (Translated Source Port) ] : 送信元アドレスのポート変換を定義します。
- [元の宛先ポート (Original Destination Port) ]、[変換済み宛先ポート (Translated Destination Port) ] : 宛先アドレスのポート変換を定義します。

**ステップ 8** (オプション) [詳細 (Advanced) ] タブで、必要なオプションを選択します。

- [このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule) ] : アイデンティティ NAT には、このオプションを設定しないでください。
- [IPv6] : [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface) ] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。
- [宛先インターフェイスのルートルックアップを実行 (Perform Route Lookup for Destination Interface) ] : 元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択していて、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代



わりに、ルーティングテーブルに基づいて宛先インターフェイスを決めさせることができます。

- [単方向 (Unidirectional) ]: 宛先アドレスから送信元アドレスへのトラフィックの送信開始を防ぐには、このオプションを選択します。宛先アドレスから送信元アドレスへのトラフィックの送信開始を防ぐには、このオプションを選択します。

**ステップ 9** [保存 (Save) ]をクリックしてルールを追加します。

**ステップ 10** NAT ページで [保存 (Save) ]をクリックして変更を保存します。

## Firepower Threat Defense の NAT ルール プロパティ

ネットワークアドレス変換 (NAT) ルールを使用して、IP アドレスを他の IP アドレスに変換します。通常は、NAT ルールを使用してプライベートアドレスをパブリックにルーティングできるアドレスに変換します。1つのアドレスを別のアドレスに変換するか、ポートアドレス変換 (PAT) を使用して多数のアドレスを1つまたは少数のアドレスに変換し、ポート番号を使用して送信元アドレスを識別することができます。

NAT ルールの基本的なプロパティは、次のとおりです。プロパティは、指示されていることを除き、自動 NAT ルールと手動 NAT ルールで同じです。

### NAT タイプ (NAT Type)

[手動 NAT ルール (Manual NAT Rule) ]または[自動 NAT ルール (Auto NAT Rule) ]のどちらを設定するのかを指定します。自動 NAT は、送信元アドレスのみを変換します。宛先アドレスに基づいた他の変換方法作成することはできません。自動 NAT のほうが設定するのが簡単なので、手動 NAT の機能を追加する必要がない限り、自動 NAT を使用してください。この2つの間の違いについて詳しくは、[自動 NAT および手動 NAT \(1106 ページ\)](#) を参照してください。

### タイプ (Type)

変換ルールを[ダイナミック (Dynamic) ]にするか、[スタティック (Static) ]にするかを指定します。ダイナミック変換では、アドレス プールからマッピングアドレスが自動的に選択されるか、または、PAT の実装時にはアドレス/ポートの組み合わせが自動的に選択されます。マッピングアドレス/ポートを明確に定義する必要がある場合は、スタティック変換を使用します。

### 有効化 (Enable) (手動 NAT のみ)

ルールをアクティブにするかどうかを指定します。ルール ページの右クリック メニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。自動 NAT ルールを無効化することはできません。

### 挿入 (Insert) (手動 NAT のみ)

ルールを追加する場所を指定します。ルールは、カテゴリ (自動 NAT ルールの前か後) 、または指定したルール番号の上か下に挿入できます。

説明 (任意、手動 NAT のみ)。

ルールの目的の説明。

以降のトピックで、NAT ルール プロパティのタブについて説明します。

## インターフェイスオブジェクト: NATのプロパティ

インターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) は、NAT ルールが適用されるインターフェイスを定義します。ルーテッドモードでは、送信元と宛先の両方にデフォルトの「任意 (Any)」を使用すれば、割り当てられたすべてのデバイスのすべてのインターフェイスに適用できます。ただし、通常は特定の送信元と宛先インターフェイスを選択します。



(注) 「任意」のインターフェイスの概念は、ブリッジグループメンバーインターフェイスには適用されません。「任意」のインターフェイスを指定すると、すべてのブリッジグループメンバーインターフェイスが除外されます。そのため、ブリッジグループメンバーに NAT を適用するには、メンバーインターフェイスを指定する必要があります。ブリッジ仮想インターフェイス (BVI) 自体に NAT を設定することはできず、メンバーインターフェイスにのみ NAT を設定できます。

インターフェイスオブジェクトを選択すると、NAT ルールはデバイスのインターフェイスが選択されたすべてのオブジェクトに含まれているときのみ設定されます。たとえば、送信元と宛先の両方のセキュリティゾーンを選択すると、特定のデバイスに対して1つ以上のインターフェイスが両方のゾーンに含まれている必要があります。

### 送信元インターフェイスオブジェクト、宛先インターフェイスオブジェクト

(ブリッジグループメンバーインターフェイスの場合に必要)

## 自動 NAT の [変換 (Translation)] プロパティ

[変換 (Translation)] タブのオプションを使って発信元アドレスやマッピングされた変換アドレスを定義します。次のプロパティは、自動 NAT にのみ適用されます。

[元の送信元 (Original Source)] (常に必須)。

変換しているアドレスを含むネットワークオブジェクト。グループではなくネットワークオブジェクトにする必要があります。ホスト、範囲、またはサブネットを含めることができます。

[変換済み送信元 (Translated Source)] (通常は必須)。

変換先のマッピングアドレス。ここで選択する内容は、定義している変換ルールのタイプによって異なります。

- [ダイナミック NAT (Dynamic NAT)] : マッピングアドレスを含むネットワークオブジェクトまたはグループ。ネットワークオブジェクトまたはグループにすることができますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6

アドレスの両方を含めることはできません。1つのタイプだけ含める必要があります。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。

- [ダイナミック PAT (Dynamic PAT)] : 次のいずれかを実行します。
  - (インターフェイス PAT) 。宛先のアドレスのインターフェイスを使用するには、[インターフェイス (Interface)] > [宛先インターフェイス IP (Destination Interface IP)] を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced)] タブで [IPv6] オプションを選択する必要があります。PAT プールは設定しないでください。
  - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールは設定しないでください。
  - PAT プールを使用するには、[変換された送信元 (Translated Source)] を空のままにしておきます。[PAT プール (PAT Pool)] タブで PAT プール オブジェクトを選択します。
- [スタティック NAT (Static NAT)] : 次のいずれかを実行します。
  - アドレスの設定グループを使用するには、[アドレス (Address)] およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループに、ホスト、範囲、またはサブネットを含めることができます。通常、1対1のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - (ポート変換を設定したスタティック インターフェイス NAT) 。宛先のアドレスのインターフェイスを使用するには、[インターフェイス (Interface)] [宛先インターフェイス IP (Destination Interface IP)] を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced)] タブで [IPv6] オプションを選択する必要があります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
- [アイデンティティ NAT (Identity NAT)] : 元の送信元と同じオブジェクト。状況に応じて、コンテンツが全く同一の別のオブジェクトを選択できます。

[元のポート (Original Port)]、[変換済みポート (Translated Port)] (スタティック NAT のみ)。

TCP または UDP ポートを変換する必要がある場合、[元のポート (Original Port)] でプロトコルを選択し、元のポートおよび変換済みポートの番号を入力します。たとえば、必要

に応じて TCP/80 を 8080 に変換できます。アイデンティティ NAT にこれらのオプションを設定しないでください。

## 手動 NAT の[一般 (General)] [変換 (Translation)] プロパティ

**[変換 (Translation)]** タブのオプションを使って発信元アドレスやマッピングされた変換アドレスを定義します。次のプロパティは、手動 NAT にのみ適用されます。指示されている場合を除き、すべてオプションです。

**[元の送信元 (Original Source)]** (常に必須)。

変換しているアドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにすることが可能で、ホスト、範囲、またはサブネットを含めることができます。元の送信元トラフィックをすべて変換する場合は、ルールに [すべて (Any)] を指定します。

**[変換済み送信元 (Translated Source)]** (通常は必須)。

変換先のマッピングアドレス。ここで選択する内容は、定義している変換ルールのタイプによって異なります。

- **[ダイナミック NAT (Dynamic NAT)]**: マッピング アドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにすることができますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1つのタイプだけ含める必要があります。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。
- **[ダイナミック PAT (Dynamic PAT)]**: 次のいずれかを実行します。
  - (インターフェイス PAT)。宛先のアドレスのインターフェイスを使用するには、[インターフェイス (Interface)] > [宛先インターフェイス IP (Destination Interface IP)] を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced)] タブで [IPv6] オプションを選択する必要があります。PAT プールは設定しないでください。
  - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールは設定しないでください。
  - PAT プールを使用するには、[変換された送信元 (Translated Source)] を空のままにしておきます。[PAT プール (PAT Pool)] タブで PAT プール オブジェクトを選択します。
- **[スタティック NAT (Static NAT)]**: 次のいずれかを実行します。
  - アドレスの設定グループを使用するには、[アドレス (Address)] およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループに、ホスト、範囲、またはサブネットを含める

ことができます。通常、1対1のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

- (ポート変換を設定したスタティック インターフェイス NAT)。宛先のアドレスのインターフェイスを使用するには、[インターフェイス (Interface)] [宛先インターフェイス IP (Destination Interface IP)] を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced)] タブで [IPv6] オプションを選択する必要もあります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。

- [アイデンティティ NAT (Identity NAT)] : 元の送信元と同じオブジェクト。状況に応じて、コンテンツが全く同一の別のオブジェクトを選択できます。

#### [元の宛先 (Original Destination)]

宛先アドレスを含むネットワーク オブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用することができます。

[送信元インターフェイス IP (Source Interface IP)] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)] は選択不可) をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスに対して、ポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポートオブジェクトも選択します。

#### [変換済みの宛先 (Translated Destination)]

変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先 (Original Destination)] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT (つまり変換なし) を設定できます。

#### 元の送信元ポート (Original Source Port)、変換済み送信ポート (Translated Source Port)、元の宛先ポート (Original Destination Port)、変換済み宛先ポート (Translated Destination Port)

元のパケットおよび変換済みパケットの送信元および宛先サービスを定義するポートオブジェクト。ポートを変換したり、ポートを変換せずに同じオブジェクトを選択してサービスに対するルールの感度を向上することができます。サービスを設定するときは、次のルールに注意してください。

- (ダイナミック NAT または PAT) [元の送信元ポート (Original Source Port)] および [変換済み送信元ポート (Translated Source Port)] では変換できません。宛先ポートでのみ変換できます。
- NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします (両方とも TCP または両方とも UDP)。アイ

デスティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

## PAT プールの NAT プロパティ

ダイナミック NAT を設定する際に、[PAT プール (PAT Pool) ] タブのプロパティを使用して、ポート アドレス変換に使用するアドレスのプールを定義できます。

### PAT プールの有効化 (Enable PAT Pool)

PAT に使用するアドレスのプールを設定する場合は、このオプションを選択します。

### PAT

PAT プールに使用するアドレスとして、以下のいずれかを指定します。

- [アドレス (Address) ] : PAT プールアドレスを定義するオブジェクト。アドレスの範囲を含むネットワーク オブジェクト、またはホスト、範囲、あるいはその両方を含むネットワーク オブジェクト グループのいずれかです。サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。
- [宛先インターフェイス IP (Destination Interface IP) ] : PAT アドレスとして使用する宛先インターフェイスを指定します。このオプションを使用する場合、特定の [宛先インターフェイス オブジェクト (Destination Interface Object) ] を選択する必要があります。[すべて (Any) ] を宛先インターフェイスとして使用することはできません。これは、インターフェイス PAT を実装するもう 1 つの方法です。

### ラウンドロビン (Round Robin)

アドレスとポートをラウンドロビン形式で割り当てます。デフォルトではラウンドロビンは使用されず、1 つの PAT アドレスのポートがすべて割り当てられてから次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレスとポートが割り当てられると、また最初のアドレスに戻り、次に 2 番目のアドレスという順に使用されます。

### 拡張 PAT テーブル (Extended PAT Table)

拡張 PAT を使用します。拡張 PAT では、変換情報に宛先アドレスとポートを含めることで、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。このオプションは、インターフェイス PAT またはインターフェイス PAT フォールバックで使用することはできません。

### フラット ポート範囲 (Flat Port Range) 、予約済みポートを含める (Include Reserved Ports)

TCP/UDP ポートを割り当てる際に、ポート範囲 (1024 ~ 65535) を単一のフラットな範囲として使用します。変換用のマッピング ポート番号を選択する場合、PAT によって、実際の送信元ポート番号が使用されます (使用可能な場合)。ただし、このオプションを

設定しないと、実際のポートが使用できない場合、デフォルトでは、実際のポート番号と同じポート範囲（1～511、512～1023、および1024～65535）からマッピングポートが選択されます。下位の範囲でポートが不足するのを回避するには、この設定を行います。1～65535の範囲全体を使用するには、[予約済みポートを含む (Include Reserved Ports)] オプションも選択します。

## 詳細 NAT プロパティ

NATを設定するとき、[詳細 (Advanced)] オプションで特別なサービスを提供するプロパティを設定できます。これらすべてのプロパティはオプションであり、サービスを必要としている場合のみ設定します。

### このルールに一致する DNS 回答の変換

DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、[NAT を使用した DNS クエリと応答の書き換え \(1203 ページ\)](#) を参照してください。スタティック NAT ルールでポート変換を行っている場合には、このオプションは使用できません。

### [インターフェイス PAT (宛先インターフェイス) へのフォールスルー (Fallthrough to Interface PAT (Destination Interface))] (ダイナミック NAT のみ)

その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。すでにインターフェイス PAT を変換済みアドレスとして設定している場合には、このオプションは使用できません。PAT プールを構成する場合も、このオプションを選択することはできません。

### IPv6

インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。

### [ネット間マッピング (Net to Net Mapping)] (スタティック NAT のみ)

NAT 46 の場合、このオプションを選択して、最初の IPv4 アドレスを最初の IPv6 アドレスに変換し、2 番目を 2 番目に変換という順序で変換します。このオプションを選択しない場合、IPv4 埋め込み方式が使用されます。1 対 1 の変換の場合、このオプションを使用する必要があります。

### 宛先インターフェイスでプロキシ ARP なし (スタティック NAT のみ)

マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ

ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

宛先インターフェイスでルートルックアップを実行します (スタティック ID NAT のみ。ルーテッドモードのみ)。

元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択していて、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代わりに、ルーティングテーブルに基づいて宛先インターフェイスを決めさせることができます。

[単方向 (Unidirectional)] (手動 NAT のみ、スタティック NAT のみ)。

宛先アドレスから送信元アドレスへのトラフィックの送信開始を防ぐには、このオプションを選択します。

## IPv6 ネットワークの変換

IPv6 専用ネットワークと IPv4 専用ネットワークの間でトラフィックを通過させる必要がある場合、NAT を使用してアドレスタイプを変換する必要があります。2 つの IPv6 ネットワークの場合でも、外部ネットワークから内部アドレスを隠す必要がある場合があります。

IPv6 ネットワークとともに次の変換タイプを使用できます。

- NAT64、NAT46 : IPv6 パケットを IPv4 (およびその反対) に変換します。IPv6 から IPv4 への変換と IPv4 から IPv6 への変換に対する 2 つのポリシーを定義する必要があります。1 つの手動 NAT ルールでこれを実現できますが、DNS サーバが外部ネットワークにある場合は、DNS 応答を書き換える必要がある可能性があります。宛先を指定するときに手動 NAT ルールで DNS の書き換えを有効にすることはできないため、2 つの自動 NAT ルールを作成する方法が適しています。



(注) NAT46 がサポートするのは、スタティックマッピングのみです。

- NAT66 : IPv6 パケットを別の IPv6 アドレスに変換します。スタティック NAT の使用をお勧めします。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要はありません。



(注) NAT64 および NAT 46 は、標準的なルーテッドインターフェイスでのみ使用できます。NAT66 は、ルーテッドインターフェイスとブリッジグループメンバーインターフェイスの両方で使用できます。



## NAT64/46 : IPv6 アドレスの IPv4 への変換

トラフィックが IPv6 ネットワークから IPv4 専用ネットワークに移動する場合、IPv6 アドレスを IPv4 アドレスに変換して、IPv4 から IPv6 にトラフィックを戻す必要があります。IPv4 ネットワークで IPv6 アドレスをバインドするための IPv4 アドレスプールと、IPv6 ネットワークで IPv4 アドレスをバインドするための IPv6 アドレスプールの 2 つを定義する必要があります。

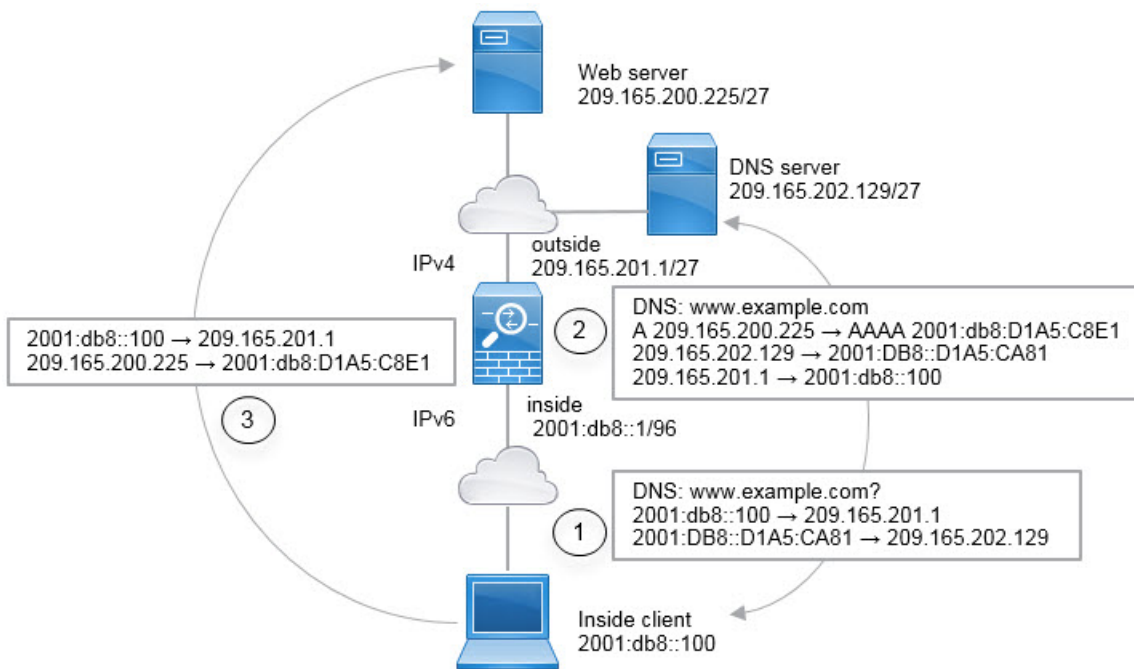
- NAT64 ルール用の IPv4 アドレスプールは通常は小さく、一般的に IPv6 クライアントアドレスを使用して 1 対 1 のマッピングを設定するにはアドレスが足りない場合があります。ダイナミック PAT は、ダイナミック NAT またはスタティック NAT と比較して、できる限り多数の IPv6 クライアントアドレスにより容易に対応します。
- NAT 46 ルールの IPv6 アドレスプールは、マッピングされる IPv4 アドレスの数と等しいか、それより多くなります。これによって、各 IPv4 アドレスを別の IPv6 アドレスにマッピングできます。NAT 46 はスタティック マッピングのみをサポートするため、ダイナミック PAT を使用することはできません。

送信元 IPv6 ネットワークと宛先 IPv4 ネットワークの 2 つのポリシーを定義する必要があります。1 つの手動 NAT ルールでこれを実現できますが、DNS サーバが外部ネットワークにある場合は、DNS 応答を書き換える必要がある可能性があります。宛先を指定するときに手動 NAT ルールで DNS の書き換えを有効にすることはできないため、2 つの自動 NAT ルールを作成する方法が適しています。

### NAT64/46 の例 : 内部 IPv6 ネットワークと外部 IPv4 インターネット

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の図は、内部の IPv6 専用ネットワークが存在し、内部ユーザが必要とするいくつかの IPv4 専用サービスが外部のインターネット上に存在する一般的な例です。



この例では、外部インターフェイスの IP アドレスを持つダイナミック インターフェイス PAT を使用して、内部の IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは、2001:db8::/96 ネットワークのアドレスにスタティックに変換され、内部ネットワークでの送信が可能になります。NAT46 ルールで DNS の書き換えを有効にすると、外部 DNS サーバからの応答を A (IPv4) レコードから AAAA (IPv6) レコードに変換でき、アドレスが IPv4 から IPv6 に変換されます。

次は、内部 IPv6 ネットワーク上の 2001:DB8::100 にあるクライアントが www.example.com を開こうとしている場合の Web 要求の一般的なシーケンスです。

1. クライアントのコンピュータが 2001:DB8::D1A5:CA81 にある DNS サーバに DNS 要求を送信します。NAT ルールにより、DNS 要求の送信元と宛先が次のように変換されます。
  - 2001:DB8::100 を 209.165.201.1 上の一意のポートに変換 (NAT64 インターフェイス PAT ルール)。
  - 2001:DB8::D1A5:CA81 を 209.165.202.129 に変換 (NAT46 ルール。D1A5:CA81 は IPv6 の 209.165.202.129 に相当します)。
2. DNS サーバが、www.example.com が 209.165.200.225 であることを示す A レコードに回答します。DNS の書き換えが有効になっている NAT46 ルールにより、A レコードが IPv6 の同等の AAAA レコードに変換されて、AAAA レコードの 209.165.200.225 が 2001:db8:D1A5:C8E1 に変換されます。なお、DNS 応答の送信元アドレスと宛先アドレスは変換されません。
  - 209.165.202.129 を 2001:DB8::D1A5:CA81 に変換
  - 209.165.201.1 を 2001:db8::100 に変換

3. これで、IPv6 クライアントが Web サーバの IP アドレスを取得し、www.example.com (2001:db8:D1A5:C8E1) に HTTP 要求を送信できます。(D1A5:C8E1 は IPv6 の 209.165.200.225 に相当します)。HTTP 要求の送信元と宛先が変換されます。
  - 2001:DB8::100 を 209.156.101.54 上の一意のポートに変換 (NAT64 インターフェイス PAT ルール)。
  - 2001:db8:D1A5:C8E1 を 209.165.200.225 に変換 (NAT46 ルール)。

次の手順では、この例の設定方法について説明します。

### 始める前に

デバイスに対応するインターフェイスが含まれているインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) があることを確認します。この例では、インターフェイスオブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、**[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択してから、**[インターフェイス (Interface)]** を選択します。

### 手順

**ステップ 1** 内部 IPv6 ネットワークと外部 IPv4 ネットワークを定義するネットワークオブジェクトを作成します。

- a) **[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択します。
- b) コンテンツのテーブルから **[ネットワーク (Network)]** を選択し、**[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックします。
- c) 内部 IPv6 ネットワークを定義します。

ネットワークオブジェクトに名前 (inside\_v6 など) を付け、ネットワークアドレス 2001:DB8::/96 を入力します。

**New Network Objects** ? x

Name:

Description:

Network:   
 Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- d) **[保存 (Save)]** をクリックします。
- e) **[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックして、外部 IPv4 ネットワークを定義します。

ネットワーク オブジェクトに名前 (たとえば、outside\_v4\_any) を付けて、ネットワーク アドレス 0.0.0.0/0 を入力します。

f) [保存 (Save) ]をクリックします。

**ステップ 2** 内部 IPv6 ネットワークの NAT64 ダイナミック PAT ルールを設定します。

- a) [デバイス (Devices) ] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule) ]をクリックします。
- c) 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 自動 NAT ルール。
  - [タイプ (Type) ] = Dynamic。
- d) [インターフェイス オブジェクト (Interface Objects) ] タブで、以下の設定を行います。
  - [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。
- e) [変換 (Translation) ] タブで、次の項目を設定します。
  - [元の送信元 (Original Source) ] = inside\_v6 ネットワーク オブジェクト。
  - [変換済みの送信元 (Translated Source) ] = 宛先インターフェイス IP (Destination Interface IP) 。

- f) [OK] をクリックします。

このルールにより、内部インターフェイスの 2001:db8::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換されます。

### ステップ 3 外部 IPv4 ネットワークのスタティック NAT46 ルールを設定します。

- a) [ルール の追加 (Add Rule)] をクリックします。
- b) 次のプロパティを設定します。
  - [NAT ルール (NAT Rule)] = 自動 NAT ルール (Auto NAT Rule)。
  - [タイプ (Type)] = スタティック (Static)。
- c) [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。
  - [送信元インターフェイス オブジェクト (Source Interface Objects)] = outside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = inside。
- d) [変換 (Translation)] タブで、次の項目を設定します。
  - [元の送信元 (Original Source)] = outside\_v4\_any ネットワーク オブジェクト。
  - [変換済みの送信元 (Translated Source)] > [アドレス (Address)] = inside\_v6 ネットワーク オブジェクト。
- e) [詳細 (Advanced)] タブで、[このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule)] を選択します。

The screenshot shows the 'Add NAT Rule' configuration interface. At the top, 'NAT Rule' is set to 'Auto NAT Rule' and 'Type' is 'Static'. Below this, there are tabs for 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Translation' tab is selected. Under 'Original Packet', 'Original Source' is 'outside\_v4\_any' and 'Original Port' is 'TCP'. Under 'Translated Packet', 'Translated Source' is 'Address' and 'inside\_v6'.

- f) [OK] をクリックします。

このルールにより、内部インターフェイスに向かう外部ネットワーク上のすべての IPv4 アドレスが、組み込み IPv4 アドレス方式を使用して 2001:db8::/96 ネットワーク上のアドレスに変換されます。また、DNS 応答が A (IPv4) レコードから AAAA (IPv6) レコードに変換され、アドレスが IPv4 から IPv6 に変換されます。

## NAT66 : IPv6 アドレスの異なる IPv6 アドレスへの変換

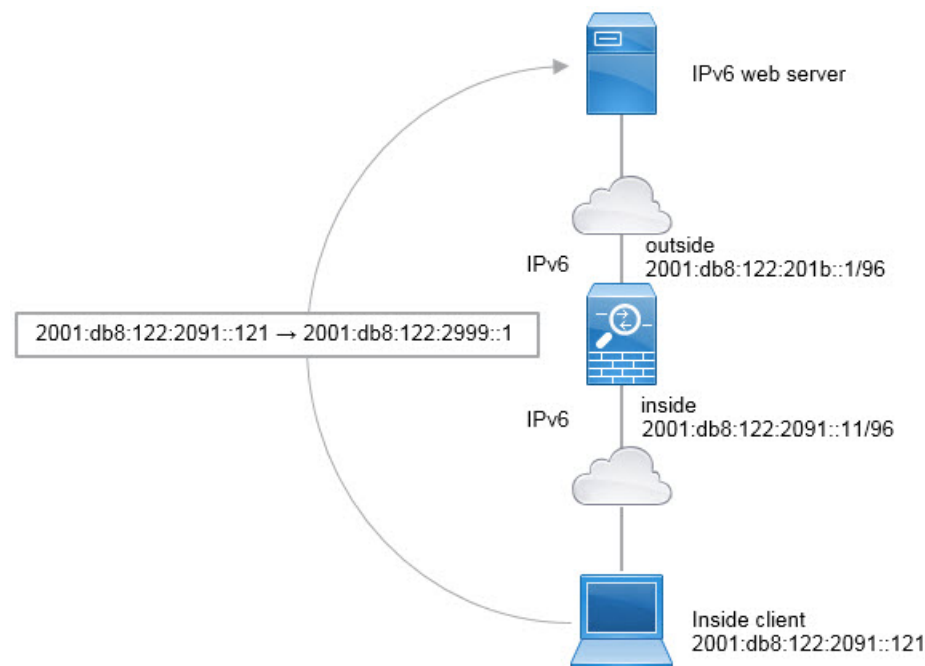
IPv6 ネットワークから別の IPv6 ネットワークに移動する場合、アドレスを外部ネットワークの別の IPv6 アドレスに変換できます。スタティック NAT の使用をお勧めします。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要はありません。

異なるアドレス タイプ間での変換ではないため、NAT66 変換の単一のルールが必要です。自動 NAT を使用して、これらのルールを簡単にモデル化できます。ただし、リターントラフィックを許可しない場合は、手動 NAT のみを使用してスタティック NAT ルールを単一方向にすることができます。

### NAT66 の例 : ネットワーク間のスタティック変換

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

自動 NAT を使用して、IPv6 アドレス プール間のスタティック変換を設定できます。次の例では、2001:db8:122:2091::/96 ネットワークの内部アドレスを 2001:db8:122:2999::/96 ネットワークの外部アドレスに変換する方法について説明します。



## 始める前に

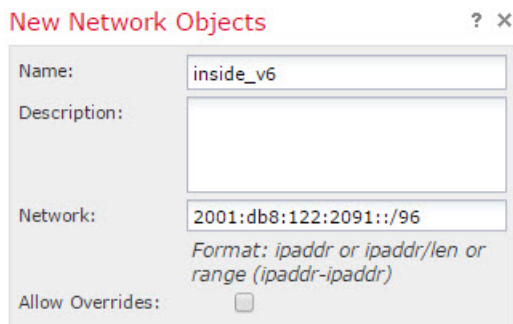
デバイスに対応するインターフェイスが含まれているインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) があることを確認します。この例では、インターフェイスオブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択してから、[インターフェイス (Interface)] を選択します。

## 手順

**ステップ 1** 内部 IPv6 ネットワークと外部 IPv6 NAT ネットワークを定義するネットワークオブジェクトを作成します。

- a) [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- b) コンテンツのテーブルから [ネットワーク (Network)] を選択し、[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- c) 内部 IPv6 ネットワークを定義します。

ネットワークオブジェクトに名前 (たとえば、inside\_v6) を付けて、ネットワークアドレス 2001:db8:122:2091::/96 を入力します。



New Network Objects ? x

Name: inside\_v6

Description:

Network: 2001:db8:122:2091::/96

Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- d) [保存 (Save)] をクリックします。
- e) [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックして、外部 IPv6 NAT ネットワークを定義します。

ネットワークオブジェクトに名前 (たとえば、outside\_nat\_v6) を付けて、ネットワークアドレス 2001:db8:122:2999::/96 を入力します。

**New Network Objects** ? x

Name:

Description:

Network:   
 Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

f) [保存 (Save)] をクリックします。

**ステップ 2** 内部 IPv6 ネットワークのスタティック NAT ルールを設定します。

- a) [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule)] をクリックします。
- c) 次のプロパティを設定します。
  - [NAT ルール (NAT Rule)] = 自動 NAT ルール (Auto NAT Rule)。
  - [タイプ (Type)] = スタティック (Static)。
- d) [インターフェイス オブジェクト (Interface Objects)] タブで、次の項目を設定します。
  - [送信元インターフェイス オブジェクト (Source Interface Objects)] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = outside。
- e) [変換 (Translation)] タブで、次の項目を設定します。
  - [元の送信元 (Original Source)] = inside\_v6 ネットワーク オブジェクト。
  - [変換済みの送信元 (Translated Source)] > [アドレス (Address)] = outside\_nat\_v6 ネットワーク オブジェクト。

#### Add NAT Rule

NAT Rule:  ▼

Type:  ▼  Enable

Interface Objects **Translation** PAT Pool Advanced

**Original Packet**  
 Original Source:\*  ▼ +

**Translated Packet**  
 Translated Source:  ▼

f) [OK] をクリックします。



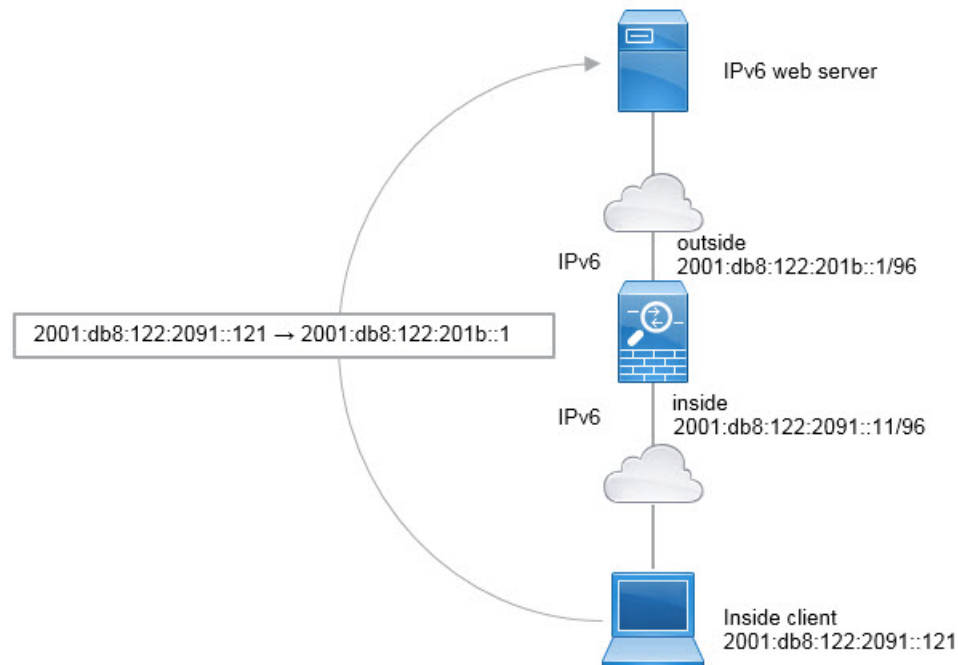
このルールにより、内部インターフェイス上の 2001:db8:122:2091::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、2001:db8:122:2999::/96 ネットワーク上のアドレスにスタティック NAT66 変換されます。

## NAT66 の例 : シンプルな IPv6 インターフェイス PAT

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

NAT66 を実装するための簡単なアプローチは、外部インターフェイスの IPv6 アドレス上の異なるポートに内部アドレスを動的に割り当てる方法です。

NAT66 のインターフェイス PAT ルールを設定すると、そのインターフェイスに設定されているすべてのグローバルアドレスが PAT のマッピングに使用されます。インターフェイスのリンクローカルアドレスまたはサイトローカルアドレスは、PAT には使用されません。



### 始める前に

デバイスに対応するインターフェイスが含まれているインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) があることを確認します。この例では、インターフェイスオブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、**[オブジェクト (Objects)] >**

[**オブジェクト管理 (Object Management)**] を選択してから、[**インターフェイス (Interface)**] を選択します。

### 手順

**ステップ 1** 内部 IPv6 ネットワークを定義するネットワーク オブジェクトを作成します。

- [**オブジェクト (Objects)**] > [**オブジェクト管理 (Object Management)**] を選択します。
- コンテンツのテーブルから [ネットワーク (Network)] を選択し、[**ネットワークを追加 (Add Network)**] > [**オブジェクトの追加 (Add Object)**] をクリックします。
- 内部 IPv6 ネットワークを定義します。

ネットワーク オブジェクトに名前 (たとえば、inside\_v6) を付けて、ネットワーク アドレス 2001:db8:122:2091::/96 を入力します。

- [**保存 (Save)**] をクリックします。

**ステップ 2** 内部 IPv6 ネットワークのダイナミック PAT ルールを設定します。

- [**デバイス (Devices)**] > [**NAT**] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- [**ルールの追加 (Add Rule)**] をクリックします。
- 次のプロパティを設定します。
  - [**NAT ルール (NAT Rule)**] = 自動 NAT ルール。
  - [**タイプ (Type)**] = Dynamic。
- [**インターフェイス オブジェクト (Interface Objects)**] タブで、以下の設定を行います。
  - [**送信元インターフェイス オブジェクト (Source Interface Objects)**] = inside。
  - [**宛先インターフェイス オブジェクト (Destination Interface Objects)**] = outside。
- [**変換 (Translation)**] タブで、次の項目を設定します。
  - [**元の送信元 (Original Source)**] = inside\_v6 ネットワーク オブジェクト。
  - [**変換済みの送信元 (Translated Source)**] = 宛先インターフェイス IP (Destination Interface IP)。

- f) [詳細 (Advanced) ] タブで、[IPv6] を選択します。これは、宛先インターフェイスの IPv6 が使用されることを意味します。

Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic  Enable

Interface Objects Translation PAT Pool Advanced

**Original Packet**

Original Source:\* inside\_v6

Original Port: TCP

**Translated Packet**

Translated Source: Destination Interface IP

The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

- g) [OK] をクリックします。

このルールでは、内部インターフェイスの 2001:db8:122:2091::/96 サブネットから外部インターフェイスへのトラフィックは、外部インターフェイス用に設定された IPv6 グローバルアドレスのいずれかに NAT66 PAT 変換されます。

## NAT のモニタリング

NAT 接続をモニタしてトラブルシューティングを実行するには、デバイス CLI にログインして次のコマンドを使用します。

- **show nat** NAT ルールとルールごとのヒット数を表示します。NAT の他の側面を表示するための追加キーワードがあります。
- **show xlate** 現在アクティブな実際の NAT 変換を表示します。
- **clear xlate** アクティブな NAT 変換を削除できます。既存の接続は接続が終了するまで古い変換スロットを継続して使用するため、NAT ルールを変更する場合はアクティブな変換を削除しなければならないことがあります。変換をクリアすると、システムは、新しいルールに基づいたクライアントの次の接続試行でクライアントの新しい変換を作成できません。

## NAT の例

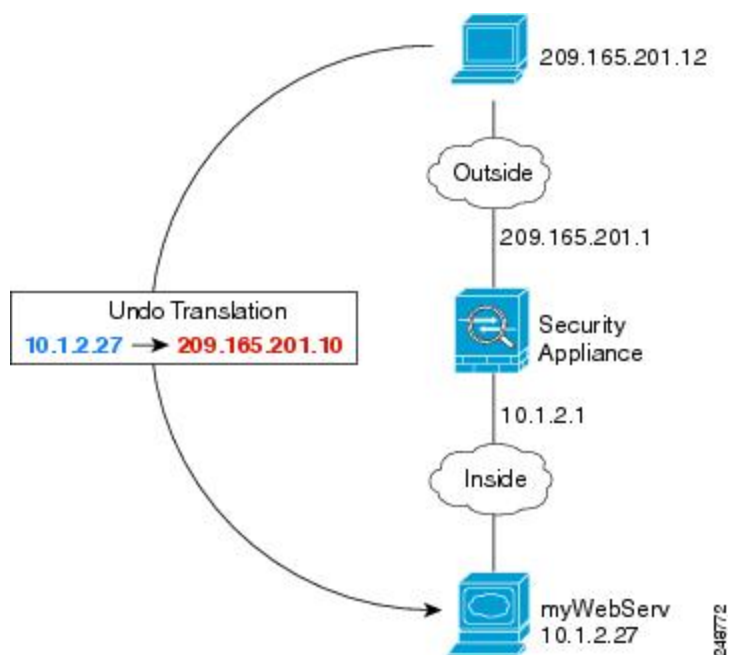
以下の各トピックでは、Threat Defense デバイスでの NAT の設定例を紹介します。

## 内部 Web サーバへのアクセスの提供 (スタティック自動 NAT)

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の例では、内部 Web サーバに対してスタティック NAT を実行します。実際のアドレスはプライベート ネットワーク上にあるため、パブリック アドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバへのトラフィックをホストが開始できるようにするために必要です

図 33: 内部 Web サーバのスタティック NAT



### 始める前に

Web サーバを保護するデバイスのインターフェイスが含まれているインターフェイス オブジェクト (セキュリティゾーンまたはインターフェイス グループ) があることを確認します。この例では、インターフェイス オブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイス オブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択してから、[インターフェイス (Interface)] を選択します。

## 手順

**ステップ 1** サーバのプライベート ホスト アドレスとパブリック ホスト アドレスを定義するネットワーク オブジェクトを作成します。

- [**オブジェクト (Objects)**] > [**オブジェクト管理 (Object Management)**] を選択します。
- 目次から[**ネットワーク (Network)**]を選択して、[**ネットワークの追加 (Add Network)**] > [**オブジェクトの追加 (Add Object)**] をクリックします。
- Web サーバのプライベート アドレスを定義します。

ネットワーク オブジェクトに名前 (たとえば、WebServerPrivate) を付けて、実際のホスト IP アドレス 10.1.2.27 を入力します。

**Edit Network Objects**

Name:

Description:

Network:

Allow Overrides:

**Override (0)**

- [**保存 (Save)**] をクリックします。
- [**ネットワークの追加 (Add Network)**] > [**オブジェクトの追加 (Add Object)**] をクリックして、パブリック アドレスを定義します。

ネットワーク オブジェクトに名前 (たとえば、WebServerPublic) を付けて、ホスト アドレス 209.165.201.10 を入力します。

**New Network Objects**

Name:

Description:

Network:

Allow Overrides:

**Override (0)**

- [**保存 (Save)**] をクリックします。

**ステップ 2** オブジェクトのスタティック NAT を設定します。

- [**デバイス (Devices)**] > [**NAT**] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- [**ルールの追加 (Add Rule)**] をクリックします。

- c) 次のプロパティを設定します。
- [NAT ルール (NAT Rule) ] = 自動 NAT ルール (Auto NAT Rule) 。
  - [タイプ (Type) ] = スタティック (Static) 。
- d) [インターフェイス オブジェクト (Interface Objects) ] タブで、次の項目を設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。
- e) [変換 (Translation) ] タブで、次の項目を設定します。
- [元の送信元 (Original Source) ] = WebServerPrivate ネットワーク オブジェクト。
  - [変換済みの送信元 (Translated Source) ] > [アドレス (Address) ] = WebServerPublic ネットワーク オブジェクト。

### Add NAT Rule

- f) [保存 (Save) ] をクリックします。

ステップ 3 [NAT ルール (NAT rule) ] ページで [保存 (Save) ] をクリックします。

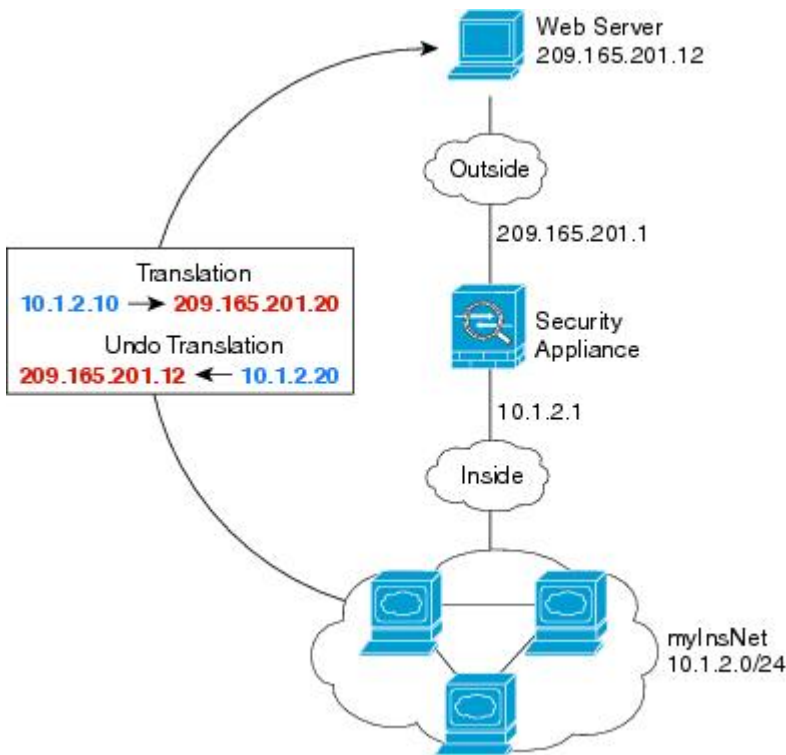
## 内部ホストのダイナミック自動 NAT および外部 Web サーバのスタティック NAT

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の例では、プライベートネットワーク上の内部ユーザが外部にアクセスする場合、このユーザにダイナミック NAT を設定します。また、内部ユーザが外部 Web サーバに接続する場合、

この Web サーバのアドレスが内部ネットワークに存在するように見えるアドレスに変換されます。

図 34: 内部の動的 NAT、外部 Web サーバの静的 NAT



#### 始める前に

Web サーバを保護するデバイスのインターフェイスが含まれているインターフェイス オブジェクト (セキュリティ ゾーンまたはインターフェイス グループ) があることを確認します。この例では、インターフェイス オブジェクトは **inside** および **outside** という名前のセキュリティ ゾーンであると仮定します。インターフェイス オブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、[インターフェイス (Interface)] を選択します。

#### 手順

- ステップ 1** 内部アドレスを変換する動的 NAT プールのネットワーク オブジェクトを作成します。
- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
  - コンテンツのテーブルから [ネットワーク (Network)] を選択し、[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
  - 動的 NAT プールを定義します。

ネットワーク オブジェクトに名前を付け (myNATpool など)、ネットワーク範囲 209.165.201.20 ~ 209.165.201.30 を入力します。

**New Network Objects** ? X

Name: myNATpool

Description:

Network: 209.165.201.20-209.165.201.30  
Format: ipaddr or ipaddr/len or range (2.2.2.10-2.2.2.20)

Allow Overrides:

d) [保存 (Save) ]をクリックします。

**ステップ 2** 内部ネットワークのネットワーク オブジェクトを作成します。

- [ネットワークを追加 (Add Network) ]>[オブジェクトの追加 (Add Object) ]をクリックします。
- ネットワーク オブジェクトに名前を付け (MyInsNet など)、ネットワーク アドレス 10.1.2.0/24 を入力します。

**New Network Objects**

Name: MyInsNet

Description:

Network: 10.1.2.0/24

Allow Overrides:

c) [保存 (Save) ]をクリックします。

**ステップ 3** 外部 Web サーバのネットワーク オブジェクトを作成します。

- [ネットワークを追加 (Add Network) ]>[オブジェクトの追加 (Add Object) ]をクリックします。
- ネットワーク オブジェクトに名前を付け (MyWebServer など)、ホストアドレス 209.165.201.12 を入力します。

**New Network Objects**

Name: myWebServer

Description:

Network: 209.165.201.12

Allow Overrides:

c) [保存 (Save) ]をクリックします。



**ステップ 4** 変換済み Web サーバアドレスのネットワーク オブジェクトを作成します。

- a) [ネットワークを追加 (Add Network) ]>[オブジェクトの追加 (Add Object) ]をクリックします。
- b) ネットワーク オブジェクトに名前を付け (TransWebServer など) 、ホストアドレス 10.1.2.20 を入力します。

The screenshot shows a configuration window titled "New Network Objects". It contains the following fields and values:

Name:	TransWebServer
Description:	
Network:	10.1.2.20
Allow Overrides:	<input checked="" type="checkbox"/>

- c) [保存 (Save) ]をクリックします。

**ステップ 5** ダイナミック NAT プール オブジェクトを使用して内部ネットワークのダイナミック NAT を設定します。

- a) [デバイス (Devices) ]>[NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule) ]をクリックします。
- c) 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 自動 NAT ルール。
  - [タイプ (Type) ] = Dynamic。
- d) [インターフェイス オブジェクト (Interface Objects) ] タブで、以下の設定を行います。
  - [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。
- e) [変換 (Translation) ] タブで、次の項目を設定します。
  - [元の発信元 (Original Source) ] = myInsNet ネットワーク オブジェクト。
  - [変換済みの発信元アドレス (Translated Source Address) ] = myNATpool ネットワーク オブジェクト。 >

## Add NAT Rule

The screenshot shows the 'Add NAT Rule' configuration interface. At the top, 'NAT Rule' is set to 'Auto NAT Rule' and 'Type' is set to 'Dynamic'. The 'Enable' checkbox is checked. Below this are tabs for 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Translation' tab is active. Under 'Original Packet', 'Original Source:\*' is set to 'myInsNet' and 'Original Port' is set to 'TCP'. Under 'Translated Packet', 'Translated Source' is set to 'Address' and 'Translated Port' is empty.

f) [保存 (Save) ]をクリックします。

### ステップ 6 Web サーバのスタティック NAT を設定します。

a) [ルール追加 (Add Rule) ]をクリックします。

b) 次のプロパティを設定します。

- [NAT ルール (NAT Rule) ] = 自動 NAT ルール (Auto NAT Rule) 。
- [タイプ (Type) ] = スタティック (Static) 。

c) [インターフェイス オブジェクト (Interface Objects) ] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = outside。
- [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = inside。

d) [変換 (Translation) ] タブで、次の項目を設定します。

- [元の発信元 (Original Source) ] = myWebServer ネットワーク オブジェクト。
- [変換済みの発信元アドレス (Translated Source Address) ] = TransWebServer ネットワーク オブジェクト。 >

## Add NAT Rule

The screenshot shows the 'Add NAT Rule' configuration interface. At the top, 'NAT Rule' is set to 'Auto NAT Rule' and 'Type' is set to 'Static'. The 'Enable' checkbox is checked. Below this are tabs for 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Translation' tab is active. Under 'Original Packet', 'Original Source:\*' is set to 'myWebServer' and 'Original Port' is set to 'TCP'. Under 'Translated Packet', 'Translated Source' is set to 'Address' and 'Translated Port' is empty.

e) [保存 (Save) ]をクリックします。

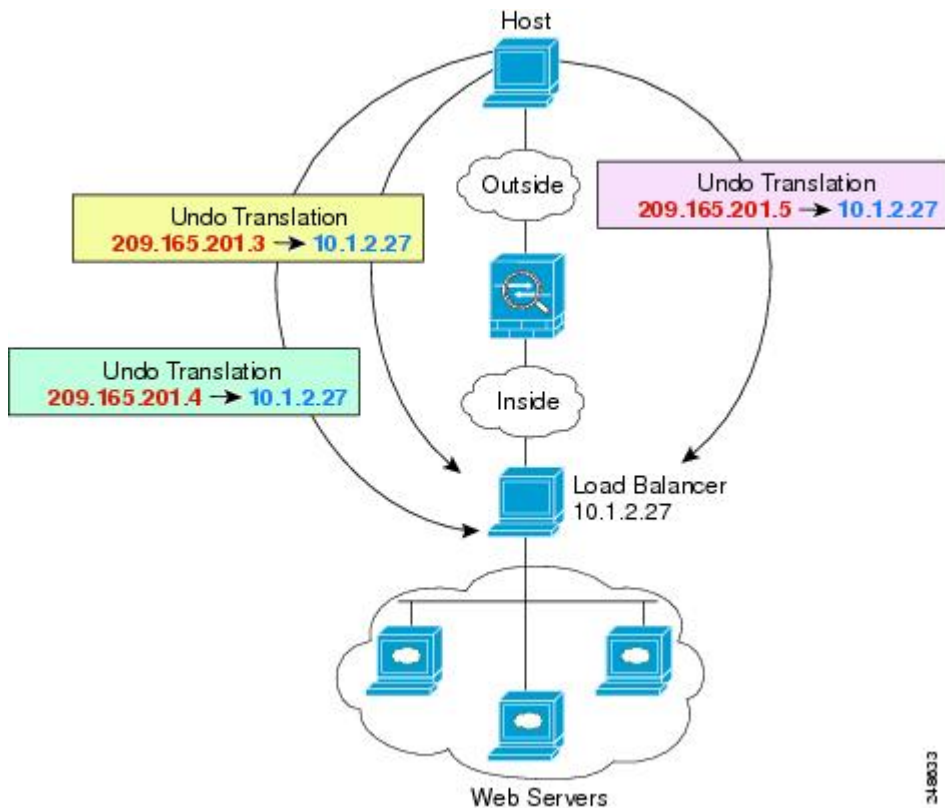
ステップ7 [NAT ルール (NAT rule) ] ページで [保存 (Save) ] をクリックします。

## 複数のマッピングアドレス (スタティック自動 NAT、1 対多) を持つ内部ロードバランサ

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の例は、複数の IP アドレスに変換される内部ロードバランサを示しています。外部ホストがマッピング IP アドレスの 1 つにアクセスする場合、1 つのロードバランサのアドレスには変換されません。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。

図 35: 内部ロードバランサのスタティック NAT (1 対多)



## 始める前に

Web サーバを保護するデバイスのインターフェイスが含まれているインターフェイス オブジェクト (セキュリティゾーンまたはインターフェイス グループ) があることを確認します。この例では、インターフェイス オブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイス オブジェクトを設定するには、**[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択してから、**[インターフェイス (Interface)]** を選択します。

## 手順

**ステップ 1** ロードバランサをマッピングするアドレスに対し、ネットワーク オブジェクトを作成します。

- a) **[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択します。
- b) コンテンツのテーブルから **[ネットワーク (Network)]** を選択し、**[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックします。
- c) アドレスを定義します。

ネットワーク オブジェクトに名前 (たとえば、myPublicIPs) を付けて、ネットワーク範囲 209.165.201.3-209.165.201.5 を入力します。

- d) **[保存 (Save)]** をクリックします。

**ステップ 2** ロードバランサに対するネットワーク オブジェクトを作成します。

- a) **[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックします。
- b) ネットワーク オブジェクトに名前 (たとえば、myLBHost) を付けて、ホストアドレス 10.1.2.27 を入力します。

c) [保存 (Save) ] をクリックします。

**ステップ 3** ロードバランサのスタティック NAT を設定します。

a) [デバイス (Devices) ] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。

b) [ルールの追加 (Add Rule) ] をクリックします。

c) 次のプロパティを設定します。

- [NAT ルール (NAT Rule) ] = 自動 NAT ルール (Auto NAT Rule) 。
- [タイプ (Type) ] = スタティック (Static) 。

d) [インターフェイス オブジェクト (Interface Objects) ] タブで、次の項目を設定します。

- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
- [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。

e) [変換 (Translation) ] タブで、次の項目を設定します。

- [元の送信元 (Original Source) ] = myLBHost ネットワーク オブジェクト。
- [変換済みの送信元 (Translated Source) ] > [アドレス (Address) ] = myPublicIPs ネットワーク グループ。

#### Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static  Enable

Interface Objects Translation PAT Pool Advanced

**Original Packet**

Original Source:\* myLBHost

Original Port: TCP

**Translated Packet**

Translated Source: Address

Translated Port: myPublicIPs

f) [保存 (Save) ] をクリックします。

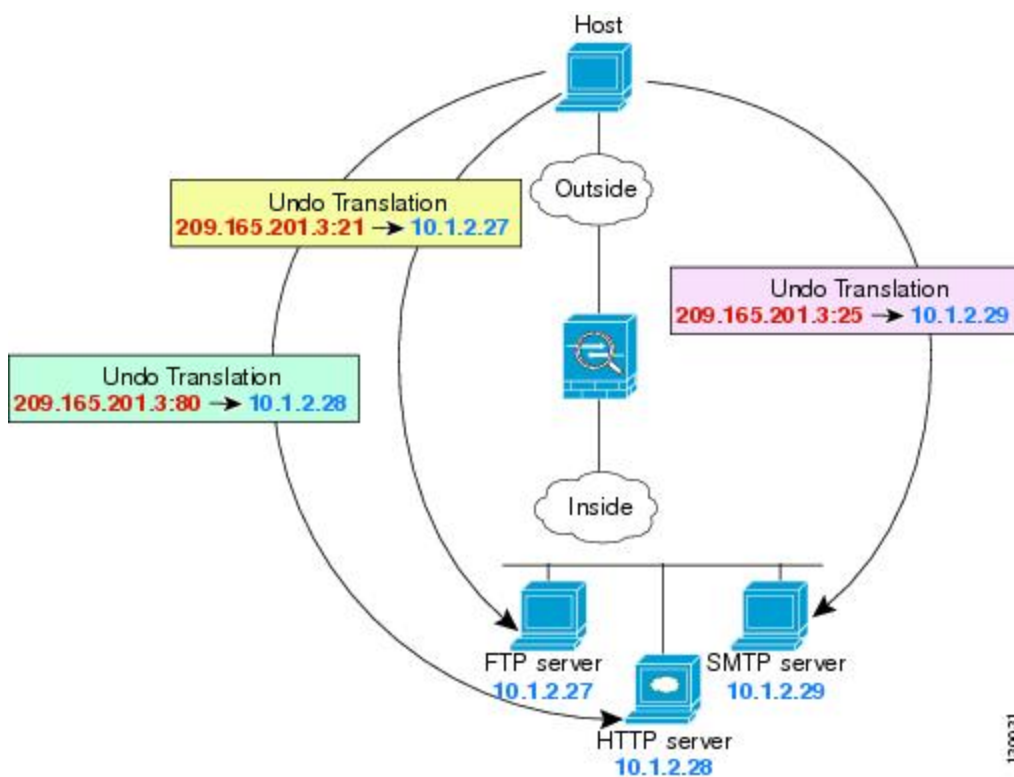
**ステップ 4** [NAT ルール (NAT rule) ] ページで [保存 (Save) ] をクリックします。

## FTP、HTTP、および SMTP の単一アドレス (ポート変換を設定したスタティック自動 NAT)

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次のポート変換を設定したスタティック NAT の例では、リモートユーザが FTP、HTTP、および SMTP にアクセスするための単一のアドレスを提供します。これらのサーバは実際には、それぞれ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定したスタティック NAT ルールを指定すると、使用するマッピング IP アドレスは同じで、それぞれ別のポートを使用することができます。

図 36: ポート変換を設定したスタティック NAT



### 始める前に

サーバを保護するデバイスのインターフェイスが含まれるインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) があることを確認します。この例では、インターフェイスオブジェクトが「inside」および「outside」という名前のセキュリティゾーンであると仮定しています。インターフェイスオブジェクトを設定するには、**[オブジェクト**

(Objects) ]> [オブジェクト管理 (Object Management) ] を選択し、[インターフェイス (Interface) ] を選択します。

#### 手順

**ステップ 1** FTP サーバのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects) ]> [オブジェクト管理 (Object Management) ] を選択します。
- コンテンツのテーブルから [ネットワーク (Network) ] を選択し、[ネットワークの追加 (Add Network) ]> [オブジェクトの追加 (Add Object) ] をクリックします。
- ネットワーク オブジェクトに名前を付け (たとえば「FTPserver」)、FTPサーバの実際の IP アドレス (10.1.2.27) を入力します。

#### New Network Objects

Name:	FTPserver
Description:	
Network:	10.1.2.27
Allow Overrides:	<input checked="" type="checkbox"/>

- [保存 (Save) ] をクリックします。

**ステップ 2** HTTP サーバのネットワーク オブジェクトを作成します。

- [ネットワークの追加 (Add Network) ]> [オブジェクトの追加 (Add Object) ] をクリックします。
- ネットワーク オブジェクトに名前を付け (たとえば「HTTPserver」)、ホストアドレス (10.1.2.28) を入力します。

#### New Network Objects

Name:	HTTPserver
Description:	
Network:	10.1.2.28
Allow Overrides:	<input checked="" type="checkbox"/>

- [保存 (Save) ] をクリックします。

**ステップ 3** SMTP サーバのネットワーク オブジェクトを作成します。

- [ネットワークの追加 (Add Network) ]> [オブジェクトの追加 (Add Object) ] をクリックします。
- ネットワーク オブジェクトに名前を付け (たとえば「SMTPserver」)、ホストアドレス (10.1.2.29) を入力します。

## Edit Network Objects

Name:	SMTPserver
Description:	
Network:	10.1.2.29
Allow Overrides:	<input checked="" type="checkbox"/>

c) [保存 (Save) ]をクリックします。

**ステップ 4** 3つのサーバに使用されるパブリック IP アドレスのネットワーク オブジェクトを作成します。

- [ネットワークの追加 (Add Network) ]>[オブジェクトの追加 (Add Object) ]をクリックします。
- ネットワーク オブジェクトに名前を付け (たとえば「ServerPublicIP」) 、ホストアドレス (209.165.201.3) を入力します。

## New Network Objects

Name:	ServerPublicIP
Description:	
Network:	209.165.201.3
Allow Overrides:	<input checked="" type="checkbox"/>

c) [保存 (Save) ]をクリックします。

**ステップ 5** FTP サーバのポート変換を設定したスタティック NAT を設定し、FTP ポートを自身にマッピングします。

- [デバイス (Devices) ]>[NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- [ルールの追加 (Add Rule) ]をクリックします。
- 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 自動 NAT ルール (Auto NAT Rule) 。
  - [タイプ (Type) ] = スタティック (Static) 。
- [インターフェイス オブジェクト (Interface Objects) ] タブで、次の項目を設定します。
  - [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。
- [変換 (Translation) ] タブで、次の項目を設定します。
  - [元の発信元 (Original Source) ] = FTPserver ネットワーク オブジェクト。
  - [変換済みの発信元 (Translated Source) ]>[アドレス (Address) ] = ServerPublicIP ネットワーク オブジェクト。



- [元のポート (Original Port) ] > [TCP] = 21。
- [変換済みポート (Translated Port) ] = 21。

## Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static  Enable

Interface Objects Translation PAT Pool Advanced

**Original Packet**

Original Source:\* FTPserver

Original Port: TCP 21

**Translated Packet**

Translated Source: Address ServerPublicIP

Translated Port: 21

f) [保存 (Save) ] をクリックします。

**ステップ 6** HTTP サーバのポート変換を設定したスタティック NAT を設定し、HTTP ポートを自身にマッピングします。

- [ルール の追加 (Add Rule) ] をクリックします。
- 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 自動 NAT ルール (Auto NAT Rule) 。
  - [タイプ (Type) ] = スタティック (Static) 。
- [インターフェイス オブジェクト (Interface Objects) ] タブで、次の項目を設定します。
  - [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。
- [変換 (Translation) ] タブで、次の項目を設定します。
  - [元の発信元 (Original Source) ] = HTTPserver ネットワーク オブジェクト。
  - [変換済みの発信元 (Translated Source) ] > [アドレス (Address) ] = ServerPublicIP ネットワーク オブジェクト。
  - [元のポート (Original Port) ] > [TCP] = 80。
  - [変換済みポート (Translated Port) ] = 80。

## Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static  Enable

Interface Objects: Translation PAT Pool Advanced

**Original Packet**

Original Source:\* HTTPserver

Original Port: TCP 80

**Translated Packet**

Translated Source: Address ServerPublicIP

Translated Port: 80

e) [保存 (Save) ]をクリックします。

**ステップ7** SMTPサーバのポート変換を設定したスタティック NAT を設定し、SMTP ポートを自身にマッピングします。

a) [ルール の追加 (Add Rule) ]をクリックします。

b) 次のプロパティを設定します。

- [NAT ルール (NAT Rule) ] = 自動 NAT ルール (Auto NAT Rule) 。
- [タイプ (Type) ] = スタティック (Static) 。

c) [インターフェイス オブジェクト (Interface Objects) ] タブで、次の項目を設定します。

- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
- [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。

d) [変換 (Translation) ] タブで、次の項目を設定します。

- [元の発信元 (Original Source) ] = SMTPserver ネットワーク オブジェクト。
- [変換済みの発信元 (Translated Source) ] > [アドレス (Address) ] = ServerPublicIP ネットワーク オブジェクト。
- [元のポート (Original Port) ] > [TCP] = 25。
- [変換済みポート (Translated Port) ] = 25。

### Add NAT Rule

e) [保存 (Save) ]をクリックします。

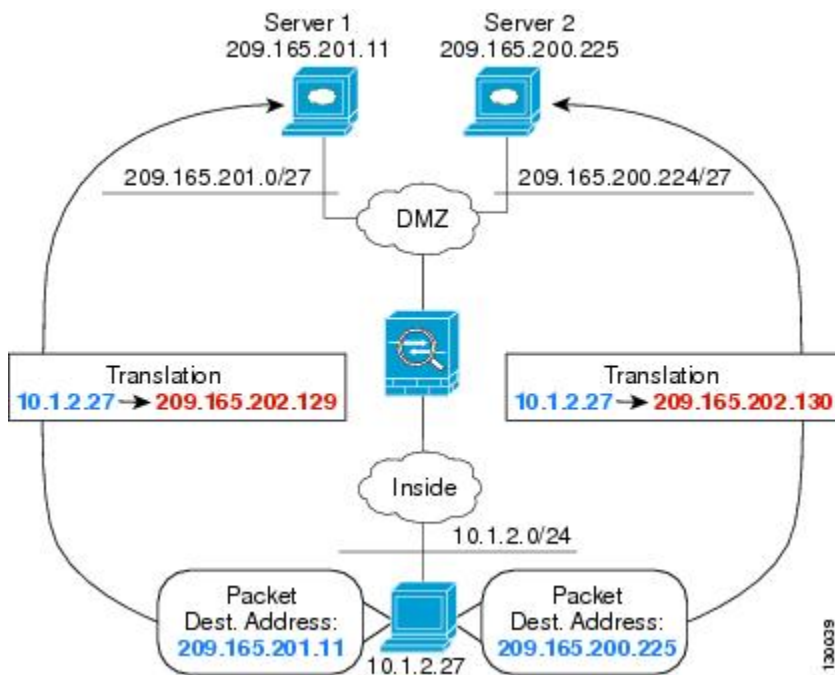
**ステップ 8** [NAT ルール (NAT rule) ] ページで [保存 (Save) ] をクリックします。

## 宛先に応じて異なる変換 (ダイナミック手動 PAT)

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の図に、2 台の異なるサーバにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129:ポートに変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

図 37:異なる宛先アドレスを使用する手動 NAT



### 始める前に

サーバを保護するデバイスのインターフェイスが含まれるインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) があることを確認します。この例では、インターフェイス オブジェクトは「inside」および「dmz」という名前のセキュリティゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、[インターフェイス (Interface)] を選択します。

### 手順

- ステップ 1** 内部ネットワークのネットワーク オブジェクトを作成します。
- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
  - コンテンツのテーブルから [ネットワーク (Network)] を選択し、[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
  - ネットワーク オブジェクトに名前を付け (myInsideNetwork など)、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

**New Network Objects**

Name:	myInsideNetwork
Description:	
Network:	10.1.2.0/24
Allow Overrides:	<input checked="" type="checkbox"/>

d) [保存 (Save) ] をクリックします。

**ステップ 2** DMZ ネットワーク 1 のネットワーク オブジェクトを作成します。

- [ネットワークを追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] をクリックします。
- ネットワーク オブジェクトに名前を付け (DMZnetwork1 など)、ネットワーク アドレス 209.165.201.0/27 を入力します (255.255.255.224 のサブネット マスク)。

**New Network Objects**

Name:	DMZnetwork1
Description:	
Network:	209.165.201.0/27
Allow Overrides:	<input checked="" type="checkbox"/>

c) [保存 (Save) ] をクリックします。

**ステップ 3** DMZ ネットワーク 1 の PAT アドレスのネットワーク オブジェクトを作成します。

- [ネットワークを追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] をクリックします。
- ネットワーク オブジェクトに名前を付け (PATaddress1 など)、ホスト アドレス 209.165.202.129 を入力します。

**New Network Objects**

Name:	PATaddress1
Description:	
Network:	209.165.202.129
Allow Overrides:	<input checked="" type="checkbox"/>

c) [保存 (Save) ] をクリックします。

**ステップ 4** DMZ ネットワーク 2 のネットワーク オブジェクトを作成します。

- [ネットワークを追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] をクリックします。

- b) ネットワーク オブジェクトに名前を付け (DMZnetwork2 など)、ネットワーク アドレス 209.165.200.224/27 を入力します (255.255.255.224 のサブネット マスク)。

**New Network Objects**

Name:	DMZnetwork2
Description:	
Network:	209.165.200.224/27
Allow Overrides:	<input checked="" type="checkbox"/>

- c) [保存 (Save) ] をクリックします。

**ステップ 5** DMZ ネットワーク 2 の PAT アドレスのネットワーク オブジェクトを作成します。

- a) [ネットワークを追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] をクリックします。
- b) ネットワーク オブジェクトに名前を付け (PATaddress2 など)、ホスト アドレス 209.165.202.130 を入力します。

**New Network Objects**

Name:	PATaddress2
Description:	
Network:	209.165.202.130
Allow Overrides:	<input checked="" type="checkbox"/>

- c) [保存 (Save) ] をクリックします。

**ステップ 6** DMZ ネットワーク 1 のダイナミック手動 PAT を設定します。

- a) [デバイス (Devices) ] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルール of の追加 (Add Rule) ] をクリックします。
- c) 次のプロパティを設定します。
- [NAT ルール (NAT Rule) ] = 手動 NAT ルール。
  - [タイプ (Type) ] = Dynamic。
- d) [インターフェイス オブジェクト (Interface Objects) ] タブで、以下の設定を行います。
- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = dmz。
- e) [変換 (Translation) ] タブで、次の項目を設定します。
- [元の発信元 (Original Source) ] = myInsideNetwork ネットワーク オブジェクト。

- [変換済みの発信元アドレス (Translated Source Address) ] = PATAddress1 ネットワーク オブジェクト。
- [元の宛先アドレス (Original Destination Address) ] = DMZnetwork1 ネットワーク オブジェクト。 >
- [変換済みの宛先 (Translated Destination) ] = DMZnetwork1 ネットワーク オブジェクト。

(注) 宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。[ポート (Port) ] フィールドはすべて空白のままにします。

### Add NAT Rule

The screenshot shows the 'Add NAT Rule' configuration interface. At the top, 'NAT Rule' is set to 'Manual NAT Rule' and 'Type' is 'Dynamic'. The 'Translation' tab is selected, showing the following settings:

Original Packet	Translated Packet
Original Source: * myInsideNetwork	Translated Source: Address
Original Destination: Address	Translated Source: PATAddress1
DMZNetwork1	Translated Destination: DMZNetwork1

f) [保存 (Save) ] をクリックします。

### ステップ7 DMZ ネットワーク 2 のダイナミック手動 PAT を設定します。

- [ルール の追加 (Add Rule) ] をクリックします。
- 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 手動 NAT ルール。
  - [タイプ (Type) ] = Dynamic。
- [インターフェイス オブジェクト (Interface Objects) ] タブで、以下の設定を行います。
  - [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = dmz。
- [変換 (Translation) ] タブで、次の項目を設定します。
  - [元の発信元 (Original Source) ] = myInsideNetwork ネットワーク オブジェクト。
  - [変換済みの発信元アドレス (Translated Source Address) ] = PATAddress2 ネットワーク オブジェクト。 >

宛先アドレスおよびポートに応じて異なる変換 (ダイナミック手動 PAT)

- [元の宛先アドレス (Original Destination Address) ] = DMZnetwork2 ネットワーク オブジェクト。 >
- [変換済みの宛先 (Translated Destination) ] = DMZnetwork2 ネットワーク オブジェクト。

Add NAT Rule

e) [保存 (Save) ] をクリックします。

ステップ 8 [NAT ルール (NAT rule) ] ページで [保存 (Save) ] をクリックします。

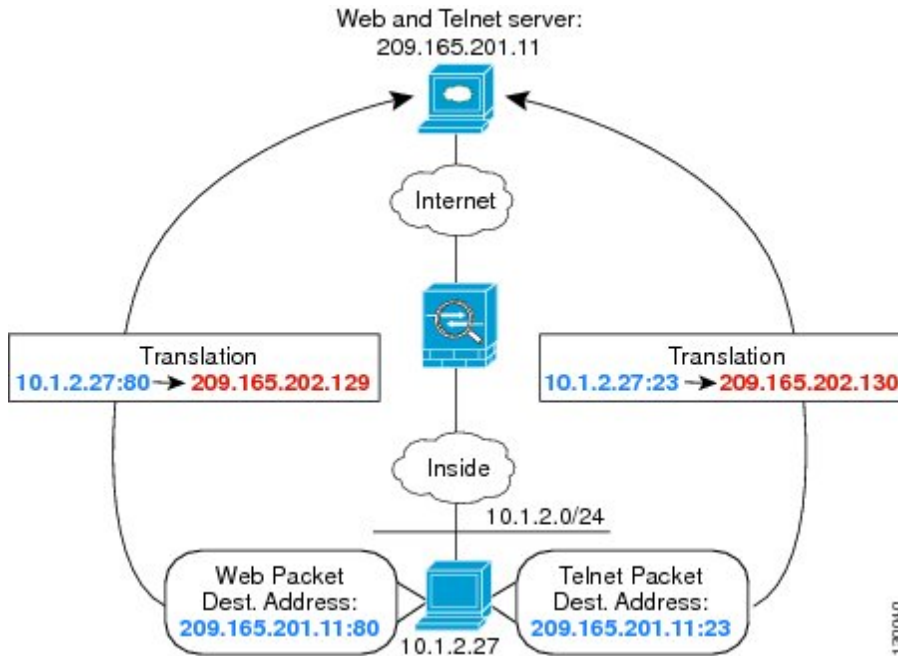
## 宛先アドレスおよびポートに応じて異なる変換 (ダイナミック手動 PAT)

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の図に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Telnet サービスを求めてサーバにアクセスすると、実際のアドレスは 209.165.202.129:ポートに変換されます。ホストが Web サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。



図 38:異なる宛先ポートを使用する手動 NAT



### 始める前に

サーバを保護するデバイスのインターフェイスが含まれるインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) があることを確認します。この例では、インターフェイス オブジェクトは「inside」および「dmz」という名前のセキュリティゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、[インターフェイス (Interface)] を選択します。

### 手順

**ステップ 1** 内部ネットワークのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- コンテンツのテーブルから [ネットワーク (Network)] を選択し、[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- ネットワーク オブジェクトに名前を付け (myInsideNetwork など)、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

## New Network Objects

Name:	myInsideNetwork
Description:	
Network:	10.1.2.0/24
Allow Overrides:	<input checked="" type="checkbox"/>

d) [保存 (Save) ]をクリックします。

**ステップ 2** Telnet/Web サーバのネットワーク オブジェクトを作成します。

- [ネットワークを追加 (Add Network) ]>[オブジェクトの追加 (Add Object) ]をクリックします。
- ネットワーク オブジェクトに名前を付け (TelnetWebServer など)、ホスト アドレス 209.165.201.11 を入力します。

## New Network Objects

Name:	TelnetWebServer
Description:	
Network:	209.165.201.11
Allow Overrides:	<input checked="" type="checkbox"/>

c) [保存 (Save) ]をクリックします。

**ステップ 3** Telnet を使用するとき、PAT アドレスのネットワーク オブジェクトを作成します。

- [ネットワークを追加 (Add Network) ]>[オブジェクトの追加 (Add Object) ]をクリックします。
- ネットワーク オブジェクトに名前を付け (PATAddress1 など)、ホスト アドレス 209.165.202.129 を入力します。

## New Network Objects

Name:	PATAddress1
Description:	
Network:	209.165.202.129
Allow Overrides:	<input checked="" type="checkbox"/>

c) [保存 (Save) ]をクリックします。

**ステップ 4** HTTP を使用するとき、PAT アドレスのネットワーク オブジェクトを作成します。

- [ネットワークを追加 (Add Network) ]>[オブジェクトの追加 (Add Object) ]をクリックします。

- b) ネットワーク オブジェクトに名前を付け (PATaddress2 など)、ホストアドレス 209.165.202.130 を入力します。

**New Network Objects**

Name:	PATaddress2
Description:	
Network:	209.165.202.130
Allow Overrides:	<input checked="" type="checkbox"/>

- c) [保存 (Save)] をクリックします。

**ステップ 5** Telnet アクセスのダイナミック手動 PAT を設定します。

- a) [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルール の追加 (Add Rule)] をクリックします。
- c) 次のプロパティを設定します。
- [NAT ルール (NAT Rule)] = 手動 NAT ルール。
  - [タイプ (Type)] = Dynamic。
- d) [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。
- [送信元インターフェイス オブジェクト (Source Interface Objects)] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = dmz。
- e) [変換 (Translation)] タブで、次の項目を設定します。
- [元の発信元 (Original Source)] = myInsideNetwork ネットワーク オブジェクト。
  - [変換済みの発信元アドレス (Translated Source Address)] = PATaddress1 ネットワーク オブジェクト。
  - [元の宛先アドレス (Original Destination Address)] = TelnetWebServer ネットワーク オブジェクト。 >
  - [変換済みの宛先 (Translated Destination)] = TelnetWebServer ネットワーク オブジェクト。
  - [元の宛先ポート (Original Destination Port)] = TELNET ポート オブジェクト (システム定義)。
  - [変換済みの宛先ポート (Translated Destination Port)] = TELNET ポート オブジェクト (システム定義)。

- (注) 宛先アドレスまたはポートを変換しないため、元のアドレスと変換済みの宛先アドレスに同じアドレスを指定し、元のポートと変換済みのポートに同じポートを指定することによって、アイデンティティ NAT を設定する必要があります。

## Add NAT Rule

NAT Rule:	Manual NAT Rule	Insert:	In Category	NAT Rules Before
Type:	Dynamic	<input checked="" type="checkbox"/> Enable		
Description:				
Interface Objects <b>Translation</b> PAT Pool   Advanced				
<b>Original Packet</b>		<b>Translated Packet</b>		
Original Source:*	myInsideNetwork	Translated Source:	Address	
Original Destination:	Address		PATAddress1	
	TelnetWebServer	Translated Destination:	TelnetWebServer	
Original Source Port:		Translated Source Port:		
Original Destination Port:	TELNET	Translated Destination Port:	TELNET	

- f) [保存 (Save)] をクリックします。

### ステップ 6 Web アクセスのダイナミック手動 PAT を設定します。

- [ルール の追加 (Add Rule)] をクリックします。
- 次のプロパティを設定します。
  - [NAT ルール (NAT Rule)] = 手動 NAT ルール。
  - [タイプ (Type)] = Dynamic。
- [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。
  - [送信元インターフェイス オブジェクト (Source Interface Objects)] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = dmz。
- [変換 (Translation)] タブで、次の項目を設定します。
  - [元の発信元 (Original Source)] = myInsideNetwork ネットワーク オブジェクト。
  - [変換済みの発信元アドレス (Translated Source Address)] = PATAddress2 ネットワーク オブジェクト。 >
  - [元の宛先アドレス (Original Destination Address)] = TelnetWebServer ネットワーク オブジェクト。 >
  - [変換済みの宛先 (Translated Destination)] = TelnetWebServer ネットワーク オブジェクト。

- [元の宛先ポート (Original Destination Port) ] = HTTP ポート オブジェクト (システム定義)。
- [変換済みの宛先ポート (Translated Destination Port) ] = HTTP ポート オブジェクト (システム定義)。

## Add NAT Rule

NAT Rule:  Insert:

Type:   Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* <input type="text" value="myInsideNetwork"/>	Translated Source: <input type="text" value="Address"/>
Original Destination: <input type="text" value="Address"/> <input type="text" value="TelnetWebServer"/>	Translated Destination: <input type="text" value="TelnetWebServer"/>
Original Source Port: <input type="text"/>	Translated Source Port: <input type="text"/>
Original Destination Port: <input type="text" value="HTTP"/>	Translated Destination Port: <input type="text" value="HTTP"/>

e) [保存 (Save) ] をクリックします。

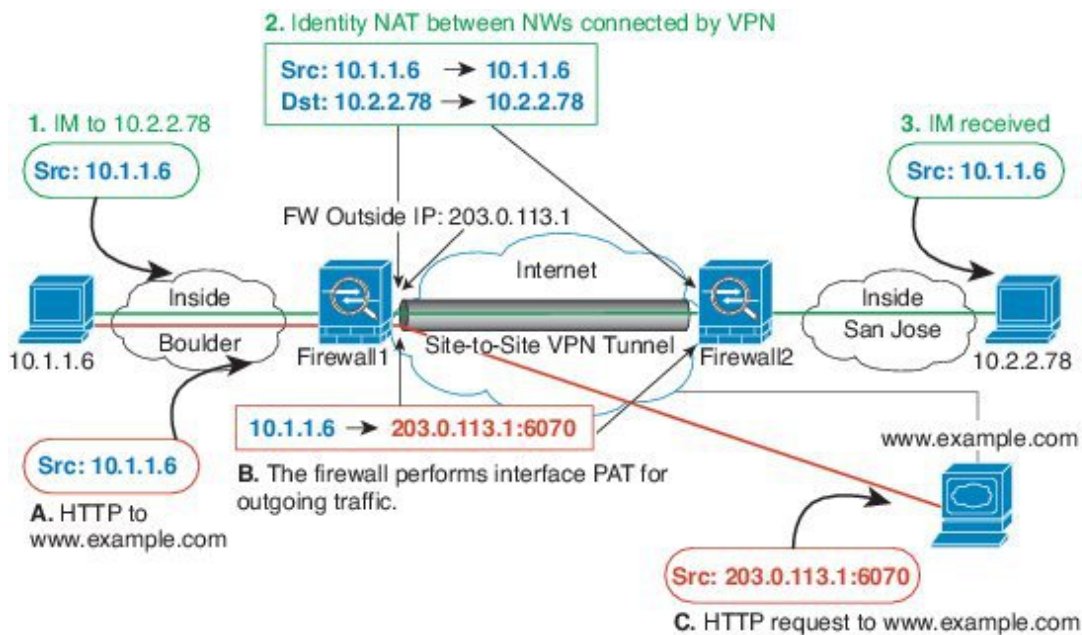
**ステップ 7** [NAT ルール (NAT rule) ] ページで [保存 (Save) ] をクリックします。

## NAT およびサイト間 VPN

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の図に、ボールダーとサンノゼのオフィスを接続するサイトツーサイト トンネルを示します。インターネットに渡すトラフィックについて (たとえばボールダーの 10.1.1.6 から www.example.com へ)、インターネットへのアクセスのために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。ただし、VPN トンネルを経由するトラフィックについては (たとえば、ボールダーの 10.1.1.6 からサンノゼの 10.2.2.78 へ)、NAT を実行しません。そのため、アイデンティティ NAT ルールを作成して、そのトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスにアドレスを変換します。

図 39: サイトツーサイト VPNのためのインターフェイス PAT およびアイデンティティ NAT



次の例は、Firewall1（ボールドー）の設定を示します。

### 始める前に

VPN 内のデバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトは、Firewall1（ボールドー）インターフェイスに対応する **inside-boulder** および **outside-boulder** という名前のセキュリティゾーンであると仮定します。インターフェイス オブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択してから、[インターフェイス (Interfaces)] を選択します。

### 手順

**ステップ 1** さまざまなネットワークを定義するには、オブジェクトを作成します。

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- 目次から [ネットワーク (Network)] を選択して、[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- ボールドー内部ネットワークを特定します。

ネットワーク オブジェクトに名前（たとえば、boulder-network）を付けて、ネットワーク アドレス 10.1.1.0/24 を入力します。

- d) [保存 (Save)] をクリックします。
- e) [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックして、内部サンノゼ ネットワークを定義します。

ネットワーク オブジェクトに名前 (たとえば、sanjose-network) を付けて、ネットワーク アドレス 10.2.2.0/24 を入力します。

- f) [保存 (Save)] をクリックします。

**ステップ 2** Firewall1 (ボールドー) 上で VPN 経由でサンノゼに向かう場合、ボールドー ネットワークの手動アイデンティティ NAT を設定します。

- a) [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule)] をクリックします。
- c) 次のプロパティを設定します。
- [NAT ルール (NAT Rule)] = 手動 NAT ルール (Manual NAT Rule)。
  - [タイプ (Type)] = スタティック (Static)。
- d) [インターフェイス オブジェクト (Interface Objects)] タブで、次の項目を設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects)] = inside-boulder。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = outside-boulder。
- e) [変換 (Translation)] タブで、次の項目を設定します。
- [元の送信元 (Original Source)] = boulder-network オブジェクト。

- [変換済みの送信元 (Translated Source) ] > [アドレス (Address) ] = boulder-network オブジェクト。
- [元の宛先 (Original Destination) ] > [アドレス (Address) ] = sanjose-network オブジェクト。
- [変換済みの宛先] = sanjose-network オブジェクト。

(注) 宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。[ポート (Port) ] フィールドはすべて空白のままにします。このルールは、送信元と宛先の両方のアイデンティティ NAT を設定します。

- f) [詳細 (Advanced) ] タブで [宛先インターフェイスでプロキシ ARP なし (Do not proxy ARP on Destination interface) ] を選択します。

### Add NAT Rule

The screenshot shows the 'Add NAT Rule' configuration page. At the top, 'NAT Rule' is set to 'Manual NAT Rule' and 'Type' is 'Static'. The 'Original Packet' section has 'Original Source' set to 'boulder-network', and 'Original Destination' set to 'Address' and 'sanjose-network'. The 'Translated Packet' section has 'Translated Source' set to 'Address' and 'Translated Destination' set to 'sanjose-network'. The 'Advanced' tab is selected.

- g) [保存 (Save) ] をクリックします。

**ステップ 3** Firewall1 (ボールダー) 上で内部ボールダーネットワークのインターネットに入る場合、手動ダイナミック インターフェイス PAT を設定します。

- [ルールの追加 (Add Rule) ] をクリックします。
- 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 手動 NAT ルール。
  - [タイプ (Type) ] = ダイナミック (Dynamic) 。
  - [挿入ルール (Insert Rule) ] = 最初のルールの後の任意の位置。このルールは任意の宛先アドレスに適用されるため、sanjose-network を宛先として使用するルールはこのルールの前に来る必要があります。そうでなければ、sanjose-network ルールは永遠に一致することがありません。デフォルトでは、新しい手動 NAT ルールは [自動 NAT の前に NAT ルール (NAT Rules Before Auto NAT) ] セクションの最後に配置されます。
- [インターフェイス オブジェクト (Interface Objects) ] タブで、次の項目を設定します。



- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside-boulder。
- [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside-boulder。

d) [変換 (Translation) ] タブで、次の項目を設定します。

- [元の送信元 (Original Source) ] = boulder-network オブジェクト。
- [変換済みの送信元 (Translated Source) ] = 宛先インターフェイス IP (Destination Interface IP) 。このオプションでは、宛先インターフェイスオブジェクトに含まれているインターフェイスを使用して、インターフェイス PAT を設定します。
- [元の宛先 (Original Destination) ] > [アドレス (Address) ] = 任意 (空白のまま) 。
- [変換済みの宛先 (Translated Destination) ] = 任意 (空白のまま) 。

#### Add NAT Rule

e) [保存 (Save) ] をクリックします。

**ステップ 4** Firewall2 (サンノゼ) の管理を行っている場合、そのデバイスに同様のルールを設定できます。

- 手動アイデンティティ NAT ルールは、宛先が boulder-network の場合は sanjose-network 向けになります。Firewall2 の内部および外部ネットワーク向けに新しいインターフェイス オブジェクトを作成します。
- 手動ダイナミックインターフェイス PAT ルールは、宛先が「任意」の場合は sanjose-network 向けになります。

## NAT を使用した DNS クエリと応答の書き換え

応答内のアドレスを NAT コンフィギュレーションと一致するアドレスに置き換えて、DNS 応答を修正するように Firepower Threat Defense デバイスを設定することが必要になる場合があります。DNS 修正は、各トランスレーションルールを設定するときに設定できます。

この機能は、NAT ルールに一致する DNS クエリと応答のアドレスをリライトします（たとえば、IPv4 の A レコード、IPv6 の AAAA レコード、または逆引き DNS クエリの PTR レコード）。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答では、A レコードはマップされた値から実際の値へリライトされます。逆に、任意のインターフェイスからマッピング インターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へリライトされます。

以下に、NAT ルールで DNS のリライトを設定する必要がある主な状況を示します。

- ルールは NAT64 または NAT46 であり、DNS サーバは外部ネットワークにあります。DNS A レコード (IPv4 用) と AAAA レコード (IPv6 用) を変換するために DNS のリライトが必要です。
- DNS サーバは外部にあり、クライアントは内部にあります。クライアントが使用する一部の完全修飾ドメイン名が他の内部ホストに解決されます。
- DNS サーバは内部にあり、プライベート IP アドレスを使用して応答します。クライアントは外部にあり、クライアントは内部でホストされているサーバを指定する完全修飾ドメイン名にアクセスします。

### DNS リライトに関する制限事項

次に DNS リライトの制限事項を示します。

- 個々の A または AAAA レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS リライトは PAT には適用されません。
- 手動 NAT ルールを設定する場合、送信元アドレスおよび宛先アドレスを指定すると、DNS 修正を設定できません。これらの種類のルールでは、A と B に向かった場合に 1 つのアドレスに対して異なる変換が行われる可能性があります。したがって、Firepower Threat Defense デバイスは、DNS 応答内の IP アドレスを適切な Twice NAT ルールに一致させることができません。DNS 応答には、DNS 要求を求めたパケット内の送信元アドレスと宛先アドレスの組み合わせに関する情報が含まれません。
- 実際には、DNS リライトは NAT ルールではなく xlate エントリで実行されます。したがって、ダイナミック ルールに xlate がない場合、リライトが正しく実行されません。スタティック NAT の場合は、同じような問題が発生しません。
- DNS のリライトによって、DNS ダイナミック アップデートのメッセージ (オペレーションコード 5) は書き換えられません。

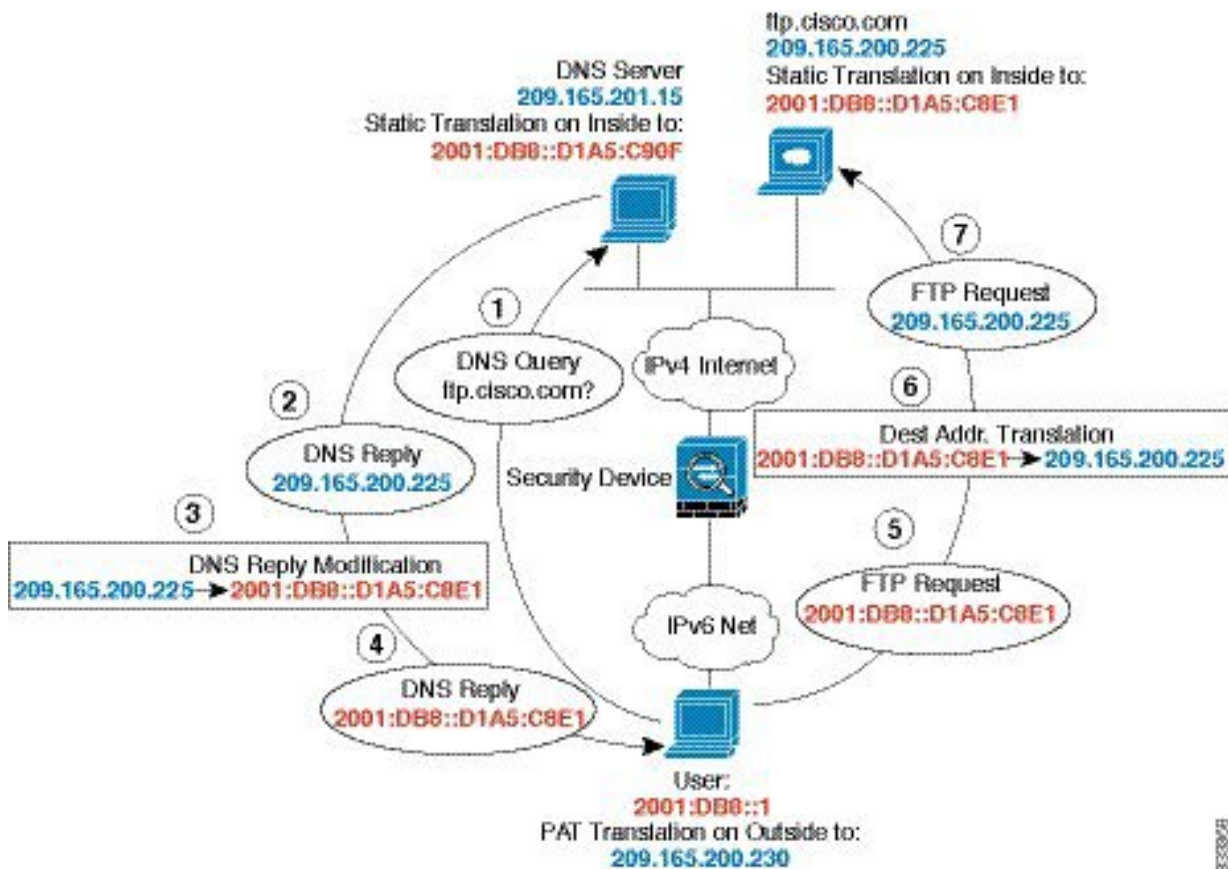
次のトピックで、NAT ルールでの DNS リライトの例を示します。

## DNS64 応答修正

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の図に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部 IPv6 ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは実際のアドレス (209.165.200.225) を応答します。

内部ユーザに ftp.cisco.com のマッピングアドレス (2001:DB8::D1A5:C8E1 : D1A5:C8E1 は IPv6 の 209.165.200.225 に相当) を使用させるには、スタティック変換用の DNS 応答修正を設定する必要があります。この例には、DNS サーバのスタティック NAT 変換、および内部 IPv6 ホストの PAT ルールも含まれています。



## 始める前に

デバイスに対応するインターフェイスが含まれているインターフェイスオブジェクト（セキュリティゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、**[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択してから、**[インターフェイス (Interface)]** を選択します。

## 手順

**ステップ 1** FTP サーバ、DNS サーバ、内部ネットワーク、および PAT プールのネットワーク オブジェクトを作成します。

- a) **[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択します。
- b) コンテンツのテーブルから **[ネットワーク (Network)]** を選択し、**[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックします。
- c) 実際の FTP サーバアドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp\_server など)、ホストアドレス 209.165.200.225 を入力します。

The screenshot shows a dialog box titled "New Network Objects" with a close button (X) and a help button (?). It contains the following fields and options:

- Name:** ftp\_server
- Description:** (empty text area)
- Network:** 209.165.200.225
- Format:** ipaddr or ipaddr/len or range (ipaddr-ipaddr)
- Allow Overrides:**

- d) **[保存 (Save)]** をクリックします。
- e) **[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックして、FTP サーバの変換済み IPv6 アドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp\_server\_v6 など)、ホストアドレス 2001:DB8::D1A5:C8E1 を入力します。

**New Network Objects** ? x

Name:

Description:

Network:   
*Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)*

Allow Overrides:

- f) [保存 (Save) ] をクリックします。
- g) [ネットワークを追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] をクリックして、DNS サーバの実際のアドレスを定義します。

ネットワーク オブジェクトに名前を付け (dns\_server など)、ホストアドレス 209.165.201.15 を入力します。

**New Network Objects** ? x

Name:

Description:

Network:   
*Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)*

Allow Overrides:

- h) [保存 (Save) ] をクリックします。
- i) [ネットワークを追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] をクリックして、DNS サーバの変換済み IPv6 アドレスを定義します。

ネットワーク オブジェクトに名前を付け (dns\_server\_v6 など)、ホストアドレス 2001:DB8::D1A5:C90F を入力します (ここで、D1A5:C90F は IPv6 の場合の 209.165.201.15 です)。

**New Network Objects** ? x

Name:

Description:

Network:   
*Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)*

Allow Overrides:

- j) [保存 (Save) ] をクリックします。

- k) [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックして、内部 IPv6 ネットワークを定義します。

ネットワーク オブジェクトに名前 (inside\_v6 など) を付け、ネットワーク アドレス 2001:DB8::/96 を入力します。

- l) [保存 (Save)] をクリックします。
- m) [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックし、内部 IPv6 ネットワークの IPv4 PAT プールを定義します。

ネットワーク オブジェクトに名前を付け (ipv4\_pool など)、範囲 209.165.200.230 ~ 209.165.200.235 を入力します。

- n) [保存 (Save)] をクリックします。

**ステップ 2** FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

- a) [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule)] をクリックします。
- c) 次のプロパティを設定します。
- [NAT ルール (NAT Rule)] = 自動 NAT ルール (Auto NAT Rule)。
  - [タイプ (Type)] = スタティック (Static)。
- d) [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。
- [送信元インターフェイス オブジェクト (Source Interface Objects)] = outside。

- [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = inside。
- e) [変換 (Translation) ] タブで、次の項目を設定します。
- [元の発信元 (Original Source) ] = ftp\_server ネットワーク オブジェクト。
  - [変換済みの発信元アドレス (Translated Source Address) ] = ftp\_server\_v6 ネットワーク オブジェクト。 >

## Add NAT Rule

- f) [詳細 (Advanced) ] タブで、以下のオプションを選択します。
- [このルールに一致する DNS 応答を変換 (Translate DNS replies that match this rule) ]。
  - [ネット間マッピング (Net to Net Mapping) ]。1 対 1 の NAT46 変換であるためです。
- g) [OK] をクリックします。

**ステップ 3** DNS サーバのためのスタティック NAT ルールを設定します。

- a) [ルール の追加 (Add Rule) ] をクリックします。
- b) 次のプロパティを設定します。
- [NAT ルール (NAT Rule) ] = 自動 NAT ルール (Auto NAT Rule) 。
  - [タイプ (Type) ] = スタティック (Static) 。
- c) [インターフェイス オブジェクト (Interface Objects) ] タブで、以下の設定を行います。
- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = outside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = inside。
- d) [変換 (Translation) ] タブで、次の項目を設定します。
- [元の発信元 (Original Source) ] = dns\_server ネットワーク オブジェクト。
  - [変換済みの発信元アドレス (Translated Source Address) ] = dns\_server\_v6 ネットワーク オブジェクト。 >
- e) これは 1 対 1 の NAT46 変換であるため、[詳細 (Advanced) ] タブで、[ネット間マッピング (Net to Net Mapping) ] を選択します。

## Add NAT Rule

f) [OK] をクリックします。

**ステップ 4** 内部 IPv6 ネットワークに対し、PAT プールルールを持つダイナミック NAT を設定します。

a) [ルールの追加 (Add Rule)] をクリックします。

b) 次のプロパティを設定します。

- [NAT ルール (NAT Rule)] = 自動 NAT ルール。
- [タイプ (Type)] = Dynamic。

c) [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト (Source Interface Objects)] = inside。
- [宛先インターフェイス オブジェクト (Destination Interface Objects)] = outside。

d) [変換 (Translation)] タブで、次の項目を設定します。

- [元の発信元 (Original Source)] = inside\_v6 ネットワーク オブジェクト。
- [変換済みの発信元アドレス (Translated Source Address)] > = このフィールドは空のままにします。

## Add NAT Rule

e) [PAT プール (PAT Pool)] タブで、以下の設定を行います。

- [PAT プールの有効化 (Enable PAT Pool)] = このオプションを選択します。
- [変換済みの発信元アドレス (Translated Source Address)] = ipv4\_pool ネットワーク オブジェクト。 >



**Add NAT Rule**

NAT Rule:

Type:   Enable

Interface Objects Translation **PAT Pool** Advanced

Enable PAT Pool

PAT:

Use Round Robin Allocation

Extended PAT Table

Flat Port Range

Include Reserve Ports

f) [OK] をクリックします。

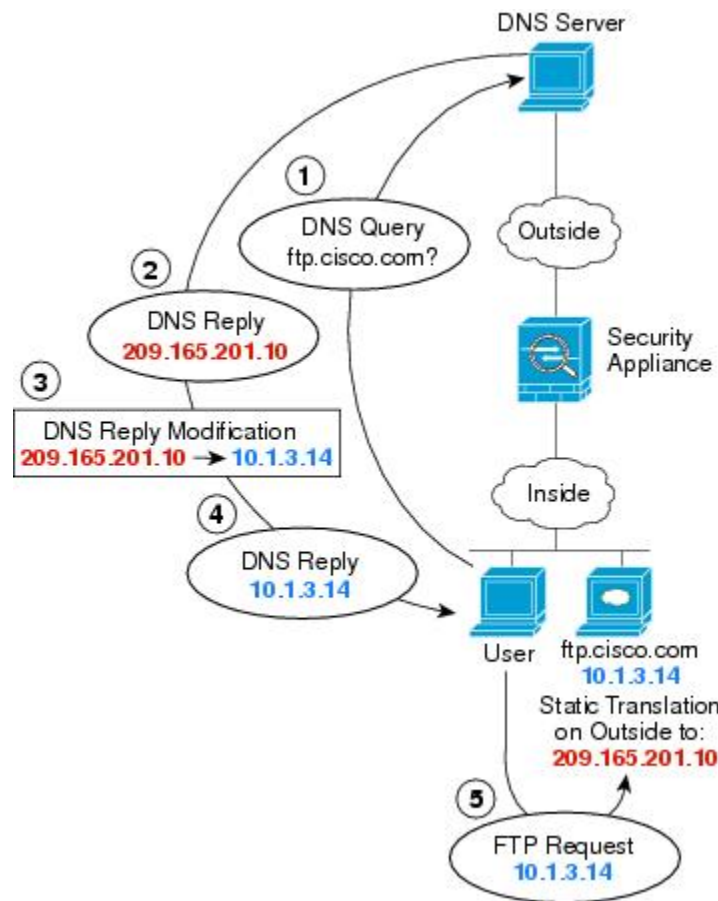
## DNS 応答修正 : 外部の DNS サーバ

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の図に、外部インターフェイスからアクセス可能な DNS サーバを示します。ftp.cisco.com というサーバが内部インターフェイス上にあります。ftp.cisco.com の実際のアドレス (10.1.3.14) を、外部ネットワーク上で確認できるマッピングアドレス (209.165.201.10) にスタティックに変換するように NAT を設定します。

この場合、このスタティック ルールで DNS 応答修正を有効にする必要があります。有効にすると、実際のアドレスを使用して ftp.cisco.com にアクセスできる内部ユーザは、マッピングアドレスではなく実際のアドレスを DNS サーバから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバはマッピングアドレス (209.165.201.10) を応答します。システムは、内部サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正を有効にしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックの送信を試みます。



### 始める前に

デバイスに対応するインターフェイスが含まれているインターフェイスオブジェクト（セキュリティゾーンまたはインターフェイスグループ）があることを確認します。この例では、インターフェイスオブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、**[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択してから、**[インターフェイス (Interface)]** を選択します。

### 手順

**ステップ 1** FTP サーバのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択します。
- コンテンツのテーブルから **[ネットワーク (Network)]** を選択し、**[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックします。
- 実際の FTP サーバアドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp\_server など)、ホストアドレス 10.1.3.14 を入力します。

**New Network Objects** ? x

Name:

Description:

Network:   
 Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- d) [保存 (Save)] をクリックします。
- e) [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックして、FTP サーバの変換済みアドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp\_server\_outside など)、ホストアドレス 209.165.201.10 を入力します。

**New Network Objects** ? x

Name:

Description:

Network:   
 Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- f) [保存 (Save)] をクリックします。

**ステップ 2** FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

- a) [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルール of の追加 (Add Rule)] をクリックします。
- c) 次のプロパティを設定します。
- [NAT ルール (NAT Rule)] = 自動 NAT ルール (Auto NAT Rule)。
  - [タイプ (Type)] = スタティック (Static)。
- d) [インターフェイス オブジェクト (Interface Objects)] タブで、次の項目を設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects)] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = outside。
- e) [変換 (Translation)] タブで、次の項目を設定します。
- [元の発信元 (Original Source)] = ftp\_server ネットワーク オブジェクト。

## DNS 応答修正 : ホスト ネットワーク上の DNS サーバ

- [変換済みの発信元アドレス (Translated Source Address)] = ftp\_server\_outside ネットワーク オブジェクト。 >

- f) [詳細 (Advanced)] タブで、[このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule)] を選択します。

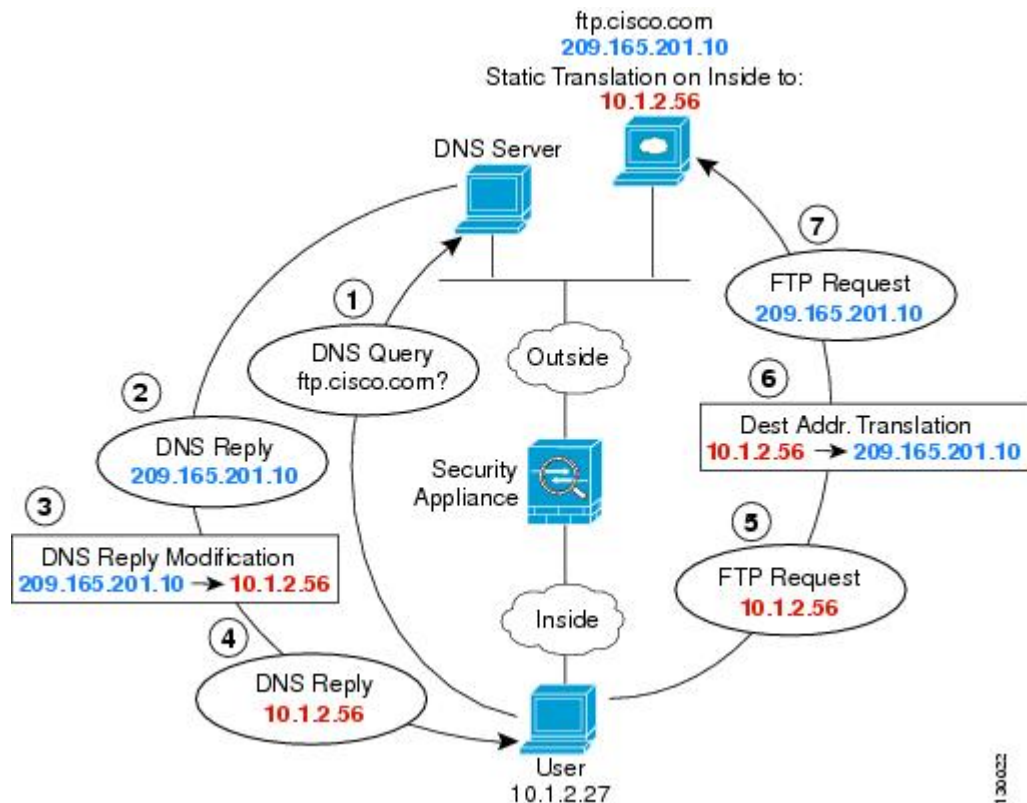
## Add NAT Rule

- g) [OK] をクリックします。

## DNS 応答修正 : ホスト ネットワーク上の DNS サーバ

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の図に、外部の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは実際のアドレス (209.165.20.10) を応答します。内部ユーザに ftp.cisco.com のマッピングアドレス (10.1.2.56) を使用させるには、スタティック変換用の DNS 応答修正を設定する必要があります。



### 始める前に

デバイスに対応するインターフェイスが含まれているインターフェイスオブジェクト（セキュリティゾーンまたはインターフェイスグループ）があることを確認します。この例では、インターフェイスオブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、**[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択してから、**[インターフェイス (Interface)]** を選択します。

### 手順

**ステップ 1** FTP サーバのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択します。
- コンテンツのテーブルから **[ネットワーク (Network)]** を選択し、**[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックします。
- 実際の FTP サーバアドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp\_server など)、ホストアドレス 209.165.201.10 を入力します。

**New Network Objects** ? x

Name:

Description:

Network:   
 Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- d) [保存 (Save) ]をクリックします。
- e) [ネットワークを追加 (Add Network) ]>[オブジェクトの追加 (Add Object) ]をクリックして、FTP サーバの変換済みアドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp\_server\_translated など)、ホストアドレス 10.1.2.56 を入力します。

**New Network Objects** ? x

Name:

Description:

Network:   
 Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- f) [保存 (Save) ]をクリックします。

**ステップ 2** FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

- a) [デバイス (Devices) ]>[NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule) ]をクリックします。
- c) 次のプロパティを設定します。
- [NAT ルール (NAT Rule) ] = 自動 NAT ルール (Auto NAT Rule) 。
  - [タイプ (Type) ] = スタティック (Static) 。
- d) [インターフェイス オブジェクト (Interface Objects) ] タブで、以下の設定を行います。
- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = outside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = inside。
- e) [変換 (Translation) ] タブで、次の項目を設定します。
- [元の発信元 (Original Source) ] = ftp\_server ネットワーク オブジェクト。

- [変換済みの発信元アドレス (Translated Source Address) ] = ftp\_server\_translated ネットワーク オブジェクト。 >

- f) [詳細 (Advanced) ] タブで、[このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule) ] を選択します。

**Add NAT Rule**

NAT Rule:  ▾

Type:  ▾  Enable

Interface Objects **Translation** PAT Pool Advanced

**Original Packet**

Original Source:\*  ▾ +

Original Port:  ▾

**Translated Packet**

Translated Source:

- g) [OK] をクリックします。







## 第 **XIV** 部

### **7000 および 8000 シリーズの高度な導入オプション**

- [仮想スイッチのセットアップ \(1221 ページ\)](#)
- [仮想ルータのセットアップ \(1233 ページ\)](#)
- [集約インターフェイスと LACP \(1273 ページ\)](#)
- [ハイブリッドインターフェイス \(1291 ページ\)](#)
- [ゲートウェイ VPN \(1297 ページ\)](#)





## 第 48 章

# 仮想スイッチのセットアップ

以下のトピックでは、Firepower システムで仮想スイッチをセットアップする方法について説明します。

- [仮想スイッチ \(1221 ページ\)](#)
- [スイッチドインターフェイスの設定 \(1222 ページ\)](#)
- [仮想スイッチの設定 \(1227 ページ\)](#)

## 仮想スイッチ

レイヤ 2 展開の 7000 または 8000 シリーズ デバイスは、2 つ以上のネットワーク間でパケットスイッチングを提供するように設定できます。レイヤ 2 展開では、仮想スイッチをスタンドアロンブロードキャスト ドメインとして機能させ、ネットワークを論理セグメントに分割するように設定できます。仮想スイッチでは、ホストからの Media Access Control (MAC) アドレスを使用して、パケットの送信先を判断します。

仮想スイッチを設定すると、スイッチはまず、スイッチ上の使用可能なすべてのポートからパケットをブロードキャストします。時間の経過とともに、スイッチはタグ付きのリターントラフィックを使用して、各ポートに接続されたネットワーク上に存在する各ホストを学習していきます。

仮想スイッチには、トラフィックを処理するためのスイッチドインターフェイスが 2 つ以上含まれている必要があります。仮想スイッチごとに、トラフィックはスイッチドインターフェイスとして設定されたポートのセットに限定されてきます。たとえば、4 つのスイッチドインターフェイスのある仮想スイッチを設定した場合、ブロードキャスト用の 1 つのポートを介して送入されたパケットは、そのスイッチ上の残る 3 つのポートからのみ送付可能です。

物理スイッチドインターフェイスを設定する際は、仮想スイッチにそれを割り当てる必要があります。また、必要に応じて、物理ポート上に追加の論理スイッチドインターフェイスを定義することもできます。複数の物理インターフェイスを Link Aggregation Group (LAG) と呼ばれる単一の論理スイッチドインターフェイスにグループ化できます。この単一の集約論理リンクによって、帯域幅と冗長性の向上と、2 つのエンドポイント間でのロードバランシングが実現されます。



**注意** レイヤ2展開に何らかの理由で障害が発生した場合、デバイスはトラフィックを転送しなくなります。

## スイッチドインターフェイスの設定

物理設定または論理設定を備えるよう、スイッチ型インターフェイスをセットアップできます。タグなし VLAN トラフィックを処理するよう物理スイッチ型インターフェイスを設定できます。また、VLAN タグが指定されたトラフィックを処理するよう論理スイッチ型インターフェイスを作成することもできます。

レイヤ2展開では、外部の物理インターフェイス上でトラフィックを受信した場合、それを待機しているスイッチ型インターフェイスがなければ、システムはそのトラフィックをドロップします。システムが VLAN タグなしの packets を受信した場合、該当するポートに物理スイッチドインターフェイスが設定されていない場合は、パケットはドロップされます。システムが VLAN タグ付きの packets を受信した場合、論理スイッチドインターフェイスが設定されていない場合は、同じくパケットはドロップされます。

スイッチドインターフェイスで VLAN タグ付きで受信されたトラフィックをシステムが処理するときには、ルールの評価や転送の決定を行う前に、入力における最も外側の VLAN タグを取り除きます。VLAN タグ付き論理スイッチ型インターフェイスを介してデバイスから出るパケットは、出力において関連する VLAN タグ付きでカプセル化されます。

親の物理インターフェイスをインラインまたはパッシブに変更すると、システムは関連するすべての論理インターフェイスを削除することに注意してください。

## スイッチ型インターフェイスの設定メモ

管理対象デバイス上の1つ以上の物理ポートはスイッチ型インターフェイスとして設定できます。トラフィックを処理できるようにするには、その前に、物理スイッチ型インターフェイスを仮想スイッチに割り当てる必要があります。リンク モード設定および MDI/MDIX 設定は、銅線インターフェイスにのみ設定できます。



(注) 8000 シリーズアプライアンスのインターフェイスは、半二重オプションをサポートしません。

物理スイッチ型インターフェイスごとに、複数の論理スイッチ型インターフェイスを追加できます。物理インターフェイスで受信した VLAN タグ付きのトラフィックは、各論理インターフェイスにその特定のタグが関連付けられていなければ処理されません。トラフィックを処理するには、論理スイッチ型インターフェイスを仮想スイッチに割り当てる必要があります。


スイッチ型インターフェイスを設定する場合、設定可能な MTU の範囲は、Firepower システムのデバイスのモデルとインターフェイスのタイプによって異なる可能性があります。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。



#### 注意

デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

既存の論理スイッチ型インターフェイスを編集するには、インターフェイスの横にある編集アイコン () をクリックします。

論理スイッチ型インターフェイスを削除すると、それが存在する物理インターフェイスから、および関連付けられている仮想スイッチとセキュリティゾーンからそれが削除されます。

#### 関連トピック



[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 \(584 ページ\)](#)

[Snort® の再起動シナリオ \(354 ページ\)](#)

## 物理スイッチドインターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

#### 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2** スイッチドインターフェイスを設定するデバイスの横にある編集アイコン () をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** スイッチドインターフェイスとして設定するインターフェイスの横にある編集アイコン () をクリックします。
- ステップ 4** [スイッチド (Switched) ] タブをクリックします。
- ステップ 5** セキュリティゾーンをスイッチドインターフェイスに関連付けるには、次のいずれかを実行します。

- [セキュリティゾーン (Security Zone) ] ドロップダウン リストから既存のセキュリティゾーンを選択します。
- [新規 (New) ] を選択して、新しいセキュリティゾーンを追加します。 [セキュリティゾーンおよびインターフェイスグループオブジェクトの作成 \(438 ページ\)](#) を参照してください。

**ステップ 6** 仮想スイッチをスイッチドインターフェイスに関連付けるには、次のいずれかを実行します。

- [仮想スイッチ (Virtual Switch) ] ドロップダウン リストから既存の仮想スイッチを選択します。
- [新規 (New) ] を選択して、新しい仮想スイッチを追加します。 [仮想スイッチの追加 \(1228 ページ\)](#) を参照してください。

**ステップ 7** [有効化 (Enabled) ] チェックボックスをオンにして、スイッチドインターフェイスがトラフィックを処理することを許可します。

(注) このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

**ステップ 8** [モード (Mode) ] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [自動ネゴシエーション (Auto Negotiation) ] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。

モード設定は銅線インターフェイスにのみ使用できます。

8000 シリーズアプライアンスのインターフェイスは、半二重オプションをサポートしません。

**ステップ 9** [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI (メディア依存型インターフェイス) 、 MDIX (メディア依存型インターフェイスクロスオーバー) 、または自動 MDIX のいずれかを指定するオプションを選択します。

デフォルトでは、[MDI/MDIX] は [自動 MDIX (Auto-MDIX) ] に設定され、MDI と MDIX の間の切り替えを自動的に処理してリンクを確立します。

**ステップ 10** [MTU] フィールドに、最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを入力します。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

**注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

**ステップ 11** [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

- [7000 および 8000 シリーズ デバイス および NGIPSv の MTU 範囲 \(584 ページ\)](#)
- [Snort® の再起動シナリオ \(354 ページ\)](#)

## 論理スイッチドインターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

#### 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。

**ステップ 2** スイッチドインターフェイスを追加するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [インターフェイスの追加 (Add Interface) ] をクリックします。

**ステップ 4** [スイッチド (Switched) ] をクリックします。

**ステップ 5** [インターフェイス (Interface) ] ドロップダウンリストから、VLAN タグ付きトラフィックを受信する物理インターフェイスを選択します。

**ステップ 6** [VLAN タグ (VLAN Tag) ] フィールドで、このインターフェイス上のインバウンド/アウトバウンドトラフィックに割り当てるタグ値を入力します。

このタグの値には、1 ~ 4094 の任意の整数を指定できます。

**ステップ 7** セキュリティゾーンをスイッチドインターフェイスに関連付けるには、次のいずれかを実行します。

- [セキュリティゾーン (Security Zone) ] ドロップダウンリストから既存のセキュリティゾーンを選択します。
- [新規 (New) ] を選択して、新しいセキュリティゾーンを追加します。[セキュリティゾーンおよびインターフェイスグループオブジェクトの作成 \(438 ページ\)](#) を参照してください。

- ステップ 8** 仮想スイッチをスイッチドインターフェイスに関連付けるには、次のいずれかを実行します。
- [仮想スイッチ (Virtual Switch) ] ドロップダウンリストから既存の仮想スイッチを選択します。
  - [新規 (New) ] を選択して、新しい仮想スイッチを追加します。 [仮想スイッチの追加 \(1228 ページ\)](#) を参照してください。
- ステップ 9** スwitchドインターフェイスにトラフィックを処理させるには、[有効 (Enabled) ] チェックボックスをオンにします。
- このチェックボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。物理インターフェイスを無効にする場合、それに関連付けられているすべての論理インターフェイスも無効にします。
- ステップ 10** [MTU] フィールドに、最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。
- MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。
- 注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。
- ステップ 11** [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

- [7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 \(584 ページ\)](#)
- [Snort® の再起動シナリオ \(354 ページ\)](#)

## 論理スイッチドインターフェイスの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin



## 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 削除するスイッチドインターフェイスが含まれる管理対象デバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** 削除する論理スイッチドインターフェイスの横にある削除アイコン (🗑️) をクリックします。

**ステップ 4** 入力を求められた場合、インターフェイスを削除することを確認します。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

# 仮想スイッチの設定

レイヤ 2 展開でスイッチドインターフェイスを使用できるようにするには、その前に仮想スイッチを設定し、スイッチドインターフェイスをその仮想スイッチに割り当てる必要があります。仮想スイッチとは、ネットワークを通過するインバウンドトラフィックとアウトバウンドトラフィックを処理する複数のスイッチドインターフェイスからなるグループのことです。

## 仮想スイッチの設定に関する注意事項

仮想スイッチは、[デバイス管理 (Device Management)] ページの [仮想スイッチ (Virtual Switches)] タブから追加することができます。[仮想スイッチ (Virtual Switches)] タブには、デバイス上で設定済みのすべての仮想スイッチのリストが表示されます。このページには、各スイッチのサマリ情報が表示されます。

表 78: 仮想スイッチ テーブルビューのフィールド

フィールド	説明
[名前 (Name)]	仮想スイッチの名前。
インターフェイス	仮想スイッチに割り当てられたすべてのスイッチ型インターフェイス。[インターフェイス (Interfaces)] タブで無効にしたインターフェイスは表示されません。
ハイブリッドインターフェイス (Hybrid Interface)	仮想スイッチを仮想ルータに結合する、オプション設定のハイブリッドインターフェイス。

フィールド	説明
ユニキャスト パケット (Unicast Packets)	次の項目を含む、仮想スイッチのユニキャスト パケット統計： <ul style="list-style-type: none"> <li>受信されたユニキャスト パケット</li> <li>転送されたユニキャスト パケット (ホストによるドロップを除く)</li> <li>誤ってドロップされたユニキャスト パケット</li> </ul>
ブロードキャスト パケット (Broadcast Packets)	次の項目を含む、仮想スイッチのブロードキャスト パケット統計： <ul style="list-style-type: none"> <li>受信されたブロードキャスト パケット</li> <li>転送されたブロードキャスト パケット</li> <li>誤ってドロップされたブロードキャスト パケット</li> </ul>

また、スイッチ型インターフェイスを設定するときにスイッチを追加することもできます。仮想スイッチには、スイッチ型インターフェイスだけ割り当てることができます。管理対象デバイス上でスイッチ型インターフェイスを設定する前に仮想スイッチを作成する必要がある場合は、空の仮想スイッチを作成し、後でその仮想スイッチにインターフェイスを追加できます。



#### ヒント

既存の仮想スイッチを編集するには、スイッチの横にある編集アイコン (✎) をクリックします。

## 仮想スイッチの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

#### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** 仮想スイッチを追加するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

- ステップ 3** [仮想スイッチ (Virtual Switches) ] タブをクリックします。
- ステップ 4** [仮想スイッチの追加 (Add Virtual Switch) ] をクリックします。
- ステップ 5** [名前 (Name) ] フィールドに名前を入力します。
- ステップ 6** [使用可能 (Available) ] リストから、仮想スイッチに追加される 1 つ以上のスイッチドインターフェイスを選択します。
- ヒント** [インターフェイス (Interfaces) ] タブですでに無効にしたインターフェイスは使用できません。インターフェイスを追加した後で無効にすると、設定からそれが削除されます。
- ステップ 7** [追加 (Add) ] をクリックします。
- ステップ 8** 仮想ルータに仮想スイッチを結びつけるには、[ハイブリッドインターフェイス (Hybrid Interface) ] ドロップダウンリストからハイブリッドインターフェイスを選択します。
- ステップ 9** 必要に応じて、スイッチの詳細設定を行います。以下を参照してください。[仮想スイッチの詳細設定 \(1229 ページ\)](#)
- ステップ 10** [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[論理ハイブリッドインターフェイス \(1291 ページ\)](#)

## 仮想スイッチの詳細設定

### スタティック MAC エントリを追加する (Adding Static MAC Entries)

仮想スイッチは、ネットワークからのリターントラフィックにタグを付けることで、時間の経過と共に MAC アドレスを学習します。手動でスタティック MAC エントリを追加できます。そのようにすることで、MAC アドレスが特定のポート上にあることを指定します。そのポートからトラフィックを受信するかどうかに関わらず、MAC アドレスはテーブル内でスタティックアドレスとして保持されます。仮想スイッチごとに 1 つ以上のスタティック MAC アドレスを指定できます。

### スパニングツリープロトコル (STP) を有効にしてブリッジプロトコルデータユニット (BPDU) をドロップする (Enabling Spanning Tree Protocol (STP) and Dropping Bridge Protocol Data Units (BPDU))

STP は、ネットワークループを防止するために使用されるネットワークプロトコルです。BPDU は、ネットワークを介して交換され、ネットワークブリッジに関する情報を伝送しま

す。ネットワーク内に冗長リンクがある場合、プロトコルはBPDUを使用して最も高速なネットワークリンクを識別し、選択します。ネットワークリンクで障害が発生した場合、スパンニングツリーは既存の代替リンクにフェールオーバーします。



- (注) Cisco では、高可用性ペアで 7000 または 8000 シリーズ デバイスに展開する予定の仮想スイッチを設定する場合は、STP を有効にすることを強く推奨しています。仮想スイッチが複数のネットワーク インターフェイス間のトラフィックを切り替える場合は、STP のみを有効にします。

仮想スイッチが複数の VLAN 間のトラフィックをルーティングする場合、ルータ オン アス ティックと同様に、BPDU はさまざまな論理スイッチ インターフェイスを介してデバイスを出入りますが、物理スイッチ インターフェイスは同じです。その結果、STP はデバイスを冗長ネットワーク ループと見なします。特定のレイヤ 2 展開では、これによって問題が発生する場合があります。それを防ぐため、トラフィックのモニタリング時にデバイスが BPDU をドロップするようにドメイン レベルで仮想スイッチを設定することができます。STP を無効にする場合は、BPDU をドロップするしかありません。



- (注) 仮想スイッチが 1 つの物理 インターフェイス上の VLAN 間でトラフィックをルーティングする場合にのみ、BPDU をドロップしてください。

#### 厳格な TCP 強制を有効にする (Enabling Strict TCP Enforcement)

最大限の TCP セキュリティを実現するため、厳格な強制を有効にすることができます。この機能は、3 ウェイ ハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
- 応答側が SYN-ACK を送信する前に TCP 接続の発信側から送信された非 SYN/RST パケット
- SYN の後、セッションの確立前に TCP 接続のレスポンドから送信された非 SYN-ACK/RST パケット
- イニシエータまたはレスポンドから確立された TCP 接続の SYN パケット

仮想スイッチを論理ハイブリッド インターフェイスに関連付けると、そのスイッチでは、論理ハイブリッド インターフェイスに関連付けられている仮想ルータと同じ厳格な TCP 強制設定が使用されることに注意してください。その場合、スイッチで厳格な TCP 強制を指定することはできません。

## 仮想スイッチの詳細設定の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

### 手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 編集する仮想スイッチが含まれるデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3 [仮想スイッチ (Virtual Switches)] タブをクリックします。
- ステップ 4 編集する仮想スイッチの横にある編集アイコン (✎) をクリックします。
- ステップ 5 [Advanced] タブをクリックします。
- ステップ 6 スタティック MAC エントリを追加するには、[追加 (Add)] をクリックします。
- ステップ 7 [MAC アドレス (MAC Address)] フィールドで、2 桁の 16 進数 6 組をコロンで区切った標準形式を使用して、アドレスを入力します (たとえば 01:23:45:67:89:AB)。  
  
(注) ブロードキャストアドレス (00:00:00:00:00:00 と FF:FF:FF:FF:FF:FF) をスタティック MAC アドレスとして追加することはできません。
- ステップ 8 [インターフェイス (Interface)] ドロップダウンリストから、MAC アドレスを割り当てるインターフェイスを選択します。
- ステップ 9 [OK] をクリックします。
- ステップ 10 スパニング ツリー プロトコルを有効にする場合は、[スパニング ツリー プロトコルを有効にする (Enable Spanning Tree Protocol)] チェックボックスをオンにします。
- ステップ 11 厳密な TCP 強制を有効にするには、[厳密な TCP 強制 (Strict TCP Enforcement)] チェックボックスをオンにします。  
  
仮想スイッチを論理ハイブリッドインターフェイスに関連付けると、このオプションは表示されず、論理ハイブリッドインターフェイスに関連付けられた仮想ルータと同じ設定がスイッチで使用されます。
- ステップ 12 ドメイン レベルで BPDU をドロップするには、[BPDU のドロップ (Drop BPDUs)] チェックボックスをオンにします。
- ステップ 13 [保存 (Save)] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 仮想スイッチの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

仮想スイッチを削除すると、そのスイッチに割り当てられたスイッチドインターフェイスを別のスイッチに含めることができるようになります。

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 削除する仮想スイッチが含まれる管理対象デバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [仮想スイッチ (Virtual Switches)] タブをクリックします。

**ステップ 4** 削除する仮想スイッチの横にある削除アイコン (🗑️) をクリックします。

**ステップ 5** プロンプトが表示されたら、仮想スイッチを削除することを確認します。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。



## 第 49 章

# 仮想ルータのセットアップ

以下のトピックでは、Firepower システムで仮想ルータをセットアップする方法について説明します。

- [仮想ルータ \(1233 ページ\)](#)
- [ルーテッドインターフェイス \(1234 ページ\)](#)
- [物理ルーテッドインターフェイスの設定 \(1235 ページ\)](#)
- [論理ルーテッドインターフェイスの追加 \(1238 ページ\)](#)
- [論理ルーテッドインターフェイスの削除 \(1241 ページ\)](#)
- [SFRP の設定 \(1242 ページ\)](#)
- [仮想ルータ設定 \(1244 ページ\)](#)
- [仮想ルータの追加 \(1245 ページ\)](#)
- [DHCP リレー \(1246 ページ\)](#)
- [スタティック ルート \(1248 ページ\)](#)
- [ダイナミック ルーティング \(1251 ページ\)](#)
- [仮想ルータのフィルタ \(1266 ページ\)](#)
- [仮想ルータ認証プロファイルの追加 \(1269 ページ\)](#)
- [仮想ルータ統計情報の表示 \(1270 ページ\)](#)
- [仮想ルータの削除 \(1271 ページ\)](#)

## 仮想ルータ

レイヤ3展開の管理対象デバイスは、2つ以上のインターフェイス間のトラフィックをルーティングするように設定できます。トラフィックをルーティングするには、IP アドレスを各インターフェイスに割り当ててから、これらのインターフェイスを仮想ルータに割り当てる必要があります。仮想ルータに割り当てるインターフェイスは、物理インターフェイス、論理インターフェイス、または Link Aggregation Group (LAG) インターフェイスのいずれかにできます。

システムは、宛先アドレスに従ってパケット転送の決定を行うことで、パケットをルーティングするように設定できます。ルーテッドインターフェイスとして設定されたインターフェイスは、レイヤ3トラフィックを受信し、転送します。ルータは転送基準に基づいて発信インター

フェイスから宛先を取得し、アクセスコントロールルールが、適用するセキュリティポリシーを指定します。

レイヤ3 展開では、スタティック ルートを定義できます。また、Routing Information Protocol (RIP) および Open Shortest Path First (OSPF) のダイナミック ルーティング プロトコルを設定できます。さらに、スタティック ルートと RIP、またはスタティック ルートと OSPF の組み合わせを設定することもできます。

7000 または 8000 シリーズ デバイス 上には、仮想 ルータ、物理 ルーテッド インターフェイス、または論理 ルーテッド インターフェイス しか 設定 できない ことに 注意 してください。



**注意** レイヤ3 展開に何らかの理由で障害が発生した場合、デバイスはトラフィックを転送しなくなります。

#### 関連トピック

[LAG 設定](#) (1274 ページ)

## ルーテッド インターフェイス

物理的設定または論理的設定のいずれかでルーテッドインターフェイスをセットアップできます。タグのない VLAN トラフィックを処理するために、物理的ルーテッドインターフェイスを設定できます。指定された VLAN タグのあるトラフィックを処理するために、論理的ルーテッドインターフェイスも作成できます。

レイヤ3の展開では、システムは待機しているルーテッドインターフェイスのない外部の物理的インターフェイスから受信したトラフィックをドロップします。このシステムでは、以下の場合パケットをドロップします。

- VLAN タブのないパケットを受信した場合、そのポート向けにルーテッドインターフェイスを設定したことがない場合。
- VLAN タグ付きパケットを受信した場合、そのポートの論理的ルーテッドインターフェイスを設定したことがない場合。

このシステムでは、ルールを評価するか、決定を転送する前にイングレスの最も外側の VLAN タグを削除して、スイッチ インターフェイス 上で VLAN タグで受信したトラフィックを処理します。VLAN タグ付きの論理的ルーテッドインターフェイスを介してデバイスに残っているパケットは、イーグレスの関連付けられた VLAN タブによりカプセル化します。このシステムでは、削除プロセスの完了後、VLAN タブで受信したトラフィックをドロップします。

スタティック Address Resolution Protocol (ARP) エントリをルーテッドインターフェイスに追加できます。外部ホストは、トラフィックの送信先となるローカル ネットワーク 上の宛先 IP アドレスの MAC アドレスを知る必要がある場合は、ARP 要求を送信します。スタティック ARP エントリを設定する場合、仮想ルータは IP アドレスや関連付けられた MAC アドレスに応答します。



論理ルーテッドLAGインターフェイスの [ICMP 有効応答 (ICMP Enable Responses) ] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑制されるわけではありません。宛先 IP がルーテッドインターフェイスの IP で、プロトコルが ICMP であるパケットをドロップするように、アクセス コントロール ポリシーにネットワークベースのルールを追加できます。

管理対象デバイスの [ローカルルータ トラフィックを検査する (Inspect Local Router Traffic) ] オプションを有効にすると、システムは、ホストに到着する前にパケットをドロップし、これによっていかなる応答も阻止できます。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。



#### 注意

デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

上位の物理的インターフェイスをインラインまたはパッシブに変更する場合、システムでは、関連付けられた論理的インターフェイスをすべて削除します。

#### 関連トピック

[デバイスの詳細設定 \(555 ページ\)](#)

[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 \(584 ページ\)](#)

[Snort® の再起動シナリオ \(354 ページ\)](#)

## 物理ルーテッドインターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルーテッドインターフェイスとして管理対象デバイスの 1 つ以上の物理ポートを設定できます。トラフィックをルーティングする前に、物理ルーテッドインターフェイスを仮想ルータに割り当てる必要があります。



**注意** ルーテッドインターフェイス ペアを 7000 または 8000 シリーズ デバイスに追加すると、設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作 \(356ページ\)](#) を参照してください。

## 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2** 変更するデバイスの横にある編集アイコン (✎) をクリックします。
- マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** 変更するインターフェイスの横にある編集アイコン (✎) をクリックします。
- ステップ 4** [ルーテッド (Routed) ] をクリックして、ルーテッドインターフェイス オプションを表示します。
- ステップ 5** セキュリティゾーンを適用するには、次のいずれかを実行します。
- [セキュリティゾーン (Security Zone) ] ドロップダウン リストから既存のセキュリティゾーンを選択します。
  - [新規 (New) ] を選択して、新しいセキュリティゾーンを追加します。[セキュリティゾーンおよびインターフェイスグループオブジェクトの作成 \(438ページ\)](#) を参照してください。
- ステップ 6** 仮想ルータを指定するには、次のいずれかを実行します。
- [仮想ルータ (Virtual Router) ] ドロップダウン リストから既存の仮想ルータを選択します。
  - [新規 (New) ] を選択して、新しい仮想ルータを追加します。[仮想ルータの追加 \(1245ページ\)](#) を参照してください。
- ステップ 7** [有効化 (Enabled) ] チェックボックスをオンにして、ルーテッドインターフェイスがトラフィックを処理することを許可します。このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。
- ステップ 8** [モード (Mode) ] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [自動ネゴシエーション (Auto Negotiation) ] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。
- モード設定は銅線インターフェイスにのみ使用できます。
- 8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

**ステップ 9** [MDI/MDIX] ドロップダウンリストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイスクロスオーバー）、または自動 MDIX のいずれかを指定するオプションを選択します。

通常、[MDI/MDIX] は [自動 MDIX (Auto-MDIX)] に設定します。これにより、MDI と MDIX の間の切り替えが自動的に処理され、リンクが確立されます。

[MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。

**ステップ 10** [MTU] フィールドに、最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。

MTU はレイヤ 2 MTU/MRU であり、レイヤ 3 MTU ではありません。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイスタイプによって異なる場合があります。

**注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

**ステップ 11** [ICMP] の横にある [応答を有効にする (Enable Responses)] チェックボックスをオンにして、インターフェイスを ping や traceroute などの ICMP トラフィックに応答可能にします。

**ステップ 12** [IPv6 NDP] の横にある [ルータ アドバタイズメントの有効化 (Enable Router Advertisement)] チェックボックスをオンにして、インターフェイスがルータアドバタイズメントを送送できるようにします。

**ステップ 13** IP アドレスを追加するには、[追加 (Add)] をクリックします。

**ステップ 14** [アドレス (Address)] フィールドに、ルーテッドインターフェイスの IP アドレスとサブネットマスクを CIDR 表記で入力します。

次の点に注意してください。

- ネットワークおよびブロードキャストアドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネットマスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

**ステップ 15** 組織が IPv6 アドレスを使用している場合、インターフェイスの IP アドレスを自動的に設定するには、[IPv6] フィールドの横の [アドレス自動設定 (Address Autoconfiguration)] チェックボックスをオンにします。

**ステップ 16** [タイプ (Type)] には、[標準 (Normal)] または [SFRP] を選択します。

SFRP オプションの詳細については [SFRP の設定 \(1242 ページ\)](#) を参照してください。

**ステップ 17** [OK] をクリックします。

- IP アドレスを編集するには、編集アイコン (✎) をクリックします。
- IP アドレスを削除するには、削除アイコン (🗑) をクリックします。

(注) IP アドレスを 7000 または 8000 シリーズ デバイスのルーテッドインターフェイスに追加する場合、ハイアベイラビリティ ペア ピアのルーテッドインターフェイスに対応する IP アドレスを追加する必要があります。

**ステップ 18** スタティック ARP エントリを追加するには、[追加 (Add)] をクリックします。

**ステップ 19** [IP アドレス (IP Address)] フィールドに、スタティック ARP エントリの IP アドレスを入力します。

**ステップ 20** [MAC アドレス (MAC Address)] フィールドに、IP アドレスに関連付ける MAC アドレスを入力します。2 桁の 16 進数の 6 個のグループをコロンで区切る標準アドレス形式を使用します (たとえば、01:23:45:67:89:AB)。

**ステップ 21** [OK] をクリックします。

**ヒント** スタティック ARP エントリを編集するには、編集アイコン (✎) をクリックします。  
スタティック ARP エントリを削除するには、削除アイコン (🗑) をクリックします。

**ステップ 22** [保存 (Save)] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

- [7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 \(584 ページ\)](#)
- [Snort® の再起動シナリオ \(354 ページ\)](#)

## 論理ルーテッドインターフェイスの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin


各物理ルーテッドインターフェイスで、複数の論理ルーテッドインターフェイスを追加できます。物理インターフェイスで受信した VLAN タグ付きのトラフィックは、各論理インターフェイスにその特定のタグが関連付けられていなければ処理されません。トラフィックをルー

ティングするには、論理ルーテッドインターフェイスを仮想ルータに割り当てる必要があります。



**注意** 7000 または 8000 シリーズ デバイス 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作 \(356ページ\)](#) を参照してください。でのルーテッドインターフェイス ペアの追加

## 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2** 変更するデバイスの横にある編集アイコン (  ) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** [インターフェイスの追加 (Add Interface) ] をクリックします。
- ステップ 4** [ルーテッド (Routed) ] をクリックして、ルーテッドインターフェイス オプションを表示します。
- ステップ 5** [インターフェイス (Interface) ] ドロップダウン リストから、論理インターフェイスを追加する物理インターフェイスを選択します。
- ステップ 6** [VLAN タグ (VLAN Tag) ] フィールドで、このインターフェイス上のインバウンド/アウトバウンドトラフィックに割り当てるタグ値を入力します。この値には、1 ~ 4094 の任意の整数を指定できます。
- ステップ 7** セキュリティ ゾーンを適用するには、次のいずれかを実行します。
  - [セキュリティゾーン (Security Zone) ] ドロップダウン リストから既存のセキュリティゾーンを選択します。
  - [新規 (New) ] を選択して、新しいセキュリティゾーンを追加します。 [セキュリティゾーンおよびインターフェイスグループオブジェクトの作成 \(438ページ\)](#) を参照してください。
- ステップ 8** 仮想ルータを指定するには、次のいずれかを実行します。
  - [仮想ルータ (Virtual Router) ] ドロップダウン リストから既存の仮想ルータを選択します。
  - [新規 (New) ] を選択して、新しい仮想ルータを追加します。 [仮想ルータの追加 \(1245ページ\)](#) を参照してください。
- ステップ 9** ルーテッドインターフェイスにトラフィックを処理させるには、[有効 (Enabled) ] チェックボックスをオンにします。

このチェックボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。物理インターフェイスを無効にする場合、それに関連付けられているすべての論理インターフェイスも無効にします。

**ステップ 10** [MTU] フィールドに、最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。

MTU はレイヤ 2 MTU/MRU であり、レイヤ 3 MTU ではありません。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

**注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

**ステップ 11** [ICMP] の横にある [応答を有効にする (Enable Responses)] チェックボックスをオンにして、他のルータ、中間デバイス、またはホストに更新またはエラー情報を伝送します。

**ステップ 12** [IPv6 NDP] の横にある [ルータ アドバタイズメントを有効にする (Enable Router Advertisement)] チェックボックスをオンにして、インターフェイスがルータ アドバタイズメントを伝送できるようにします。

**ステップ 13** IP アドレスを追加するには、[追加 (Add)] をクリックします。

**ステップ 14** [アドレス (Address)] フィールドに、IP アドレスを CIDR 表記で入力します。

次の点に注意してください。

- ネットワークおよびブロードキャストアドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

**ステップ 15** IPv6 を使用した環境で、インターフェイスの IP アドレスを自動設定するには、[IPv6] フィールドの横にある [アドレスの自動設定 (Address Autoconfiguration)] チェックボックスを選択します。

**ステップ 16** [タイプ (Type)] には、[普通 (Normal)] または [SFRP] を選択します。

SFRP オプションの詳細については [SFRP の設定 \(1242 ページ\)](#) を参照してください。

**ステップ 17** [OK] をクリックします。

- IP アドレスを編集するには、編集アイコン (✎) をクリックします。
- IP アドレスを削除するには、削除アイコン (🗑) をクリックします。

(注) IP アドレスを 7000 または 8000 シリーズ デバイスの高可用性ペアのルーテッドインターフェイスに追加する場合、高可用性ペアピアのルーテッドインターフェイスに対応する IP アドレスを追加する必要があります。

**ステップ 18** スタティック ARP エントリを追加するには、[追加 (Add)] をクリックします。

**ステップ 19** [IP アドレス (IP Address)] フィールドに、スタティック ARP エントリの IP アドレスを入力します。

**ステップ 20** [MAC アドレス (MAC Address)] フィールドに、IP アドレスに関連付ける MAC アドレスを入力します。2 桁の 16 進数の 6 個のグループをコロンで区切る標準アドレス形式を使用します (たとえば、01:23:45:67:89:AB)。

**ステップ 21** [OK] をクリックします。スタティック ARP エントリが追加されます。

**ヒント** スタティック ARP エントリを編集するには、編集アイコン (✎) をクリックします。スタティック ARP エントリを削除するには、削除アイコン (🗑️) をクリックします。

**ステップ 22** [保存 (Save)] をクリックします。

#### 次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

#### 関連トピック

[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲](#) (584 ページ)  
[Snort® の再起動シナリオ](#) (354 ページ)

## 論理ルーテッドインターフェイスの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

論理ルーテッドインターフェイスを削除すると、帰属する物理インターフェイスのほか、割り当てられた仮想ルータおよびセキュリティゾーンからも削除されます。

#### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 変更するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** 削除する論理ルーテッドインターフェイスの横にある削除アイコン (🗑️) をクリックします。

**ステップ 4** 入力を求められた場合、インターフェイスを削除することを確認します。

#### 次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

## SFRP の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

Cisco 冗長プロトコル (SFRP) を設定して、7000 または 8000 シリーズデバイスのハイアベイラビリティペアまたは個別のデバイスのハイアベイラビリティを得るためのネットワーク冗長性を実現できます。SFRP は IPv4 と IPv6 の両方のアドレスのゲートウェイ冗長性を提供します。ルーテッドインターフェイスおよびハイブリッドインターフェイスの SFRP を設定できます。

インターフェイスが個別のデバイスに設定される場合、同じブロードキャストドメインに存在する必要があります。インターフェイスのうち少なくとも1つをマスターに指定し、同じ数をバックアップとして指定する必要があります。システムは IP アドレスごとに1つのマスターと1つのバックアップのみをサポートします。ネットワーク接続が失われた場合、システムは自動的にバックアップをマスターに昇格し、接続を維持します。

SFRP に設定するオプションは、SFRP インターフェイスグループのすべてのインターフェイスで同じにする必要があります。グループ内の複数の IP アドレスのマスターとバックアップの状態は同じである必要があります。そのため、IP アドレスを追加または編集する場合、そのアドレスに設定する状態はグループ内のすべてのアドレスに適用されます。セキュリティのために、グループ内のインターフェイス間で共有される [グループ ID (Group ID)] と [共有秘密 (Shared Secret)] の値を入力する必要があります。

仮想ルータで SFRP IP アドレスを有効にするには、1つの非 SFRP IP アドレスを設定する必要があります。インターフェイスごとに、非 SFRP アドレスを1つだけ設定する必要があることにご注意ください。

あるグループに含まれる SFRP はすべて一緒にフェールオーバーするので、同じ仮想ルータ上のすべての SFRP は同じ SFRP グループに属する必要があります。さらに、NAT、HA 状態共有、または VPN を使用している場合は、高可用性ペアの各デバイスに HA リンクインターフェ



イスを設定する必要もあります。HA リンク インターフェイスの詳細については、次を参照してください。 [HA リンク インターフェイスの設定 \(580 ページ\)](#)

高可用性ペアの 7000 または 8000 シリーズ デバイスの場合、共有秘密を指定すると、SFRP の IP 設定とともに高可用性ペアのピアにコピーされます。共有秘密は、ピアのデータを認証します。



- (注) 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアのルーティングされたインターフェイスまたはハイブリッドインターフェイスで SFRP IP アドレスがすでに 1 つ構成されている場合、複数の非 SFRP IP アドレスを有効にすることは推奨しません。7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアがスタンバイ モードでフェールオーバーした場合、NAT は実行されません。

#### 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** 変更するデバイスの横にある編集アイコン (✎) をクリックします。
- マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** SFRP を設定するインターフェイスの横にある編集アイコン (✎) をクリックします。
- ステップ 4** SFRP を設定するインターフェイスのタイプ ([ルーテッド (Routed)] または [ハイブリッド (Hybrid)]) を選択します。
- ステップ 5** IP アドレスを追加または編集するときに SFRP を設定できます。[追加 (Add)] をクリックして、IP アドレスを追加します。IP アドレスを編集するには、編集アイコン (✎) をクリックします。
- ステップ 6** [タイプ (Type)] に [SFRP] を選択して SFRP オプションを表示します。
- ステップ 7** [グループ ID (Group ID)] フィールドに、SFRP 用に設定されたマスターまたはバックアップインターフェイスグループを指定する値を入力します。
- ステップ 8** [優先順位 (Priority)] で、[マスター (Master)] または [バックアップ (Backup)] のどちらかを選択して、優先するインターフェイスを指定します。
- 個別のデバイスの場合、1 つのデバイスにマスターへのインターフェイスを 1 個設定し、2 番目のデバイスにバックアップへのインターフェイスを設定する必要があります。
  - 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアの場合、マスターとして 1 個のインターフェイスを設定すると、もう 1 個のインターフェイスは自動的にバックアップになります。
- ステップ 9** [共有秘密 (Shared Secret)] フィールドに、共有秘密を入力します。

[共有秘密 (Shared Secret)] フィールドには、7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペア内のグループに関するデータが自動的に入力されます。

- ステップ 10** [アドバタイズメントの間隔： (Advertisement Interval)] フィールドに、レイヤ 3 トラフィックのルート アドバタイズメントの間隔を入力します。
- ステップ 11** [OK] をクリックします。
- ステップ 12** [保存 (Save)] をクリックします。

### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて \(603 ページ\)](#)

## 仮想ルータ設定



**注意** 7000 または 8000 シリーズ デバイスで仮想ルータを追加した場合設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

レイヤ 3 配置でルーテッドインターフェイスを使用する前に、仮想ルータを設定し、ルーテッドインターフェイスを割り当てる必要があります。仮想ルータは、レイヤ 3 トラフィックをルーティングするルーテッドインターフェイスのグループです。

1つの仮想ルータに割り当てることができるのは、ルーテッドインターフェイスとハイブリッドインターフェイスのみです。

最大限の TCP セキュリティを実現するため、厳格な強制を有効にすることができます。この機能は、3 ウェイ ハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
- 応答側が SYN-ACK を送信する前に TCP 接続の発信側から送信された非 SYN/RST パケット
- SYN の後、セッションの確立前に TCP 接続のレスポンドから送信された非 SYN-ACK/RST パケット
- 発信側または応答側のどちらかから送信された、確立された TCP 接続の SYN パケット

レイヤ3インターフェイスの設定を非レイヤ3インターフェイスに変更したり、仮想ルータからレイヤ3インターフェイスを削除したりすると、ルータは無効な状態になる場合があることに注意してください。たとえば、DHCPv6で使用されている場合、アップストリームとダウンストリームの不一致が生じることがあります。

## 仮想ルータの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

[デバイス管理 (Device Management) ] ページの [仮想ルータ (Virtual Routers) ] タブから仮想ルータを追加できます。ルーテッドインターフェイスを設定するときに、ルータを追加することもできます。

管理対象デバイスのインターフェイスを設定する前に仮想ルータを作成する場合は、空の仮想ルータを作成し、後でインターフェイスを追加できます。



### 注意

7000 または 8000 シリーズデバイスで仮想ルータを追加した場合設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。

**ステップ 2** 変更するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [仮想ルータ (Virtual Routers) ] タブをクリックします。

**ヒント** デバイスが高可用性ペアのスタックにある場合、[選択済みデバイス (Selected Device) ] ドロップダウン リストから、変更するスタックを選択します。

**ステップ 4** [仮想ルータの追加 (Add Virtual Router) ] をクリックします。

**ステップ 5** [名前 (Name) ] フィールドに仮想ルータの名前を入力します。英数字とスペースを使用できます。

**ステップ 6** [IPv6 サポート (IPv6 Support)] チェックボックスをオンまたはオフにして、仮想ルータで IPv6 スタティック ルーティング、OSPFv3 と RIPng を設定します。

**ステップ 7** TCP の厳密な適用をやめるには、[TCP の厳密な適用 (Strict TCP Enforcement)] チェックボックスをオフにします。このオプションは、デフォルトで有効です。

**ステップ 8** [インターフェイス (Interfaces)] の [使用可能 (Available)] リストから 1 つまたは複数のインターフェイスを選択し、[追加 (Add)] をクリックします。

[使用可能 (Available)] リストには、仮想ルータに割り当てることが可能なデバイス上のすべての有効なレイヤ 3 インターフェイス (ルーテッドおよびハイブリッド) が含まれます。

**ヒント** 仮想ルータからルーテッドまたはハイブリッドインターフェイスを削除するには、削除アイコン (🗑️) をクリックします。[インターフェイス (Interfaces)] タブで、設定したインターフェイスを無効にすることによっても削除できます。

**ステップ 9** [保存 (Save)] をクリックします。

---

#### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## DHCP リレー

DHCP はインターネットホストに設定パラメータを提供します。IP アドレスを未取得の DHCP クライアントは、ブロードキャストドメインの外にある DHCP サーバと直接通信できません。DHCP クライアントが DHCP サーバと通信できるようにするには、クライアントがサーバと同じブロードキャストドメイン内にはない状況に対応できるように DHCP リレー インスタンスを設定します。

ユーザは、設定するそれぞれの仮想ルータに対して DHCP リレーを設定できます。デフォルトでは、この機能は無効になっています。DHCPv4 リレーまたは DHCPv6 リレーのどちらかを有効にできます。



---

(注) 同じデバイスで実行中の複数の仮想ルータを介して DHCPv6 リレー チェーンを実行することはできません。

---

## DHCPv4 リレーの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

次の手順は、仮想ルータで DHCPv4 リレーを設定する方法について説明します。

### 手順

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。

**ステップ 2** 変更するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [仮想ルータ (Virtual Routers) ] タブをクリックします。

**ステップ 4** 変更する仮想ルータの横にある編集アイコン (✎) をクリックします。

**ステップ 5** [DHCPv4 (DHCPv6) ] チェックボックスをオンにします。

**ステップ 6** [サーバ (Servers) ] フィールドに、サーバの IP アドレスを入力します。

**ステップ 7** [追加 (Add) ] をクリックします。

最大 4 台の DHCP サーバを追加できます。

**ステップ 8** [最大ホップ (Max Hops) ] フィールドに 1 ~ 255 の最大ホップ カウントを入力します。

**ステップ 9** [保存 (Save) ] をクリックします。

### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## DHCPv6 リレーの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

同じデバイスで実行中の複数の仮想ルータを介して DHCPv6 リレー チェーンを実行することはできません。

## 手順

- 
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2** 変更するデバイスの横にある編集アイコン (✎) をクリックします。
- マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** [仮想ルータ (Virtual Routers)] タブをクリックします。
- ステップ 4** DHCP リレーを設定する仮想ルータの横にある編集アイコン (✎) をクリックします。
- ステップ 5** [DHCPv6] チェックボックスをオンにします。
- ステップ 6** [インターフェイス (Interfaces)] フィールドで、仮想ルータに割り当てられている 1 つ以上のインターフェイスの横にあるチェックボックスをオンにします。
- ヒント** DHCPv6 リレー用に設定されているインターフェイスは、[インターフェイス (Interfaces)] タブから無効にできません。最初に [DHCPv6 リレー インターフェイス (DHCPv6 Relay interfaces)] チェックボックスをオフにして、設定を保存する必要があります。
- ステップ 7** 選択したインターフェイスの横にあるドロップダウンアイコンをクリックし、インターフェイスが DHCP 要求をリレーする方式として、[アップストリーム (Upstream)]、[ダウンストリーム (Downstream)]、または [両方 (Both)] を選択します。
- (注) 少なくとも 1 つのダウンストリーム インターフェイスと 1 つのアップストリーム インターフェイスを含める必要があります。[両方 (Both)] を選択することは、インターフェイスがダウンストリームとアップストリームの両方であることを意味します。
- ステップ 8** [最大ホップ (Max Hops)] フィールドに 1 ~ 255 の最大ホップ カウントを入力します。
- ステップ 9** [保存 (Save)] をクリックします。
- 

## 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

# スタティック ルート

スタティックルーティングにより、ルータを通過するトラフィックの IP アドレスに関するルールを作成することができます。これはネットワークの現在のトポロジに関して他のルータとの通信がないため、仮想ルータのパス選択を設定する最も簡単な方法です。

スタティック ルート テーブルには次の表に示すように、各ルートに関するサマリー情報が含まれます。

表 79:スタティック ルート テーブル ビュー フィールド

フィールド	説明
[有効 (Enabled) ]	このルートが現在有効であるか、無効であるかを示します。
[名前 (Name) ]	スタティック ルートの名前。
[接続先 (Destination) ]	トラフィックがルーティングされる宛先ネットワーク。
タイプ (Type)	このルートに対して実行するアクションを指定します。次のいずれかです。 <ul style="list-style-type: none"> <li>• [IP] : パケットが、隣接ルータのアドレスに転送されることを指定します。</li> <li>• [インターフェイス (Interface) ] : そのインターフェイスを介してトラフィックが直接接続されたネットワーク上のホストにルーティングされるインターフェイスにパケットが転送されることを指定します。</li> <li>• [破棄 (Discard) ] : スタティック ルートでパケットをドロップすることを指定します。</li> </ul>
ゲートウェイ (Gateway)	スタティック ルートのタイプとして IP を選択した場合はターゲット IP アドレス、またはスタティック ルートタイプとしてインターフェイスを選択した場合はインターフェイス。
優先順位 (Preference)	ルート選択を決定します。同じ宛先に対する複数のルートが存在する場合、より高い優先順位のルートが選択されます。

## 静的ルート テーブルの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

## 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 表示するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [仮想ルータ (Virtual Routers)] タブをクリックします。

**ステップ 4** 静的ルートを表示する仮想ルータの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は子孫ドメインに属しているか、設定を変更する権限がありません。

**ステップ 5** [静的 (Static)] タブをクリックします。

## スタティック ルートの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

## 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** スタティック ルートを追加するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [仮想ルータ (Virtual Routers)] タブをクリックします。

**ステップ 4** スタティックルートを追加する仮想ルータの横にある編集アイコン (✎) をクリックします。

**ステップ 5** [静的 (Static)] をクリックして、スタティック ルートのオプションを表示します。

**ステップ 6** [静的ルートの追加 (Add Static Route)] をクリックします。

**ステップ 7** [ルート名 (Route Name)] フィールドに、スタティック ルートの名前を入力します。英数字とスペースを使用できます。

**ステップ 8** [有効 (Enabled)] チェックボックスをオンにして、ルートが現在有効であることを指定します。



**ステップ 9** [優先 (Preference) ] フィールドに、ルート選択を決定するための 1 ~ 65535 の数値を入力します。

(注) 同じ宛先に対する複数のルートが存在する場合、より高い優先順位のルートが使用されます。

**ステップ 10** [タイプ (Type) ] ドロップダウン リストから、設定するスタティック ルートのタイプを選択します。

**ステップ 11** [宛先 (Destination) ] フィールドに、トラフィックがルーティングされる宛先ネットワークの IP アドレスを入力します。

**ステップ 12** [ゲートウェイ (Gateway) ] フィールドでは、次の 2 つの選択肢があります。

- スタティック ルート タイプとして [IP] を選択した場合は、IP アドレスを選択します。
- スタティック ルートタイプとして [インターフェイス (Interface) ] を選択した場合は、ドロップダウン リストから有効なインターフェイスを選択します。

ヒント [インターフェイス (Interfaces) ] タブから無効にしたインターフェイスは使用できません。追加したインターフェイスを無効にすると、設定から削除されます。

**ステップ 13** [OK] をクリックします。

**ステップ 14** [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## ダイナミック ルーティング

ダイナミックつまり適応型のルーティングは、ルーティングプロトコルを使用して、ルートが取るパスをネットワーク条件の変化に応じて変更します。この適応は、できるだけ多くのルートの有効性を維持し、変更に応じて宛先に到達可能とすることを目的としたものです。このため、他のパスを選択できる限り、ネットワークはノードまたはノード間の接続の損失といった障害を「迂回」することができます。ダイナミックルーティングなしでルータを設定することも、Routing Information Protocol (RIP) または Open Shortest Path First (OSPF) のルーティングプロトコルを設定することもできます。

## RIP コンフィギュレーション

Routing Information Protocol (RIP) はホップ カウントを使用してルートを決定する、小規模な IP ネットワーク向けのダイナミック ルーティング プロトコルです。最適なルートは最小数のホップを使用します。RIP で許可されるホップの最大数は 15 です。このホップ制限により、RIP がサポートできるネットワークのサイズも制限されます。

## RIP 設定のインターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

RIP を設定する際、RIP を設定する仮想ルータにすでに含まれているインターフェイスを選択する必要があります。無効になっているインターフェイスを使用することはできません。

### 手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 変更するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3 [仮想ルータ (Virtual Routers)] タブをクリックします。
- ステップ 4 変更する仮想ルータの横にある編集アイコン (✎) をクリックします。
- ステップ 5 [ダイナミックルーティング (Dynamic Routing)] をクリックして、ダイナミックルーティングのオプションを表示します。
- ステップ 6 [RIP] をクリックして、RIP オプションを表示します。
- ステップ 7 [インターフェイス (Interfaces)] の下で、追加アイコン (+) をクリックします。
- ステップ 8 [名前 (Name)] ドロップダウンリストから、RIP を設定するインターフェイスを選択します。  
ヒント [インターフェイス (Interfaces)] タブから無効にしたインターフェイスは使用できません。追加したインターフェイスを無効にすると、設定から削除されます。
- ステップ 9 [メトリック (Metric)] フィールドに、インターフェイスのメトリックを入力します。異なる RIP インスタンスからのルートを使用可能で、すべてが同じ設定である場合、メトリックが最小のルートが優先ルートになります。
- ステップ 10 [モード (Mode)] ドロップダウンリストから、次のいずれかのオプションを選択します。
  - [マルチキャスト (Multicast)] : RIP が指定されたアドレスですべての隣接ルータにルーティングテーブル全体をマルチキャストするデフォルトのモード。
  - [ブロードキャスト (Broadcast)] : マルチキャストモードが可能な場合でも、RIP にブロードキャスト (RIPv1 など) の使用を強制します。
  - [送信なし (Quiet)] : RIP は、このインターフェイスに定期メッセージを送信しません。
  - [リッスンなし (No Listen)] : RIP は、このインターフェイスに送信しますが、リッスンしません。

ステップ 11 [保存 (Save)] をクリックします。

#### 次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

## RIP の認証設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

RIP 認証では、仮想ルータに設定した認証プロファイルの 1 つが使用されます。

#### 手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ (Virtual Routers)] タブをクリックします。

ステップ 4 RIP 認証プロファイルを追加する仮想ルータの横にある編集アイコン (✎) をクリックします。

ステップ 5 [ダイナミック ルーティング (Dynamic Routing)] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [認証 (Authentication)] で、[プロファイル (Profile)] ドロップダウン リストから既存の仮想ルータの認証プロファイルを選択するか、[なし (None)] を選択します。

ステップ 8 [保存 (Save)] をクリックします。

#### 次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

## 高度な RIP の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

プロトコルの動作に影響するさまざまなタイムアウト値およびその他の機能に関していくつかの高度な RIP 設定を構成できます。



**注意** 不正な値に対する高度な RIP 設定を変更すると、ルータが他の RIP ルータと正常に通信することを妨げる場合があります。

## 手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 変更するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3 [仮想ルータ (Virtual Routers)] タブをクリックします。
- ステップ 4 変更する仮想ルータの横にある編集アイコン (✎) をクリックします。
- ステップ 5 [ダイナミック ルーティング (Dynamic Routing)] をクリックして、ダイナミック ルーティングのオプションを表示します。
- ステップ 6 [RIP] をクリックして、RIP オプションを表示します。
- ステップ 7 [優先順位 (Preference)] フィールドに、ルーティング プロトコルの優先度の数値 (高いほど優先される) を入力します。システムはスタティック ルートよりも RIP を使用して学習したルートを優先します。
- ステップ 8 [期間 (Period)] フィールドに、定期的な更新間隔 (秒単位) を入力します。低い数値は高速なコンバージェンスを示しますが、ネットワーク負荷が大きくなります。
- ステップ 9 [タイムアウト時間 (Timeout Time)] フィールドに、到達不能とみなされるまでのルートの存続時間 (秒単位) を指定する数値を入力します。
- ステップ 10 [ガベージ時間 (Garbage Time)] フィールドに、破棄されるまでのルートの存続時間 (秒単位) を指定する数値を入力します。
- ステップ 11 [無限 (Infinity)] フィールドに、コンバージェンスの計算で無限間隔の値を指定する数値を入力します。値が大きいほど、プロトコル コンバージェンスが遅くなります。
- ステップ 12 [実行 (Honor)] ドロップダウンリストから、ルーティング テーブルをダンプする要求がいつ実行されるかを指定する、次のいずれかのオプションを選択します。
  - [常時 (Always)] : 常に要求を実行する

- [ネイバー (Neighbor)] : 直接接続されたネットワーク上のホストから送信された要求のみを実行する
- [なし (Never)] : 要求を実行しない

ステップ 13 [保存 (Save)] をクリックします。

#### 次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

## RIP 設定へのインポート フィルタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルート テーブルに対して RIP からの受け入れまたは拒否を行うルートを指定するために、インポート フィルタを追加できます。インポート フィルタはテーブルに表示される順に適用されます。

インポート フィルタを追加するときは、仮想ルータに設定したフィルタの1つを使用します。



#### ヒント

RIP インポート フィルタを編集するには、編集アイコン (✎) をクリックします。RIP インポート フィルタを削除するには、削除アイコン (🗑️) をクリックします。

#### 始める前に

- [仮想ルータの追加 \(1245 ページ\)](#) の説明に従い、仮想ルータを追加します。
- [仮想ルータのフィルタの設定 \(1268 ページ\)](#) の説明に従い、仮想ルータにフィルタを設定します。

#### 手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

## RIP 設定へのエクスポート フィルタの追加

- ステップ 3** [仮想ルータ (Virtual Routers) ] タブをクリックします。
- ステップ 4** RIP 仮想ルータフィルタを追加する仮想ルータの横にある編集アイコン (✎) をクリックします。
- ステップ 5** [ダイナミック ルーティング (Dynamic Routing) ] をクリックして、ダイナミック ルーティングのオプションを表示します。
- ステップ 6** [RIP] をクリックして、RIP オプションを表示します。
- ステップ 7** [インポート フィルタ (Import Filters) ] の下で、追加アイコン (+) をクリックします。
- ステップ 8** [名前 (Name) ] ドロップダウン リストから、インポート フィルタとして追加するフィルタを選択します。
- ステップ 9** [アクション (Action) ] の横にある [承認 (Accept) ] または [拒否 (Reject) ] を選択します。
- ステップ 10** [OK] をクリックします。

**ヒント** インポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン (▲) または下へ移動するアイコン (▼) をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

- ステップ 11** [保存 (Save) ] をクリックします。

## 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## RIP 設定へのエクスポート フィルタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルート テーブルから RIP に対しての受け入れまたは拒否を行うルートを定義するために、エクスポート フィルタを追加できます。エクスポート フィルタはテーブルに表示される順に適用されます。

エクスポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。

## 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2** 変更するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

- ステップ 3** [仮想ルータ (Virtual Routers) ] タブをクリックします。
- ステップ 4** RIP 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン (✎) をクリックします。
- ステップ 5** [ダイナミック ルーティング (Dynamic Routing) ] をクリックして、ダイナミック ルーティングのオプションを表示します。
- ステップ 6** [RIP] をクリックして、RIP オプションを表示します。
- ステップ 7** [エクスポート フィルタ (Export Filters) ] の下で、追加アイコン (+) をクリックします。
- ステップ 8** [名前 (Name) ] ドロップダウンリストから、エクスポート フィルタとして追加するフィルタを選択します。
- ステップ 9** [アクション (Action) ] の横にある [承認 (Accept) ] または [拒否 (Reject) ] を選択します。
- ステップ 10** [OK] をクリックします。

**ヒント** エクスポートフィルタの順序を変更するには、必要に応じて、上へ移動するアイコン (▲) または下へ移動するアイコン (▼) をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

- ステップ 11** [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## OSPF の設定

Open Shortest Path First (OSPF) は、他のルータから情報を取得し、リンク ステート アドバタイズメントを使用してルートを他のルータにアドバタイズすることで、ルートを動的に定義する適応型ルーティングプロトコルです。ルータは、それ自体と宛先との間のリンクに関する情報を維持し、ルーティングを決定します。OSPF は、各ルーテッドインターフェイスにコストを割り当て、コストが最低のルータを最適であるとみなします。

### OSPF ルーティング エリア

OSPF ネットワークは、管理を簡略化し、トラフィックおよびリソースの使用を最適化するために、ルーティング エリアに構造化つまり分割することができます。エリアは、単純な 10 進数またはよく使用されるオクテットベースのドット付き 10 進数表記のいずれかで表現される 32 ビットの数字により識別されます。

慣習により、エリア ゼロつまり 0.0.0.0 は OSPF ネットワークのコアまたはバックボーン エリアを表します。他のエリアも指定できます。多くの場合、管理者はエリアのメインルータの IP アドレスをエリア ID として選択します。追加の各エリアはバックボーンの OSPF エリアに

直接または仮想接続できる必要があります。そうした接続は、エリア境界ルータ（ABR）と呼ばれる相互接続ルータによって保持されます。ABR は、管轄する各エリアの個々のリンクステートデータベースを管理し、ネットワーク内のすべてのエリアの集約ルートを保守します。

## OSPF エリアの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

### 手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 変更するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3 [仮想ルータ (Virtual Routers)] タブをクリックします。
- ステップ 4 変更する仮想ルータの横にある編集アイコン (✎) をクリックします。
- ステップ 5 [ダイナミック ルーティング (Dynamic Routing)] をクリックして、ダイナミック ルーティングのオプションを表示します。
- ステップ 6 [OSPF] をクリックして、OSPF オプションを表示します。
- ステップ 7 [エリア (Areas)] の下で、追加アイコン (+) をクリックします。
- ステップ 8 [エリア ID (Area Id)] フィールドに、エリアを表す数値を入力します。この値には整数または IPv4 アドレスを指定できます。
- ステップ 9 オプションで、[スタブネット (Stubnet)] チェックボックスをオンにし、エリアが自律システムの外部のルータアドバタイズメントを受信せず、エリア内のルーティングは完全にデフォルトルートに基づくことを指定します。チェックボックスをオフにすると、このエリアはバックボーンエリアになります。それ以外の場合は、非スタブエリアになります。
- ステップ 10 [デフォルト コスト (Default cost)] フィールドに、エリアのデフォルト ルートに関連付けられたコストを入力します。
- ステップ 11 [スタブネット (Stubnets)] の下で、追加アイコン (+) をクリックします。
- ステップ 12 [IP アドレス (IP Address)] フィールドに、IP アドレスを CIDR 表記で入力します。
- ステップ 13 [非表示 (Hidden)] チェックボックスを選択して、スタブネットが非表示であることを示します。  
非表示のスタブネットは別のエリアに伝播されません。
- ステップ 14 [サマリ (Summary)] チェックボックスを選択して、このスタブネットのサブネットワークであるデフォルトのスタブネットが非表示となるように指定します。



- ステップ 15** [スタブコスト (Stub cost) ]フィールドに、このスタブ ネットワークへのルーティングに関連付けられたコストを定義する値を入力します。
- ステップ 16** [OK] をクリックします。
- ステップ 17** ネットワークを追加するには[ネットワーク (Networks) ]の下の追加アイコン (+) をクリックします。
- ステップ 18** [IP アドレス (IP Address) ]フィールドに、ネットワークの IP アドレスを CIDR 表記で入力します。
- ステップ 19** [非表示 (Hidden) ]チェックボックスをオンにして、ネットワークが非表示であることを示します。非表示のネットワークは別のエリアに伝播されません。
- ステップ 20** [OK] をクリックします。
- ステップ 21** [保存 (Save) ] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## OSPF エリア インターフェイス

OSPF 用に仮想ルータに割り当てられたインターフェイスのサブセットを設定できます。次のリストに、各インターフェイスで指定できるオプションを示します。

### インターフェイス

OSPF を設定するインターフェイスを選択します。[インターフェイス (Interfaces) ] タブから無効にしたインターフェイスは使用できません。

### タイプ (Type)

次のオプションから、OSPF インターフェイスのタイプを選択します。

- [ブロードキャスト (Broadcast) ]: ブロードキャストネットワークでは、フラッドイングおよび hello メッセージはマルチキャストを使用し、すべてのネイバーに対して 1 つのパケットで送信されます。このオプションは、ルータがリンク ステート データベースと同期し、ネットワーク リンク ステート アドバタイズメントを発信するように指定します。このネットワークタイプは、物理的なノンブロードキャストマルチプルアクセス (NBMP) ネットワークと適切な IP プレフィクスなしのアンナンバード ネットワークには使用できません。
- [ポイントツーポイント (PtP) (Point-to-Point (PtP)) ]: ポイントツーポイントネットワークでは、2 台のルータのみを接続します。選定は実行されず、ネットワーク リンク ステート アドバタイズメントは発生しないので、より単純かつ高速に確立されます。このネットワークタイプは物理的な PtP インターフェイスだけでなく、PtP リンクとして使用されるブロードキャストネットワークにも役立ちます。このネットワークタイプは物理的な NBMP ネットワークでは使用できません。

- **[ノンブロードキャスト (Non-Broadcast)]** : NBMP ネットワークで、パケットはマルチキャスト機能がないために各ネイバーに別々に送信されます。ブロードキャスト ネットワークと同様に、このオプションはリンク ステート アドバタイズメント伝播で中心的な役割を果たすルータを指定します。このネットワーク タイプはアンナンバードネットワークでは使用できません。
- **[自動検出 (Autodetect)]** : システムは指定されたインターフェイスに基づいて正しいタイプを判別します。

### コスト

インターフェイスの出力コストを指定します。

### Stub

インターフェイスが OSPF トラフィックをリッスンし、独自のトラフィックを送信する必要があるかどうかを指定します。

### [プライオリティ (Priority)]

指定ルータの選定に使用される優先度を示す数値を入力します。多重アクセスネットワークごとに、システムはルータおよびバックアップルータを指定します。これらのルータには、フラiddiingプロセスでの特別な機能があります。優先度を高くすると、この選定での優先順位が上がります。優先度 0 でルータを設定することはできません。

### [ノンブロードキャスト (Nonbroadcast)]

hello パケットが任意の未定義のネイバーに送信されるかどうかを指定します。このスイッチは、任意の NBMA ネットワークでは無視されます。

### 認証

仮想ルータに設定した認証プロファイルの 1 つからこのインターフェイスが使用する OSPF 認証プロファイルを選択するか、または [なし (None)] を選択します。認証プロファイルの設定に関する詳細については、[仮想ルータ認証プロファイルの追加 \(1269 ページ\)](#) を参照してください。

### [Hello 間隔 (Hello Interval)]

hello メッセージの送信間隔 (秒単位) を入力します。

### [ポーリング (Poll)]

NBMA ネットワーク上の一部のネイバーに対する hello メッセージの送信間隔 (秒単位) を入力します。

### [再送間隔 (Retrans Interval)]

確認応答されていないアップデートの再送信間隔 (秒単位) を入力します。

**[再送遅延 (Retrans Delay) ]**

インターフェイス経由でのリンクステート アップデート パケットの送信に要する推定秒数を入力します。

**待ち時間 (Wait Time)**

ルータが選定の開始と隣接関係の構築の間で待機する秒数を入力します。

**[デッド間隔 (Dead Interval) ]**

ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を入力します。この値が定義されている場合、dead カウントから計算された値はオーバーライドされます。

**[無レスポンス カウント (Dead Count) ]**

hello 間隔と乗算されるときに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を指定する、数値を入力します。

OSPF エリア インターフェイスを編集するには、編集アイコン (✎) をクリックします。OSPF エリア インターフェイスを削除するには、削除アイコン (🗑️) をクリックします。[インターフェイス (Interfaces) ] タブで設定されたインターフェイスを無効にすると削除されます。

**OSPF エリア インターフェイスの追加**

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

OSPF 用に仮想ルータに割り当てられたインターフェイスのサブセットを設定できます。

OSPF エリアで使用するインターフェイスは 1 つのみ選択できます。

**手順**

- 
- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2** OSPF インターフェイスを追加するデバイスの横にある編集アイコン (✎) をクリックします。
- マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** [仮想ルータ (Virtual Routers) ] タブをクリックします。

- ステップ 4** OSPF インターフェイスを追加する仮想ルータの横にある編集アイコン (✎) をクリックします。
- ステップ 5** [ダイナミック ルーティング (Dynamic Routing)] をクリックして、ダイナミック ルーティングのオプションを表示します。
- ステップ 6** [OSPF] をクリックして、OSPF オプションを表示します。
- ステップ 7** [エリア (Areas)] の下で、追加アイコン (+) をクリックします。
- ステップ 8** [インターフェイス (Interfaces)] をクリックします。
- ステップ 9** 追加アイコン (+) をクリックします。
- ステップ 10** [OSPF エリア インターフェイス \(1259 ページ\)](#) で説明されているアクションのいずれかを実行します。
- ステップ 11** ネットワークを追加するには[ネットワーク (Networks)] の下の追加アイコン (+) をクリックします。
- ステップ 12** [IP アドレス (IP address)] フィールドに、このインターフェイスから非ブロードキャストネットワークの hello メッセージを受信するネイバーの IP アドレスを入力します。
- ステップ 13** [資格あり (Eligible)] チェックボックスをオンにして、ネイバーがメッセージを受け取る資格があることを示します。
- ステップ 14** [OK] をクリックします。
- ヒント** ネイバーを編集するには、編集アイコン (✎) をクリックします。ネイバーを削除するには、削除アイコン (🗑) をクリックします。
- ステップ 15** [OK] をクリックします。
- ステップ 16** [保存 (Save)] をクリックします。
- ステップ 17** [保存 (Save)] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## OSPF エリア vlink の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

OSPF 自律システムのすべてのエリアは、物理的にバックボーンエリアと接続されている必要があります。この物理接続が不可能である場合は、vlink を使用して、非バックボーン エリアを経由してバックボーンに接続できます。また vlink を使用して、非バックボーン エリアを経由し、分割されたバックボーンの 2 つの部分を接続することもできます。

vlink を追加するには、最低 2 つの OSPF エリアを追加しておく必要があります。

## 手順

- ステップ 1 [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2 変更するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3 [仮想ルータ (Virtual Routers) ] タブをクリックします。
- ステップ 4 変更する仮想ルータの横にある編集アイコン (✎) をクリックします。
- ステップ 5 [ダイナミック ルーティング (Dynamic Routing) ] をクリックして、ダイナミック ルーティングのオプションを表示します。
- ステップ 6 [OSPF] をクリックして、OSPF オプションを表示します。
- ステップ 7 [エリア (Areas) ] の下で、追加アイコン (+) をクリックします。
- ステップ 8 [Vlinks] をクリックします。
- ステップ 9 追加アイコン (+) をクリックします。
- ステップ 10 [ルータ ID (Router ID) ] フィールドに、ルータの IP アドレスを入力します。
- ステップ 11 [認証 (Authentication) ] ドロップダウンリストから、vlink が使用する認証プロファイルを選択します。
- ステップ 12 [Hello インターバル (Hello Interval) ] フィールドに、hello メッセージの送信間隔 (秒単位) を入力します。
- ステップ 13 [再送信間隔 (Retrans Interval) ] フィールドに、確認応答されていないアップデートの再送信間隔 (秒単位) を入力します。
- ステップ 14 [待機時間 (Wait Time) ] フィールドに、ルータが選定の開始と隣接関係の構築の間で待機する秒数を入力します。
- ステップ 15 [Dead 間隔 (Dead Interval) ] フィールドに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を入力します。この値が定義されている場合、dead カウントから計算された値はオーバーライドされます。
- ステップ 16 [Dead 回数 (Dead Count) ] フィールドに、hello 間隔と乗算されるときに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を指定する、数値を入力します。
- ステップ 17 [OK] をクリックします。
- ステップ 18 [保存 (Save) ] をクリックします。
- ステップ 19 [保存 (Save) ] をクリックします。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## OSPF 設定へのインポート フィルタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルートテーブルに対して OSPF からの受け入れまたは拒否を行うルートを定義するために、インポート フィルタを追加できます。インポート フィルタはテーブルに表示される順に適用されます。

インポート フィルタを追加するときは、仮想ルータに設定したフィルタの1つを使用します。

### 手順

- ステップ 1 [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2 変更するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3 [仮想ルータ (Virtual Routers) ] をクリックします。
- ステップ 4 変更する仮想ルータの横にある編集アイコン (✎) をクリックします。
- ステップ 5 [ダイナミック ルーティング (Dynamic Routing) ] をクリックして、ダイナミック ルーティングのオプションを表示します。
- ステップ 6 [OSPF] をクリックして、OSPF オプションを表示します。
- ステップ 7 [インポート フィルタ (Import Filters) ] の下で、追加アイコン (+) をクリックします。
- ステップ 8 [名前 (Name) ] ドロップダウン リストから、インポート フィルタとして追加するフィルタを選択します。
- ステップ 9 [アクション (Action) ] の横にある [承認 (Accept) ] または [拒否 (Reject) ] を選択します。
- ステップ 10 [OK] をクリックします。  
ヒント インポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン (▲) または下へ移動するアイコン (▼) をクリックします。リスト内でフィルタを上下にドラッグすることもできます。
- ステップ 11 [保存 (Save) ] をクリックします。

### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## OSPF 設定へのエクスポート フィルタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルートテーブルから OSPF に対しての受け入れまたは拒否を行うルートを定義するために、エクスポート フィルタを追加できます。エクスポート フィルタはテーブルに表示される順に適用されます。

エクスポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。

### 手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 変更するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3 [仮想ルータ (Virtual Routers)] タブをクリックします。
- ステップ 4 OSPF 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン (✎) をクリックします。
- ステップ 5 [ダイナミックルーティング (Dynamic Routing)] タブをクリックして、ダイナミックルーティングのオプションを表示します。
- ステップ 6 [OSPF] をクリックして、OSPF オプションを表示します。
- ステップ 7 [エクスポート フィルタ (Export Filters)] の下で、追加アイコン (+) をクリックします。
- ステップ 8 [名前 (Name)] ドロップダウン リストから、エクスポート フィルタとして追加するフィルタを選択します。
- ステップ 9 [アクション (Action)] の横にある [承認 (Accept)] または [拒否 (Reject)] を選択します。
- ステップ 10 [OK] をクリックします。  
ヒント エクスポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン (▲) または下へ移動するアイコン (▼) をクリックします。リスト内でフィルタを上下にドラッグすることもできます。
- ステップ 11 [保存 (Save)] をクリックします。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 仮想ルータのフィルタ

フィルタは、仮想ルータのルートテーブルへのインポートおよびルートのダイナミック プロトコルへのエクスポートを行うために、ルートを照合する方法を提供します。フィルタのリストを作成および管理できます。各フィルタは特定の基準を定義し、静的に定義されるか、またはダイナミック プロトコルから受信したルートを検索します。

仮想ルータ フィルタ テーブルには、仮想ルータに設定した各フィルタのサマリ情報が表示されます（次の表を参照してください）。

表 80: 仮想ルータ フィルタ テーブル ビューのフィールド

フィールド	説明
[名前 (Name) ]	フィルタの名前。
プロトコル	ルートが発生するプロトコル。 <ul style="list-style-type: none"> <li>• [スタティック (Static) ]: ルートはローカルスタティックルートとして発生します。</li> <li>• [RIP]: ルートはダイナミックな RIP 設定から発生します。</li> <li>• [OSPF]: ルートはダイナミックな OSPF 設定から発生します。</li> </ul>
ルータから (From Router)	このフィルタがルートで一致を試みるルータの IP アドレス。スタティックフィルタおよび RIP フィルタに対してこの値を入力する必要があります。
Next Hop (ネクスト ホップ)	このルートを使用するパケットが転送されるネクストホップ。スタティックフィルタおよび RIP フィルタに対してこの値を入力する必要があります。
接続先タイプ (Destination Type)	パケットが送信される宛先のタイプ。 <ul style="list-style-type: none"> <li>• ルータ</li> <li>• Device</li> <li>• 廃棄 (Discard)</li> </ul>



フィールド	説明
宛先ネットワーク (Destination Network)	このフィルタがルートで一致を試みるネットワーク。
OSPF パス タイプ (OSPF Path Type)	OSPF プロトコルにのみ適用されます。パスタイプは次のいずれかです。 <ul style="list-style-type: none"> <li>• Ext-1</li> <li>• Ext-2</li> <li>• エリア間 (Inter Area)</li> <li>• 内部エリア (Intra Area)</li> </ul>
OSPF ルータ ID (OSPF Router ID)	OSPF プロトコルにのみ適用されます。ルート/ネットワークをアドバタイズするルータのルータ ID。

## 仮想ルータ フィルタの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

仮想ルータ エディタの [フィルタ (Filter)] タブには、仮想ルータに設定したすべてのフィルタを含むテーブルが表示されます。テーブルには、各フィルタに関するサマリー情報が含まれています。

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 表示するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** [仮想ルータ (Virtual Routers)] タブをクリックします。



**ステップ 4** フィルタを表示する仮想ルータの横にある編集アイコン (✎) をクリックします。

**ステップ 5** [フィルタ (Filter)] タブをクリックします。

## 仮想ルータのフィルタの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

### 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2** 変更するデバイスの横にある編集アイコン (  ) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** [仮想ルータ (Virtual Routers) ] タブをクリックします。
- ステップ 4** 変更する仮想ルータの横にある編集アイコン (  ) をクリックします。
- ステップ 5** [フィルタ処理 (Filter) ] タブをクリックします。
- ステップ 6** [フィルタの追加 (Add Filter) ] をクリックします。
- ステップ 7** [名前 (Name) ] フィールドにフィルタの名前を入力します。英数字のみを使用できます。
- ステップ 8** [プロトコル (Protocol) ] で、[すべて (All) ] を選択するか、フィルタに適用するプロトコルを選択します。
- ステップ 9** [プロトコル (Protocol) ] として [すべて (All) ]、[スタティック (Static) ]、または [RIP] を選択した場合は、[ルータから (From Router) ] で、このフィルタがルートで一致を試みるルータ IP アドレスを入力します。  
(注) IPv4 アドレスに対する /32 の CIDR ブロックと IPv6 アドレスに対する /128 のプレフィクス長も入力可能です。他のすべてのアドレスブロックは、このフィールドでは無効です。
- ステップ 10** [追加 (Add) ] をクリックします。
- ステップ 11** [プロトコル (Protocol) ] として [すべて (All) ]、[スタティック (Static) ]、または [RIP (RIP) ] を選択した場合は、[ネクストホップ (NextHop) ] で、このフィルタがルートで一致を試みるゲートウェイの IP アドレスを入力します。  
(注) IPv4 アドレスに対する /32 の CIDR ブロックと IPv6 アドレスに対する /128 のプレフィクス長も入力可能です。他のすべてのアドレスブロックは、このフィールドでは無効です。
- ステップ 12** [追加 (Add) ] をクリックします。
- ステップ 13** [送信先のタイプ (Destination Type) ] で、フィルタに適用するオプションを選択します。

- ステップ 14** [宛先ネットワーク (Destination Network) ]で、このフィルタがルートで一致を試みるネットワークの IP アドレスを入力します。
- ステップ 15** [追加 (Add) ]をクリックします。
- ステップ 16** [プロトコル (Protocol) ]として[すべて (All) ]または[OSPF] を選択した場合は、[パスのタイプ (Path Type) ]で、フィルタに適用するオプションを選択します。少なくとも 1 つのパスタイプを選択する必要があります。
- ステップ 17** [プロトコル (Protocol) ]として[OSPF] を選択した場合は、[ルータ ID (Router ID) ]で、ルート/ネットワークをアドバタイズするルータのルータ ID の役割を持つ IP アドレスを入力します。
- ステップ 18** [追加 (Add) ]をクリックします。
- ステップ 19** [OK] をクリックします。
- ステップ 20** [保存 (Save) ]をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 仮想ルータ認証プロファイルの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

RIP および OSPF の設定で使用する認証プロファイルをセットアップできます。簡易パスワードを設定するか、共有暗号キーを指定できます。簡易パスワードでは、すべてのパケットが 8 バイトのパスワードを伝送できます。システムはこのパスワードが欠如している受信パケットを無視します。暗号キーでは検証が可能で、パスワードから生成される 16 バイト長のダイジェストがすべてのパケットに付加されます。

OSPF の場合、各エリアは異なる認証方式を使用できることに注意してください。そのため、多くのエリア間で共有できる認証プロファイルを作成します。OSPFv3 の認証は追加できません。

#### 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ]を選択します。
- ステップ 2** 変更するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

- ステップ 3 [仮想ルータ (Virtual Routers) ] タブをクリックします。
- ステップ 4 変更する仮想ルータの横にある編集アイコン (✎) をクリックします。
- ステップ 5 [認証プロファイル (Authentication Profile) ] をクリックします。
- ステップ 6 [認証プロファイルの追加 (Add Authentication Profile) ] をクリックします。
- ステップ 7 [認証プロファイル名 (Authentication Profile Name) ] フィールドに、認証プロファイルの名前を入力します。
- ステップ 8 [認証タイプ (Authentication Type) ] ドロップダウンリストから、[単純 (simple) ] または [暗号化 (cryptographic) ] を選択します。
- ステップ 9 [パスワード (Password) ] フィールドに、安全なパスワードを入力します。
- ステップ 10 確認のために [パスワードの確認 (Confirm Password) ] フィールドにもう一度パスワードを入力します。
- ステップ 11 [OK] をクリックします。
- ステップ 12 [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## 仮想ルータ統計情報の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

各仮想ルータの実行時統計情報を表示できます。統計情報にはユニキャストパケット、ドロップされたパケット、IPv4 および IPv6 アドレスの個別のルーティングテーブルが表示されます。

#### 手順

- ステップ 1 [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2 統計情報を表示するデバイスの横にある編集アイコン (✎) をクリックします。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ3** [仮想ルータ (Virtual Routers)] タブをクリックします。

**ステップ4** ルータ統計情報を表示する仮想ルータの横にある表示アイコン (🔍) をクリックします。

## 仮想ルータの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

仮想ルータを削除すると、ルータに割り当てられているすべてのルーテッドインターフェイスを他のルータに含めることができますようになります。

### 手順

**ステップ1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ2** 変更するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ3** [仮想ルータ (Virtual Routers)] タブをクリックします。

**ステップ4** 削除する仮想ルータの横にある削除アイコン (🗑️) をクリックします。

**ステップ5** 入力を求められた場合、仮想ルータを削除することを確認します。

### 次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。





## 第 50 章

# 集約インターフェイスと LACP

以下のトピックでは、集約インターフェイスの設定について、および管理対象デバイスで LACP がどのように機能するかについて説明します。

- [集約インターフェイスについて \(1273 ページ\)](#)
- [LAG 設定 \(1274 ページ\)](#)
- [リンク集約制御プロトコル \(LACP\) \(1279 ページ\)](#)
- [集約スイッチドインターフェイスの追加 \(1280 ページ\)](#)
- [集約ルーテッドインターフェイスの追加 \(1283 ページ\)](#)
- [論理集約インターフェイスの追加 \(1287 ページ\)](#)
- [集約インターフェイス統計情報の表示 \(1288 ページ\)](#)
- [集約インターフェイスの削除 \(1289 ページ\)](#)

## 集約インターフェイスについて

Firepower システムでは、管理対象デバイスがレイヤ 2 (ネットワーク間でパケットスイッチングを行う)、またはレイヤ 3 (インターフェイス間でトラフィックをルーティングする) に展開されている場合、複数の物理イーサネットインターフェイスを管理対象デバイス上で 1 つの論理リンクにグループ化できます。このように 1 つに集約された論理リンクは、帯域幅と冗長性の向上および、2 つのエンドポイント間でのロードバランシングを実現します。

集約リンクを作成するには、スイッチドまたはルーテッド Link Aggregation Group (LAG) を作成します。集約グループを作成すると、集約インターフェイスと呼ばれる論理インターフェイスが作成されます。上位層エンティティである LAG は単一の論理リンクに似ており、データトラフィックは集約インターフェイスを介して送信されます。集約リンクは、複数のリンクの帯域幅をまとめて追加することによって帯域幅を増加させます。また、使用可能なすべてのリンクのトラフィックをロードバランシングすることで、冗長性を実現します。リンクの 1 つで障害が発生すると、トラフィックは残りのリンク全体にロードバランシングされます。



LAG のエンドポイントは、7000 または 8000 シリーズ デバイス (上記の図を参照) が 2 つの場合もあれば、一方がサードパーティ アクセス スイッチまたはルータに接続されている 7000

または 8000 シリーズ デバイスの場合もあります。2つのデバイスは一致している必要はありませんが、同じ物理構成で、IEEE 802.ad リンク アグリゲーション標準規格をサポートしている必要があります。LAG の通常の展開では、2つの管理対象デバイス間のアクセス リンクを集約するか、管理対象デバイスとアクセススイッチまたはルータ間にポイントツーポイント接続を確立します。

NGIPsv デバイスや ASA FirePOWER モジュールでは集約インターフェイスを設定することはできません。

## LAG 設定

集約インターフェイスには次の 2 種類があります。

- スイッチド：レイヤ 2 集約インターフェイス
- ルーテッド：レイヤ 3 集約インターフェイス

リンク集約は、リンク集約グループ (LAG) を使用して実装します。LAG を設定するには、集約スイッチドまたはルーテッドインターフェイスを作成して、一連の物理インターフェイスをリンクに関連付けます。すべての物理インターフェイスは同じ速度とメディアでなければなりません。

集約リンクは動的または静的に作成します。動的リンク集約では、IEEE 802.ad リンク集約標準のコンポーネットである Link Aggregation Control Protocol (LACP) が使用されますが、静的リンク集約では使用されません。LACP は、LAG の両端の各デバイスでリンクおよびシステムの情報と交換できるようにして、集約でアクティブに使用するリンクを決定します。静的LAG構成では、手動でリンク集約を維持し、ロード バランシング ポリシーとリンク選択ポリシーを展開する必要があります。

スイッチドまたはルーテッド集約インターフェイスを作成すると、同じタイプのリンク集約グループが自動的に作成され、それに番号が付けられます。たとえば、最初の LAG (スイッチドまたはルーテッド) を作成すると、その集約インターフェイスは、管理対象デバイスの [インターフェイス (Interfaces) ] タブの **lag0** ラベルによって識別できます。物理インターフェイスと論理インターフェイスをこの LAG に関連付けると、それらは階層ツリーメニューのプライマリ LAG の下にネスト表示されます。ただし、スイッチド LAG にはスイッチド物理インターフェイスのみを含めることができ、ルーテッド LAG にはルーテッド物理インターフェイスのみを含めることができます。

LAG を設定する際は、以下の要件を考慮してください。

- Firepower システムは、最大 14 の LAG をサポートし、各 LAG インターフェイスに 0 ~ 13 の一意の ID を割り当てます。LAG ID は設定できません。
- リンクの両側に LAG を設定し、どちらの側のインターフェイスも同じ速度に設定する必要があります。
- 各 LAG ごとに少なくとも 2 つの物理インターフェイスを関連付ける必要があります (最大 8 つ)。物理インターフェイスは複数の LAG に属することはできません。



- LAG の物理インターフェイスは、他の動作モードでインラインまたはパッシブとして使用できず、タグ付きトラフィックの別の論理インターフェイスの一部として使用することもできません。
- LAG の物理インターフェイスは複数の NetMods にまたがることが可能ですが、複数のセンサーにまたがることはできません（すべての物理インターフェイスが同じデバイス上に存在する必要があります）。
- LAG にはスタック構成の NetMod を含めることができません。

## スイッチドインターフェイスの集約

管理対象デバイスの 2～8 つの物理ポートを組み合わせ、スイッチド LAG インターフェイスを作成できます。トラフィックを処理できるようにするには、その前に、スイッチド LAG インターフェイスを仮想スイッチに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイスタイプによって異なる場合があります。



### 注意

デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### 関連トピック

- [7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 \(584 ページ\)](#)
- [Snort® の再起動シナリオ \(354 ページ\)](#)

## ルーテッドインターフェイスの集約

7000 または 8000 シリーズ デバイスの 2～8 つの物理ポートを組み合わせ、ルーテッド LAG インターフェイスを作成できます。トラフィックをルーティングする前に、ルーテッド LAG インターフェイスを仮想ルータに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

ルーテッド LAG インターフェイスにスタティック Address Resolution Protocol (ARP) エントリを追加できます。外部ホストは、トラフィックの送信先となるローカルネットワーク上の宛先 IP アドレスの MAC アドレスを知る必要がある場合は、ARP 要求を送信します。スタティック ARP エントリを設定する場合、仮想ルータは IP アドレスや関連付けられた MAC アドレスに応答します。

ルーテッド LAG インターフェイスの [ICMP 対応の応答数 (ICMP Enable Responses)] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑制されるわけではありません。引き続き、アクセス コントロールルールを使用して、宛先 IP がルーテッドインターフェイスの IP であり、プロトコルが ICMP である接続を処理することができます。[ポートおよび ICMP コードの条件 \(382 ページ\)](#) を参照してください。

[ローカルルータ トラフィックを検査する (Inspect Local Router Traffic)] オプションを有効にすると、パケットはホストに到達する前にドロップされるため、あらゆる応答が抑制されます。ローカルルータ トラフィックの検査の詳細については、[デバイスの詳細設定 \(555 ページ\)](#) を参照してください。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。



#### 注意

デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

#### 関連トピック

[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 \(584 ページ\)](#)

[Snort® の再起動シナリオ \(354 ページ\)](#)

## 論理集約インターフェイス

各スイッチドまたはルーテッド集約インターフェイスごとに、複数の論理スイッチドインターフェイスを追加できます。論理 LAG インターフェイスで受信した VLAN タグ付きトラフィックを処理するには、各論理 LAG インターフェイスをその特定のタグに関連付ける必要があります。物理スイッチドまたはルーテッドインターフェイスに追加するのと同じ方法で、論理インターフェイスをスイッチドまたはルーテッド集約インターフェイスに追加します。



- (注) LAG インターフェイスを作成すると、デフォルトで「タグなし」論理インターフェイスが作成されます。このインターフェイスは **lagn.0** ラベルによって識別されます (**n** は 0 ~ 13 の整数)。動作させるには、各 LAG にこの論理インターフェイスが少なくとも 1 つ必要です。LAG に追加の論理インターフェイスを関連付けて、VLAN タグ付きトラフィックを処理できます。追加する各論理インターフェイスには固有の VLAN タグが必要です。Firepower System は 1 ~ 4094 の VLAN タグをサポートします。

論理ルーテッドインターフェイスには、シスコ冗長プロトコル (SFRP) を設定することもできます。SFRP では、指定した IP アドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。

論理ルーテッド LAG インターフェイスの [ICMP 有効応答 (ICMP Enable Responses) ] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑制されるわけではありません。宛先 IP がルーテッドインターフェイスの IP で、プロトコルが ICMP であるパケットをドロップするように、アクセスコントロールポリシーにネットワークベースのルールを追加できます。

管理対象デバイスの詳細設定である [ローカルルータトラフィックの検閲 (Inspect Local Router Traffic) ] オプションを有効にした場合、パケットはホストに到達する前にドロップされるため、すべての応答を防ぐことができます。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイスタイプによって異なる場合があります。

**注意**

デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィックインスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

**関連トピック**[SFRP](#)[デバイスの詳細設定 \(555 ページ\)](#)[7000 および 8000 シリーズデバイスおよび NGIPSv の MTU 範囲 \(584 ページ\)](#)[Snort® の再起動シナリオ \(354 ページ\)](#)

## ロードバランシングアルゴリズム

LAG バンドルのメンバーリンクへのトラフィックの分散方法を決定する出口ロードバランシングアルゴリズムを LAG に割り当てます。ロードバランシングアルゴリズムは、レイヤ 2 MAC アドレス、レイヤ 3 IP アドレス、レイヤ 4 ポート番号 (TCP/UDP トラフィック) など、さまざまなパケットフィールドの値に基づいてハッシュを決定します。選択したロードバランシングアルゴリズムは、LAG バンドルのメンバーリンクすべてに適用されます。

LAG を設定する場合は、次のオプションから展開シナリオに対応するロードバランシングアルゴリズムを選択します。

- 宛先 IP (Destination IP)
- [宛先 MAC (Destination MAC) ]
- [接続先ポート (Destination Port) ]

- ソース IP
- [送信元 MAC (Source MAC) ]
- 送信元ポート
- [送信元/宛先 IP (Source and Destination IP) ]
- [送信元/宛先 MAC (Source and Destination MAC) ]
- [送信元/宛先ポート (Source and Destination Port) ]



(注) LAG の両端に同じロード バランシング アルゴリズムを設定する必要があります。必要に応じて、上位層のアルゴリズムが下位層のアルゴリズムにバックオフされます (例: ICMP トラフィックに対してレイヤ 3 にバックオフされるレイヤ 4 アルゴリズムなど)。

## リンク セレクション ポリシー

リンク アグリゲーションでは、両方のエンドポイントで各リンクの速度とメディアが同じである必要があります。リンク プロパティを動的に変更できるので、リンク 選択ポリシーは、システムによるリンク 選択プロセスの管理方法を決定する上で役立ちます。最大ポート数を最大化するリンク 選択ポリシーはリンク 冗長性をサポートし、総帯域幅を最大化するリンク 選択ポリシーを全体的なリンク速度をサポートします。安定したリンク 選択ポリシーは、リンク 状態の過剰な変更を最小限に抑えようとしています。



(注) LAG の両端に同じリンク 選択ポリシーを設定する必要があります。

次のオプションから展開シナリオに対応するリンク 選択ポリシーを選択します。

- [最大ポート数 (Highest Port Count) ]: 冗長性を向上させる最大アクティブ ポート数を割り当てするには、このオプションを選択します。
- [最大合計帯域幅 (Highest Total Bandwidth) ]: 集約リンクに最大合計帯域幅を割り当てするには、このオプションを選択します。
- [安定 (Stable) ]: 最大の課題がリンクの安定性と信頼性である場合は、このオプションを選択します。LAG を設定すると、アクティブ リンクは、ポート数や帯域幅が追加された場合ではなく、どうしても必要な場合 (リンク障害などの場合) にのみ変更されます。
- [LACP 優先順位 (LACP Priority) ]: LAG でアクティブにするリンクを LACP アルゴリズムにより決定するには、このオプションを選択します。この設定は、展開目標が未定義の場合や、LAG の一端のデバイスが Firepower Management Center によって管理されていない場合に適しています。

LACPは、動的リンクアグリゲーションをサポートするリンク選択方式の自動化における主要部分です。LACPを有効にすると、LACPの優先度に基づいたリンク選択ポリシーはLACPの次のプロパティを使用します。

#### LACP システム プライオリティ

リンクアグリゲーションにおいて優位なデバイスを判断するには、LACPを実行している各パートナー デバイスにこの値を設定します。値が小さいシステムほど、システム プライオリティが高くなります。動的リンクアグリゲーションでは、最初に、LACPシステム優先順位の高いシステム側でメンバーリンクに選択された状態が設定され、次に、優先順位の低いシステムでメンバーリンクが適宜設定されます。0～65535を指定できます。値を指定しない場合、デフォルトの優先順位は32768になります。

#### LACP リンク優先順位。

集約グループに属する各リンクにこの値を設定します。リンク優先順位によって、LAGにおけるアクティブリンクとスタンバイリンクが決まります。値が小さいリンクほど優先順位が高くなります。アクティブリンクがダウンすると、最も優先順位の高いスタンバイリンクが選択され、ダウンしたリンクと交換されます。ただし、複数のリンクのLACPリンク優先順位が同じである場合は、物理ポート番号が最も小さいリンクがスタンバイリンクとして選択されます。0～65535を指定できます。値を指定しない場合、デフォルトの優先順位は32768になります。

## リンク集約制御プロトコル (LACP)

IEEE 802.3adのコンポーネントであるリンク集約制御プロトコル (LACP) は、LAGバンドルを作成して維持するためにシステムおよびポートの情報を交換する1つの方式です。LACPを有効にすると、LAGの両端の各デバイスはLACPを使用して、集約においてアクティブに使用されているリンクを特定します。LACPは、リンク間でLACPパケット (または制御メッセージ) を交換することによって、アベイラビリティと冗長性を実現します。このプロトコルは、リンクの能力を動的に学習し、他のポートに通知します。LACPは、適合するリンクを特定すると、それらのリンクをLAGにグループ化します。あるリンクで障害が発生した場合、トラフィックは他のリンクで継続されます。リンクを機能させるには、LAGの両端でLACPを有効にする必要があります。

## LACP

LACPを有効にする場合は、LAGの両端で転送モードを指定して、ペアになったデバイス間でのLACPパケットの交換方法を指定する必要があります。LACPモードには次の2つのオプションがあります。

- [アクティブ (Active) ]: デバイスをアクティブネゴシエーションステートにするにはこのモードを選択します。このモードでは、デバイスはLACPパケットを送信することにより、リモートリンクとのネゴシエーションを開始します。

- [パッシブ (Passive) ] : デバイスをパッシブ ネゴシエーション ステートにするにはこのモードを選択します。このモードでは、デバイスは受信した LACP パケットには応答しますが、LACP ネゴシエーションを開始しません。



(注) どちらのモードでも、LACP はリンク間でネゴシエートして、それらのリンクがポート速度などの基準に基づいてリンクバンドルを形成可能かどうかを判定できます。ただし、パッシブ対パッシブの構成は避けるようにしてください。そのような構成では、基本的に LAG の両端がリスニング モードになります。

LACP には、デバイス間での LACP パケットの送信頻度を定義するタイマーがあります。LACP は次のレートでパケットを交換します。

- [低速 (Slow) ] : 30 秒
- [高速 (Fast) ] : 1 秒

このオプションが適用されたデバイスは、LAG の反対側のパートナー デバイスからこの頻度で LACP パケットを受信することを予期します。



(注) LAG がデバイス スタック内の管理対象デバイスに設定されている場合は、プライマリ デバイスだけがパートナー システムとの LACP 通信に参加します。すべてのセカンダリ デバイスは、LACP メッセージをプライマリ デバイスに転送します。プライマリ デバイスは、動的な LAG の変更をセカンダリ デバイスにリレーします。

## 集約スイッチドインターフェイスの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

管理対象デバイスの 2 ~ 8 つの物理ポートを組み合わせ、スイッチド LAG インターフェイスを作成できます。トラフィックを処理できるようにするには、その前に、スイッチド LAG インターフェイスを仮想スイッチに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

### 手順

ステップ 1 [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。

- ステップ 2** スイッチド LAG インターフェイスを設定するデバイスの横にある編集アイコン (✎) をクリックします。
- マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** [追加 (Add)] ドロップダウンメニューから [集約インターフェイスの追加 (Add Aggregate Interface)] を選択します。
- ステップ 4** [スイッチド (Switched)] をクリックして、スイッチド LAG インターフェイスのオプションを表示します。
- ステップ 5** セキュリティゾーンを適用するには、次のいずれかを実行します。
- [セキュリティゾーン (Security Zone)] ドロップダウンリストから既存のセキュリティゾーンを選択します。
  - [新規 (New)] をクリックして新しいセキュリティゾーンを追加します。 [セキュリティゾーンおよびインターフェイスグループオブジェクトの作成 \(438 ページ\)](#) を参照してください。
- ステップ 6** 仮想スイッチを指定します。
- [仮想スイッチ (Virtual Switch)] ドロップダウンリストから既存の仮想スイッチを選択します。
  - [新規 (New)] を選択して新しい仮想スイッチを追加します。 [仮想スイッチの追加 \(1228 ページ\)](#) を参照してください。
- ステップ 7** [有効 (Enabled)] チェックボックスをオンにして、スイッチド LAG インターフェイスがトラフィックを処理できるようにします。
- このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。
- ステップ 8** [モード (Mode)] からリンクモードを指定するオプションを選択するか、または [Autonegotiation] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。
- モード設定は銅線インターフェイスにのみ使用できます。
- 8000 シリーズアプライアンスのインターフェイスは、半二重オプションをサポートしません。リンクが自動的に速度をネゴシエートする場合は、同じ速度設定に基づいて LAG のすべてのアクティブリンクが選択されます。
- ステップ 9** [MDI/MDIX] ドロップダウンリストから、インターフェイスの設定対象として MDI (メディア依存型インターフェイス)、MDIX (メディア依存型インターフェイスクロスオーバー)、または Auto-MDIX のいずれかを指定するオプションを選択します。
- [MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。
- デフォルトでは、MDI/MDIX は自動 MDI に設定され、MDI と MDIX の間のスイッチングを自動的に処理してリンクを確立します。
- ステップ 10** [MTU] フィールドに最大伝送ユニット (MTU) を入力します。

設定可能な MTU の範囲は、Firepower System のデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、[7000 および 8000 シリーズ デバイス および NGIPSv の MTU 範囲 \(584 ページ\)](#) を参照してください。

**ステップ 11** [リンクアグリゲーション (Link Aggregation) ]で、LAG バンドルに追加する物理インターフェイスを [使用できるインターフェイス (Available Interfaces) ]から 1 つまたは複数選択します。

**ヒント** LAG バンドルから物理インターフェイスを削除するには、1 つ以上の物理インターフェイスを選択して、選択項目の削除アイコン (✖) をクリックします。LAG バンドルからすべての物理インターフェイスを削除するには、すべてを削除アイコン (✖) をクリックします。[インターフェイス (Interfaces) ]タブから LAG インターフェイスを削除すると、そのインターフェイスも削除されます。

**ステップ 12** [ロードバランシング アルゴリズム (Load-Balancing Algorithm) ] ドロップダウン リストからオプションを選択します。

**ステップ 13** ドロップダウンリストから [リンク選択ポリシー (Link Selection Policy) ]を選択します。

**ヒント** Firepower System デバイスとサードパーティ製ネットワーク デバイスとの間に集約インターフェイスを設定する場合は、[LACP 優先 (LACP Priority) ]を選択します。

**ステップ 14** [リンク選択ポリシー (Link Selection Policy) ]に [LACP 優先 (LACP Priority) ]を選択した場合は、[システム優先度 (System Priority) ]に値を割り当て、[インターフェイスの優先度の設定 (Configure Interface Priority) ]リンクをクリックして優先度の値を LAG の各インターフェイスに割り当てます。

**ステップ 15** [トンネルレベル (Tunnel Level) ] ドロップダウン リストから [内部 (Inner) ]または [外部 (Outer) ]を選択します。

(注) レイヤ 3 ロードバランシングが設定されている場合、トンネルレベルは IPv 4 トラフィックにのみ適用されます。外部トンネルは常に、レイヤ 2 と IPv6 トラフィックに使用されます。[トンネルレベル (Tunnel Level) ]が明示的に設定されていない場合、デフォルトは [外部 (Outer) ]になります。

**ステップ 16** [LACP] で [有効 (Enabled) ]チェックボックスをオンにして、スイッチド LAG インターフェイスがリンク集約制御プロトコルを使用してトラフィックを処理できるようにします。

このチェックボックスをオフにすると、LAG インターフェイスは静的設定になり、Firepower System は選択されたすべての物理インターフェイスを集約に使用します。

**ステップ 17** [レート (Rate) ] オプション ボタンをクリックし、パートナー デバイスから LACP 制御メッセージを受信する頻度を設定します。

- パケットを 30 秒ごとに受信するには、[遅い (Slow) ]をクリックします。
- パケットを 1 秒ごとに受信するには、[速い (Fast) ]をクリックします。

**ステップ 18** [モード (Mode) ] オプション ボタンをクリックし、デバイスのリスニング モードを設定します。

- パートナー デバイスに LACP パケットを送信してリモートリンクとのネゴシエーションを開始するには、[アクティブ (Active) ]をクリックします。



- 受信した LACP パケットに応答するには、[パッシブ (Passive)] をクリックします。

ステップ 19 [保存 (Save)] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

- [7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 \(584 ページ\)](#)
- [Snort® の再起動シナリオ \(354 ページ\)](#)

## 集約ルーテッドインターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

管理対象デバイスの 2 ~ 8 つの物理ポートを組み合わせ、ルーテッド LAG インターフェイスを作成できます。トラフィックをルーティングする前に、ルーテッド LAG インターフェイスを仮想ルータに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。



**注意** 7000 または 8000 シリーズ デバイス 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。でのルーテッドインターフェイス ペアの追加

#### 手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

ステップ 2 ルーテッド LAG インターフェイスを設定するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

- ステップ 3** [追加 (Add) ] ドロップダウン メニューから [集約インターフェイスの追加 (Add Aggregate Interface) ] を選択します。
- ステップ 4** [Routed] をクリックして、ルーテッド LAG インターフェイス オプションを表示します。
- ステップ 5** セキュリティゾーンを適用するには、次のいずれかを実行します。
- [セキュリティゾーン (Security Zone) ] ドロップダウン リストから既存のセキュリティゾーンを選択します。
  - [新規 (New) ] を選択して新しいセキュリティゾーンを追加します。 [セキュリティゾーンおよびインターフェイス グループ オブジェクトの作成 \(438 ページ\)](#) を参照してください。
- ステップ 6** 仮想ルータを指定します。
- [仮想ルータ (Virtual Router) ] ドロップダウン リストから既存の仮想ルータを選択します。
  - [新規 (New) ] を選択して新しい仮想ルータ [仮想ルータの追加 \(1245 ページ\)](#) を追加します。
- ステップ 7** [有効 (Enabled) ] チェックボックスをオンにして、ルーテッド LAG インターフェイスがトラフィックを処理できるようにします。
- このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。
- ステップ 8** [モード (Mode) ] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [Autonegotiation] を選択して、速度とデュプレックス設定を自動的にネゴシエートするよう LAG インターフェイスを設定します。
- モード設定は銅線インターフェイスにのみ使用できます。
- 8000 シリーズアプライアンスのインターフェイスは、半二重オプションをサポートしません。リンクが自動的に速度をネゴシエートする場合は、同じ速度設定に基づいて LAG のすべてのアクティブリンクが選択されます。
- ステップ 9** [MDI/MDIX] ドロップダウンリストから、インターフェイスの設定対象として MDI (メディア依存型インターフェイス) 、 MDIX (メディア依存型インターフェイスクロスオーバー) 、または Auto-MDIX のいずれかを指定するオプションを選択します。
- [MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。
- デフォルトでは、MDI/MDIX は自動 MDI に設定され、MDI と MDIX の間のスイッチングを自動的に処理してリンクを確立します。
- ステップ 10** [MTU] フィールドに最大伝送ユニット (MTU) を入力します。
- MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

**注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

**ステップ 11** LAG インターフェイスが ping や traceroute のような ICMP トラフィックに応答できるようにするには、[ICMP] の横にある [応答を有効にする (Enable Responses)] チェックボックスをオンにします。

**ステップ 12** LAG インターフェイスがルータアドバタイズメントをブロードキャストできるようにするには、[IPv6 NDP] の横にある [ルータアドバタイズメントを有効にする (Enable Router Advertisement)] チェックボックスをオンにします。

**ステップ 13** [追加 (Add)] をクリックして、IP アドレスを追加します。

**ステップ 14** [アドレス (Address)] フィールドで、CIDR 表記を使用して、ルーテッド LAG インターフェイスの IP アドレスとサブネット マスクを入力します。

次の点に注意してください。

- ネットワークおよびブロードキャストアドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

**ステップ 15** IPv6 を使用した環境で、LAG インターフェイスの IP アドレスを自動設定するには、[IPv6] フィールドの横にある [アドレスの自動設定 (Address Autoconfiguration)] チェックボックスをオンにします。

**ステップ 16** [タイプ (Type)] には、[普通 (Normal)] または [SFRP] を選択します。

**ステップ 17** [タイプ (Type)] に SFRP を選択した場合は、[SFRP](#) の説明に従いオプションを設定してください。

**ステップ 18** [OK] をクリックします。

(注) IP アドレスを 7000 または 8000 シリーズ デバイスの高可用性ペアのルーテッド インターフェイスに追加する場合、高可用性ペアのルーテッドインターフェイスに対応する IP アドレスを追加する必要があります。

**ステップ 19** [追加 (Add)] をクリックして、スタティック ARP エントリを追加します。

**ステップ 20** [IP アドレス (IP Address)] フィールドに IP アドレスを入力します。

**ステップ 21** [MAC アドレス (MAC Address)] フィールドに IP アドレスに関連付ける MAC アドレスを入力します。標準形式を使用します (たとえば、01:23:45:67:89:AB)。

**ステップ 22** [OK] をクリックします。

- ステップ 23** [リンクアグリゲーション (Link Aggregation)] で、LAGバンドルに追加する物理インターフェイスを [使用できるインターフェイス (Available Interfaces)] から 1 つまたは複数選択します。
- ヒント LAG バンドルから物理インターフェイスを削除するには、1 つ以上の物理インターフェイスを選択して、選択項目の削除アイコン (✖) をクリックします。LAG バンドルからすべての物理インターフェイスを削除するには、すべてを削除アイコン (✖) をクリックします。[インターフェイス (Interfaces)] タブから LAG インターフェイスを削除すると、そのインターフェイスも削除されます。
- ステップ 24** ドロップダウンリストから [ロードバランシング アルゴリズム (Load-Balancing Algorithm)] を選択します。
- ステップ 25** ドロップダウンリストから [リンク選択ポリシー (Link Selection Policy)] を選択します。
- ヒント Firepower System デバイスとサードパーティ製ネットワーク デバイスとの間に集約インターフェイスを設定する場合は、[LACP 優先 (LACP Priority)] を選択します。
- ステップ 26** [リンク選択ポリシー (Link Selection Policy)] に [LACP 優先 (LACP Priority)] を選択した場合は、[システム優先度 (System Priority)] に値を割り当て、[インターフェイスの優先度の設定 (Configure Interface Priority)] リンクをクリックして優先度の値を LAG の各インターフェイスに割り当てます。
- ステップ 27** [トンネルレベル (Tunnel Level)] ドロップダウン リストから [内部 (Inner)] または [外部 (Outer)] を選択します。
- (注) レイヤ 3 ロードバランシングが設定されている場合、トンネルレベルは IPv 4 トラフィックにのみ適用されます。外部トンネルは常に、レイヤ 2 と IPv6 トラフィックに使用されます。[トンネルレベル (Tunnel Level)] が明示的に設定されていない場合、デフォルトは [外部 (Outer)] になります。
- ステップ 28** [LACP] で [有効 (Enabled)] チェックボックスをオンにして、ルーテッド LAG インターフェイスがリンク集約制御プロトコルを使用してトラフィックを処理できるようにします。
- このチェックボックスをオフにすると、LAG インターフェイスは静的設定になり、Firepower System はすべての物理インターフェイスを集約に使用します。
- ステップ 29** [レート (Rate)] オプション ボタンをクリックし、パートナー デバイスから LACP 制御メッセージを受信する頻度を設定します。
- パケットを 30 秒ごとに受信するには、[遅い (Slow)] をクリックします。
  - パケットを 1 秒ごとに受信するには、[速い (Fast)] をクリックします。
- ステップ 30** [モード (Mode)] オプション ボタンをクリックし、デバイスのリスニング モードを設定します。
- パートナー デバイスに LACP パケットを送信してリモートリンクとのネゴシエーションを開始するには、[アクティブ (Active)] をクリックします。
  - 受信した LACP パケットに応答するには、[パッシブ (Passive)] をクリックします。

ステップ 31 [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[デバイスの詳細設定 \(555 ページ\)](#)

## 論理集約インターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

各スイッチドまたはルーテッド集約インターフェイスごとに、複数の論理インターフェイスを追加できます。論理 LAG インターフェイスで受信した VLAN タグ付きトラフィックを処理するには、各論理 LAG インターフェイスをその特定のタグに関連付ける必要があります。物理スイッチドまたはルーテッドインターフェイスに追加するのと同じ方法で、論理インターフェイスをスイッチドまたはルーテッド集約インターフェイスに追加します。



- (注) LAG インターフェイスを作成すると、デフォルトで「タグなし」論理インターフェイスが作成されます。このインターフェイスは **lagn.0** ラベルによって識別されます ( $n$  は 0 ~ 13 の整数)。動作させるには、各 LAG にこの論理インターフェイスが少なくとも 1 つ必要です。LAG に追加の論理インターフェイスを関連付けて、VLAN タグ付きトラフィックを処理できます。追加する各論理インターフェイスには固有の VLAN タグが必要です。Firepower System は 1 ~ 4094 の VLAN タグをサポートします。



- 注意 7000 または 8000 シリーズ デバイス 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。でのルーテッドインターフェイス ペアの追加

## 手順

- ステップ1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ2 論理 LAG インターフェイスを追加するデバイスの横にある、編集アイコン (✎) をクリックします。
- マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ3 [追加 (Add)] ドロップダウンメニューから、[論理インターフェイスの追加 (Add Logical Interface)] を選択します。
- ステップ4 [スイッチド (Switched)] をクリックしてスイッチドインターフェイスオプションを表示するか、[ルーテッド (Routed)] をクリックしてルーテッドインターフェイスオプションを表示します。
- ステップ5 [インターフェイス (Interface)] ドロップダウンリストから使用可能な LAG を選択します。集約インターフェイスは **lagn** ラベルによって識別されます ( $n$  は 0 ~ 13 の整数)。
- ステップ6 選択したインターフェイスのタイプに適した残りの設定を行います。
- スwitchド：スイッチドインターフェイスへの論理インターフェイスの追加方法の詳細については、[論理スイッチドインターフェイスの追加 \(1225 ページ\)](#) を参照してください。
  - ルーテッド：ルーテッドインターフェイスへの論理インターフェイスの追加方法の詳細については、[論理ルーテッドインターフェイスの追加 \(1238 ページ\)](#) を参照してください。

## 関連トピック

[SFRP](#)[デバイスの詳細設定 \(555 ページ\)](#)[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 \(584 ページ\)](#)[Snort® の再起動シナリオ \(354 ページ\)](#)

## 集約インターフェイス統計情報の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

各集約インターフェイスのプロトコルおよびトラフィックの統計情報を表示できます。統計情報には、LACP キーとパートナー情報などの LACP プロトコル情報、受信パケット、転送パケット、ドロップパケットが表示されます。統計情報は、メンバーインターフェイスごとに詳細化されており、ポート単位でトラフィックとリンクの情報が表示されます。

集約インターフェイス情報は、事前定義されたウィジェットを介してダッシュボードにも表示されます。[現在のインターフェイス ステータス (Current Interface Status)] ウィジェットは、有効になっているか未使用のアプライアンスのすべてのインターフェイスのステータスを示します。Interface Traffic ウィジェットには、ダッシュボードの時間範囲においてアプライアンスのインターフェイスで送受信された受信 (Rx) トラフィックと送信 (Tx) トラフィックの割合が示されます。[定義済みダッシュボードウィジェット \(251ページ\)](#) を参照してください。

#### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 論理集約インターフェイス統計情報を表示するデバイスの横にある、編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** インターフェイス統計情報を表示するインターフェイスの横にある、表示アイコン (🔍) をクリックします。

## 集約インターフェイスの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

集約インターフェイスは **lagn** ラベルによって識別できます ( $n$  は 0 ~ 13 の整数)。

#### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 集約インターフェイスを削除するデバイスの横にある、編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** 削除する集約インターフェイスの横にある、削除アイコン (🗑️) をクリックします。

**ステップ 4** プロンプトが表示されたら、集約インターフェイスを削除することを確認します。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。





## 第 51 章

# ハイブリッド インターフェイス

次のトピックでは、ローカルハイブリッドインターフェイスの設定方法を示します。

- [ハイブリッドインターフェイスについて \(1291 ページ\)](#)
- [論理ハイブリッドインターフェイス \(1291 ページ\)](#)
- [論理ハイブリッドインターフェイスの追加 \(1292 ページ\)](#)
- [論理ハイブリッドインターフェイスの削除 \(1295 ページ\)](#)

## ハイブリッド インターフェイスについて

管理対象デバイス上に論理ハイブリッドインターフェイスを設定することで、Firepower システムが仮想ルータと仮想スイッチの間でトラフィックをブリッジできるようになります。仮想スイッチのインターフェイスで受信した IP トラフィックの宛先が、そのスイッチに関連付けられた論理ハイブリッドインターフェイスの MAC アドレスとなっている場合、システムは、そのトラフィックをレイヤ3トラフィックとして処理し、宛先 IP アドレスに応じてトラフィックをルーティングするかトラフィックに応答します。それ以外の宛先が設定されたトラフィックを受信した場合、システムはそのトラフィックをレイヤ2トラフィックとして処理し、適切なスイッチングを行います。NGIPSv デバイス上で論理ハイブリッドインターフェイスを設定することはできません。

仮想スイッチと仮想ルータの両方に関連付けられていないハイブリッドインターフェイスは、ルーティングに使用できず、トラフィックを生成することも、トラフィックに応答することもありません。

## 論理ハイブリッド インターフェイス

レイヤ2とレイヤ3の間でトラフィックを中継するには、論理ハイブリッドインターフェイスを仮想ルータと仮想スイッチに関連付ける必要があります。仮想スイッチに関連付けることができるハイブリッドインターフェイスは1つだけです。一方、仮想ルータには複数のハイブリッドインターフェイスを関連付けることができます。

論理ハイブリッドインターフェイスには、シスコ冗長プロトコル (SFRP) を設定することもできます。SFRP では、指定した IP アドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。

ハイブリッドインターフェイスの [ICMP 有効応答 (ICMP Enable Responses) ] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑止されるわけではありません。宛先 IP がハイブリッドインターフェイスの IP で、プロトコルが ICMP であるパケットをドロップするように、アクセス コントロール ポリシーにネットワークベースのルールを追加できます。

管理対象デバイスの [ローカルルータ トラフィックの検閲 (Inspect Local Router Traffic) ] オプションを有効にした場合、パケットはホストに到達する前にドロップされるため、すべての応答を防ぐことができます。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。



#### 注意

デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

#### 関連トピック

[SFRP の設定 \(1242 ページ\)](#)

[デバイスの詳細設定 \(555 ページ\)](#)

[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 \(584 ページ\)](#)

[Snort® の再起動シナリオ \(354 ページ\)](#)


## 論理ハイブリッドインターフェイスの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin



**注意** 7000 または 8000 シリーズ デバイス 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作 \(356ページ\)](#) を参照してください。でのルーテッドインターフェイス ペアの追加

## 手順

- ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。
- ステップ 2** ハイブリッドインターフェイスを追加するデバイスの横にある編集アイコン (  ) をクリックします。
- マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 3** [追加 (Add) ] ドロップダウンメニューから、[論理インターフェイスの追加 (Add Logical Interface) ] を選択します。
- ステップ 4** [ハイブリッド (Hybrid) ] をクリックして、ハイブリッドインターフェイスオプションを表示します。
- ステップ 5** [名前 (Name) ] フィールドに、インターフェイスの名前を入力します。
- ステップ 6** [仮想ルータ (Virtual Router) ] ドロップダウンリストから既存の仮想ルータを選択し、[なし (None) ] を選択するか、または [新規 (New) ] を選択して新しい仮想ルータを追加します。
- (注) 新しい仮想ルータを追加する場合は、ハイブリッドインターフェイスのセットアップが完了した後に、[デバイス管理 (Device Management) ] ページで、その仮想ルータを設定する必要があります。 [仮想ルータの追加 \(1245 ページ\)](#) を参照してください。
- ステップ 7** [仮想スイッチ (Virtual Switch) ] ドロップダウンリストから既存の仮想スイッチを選択し、[なし (None) ] を選択するか、または [新規 (New) ] を選択して新しい仮想スイッチを追加します。
- (注) 新しい仮想スイッチを追加する場合は、ハイブリッドインターフェイスのセットアップが完了した後に、[デバイス管理 (Device Management) ] ページで、その仮想スイッチを設定する必要があります。 [仮想スイッチの追加 \(1228 ページ\)](#) を参照してください。
- ステップ 8** ハイブリッドインターフェイスにトラフィックを処理させるには、[有効 (Enabled) ] チェックボックスをオンにします。
- (注) このチェックボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。

- ステップ 9** [MTU] フィールドに、最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。
- MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。
- 注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。
- ステップ 10** [ICMP] の横にある [応答を有効にする (Enable Responses)] チェックボックスをオンにして、インターフェイスを ping や traceroute などの ICMP トラフィックに応答可能にします。
- ステップ 11** [IPv6 NDP] の横にある [ルータ アドバタイズメントを有効にする (Enable Router Advertisement)] チェックボックスをオンにして、インターフェイスがルータアドバタイズメントを送信できるようにします。このオプションを有効にできるのは、IPv6 アドレスを追加した場合のみです。
- ステップ 12** IP アドレスを追加するには、[追加 (Add)] をクリックします。
- ステップ 13** [アドレス (Address)] フィールドに、IP アドレスとサブネット マスクを入力します。次の点に注意してください。
- ネットワークおよびブロードキャスト アドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
  - サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。
- ステップ 14** IPv6 アドレスがある場合、オプションで、[IPv6] フィールドの横にある [アドレスの自動設定 (Address Autoconfiguration)] チェックボックスをオンにして、インターフェイスの IP アドレスを自動的に設定します。
- ステップ 15** [タイプ (Type)] には、[普通 (Normal)] または [SFRP] を選択します。
- ステップ 16** [タイプ (Type)] に SFRP を選択した場合は、[SFRP](#) の説明に従いオプションを設定してください。
- ステップ 17** [OK] をクリックします。
- ステップ 18** [保存 (Save)] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 \(584 ページ\)](#)

[Snort® の再起動シナリオ](#) (354 ページ)

## 論理ハイブリッドインターフェイスの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

**ステップ 2** 論理ハイブリッドインターフェイスを削除するデバイスの横にある編集アイコン (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 3** 削除する論理ハイブリッドインターフェイスの横にある削除アイコン (🗑️) をクリックします。

**ステップ 4** 入力を求められた場合、インターフェイスを削除することを確認します。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。





## 第 52 章

# ゲートウェイ VPN

次のトピックでは、VPN 展開を管理する方法について説明します。

- [ゲートウェイ VPN の基本 \(1297 ページ\)](#)
- [VPN 展開 \(1299 ページ\)](#)
- [VPN 展開の管理 \(1301 ページ\)](#)
- [VPN 展開のステータス \(1314 ページ\)](#)
- [VPN の統計およびログ \(1315 ページ\)](#)

## ゲートウェイ VPN の基本

バーチャルプライベートネットワーク (VPN) は、インターネットや他のネットワークなどのパブリックソースを介したエンドポイント間でセキュアなトンネルを確立するネットワーク接続です。Firepower 管理対象デバイスの仮想ルータ間にセキュア VPN トンネルを確立するように Firepower システムを設定できます。システムは、インターネットプロトコルセキュリティ (IPsec) プロトコルスイートを使用してトンネルを構築します。

VPN 接続が確立されると、ローカルゲートウェイの背後にあるホストはセキュアな VPN トンネルを介して、リモートゲートウェイの背後にあるホストに接続することができます。接続は、2つのゲートウェイのIPアドレスとホスト名、その背後のサブネット、および相互認証のための2つのゲートウェイの共有秘密で構成されます。

VPN エンドポイントは、Internet Key Exchange (IKE) のバージョン1またはバージョン2のいずれかのプロトコルを使用して相互に認証し、トンネルに対してセキュリティアソシエーションを作成します。システムは IPsec Authentication Header (AH) プロトコルまたは IPsec Encapsulating Security Payload (ESP) プロトコルのいずれかを使用して、トンネルに入るデータを認証します。ESP プロトコルは、AH と同じ機能を提供する他にデータの暗号化も行います。

展開にアクセスコントロールポリシーが存在する場合、システムは、VPN トラフィックがアクセスコントロールを通過するまでVPN トラフィックを送信しません。さらに、システムは、トンネルがダウンしている場合は、トンネルトラフィックをパブリックなソースに送信しません。

VPN を Firepower 用に設定して展開するには、展開先の各管理対象デバイスで VPN ライセンスを有効しておく必要があります。また、VPN 機能は 7000 および 8000 シリーズデバイスでのみ使用できます。

## IPsec

IPsec プロトコルスイートは、VPN トンネルにおいて、IP パケットが ESP または AH セキュリティプロトコルでどのようにハッシュ、暗号化、およびカプセル化されるかを定義します。Firepower システムはハッシュアルゴリズムおよび Security Association (SA) の暗号キーを使用しますが、これは、Internet Key Exchange (IKE) プロトコルによって 2 つのゲートウェイ間で確立されています。

セキュリティアソシエーション (SA) は 2 つのデバイス間で共有のセキュリティ属性を確立し、VPN エンドポイントがセキュアな通信をサポートできるようにします。SA は、2 つの VPN エンドポイントが、VPN トンネルがどのようにセキュアにされているかを表すパラメータを処理することができます。

システムは、IPsec 接続のネゴシエーションの最初の段階で Internet Security Association and Key Management Protocol (ISAKMP) を使用し、エンドポイントと認証キー交換の間で VPN を確立します。IKE プロトコルは ISAKMP 内にあります。

AH セキュリティプロトコルは、パケット見出しとデータを保護しますが、暗号化はできません。ESP はパケットを暗号化および保護しますが、最も外側の IP 見出しをセキュアにすることはできません。多くの場合、この保護は必要なく、大半の VPN 展開は、(暗号化の機能により) AH よりも頻繁に ESP を使用します。VPN はトンネルモードのみで動作するため、システムはレイヤ 3 からのパケット全体を暗号化および認証し、ESP プロトコル内で稼働します。トンネルモードの ESP は、後者の暗号化機能だけでなく、データを暗号化します。

## IKE

Firepower システムは IKE プロトコルを使用して、トンネルに対して SA をネゴシエートする他に、2 つのゲートウェイを相互に認証します。プロセスは、次の 2 つのフェーズで構成されます。

IKE フェーズ 1 では、Diffie-Hellman キー交換によってセキュアに認証された通信チャネルを確立し、その後の IKE 通信を暗号化するために事前共有キーを生成します。このネゴシエーションにより、双方向の ISAKMP セキュリティアソシエーションが生じます。ユーザは、事前共有キーを使用して認証を行うことができます。フェーズ 1 はメインモードで機能します。このフェーズでは、ネゴシエーションの間にすべてのデータを保護しようとはしますが、ピアのアイデンティティも保護します。

IKE フェーズ 2 では、IKE ピアが、フェーズ 1 で確立されたセキュアなチャネルを使用して、IPsec の代わりにセキュリティアソシエーションにネゴシエートします。ネゴシエーションにより、最低 2 つの単方向セキュリティアソシエーション (一方は着信、他方は発信) が生じます。



## VPN 展開

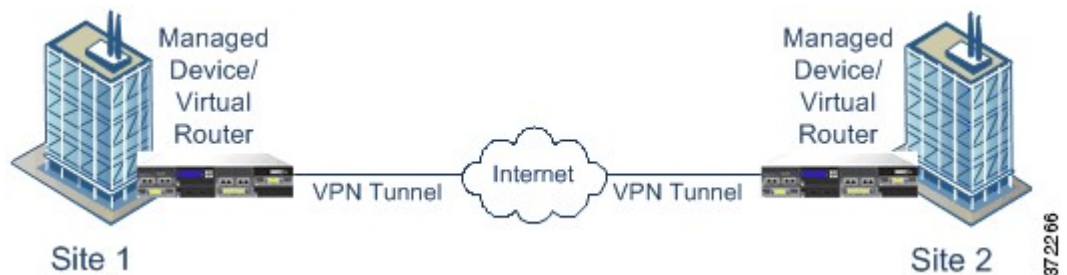
VPN 展開は、VPN に含まれているエンドポイントおよびネットワークを指定し、またそれらが相互にどのように接続しているかを指定します。VPN 展開を Firepower Management Center に設定すると、次に管理対象デバイス、または別の Firepower Management Center によって管理されているデバイスにその VPN 展開を導入できます。

システムでは、ポイントツーポイント、スター、およびメッシュという 3 つのタイプの VPN 展開がサポートされています。

### ポイントツーポイントの VPN 展開

ポイントツーポイントの VPN 展開では、2 つのエンドポイントが相互に直接通信します。2 つのエンドポイントをピアデバイスとして設定し、いずれかのデバイスでセキュアな接続を開始することができます。この設定の各デバイスは、VPN 対応の管理対象デバイスである必要があります。

次の図は、一般的なポイントツーポイントの VPN 展開を示しています。



### スター VPN 導入

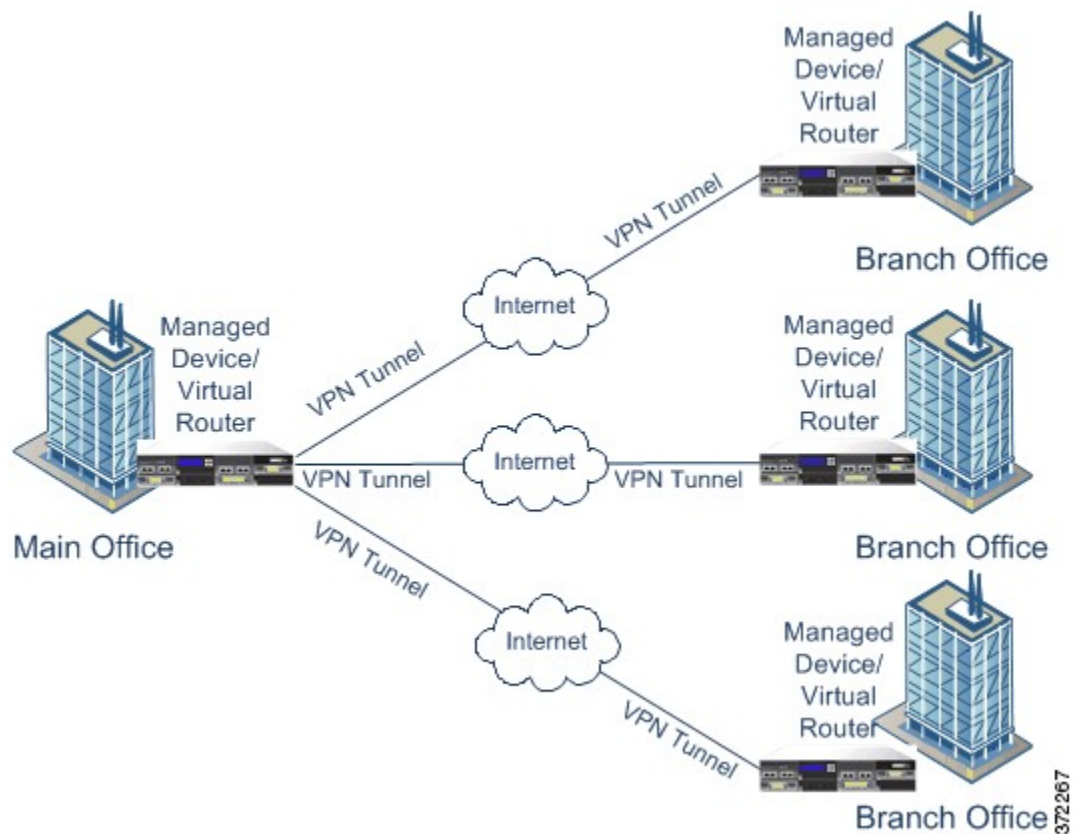
スター VPN 導入では、中央のエンドポイント（ハブ ノード）が、複数のリモートエンドポイント（リーフ ノード）とのセキュアな接続を確立します。ハブ ノードと個々のリーフ ノード間のそれぞれの接続は、別の VPN トンネルです。いずれかのリーフ ノードの背後にあるホストは、ハブ ノードを介して互いに通信できます。

スター型の展開は一般的に、インターネットや他のサードパーティのネットワークを介してセキュアな接続を使用している組織の本店と支店を接続する VPN を表します。スター VPN 導入は、すべての従業員に対して、組織のネットワークへのコントロールされたアクセスを提供します。

一般的なスター型の導入では、ハブ ノードは本社に配置します。リーフ ノードは支社に配置します。トラフィックの大部分は、これらのリーフ ノードから開始されます。各ノードは、VPN 対応の管理対象デバイスである必要があります。

スター型の導入は、IKE バージョン 2 のみをサポートします。

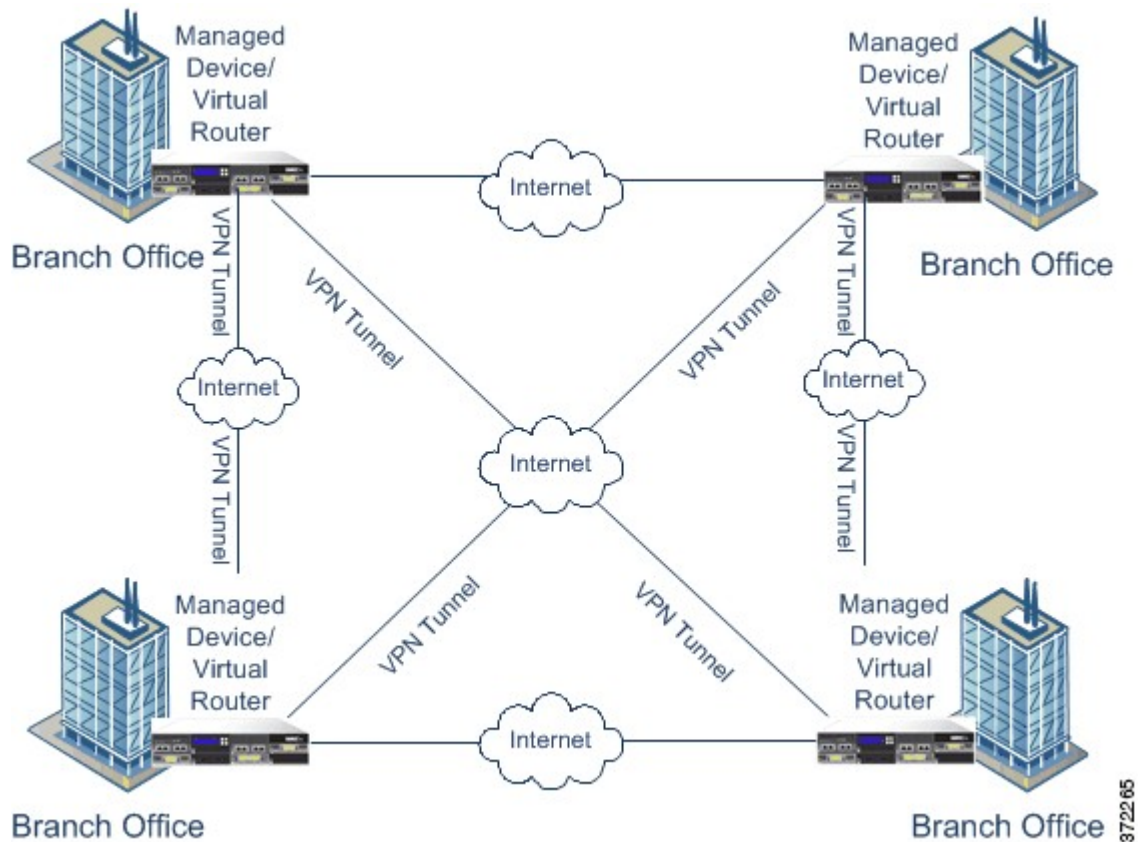
次の図は、一般的なスター VPN 導入を示しています。



## メッシュ VPN 展開

メッシュ VPN 展開では、すべてのエンドポイントが個々の VPN トンネルによって他のエンドポイントと通信できます。メッシュ型の展開では1つのエンドポイントで障害が発生しても残りのエンドポイントが相互に通信できるように、冗長性を備えています。このタイプの展開は一般的に、分散した支店が配置されたグループを接続する VPN を表します。この設定で展開する VPN 対応の管理対象デバイスの数は、必要な冗長性のレベルによって異なります。各エンドポイントは、VPN 対応の管理対象デバイスであることが必要です。

次の図は、一般的なメッシュ VPN 展開を示しています。



372265

## VPN 展開の管理

[VPN] ページ ([**デバイス (Devices)**] > [VPN]) で、現行のすべての VPN 展開を、展開に含まれている名前およびエンドポイントごとに表示することができます。このページ内のオプションを使用して、VPN 展開のステータスを表示する、新しい展開を作成する、管理対象デバイスに展開する、展開を修正または削除する、といった操作を実行することができます。

デバイスを Firepower Management Center に登録すると、登録中に、展開済みの VPN が Firepower Management Center と同期されることに注意してください。

### 関連トピック

[VPN 展開の管理](#) (1308 ページ)

## VPN 展開オプション

新しい VPN 展開を作成する場合には、最小限の処理として、一意の名前と展開のタイプを指定し、事前共有キーを指定する必要があります。次の3つのタイプの展開から選択することができ、それぞれの展開には VPN トンネルが含まれています。

- ポイントツーポイント (PTP) 型の展開は、2つのエンドポイント間で VPN トンネルを確立します。

- スター型の展開は VPN トンネルのグループを確立し、ハブ エンドポイントをリーフ エンドポイントのグループに接続します。
- メッシュ型の展開は、エンドポイントのセット内で VPN トンネルのグループを確立します。

VPN 展開でエンドポイントとして使用できるのは、Cisco の管理対象デバイスのみです。サードパーティ製のエンドポイントはサポートされません。

VPN 認証に対して事前共有キーを定義する必要があります。展開内で生成したすべての VPN 接続で使用するデフォルトのキーを指定できます。ポイントツーポイント型の展開では、各エンドポイントのペアに事前共有キーを指定できます。

マルチドメイン展開では、ドメイン間で VPN 展開を構成できます。つまり、異なるドメインに属するデバイスにエンドポイントを割り当てることができます。このような場合は、関連する子孫ドメインで先祖の展開を表示できますが、変更することはできません。ドリルダウンして展開の詳細を表示すると、現在のドメインに属するデバイスの情報のみが表示されます。

## ポイントツーポイント VPN 展開オプション

ポイントツーポイント VPN 展開を設定する場合は、エンドポイントペアのグループを定義し、各ペアの 2 つのノード間に VPN を作成します。

次に、展開で指定できるオプションについて示します。

### [名前 (Name)]

展開の一意の名前を指定します。

### タイプ (Type)

ポイントツーポイント型の展開を設定するには、[PTP] をクリックします。

### 事前共有キー (Pre-Shared Key)

認証に対して一意の事前共有キーを定義します。各エンドポイントペアに対して事前共有キーを指定しない場合は、システムで展開内のすべての VPN に対してこのキーが使用されます。

### Device

展開のエンドポイントとして、デバイススタックやデバイス高可用性ペアなどの管理対象デバイスを選択できます。使用している Firepower Management Center で管理されていないシスコの管理対象デバイスの場合は、[その他 (Other)] を選択し、エンドポイントの IP アドレスを指定します。

### [仮想ルータ (Virtual Router)]

エンドポイントとして管理対象デバイスを選択する場合は、選択したデバイスに現在適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

### インターフェイス (Interface)

エンドポイントとして管理対象デバイスを選択した場合は、指定した仮想ルータに割り当てられているルーテッドインターフェイスを選択します。

#### [IPアドレス (IP Address) ]

- エンドポイントとして管理対象デバイスを選択する場合は、指定されたルーテッドインターフェイスに割り当てられている IP アドレスを選択します。
- 管理対象デバイスがデバイス高可用性ペアの場合は、SFRP IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスが Firepower Management Center で管理されていない場合は、エンドポイントに IP アドレスを指定します。

#### [保護されたネットワーク (Protected Networks) ]

暗号化された展開でネットワークを指定します。各ネットワークに対して CIDR ブロックでサブネットを入力します。IKE バージョン 1 は、保護された単一のネットワークのみサポートしています。

VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイントペアの保護されたネットワークは重複することはできないことに注意してください。エンドポイントについて保護されたネットワークのリストに 1 つ以上の IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ (IPv4 または IPv6) のエントリを少なくとも 1 つ持っていることが必要です。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です。

(IPv4 については /32 CIDR アドレスを使用し、IPv6 については /128 CIDR アドレスブロックを使用します)。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

#### [内部 IP (Internal IP) ]

エンドポイントが、ネットワークアドレス変換を備えたファイアウォールの背後に配置されている場合は、このチェックボックスをオンにします。

#### [パブリック IP (Public IP) ]

[内部 IP (Internal IP) ] チェックボックスをオンにした場合は、ファイアウォールに対してパブリック IP アドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

#### [パブリック IKE ポート (Public IKE Port) ]

[内部 IP (Internal IP) ] チェックボックスをオンにした場合は、内部のエンドポイントにポート転送されているファイアウォール上の UDP ポートに対して、1 ~ 65535 の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが 500 または 4500 ではない場合、この値を指定する必要があります。

**[実装キーを使用する (Use Deployment Key) ]**

展開に対して定義されている事前共有キーを使用する場合は、チェックボックスをオンにします。このエンドポイント ペアに対して VPN 認証の事前共有キーを指定するには、チェックボックスをオフにします。

**事前共有キー (Pre-Shared Key)**

[実装キーを使用する (Use Deployment Key) ] チェックボックスをオフにした場合は、このフィールドに事前共有キーを指定します。

**関連トピック**

[ポイントツーポイント VPN 展開の設定](#) (1309 ページ)

**スター VPN の展開オプション**

スター VPN 展開を設定する場合は、1つのハブ ノードエンドポイント、およびリーフ ノードエンドポイントのグループを定義します。展開を設定するには、ハブ ノードエンドポイントと、少なくとも1つのリーフ ノードエンドポイントを定義する必要があります。

次に、展開で指定できるオプションについて示します。

**[名前 (Name) ]**

展開の一意の名前を指定します。

**タイプ (Type)**

スター型の展開を設定するには、[スター (Star) ] をクリックします。

**事前共有キー (Pre-Shared Key)**

認証に対して一意の事前共有キーを定義します。

**Device**

展開のエンドポイントとして、デバイススタックやデバイス高可用性ペアなどの管理対象デバイスを選択できます。使用している Firepower Management Center で管理されていないシスコの管理対象デバイスの場合は、[その他 (Other) ] を選択し、エンドポイントの IP アドレスを指定します。

**[仮想ルータ (Virtual Router) ]**

エンドポイントとして管理対象デバイスを選択する場合は、選択したデバイスに現在適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

**インターフェイス (Interface)**

エンドポイントとして管理対象デバイスを選択する場合は、選択した仮想ルータに割り当てられているルーテッドインターフェイスを選択します。

**[IP アドレス (IP Address) ]**

- エンドポイントとして管理対象デバイスを選択する場合は、指定されたルーテッドインターフェイスに割り当てられている IP アドレスを選択します。

- 管理対象デバイスがデバイス高可用性ペアの場合は、SFRP IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスが Firepower Management Center で管理されていない場合は、エンドポイントに IP アドレスを指定します。

#### [保護されたネットワーク (Protected Networks) ]

暗号化された展開でネットワークを指定します。各ネットワークに対して CIDR ブロックでサブネットを入力します。

VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイントペアの保護されたネットワークは重複することはできないことに注意してください。エンドポイントについて保護されたネットワークのリストに 1 つ以上の IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ (IPv4 または IPv6) のエントリを少なくとも 1 つ持っていることが必要です。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です。

(IPv4 については /32 CIDR アドレスを使用し、IPv6 については /128 CIDR アドレスブロックを使用します)。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

#### [内部 IP (Internal IP) ]

エンドポイントが、ネットワークアドレス変換を備えたファイアウォールの背後に配置されている場合は、このチェックボックスをオンにします。

#### [パブリック IP (Public IP) ]

[内部 IP (Internal IP) ] チェックボックスをオンにした場合は、ファイアウォールに対してパブリック IP アドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

#### [パブリック IKE ポート (Public IKE Port) ]

[内部 IP (Internal IP) ] チェックボックスをオンにした場合は、内部のエンドポイントにポート転送されているファイアウォール上の UDP ポートに対して、1 ~ 65535 の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが 500 または 4500 ではない場合、この値を指定する必要があります。

#### 関連トピック

[スター VPN 展開の設定](#) (1310 ページ)

## メッシュ VPN 展開オプション

メッシュ VPN 展開を設定する場合は、VPN のグループを定義して、特定のエンドポイントセットに任意の 2 つのポイントをリンクさせます。

次に、展開で指定できるオプションについて示します。

#### [名前 (Name) ]

展開の一意の名前を指定します。

## タイプ (Type)

メッシュ型の展開を設定するには、[メッシュ (Mesh)] をクリックします。

## 事前共有キー (Pre-Shared Key)

認証に対して一意の事前共有キーを定義します。

## Device

展開のエンドポイントとして、デバイススタックやデバイス高可用性ペアなどの管理対象デバイスを選択できます。使用している Firepower Management Center で管理されていないシスコの管理対象デバイスの場合は、[その他 (Other)] を選択し、エンドポイントの IP アドレスを指定します。

## [仮想ルータ (Virtual Router)]

エンドポイントとして管理対象デバイスを選択した場合は、指定したデバイスに適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

## インターフェイス (Interface)

エンドポイントとして管理対象デバイスを選択した場合は、指定した仮想ルータに割り当てられているルーテッドインターフェイスを選択します。

## [IPアドレス (IP Address)]

- エンドポイントとして管理対象デバイスを選択した場合は、選択したルーテッドインターフェイスに割り当てられている IP アドレスを選択します。
- 管理対象デバイスがデバイス高可用性ペアの場合は、SFRP IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスが Firepower Management Center で管理されていない場合は、エンドポイントに IP アドレスを指定します。

## [保護されたネットワーク (Protected Networks)]

暗号化された展開でネットワークを指定します。各ネットワークに対して CIDR ブロックでサブネットを入力します。IKE バージョン 1 は、保護された単一のネットワークのみサポートしています。

VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイントペアの保護されたネットワークは重複することはできないことに注意してください。エンドポイントについて保護されたネットワークのリストに 1 つ以上の IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ (IPv4 または IPv6) のエントリを少なくとも 1 つ持っていることが必要です。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です。

(IPv4 については /32 CIDR アドレスを使用し、IPv6 については /128 CIDR アドレスブロックを使用します)。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。



### [内部 IP (Internal IP) ]

エンドポイントが、ネットワークアドレス変換を備えたファイアウォールの背後に配置されている場合は、このチェックボックスをオンにします。

### [パブリック IP (Public IP) ]

[内部 IP (Internal IP) ] チェックボックスをオンにした場合は、ファイアウォールに対してパブリック IP アドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

### [パブリック IKE ポート (Public IKE Port) ]

[内部 IP (Internal IP) ] チェックボックスをオンにした場合は、内部のエンドポイントにポート転送されているファイアウォール上の UDP ポートに対して、1～65535 の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが 500 または 4500 ではない場合、この値を指定する必要があります。

### 関連トピック

[メッシュ VPN 展開の設定](#) (1311 ページ)

## VPN 展開の詳細オプション

VPN の展開には、展開の VPN で共有できる共通設定がいくつか含まれています。各 VPN では、デフォルトの設定を使用するか、またはそのデフォルトの設定を上書きすることができます。通常、詳細設定はほとんど、あるいはまったく変更する必要がありません。詳細設定は導入環境ごとに異なります。

次に、展開で指定できる詳細オプションについて説明します。

### 許可されるその他のアルゴリズム (Other Algorithm Allowed)

このチェックボックスをオンにすると、[アルゴリズム (Algorithm) ] リストに含まれていないがリモートピアによって提案されるアルゴリズムについて、自動ネゴシエーションが有効になります。

### アルゴリズム (SNMP (v3) Auth. Alrorphism)

展開でデータのセキュリティを確保するため、フェーズ 1 とフェーズ 2 のアルゴリズムの提案を指定します。両方のフェーズに対して、[暗号 (Cipher) ]、[ハッシュ (Hash) ]、および [Diffie-Hellman (DH) ] グループ認証メッセージを選択します。

### IKE ライフタイム (IKE Life Time)

IKE SA の最大ネゴシエーション間隔について、数値を指定し、時間単位を選択します。最小 15 分、最大 30 日を指定できます。

### IKE v2

システムで IKE バージョン 2 を使用する場合は、このチェックボックスをオンにします。このバージョンでは、スター型の展開と複数の保護ネットワークがサポートされます。

**ライフタイム (Life Time)**

SA の最大ネゴシエーション間隔について、数値を指定し、時間単位を選択します。最小 5 分、最大 24 時間を指定できます。

**ライフ パケット数 (Life Packets)**

有効期限までに IPsec SA を介して伝送できるパケット数を指定します。0 ～ 18446744073709551615 の整数を使用できます。

**ライフ バイト (Life Bytes)**

有効期限までに IPsec SA を介して伝送できるバイト数を指定します。0 ～ 18446744073709551615 の整数を使用できます。

**AH**

保護対象のデータに対して認証ヘッダーセキュリティプロトコルを使用するように指定する場合は、このチェックボックスをオンにします。暗号化サービスペイロード (ESP) プロトコルを使用する場合は、このチェックボックスをオフにします。

**関連トピック**

[高度な VPN 展開を設定する方法 \(1312 ページ\)](#)

## VPN 展開の管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	VPN	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin



**注意** 7000 または 8000 シリーズ デバイス上の VPN を追加または削除して、設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

**手順**

**ステップ 1** [デバイス (Devices) ] > [VPN] を選択します。

**ステップ 2** VPN の展開を管理します。

- 追加：新しい VPN の展開を作成するには、[VPN の追加 (Add VPN) ] > [Firepower デバイス (Firepower Device) ] をクリックして、展開タイプに応じて次の手順を実行します。

- [メッシュ VPN 展開の設定 \(1311 ページ\)](#)
- [ポイントツーポイント VPN 展開の設定 \(1309 ページ\)](#)
- [スター VPN 展開の設定 \(1310 ページ\)](#)
- **編集**：既存の VPN 展開の設定を変更するには、編集アイコン (✎) をクリックします。[VPN 展開の編集 \(1313 ページ\)](#) を参照してください。
- **削除**：VPN 展開を削除するには、削除アイコン (🗑️) をクリックします。
- **展開**：[展開 (Deploy)] をクリックします ([設定変更の導入 \(350 ページ\)](#) を参照)。
- **VPN ステータスの表示**：既存の VPN 展開のステータスを表示するには、ステータスアイコンをクリックします。[VPN ステータスの表示 \(1314 ページ\)](#) を参照してください。

#### 関連トピック

[Snort® の再起動シナリオ \(354 ページ\)](#)

## ポイントツーポイント VPN 展開の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	VPN	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

#### 始める前に

管理対象デバイスをエンドポイントとして使用している場合、仮想ルータを作成し、それを適切なデバイスに適用します。



- (注) 複数のエンドポイントに同じ仮想ルータを使用することはできません。詳細については、次を参照してください。[仮想ルータのセットアップ \(1233 ページ\)](#)

#### 手順

- ステップ 1** [デバイス (Devices)] > [VPN] を選択します。
- ステップ 2** [VPN の追加 (Add VPN)] > [Firepower デバイス (Firepower Device)] をクリックします。
- ステップ 3** 一意の名前を入力します。
- ステップ 4** [タイプ (Type)] として [PTP] が選択されていることを確認します。
- ステップ 5** 一意の事前共有キーを入力します。

- ステップ 6** [ノード ペア (Node Pairs)] の隣の追加アイコン (+) をクリックします。
- ステップ 7** [ポイントツーポイント VPN 展開オプション \(1302 ページ\)](#) で説明されている VPN 展開オプションを設定します。
- ステップ 8** [ノード A (Node A)] の下の [保護されたネットワーク (Protected Networks)] の隣にある追加アイコン (+) をクリックします。
- ステップ 9** 保護されたネットワークの CIDR ブロックを入力します。
- ステップ 10** [OK] をクリックします。
- ステップ 11** [ノード B (Node B)] に対して手順 8 ~ 10 を繰り返します。
- ステップ 12** [保存 (Save)] をクリックします。  
エンドポイント ペアが展開に追加されます。
- ステップ 13** [保存 (Save)] をクリックして、展開の設定を終了します。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## スター VPN 展開の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	VPN	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

### 始める前に

管理対象デバイスをエンドポイントとして使用している場合、仮想ルータを作成し、それを適切なデバイスに適用します。



- (注) 複数のエンドポイントに同じ仮想ルータを使用することはできません。詳細については、次を参照してください。[仮想ルータのセットアップ \(1233 ページ\)](#)

### 手順

- ステップ 1** [デバイス (Devices)] > [VPN] を選択します。
- ステップ 2** [VPN の追加 (Add VPN)] > [Firepower デバイス (Firepower Device)] をクリックします。
- ステップ 3** 一意の名前を入力します。
- ステップ 4** [スター (Star)] をクリックしてタイプを指定します。
- ステップ 5** 一意の事前共有キーを入力します。

- ステップ 6** [ハブ ノード (Hub Node)] の隣の編集アイコン (✎) をクリックします。
- ステップ 7** [スター VPN の展開オプション \(1304 ページ\)](#) で説明されている VPN 展開オプションを設定します。
- ステップ 8** [保護されたネットワーク (Protected Networks)] の隣の追加アイコン (+) をクリックします。
- ステップ 9** 保護されたネットワークの IP アドレスを入力します。
- ステップ 10** [OK] をクリックします。
- ステップ 11** [保存 (Save)] をクリックします。ハブ ノードが展開に追加されます。
- ステップ 12** [リーフ ノード (Leaf Nodes)] の隣の追加アイコン (+) をクリックします。
- ステップ 13** リーフ ノードを完了するには、手順 7 ~ 10 を繰り返します。これにより、ハブ ノードと同じオプションが設定されます。
- ステップ 14** [保存 (Save)] をクリックします。リーフ ノードが展開に追加されます。
- ステップ 15** [保存 (Save)] をクリックして、展開の設定を終了します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## メッシュ VPN 展開の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	VPN	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

#### 始める前に

管理対象デバイスをエンドポイントとして使用している場合、仮想ルータを作成し、それを適切なデバイスに適用します。



- (注) 複数のエンドポイントに同じ仮想ルータを使用することはできません。詳細については、次を参照してください。[仮想ルータのセットアップ \(1233 ページ\)](#)

#### 手順

- ステップ 1** [デバイス (Devices)] > [VPN] を選択します。
- ステップ 2** [VPN の追加 (Add VPN)] > [Firepower デバイス (Firepower Device)] をクリックします。

- ステップ 3** 一意の名前を入力します。
- ステップ 4** [メッシュ (Mesh)] をクリックして [タイプ (Type)] を指定します。
- ステップ 5** 一意の事前共有キーを入力します。
- ステップ 6** [ノード (Nodes)] の隣の追加アイコン (+) をクリックします。
- ステップ 7** [メッシュ VPN 展開オプション \(1305 ページ\)](#) で説明されている VPN 展開オプションを設定します。
- ステップ 8** [保護されたネットワーク (Protected Networks)] の隣の追加アイコン (+) をクリックします。
- ステップ 9** 保護されたネットワークの CIDR ブロックを入力します。
- ステップ 10** [OK] をクリックします。  
保護されたネットワークが追加されます。
- ステップ 11** [保存 (Save)] をクリックします。  
展開にエンドポイントが追加されます。
- ステップ 12** エンドポイントをさらに追加するには、ステップ 6 ~ 11 を繰り返します。
- ステップ 13** [保存 (Save)] をクリックして展開を完了します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 高度な VPN 展開を設定する方法

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	VPN	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin


マルチドメイン展開では、現在のドメインで作成された VPN 展開が表示されます。これは編集できます。また、エンドポイントデバイスの1つがドメインに属している場合は、先祖ドメインで作成された VPN 展開も表示されます。先祖ドメインで作成された VPN 展開は編集できません。下位のドメインで作成された VPN 展開を表示および編集するには、そのドメインに切り替えます。

#### 手順

**ステップ 1** [デバイス (Devices)] > [VPN] を選択します。

**ステップ 2** 編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- ステップ3 [Advanced] タブをクリックします。
- ステップ4 [VPN 展開の詳細オプション \(1307 ページ\)](#) の説明に従って、詳細設定を行います。
- ステップ5 [アルゴリズム (Algorithms) ] の隣の追加アイコン (  ) をクリックします。
- ステップ6 両方のフェーズに対して、[暗号 (Cipher) ]、[ハッシュ (Hash) ]、および [Diffie-Hellman] ([DH]) グループ認証のメッセージを選択します。
- ステップ7 [OK] をクリックします。
- ステップ8 [保存 (Save) ] をクリックします。

---

#### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。



## VPN 展開の編集



**注意** 2人のユーザが同じ展開について同時に編集してはいけません。ただし、Web インターフェイスでは同時編集を防止していないことに注意してください。

マルチドメイン展開では、現在のドメインで作成された VPN 展開が表示されます。これは編集できます。また、エンドポイントデバイスの1つがドメインに属している場合は、先祖ドメインで作成された VPN 展開も表示されます。先祖ドメインで作成された VPN 展開は編集できません。下位のドメインで作成された VPN 展開を表示および編集するには、そのドメインに切り替えます。

#### 手順

- ステップ1 [デバイス (Devices) ] > [VPN] を選択します。
- ステップ2 編集アイコン (  ) をクリックします。
- 代わりに表示アイコン (  ) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ3 必要な設定を変更します。
- [詳細設定 (Advanced) ] の設定。 [高度な VPN 展開を設定する方法 \(1312 ページ\)](#) を参照してください。
  - メッシュ展開の設定。 [メッシュ VPN 展開の設定 \(1311 ページ\)](#) を参照してください。
  - ポイントツーポイント型の展開の設定。 [ポイントツーポイント VPN 展開の設定 \(1309 ページ\)](#) を参照してください。
  - スター型の展開の設定。 [スター VPN 展開の設定 \(1310 ページ\)](#) を参照してください。

ヒント 展開を最初に保存した後で、展開のタイプを編集することはできません。展開のタイプを変更するには、展開を削除してから新しい展開を作成する必要があります。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## VPN 展開のステータス

VPN 展開を設定した後で、設定した VPN トンネルのステータスを表示できます。VPN ページには、各 VPN 展開の展開後に、その展開のステータス アイコンが表示されます。

- (🟢) アイコンは、すべての VPN エンドポイントが稼働していることを表します。
- (🔴) アイコンは、すべての VPN エンドポイントが停止していることを表します。
- (⚠️) アイコンは、稼働しているエンドポイントと停止しているエンドポイントがあることを表します。

ステータスアイコンをクリックして、展開のステータス、および展開内のエンドポイントに関する基本情報（エンドポイント名や IP アドレスなど）を表示することができます。VPN ステータスは、毎分、または（エンドポイントが停止した、または稼働したなど）ステータスの変更が生じた場合に更新されます。

#### 関連トピック

[VPN ステータスの表示 \(1314 ページ\)](#)

## VPN ステータスの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	VPN	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

マルチドメイン展開では、システムは現在のドメインで作成された VPN 展開を表示します。また、エンドポイントデバイスの1つがドメインに属している場合は、先祖ドメインで作成された VPN 展開も表示されます。下位のドメインで作成された VPN 展開を表示するには、そのドメインに切り替えます。



## 手順

**ステップ 1** [デバイス (Devices) ] > [VPN] を選択します。

**ステップ 2** ステータスを表示する展開の隣にある、VPN ステータス アイコンをクリックします。

**ステップ 3** [OK] をクリックします。

# VPN の統計およびログ

VPN 展開を設定した後で、設定した VPN トンネルを通過するデータの統計を表示することができます。また、各エンドポイントについて最新の VPN システムと IKE ログを表示することができます。

システムには、次の統計情報が表示されます。

### エンドポイント (Endpoint)

VPN エンドポイントとして指定されたルーテッドインターフェイスおよび IP アドレスへのデバイスパス。

### ステータス

VPN 接続の状態 (稼働または停止のどちらか) 。

### プロトコル

暗号化で使用するプロトコル (ESP または AH) 。

### 受信パケット数 (Packets received)

IPsec SA ネゴシエーション中に VPN トンネルが受信する、インターフェイスあたりのパケット数。

### 転送パケット数 (Packets Forwarded)

IPsec SA ネゴシエーション中に VPN トンネルが送信する、インターフェイスあたりのパケット数。

### 受信バイト数 (Bytes Received)

IPsec SA ネゴシエーション中に VPN トンネルが受信する、インターフェイスあたりのバイト数。

### 転送バイト数 (Bytes Forwarded)

IPsec SA ネゴシエーション中に VPN トンネルが送信する、インターフェイスあたりのバイト数。

### 作成時刻 (Time Created)

VPN 接続が作成された日時。

**最終使用時刻 (Time Last Used)**

ユーザが最後に VPN 接続を開始した時間。

**NAT トラバーサル (NAT Traversal)**

[はい (Yes)] が表示されている場合、ネットワーク アドレス変換を備えたデバイスの背後に少なくとも 1 つの VPN エンドポイントが存在します。

**IKE 状態 (IKE State)**

IKE SA の状態 (接続、確立、削除、または廃棄)。

**IKE イベント (IKE Event)**

IKE SA イベント (再認証、またはキー再生成)。

**IKE イベント時間 (IKE Event Time)**

次のイベントが発生する時間 (秒)。

**IKE アルゴリズム (IKE Algorithm)**

VPN 展開で使用されている IKE アルゴリズム。

**IPSec 状態 (IPSec State)**

IPSec SA の状態 (インストール中、インストール済み、更新中、キー再生成、削除、および廃棄)。

**IPSec イベント (IPSec Event)**

IPSec SA イベントがキーを再生成するタイミングの通知。

**IPSec イベント時間 (IPSec Event Time)**

次のイベントが発生するまでの時間 (秒)。

**IPSec アルゴリズム (IPSec Algorithm)**

VPN 展開で使用されている IPSec アルゴリズム。

**関連トピック**

[VPN 統計情報およびログの表示](#) (1316 ページ)

## VPN 統計情報およびログの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	VPN	7000 & 8000 シリーズ	任意 (Any)	Admin/Network Admin

マルチドメイン展開では、システムは現在のドメインで作成された VPN 展開を表示します。また、エンドポイントデバイスの 1 つがドメインに属している場合は、先祖ドメインで作成さ

れた VPN 展開も表示されます。下位のドメインで作成された VPN 展開を表示するには、そのドメインに切り替えます。

#### 手順

---

- ステップ 1 [デバイス (Devices) ] > [VPN] を選択します。
  - ステップ 2 統計情報を表示する展開の隣にある、VPN ステータス アイコンをクリックします。
  - ステップ 3 統計情報の表示アイコン (🔄) をクリックします。
  - ステップ 4 オプションで、[更新 (Refresh) ] をクリックして、VPN の統計情報を更新することもできます。
  - ステップ 5 オプションで、[最新のログの表示 (View Recent Log) ] をクリックして、各エンドポイントの最新のデータログを表示することもできます。ハイアベイラビリティペアの 7000 または 8000 シリーズ デバイス および スタック デバイスのログを表示するには、アクティブ/プライマリ、またはバックアップ/セカンダリのいずれかのデバイスへのリンクをクリックします。
-





## 第 **XV** 部

### アクセス制御

- [アクセス コントロール ポリシーの開始 \(1321 ページ\)](#)
- [アクセス コントロール ルール \(1343 ページ\)](#)
- [侵入ポリシーとファイル ポリシーを使用したアクセス制御 \(1359 ページ\)](#)
- [HTTP 応答ページとインタラクティブ ブロッキング \(1369 ページ\)](#)
- [セキュリティ インテリジェンス ブラックリスト \(1375 ページ\)](#)
- [DNS ポリシー \(1383 ページ\)](#)
- [プレフィルタ処理とプレフィルタ ポリシー \(1399 ページ\)](#)
- [インテリジェント アプリケーション バイパス \(1415 ページ\)](#)
- [コンテンツ制限を使用したアクセス制御 \(1425 ページ\)](#)





## 第 53 章

# アクセスコントロールポリシーの開始

ここでは、アクセスコントロールポリシーの使用を開始する方法について説明します。

- [アクセス制御の概要 \(1321 ページ\)](#)
- [アクセスコントロールポリシーの管理 \(1328 ページ\)](#)
- [基本的なアクセスコントロールポリシーの作成 \(1329 ページ\)](#)
- [アクセスコントロールポリシーの編集 \(1331 ページ\)](#)
- [アクセスコントロールポリシーの継承の管理 \(1333 ページ\)](#)
- [アクセスコントロールポリシーのターゲットデバイスの設定 \(1337 ページ\)](#)
- [アクセスコントロールポリシーの詳細設定 \(1338 ページ\)](#)

## アクセス制御の概要

アクセス制御は、（非高速パスを通る）ネットワークトラフィックの指定、検査、ロギングが可能な階層型ポリシーベースの機能です。アクセスコントロールポリシーはネストすることができ、これはマルチドメイン展開で特に有用です。このポリシーでは各ポリシーが先祖（または基本）ポリシーからルールや設定を継承します。この継承を強制することもできますが、下位のポリシーによる先祖ポリシーの上書きを許可することもできます。各管理対象デバイスは1つのアクセスコントロールポリシーのターゲットにすることができます。

ポリシーのターゲットデバイスがネットワークトラフィックについて収集したデータは、以下に基づいてそのトラフィックのフィルタや制御に使用できます。

- トランスポート層およびネットワーク層の特定しやすい単純な特性（送信元と宛先、ポート、プロトコルなど）
- レピュテーション、リスク、ビジネスとの関連性、使用されたアプリケーション、または訪問した URL などの特性を含む、トラフィックに関する最新のコンテキスト情報
- レルム、ユーザ、ユーザグループ、または ISE の属性
- カスタムセキュリティグループタグ (SGT)
- 暗号化されたトラフィックの特性（このトラフィックを復号してさらに分析することもできます）

- 暗号化されていないトラフィックまたは復号されたトラフィックに、禁止されているファイル、検出されたマルウェア、または侵入の試みが存在するかどうか

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。たとえば、レピュテーションベースのブラックリストはシンプルな送信元と宛先のデータを使用しているため、禁止されているトラフィックを初期の段階でブロックできます。これに対し、侵入およびエクスプロイトの検知とブロックは最終防衛ラインです。

展開のライセンスを取得せずにシステムを設定することはできますが、多くの機能では、展開する前に適切なライセンスを有効にする必要があります。また、一部の機能は、特定のデバイスモデルでのみ使用できます。サポートされていない機能は、警告アイコンおよび確認ダイアログボックスに示されます。



- (注) システムがトラフィックに影響を与えるためには、ルーテッド、スイッチド、トランスペアレント インターフェイスまたはインライン インターフェイスのペアを使用して関連する設定を管理対象デバイスに展開する必要があります。場合によっては、タップモードのインライン デバイスを含むパッシブに展開されたデバイスにインライン設定を展開することがシステムによって阻害されます。それ以外の場合、ポリシーは正常に展開されますが、パッシブに展開されたデバイスを使用してトラフィックのブロックや変更を試みると、予期しない結果になる可能性があります。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

## アクセスコントロールポリシーのコンポーネント

新しく作成したアクセスコントロールポリシーは、デフォルトアクションを使用して、すべてのトラフィックを処理するようにターゲットデバイスに指示します。

次の図で、デフォルトアクションはトラフィックが最終接続先に到達する前に、[バランスの取れたセキュリティと接続 (Balanced Security and Connectivity)] に基づく侵入ポリシーを使用してトラフィックを検査します。



## Simple Access Control Policy

inspects all traffic with a balanced intrusion policy

Identity Policy: None

次のリストに、簡単なポリシーの作成後に変更可能な設定を示します。



- (注) 現在のドメインで作成されたアクセスコントロールポリシーのみ編集できます。また、先祖アクセスコントロールポリシーによってロックされている設定は編集できません。

### 名前 (Name) と説明 (Description)

各アクセスコントロールポリシーには一意の名前が必要です。説明は任意です。

### 継承設定 (Inheritance Settings)

ポリシー継承により、アクセスコントロールポリシーの階層を作成することができます。親 (または基本) ポリシーは子孫のデフォルト設定を定義、実行します。これはマルチドメイン導入環境で特に有効です。

ポリシーの継承設定で基本ポリシーを選択できます。また、現在のポリシーで設定をロックすることで、子孫にも同じ設定を継承させることができます。ロック解除された設定については、子孫ポリシーによる上書きが可能です。

### ポリシー割り当て

各アクセスコントロールポリシーがそのポリシーを使用するデバイスを識別します。1つのデバイスに適用されるアクセスコントロールポリシーは1つのみです。マルチドメイン導入環境では、1ドメイン内のすべてのデバイスで同じ基本ポリシーを使用させることができます。

### ルール (Rule)

アクセスコントロールルールは、ネットワークトラフィックをきめ細かく処理する方法を提供します。先祖ポリシーから継承したルールを含むアクセスコントロールポリシーのルールには、1から始まる番号が付いています。システムは、ルール番号の昇順で上から順に、アクセスコントロールルールをトラフィックと照合します。

通常、システムは、ルールすべての条件がトラフィックに一致する最初のアクセスコントロールルールに従ってネットワークトラフィックを処理します。条件は単純または複雑にできます。条件の使用は特定のライセンスによって異なります。

### デフォルトアクション (Default Action)

デフォルトアクションは、他のアクセス制御設定で処理されないトラフィックをどのように処理し、ロギングするかを定義します。デフォルトアクションにより、追加のインスペクションなしですべてのトラフィックをブロックまたは信頼することができます。また、侵入およびディスクバリデータの有無についてトラフィックを検査することもできます。

アクセスコントロールポリシーのデフォルトアクションは先祖ポリシーから継承することもできますが、継承を強制的に実施することはできません。

### セキュリティインテリジェンス (Security Intelligence)

セキュリティインテリジェンスは、悪意のあるインターネットコンテンツに対する最初の防衛ラインです。この機能により、最新のIPアドレス、URL、ドメイン名レピュテーションインテリジェンスをもとに接続をブラックリストに登録（ブロック）することができます。重要なリソースへの継続的なアクセスを確保するために、ブラックリストはカスタムホワイトリストで上書きできます。

### HTTP 応答 (HTTP Responses)

システムによりユーザの Web サイトリクエストがブロックされた場合、システム提供の汎用的な応答ページを表示するか、カスタムページを表示させることができます。ユーザに警告するページを表示するものの、ユーザが最初に要求したサイトに進めるようにすることもできます。

### アクセスコントロールの詳細オプション (Advanced Access Control Options)

通常、アクセスコントロールポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。多くの場合、デフォルト設定が適切です。詳細設定では、トラフィックの前処理、SSL インスペクション、ID、種々のパフォーマンスオプションなどを変更できます。

### 関連トピック

[ルール管理：共通の特性](#) (369 ページ)

## アクセスコントロールポリシーのデフォルトアクション

単純なアクセスコントロールポリシーでは、デフォルトアクションは、ターゲットデバイスがすべてのトラフィックをどう処理するかを指定します。より複雑なポリシーでは、デフォルトアクションは次のトラフィックを処理します。

- インテリジェントアプリケーションバイパスで信頼されないトラフィック
- セキュリティインテリジェンスによってブラックリスト登録されていないトラフィック
- SSL インスペクションによってブロックされていないトラフィック（暗号化トラフィックのみ）

- ポリシー内のどのルールにも一致しないトラフィック（トラフィックの照合とロギングは行うが、処理または検査はしないモニタールールを除く）

アクセスコントロールポリシーのデフォルトアクションにより、追加のインスペクションなしでトラフィックをブロックまたは信頼することができます。また、侵入およびディスカバリデータの有無についてトラフィックを検査することもできます。



(注) デフォルトアクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行**できません**。デフォルトアクションで処理される接続のロギングは、初期設定では無効ですが、有効にすることもできます。

ポリシーを継承している場合、最下位の子孫のデフォルトアクションによってトラフィックの最終的な処理が決まります。アクセスコントロールポリシーのデフォルトアクションは基本ポリシーから継承することもできますが、継承したデフォルトアクションを強制的に実施することはできません。

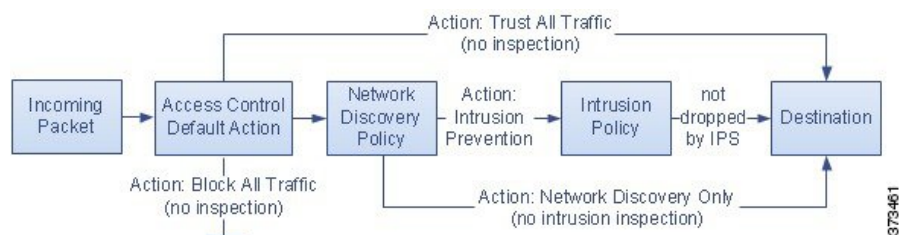
次の表に各デフォルトアクションが処理するトラフィックに対して実施可能なインスペクションの種類を示します。

表 81: アクセスコントロールポリシーのデフォルトアクション

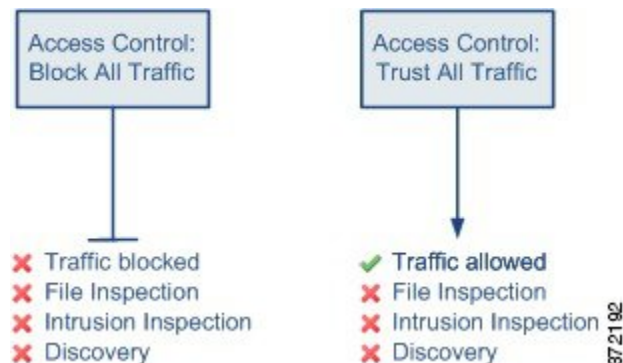
デフォルトアクション	トラフィックに対して行う処理	インスペクションタイプとポリシー
アクセスコントロール：すべてのトラフィックをブロック	それ以上のインスペクションは行わずにブロックする	none
アクセスコントロール：すべてのトラフィックを信頼	信頼（追加のインスペクションなしで最終宛先に許可）	none
侵入防御（Intrusion Prevention）	ユーザが指定した侵入ポリシーに合格する限り、許可する	侵入、指定した侵入ポリシーおよび関連する変数セットを使用、および 検出（discovery）、ネットワーク検出ポリシーを使用
ネットワーク検出のみ（Network Discovery Only）	許可（allow）	検出のみ（discovery only）、ネットワーク検出ポリシーを使用
基本ポリシーから継承	基本ポリシーで定義	基本ポリシーで定義

次の図は、表を図で表したものです。

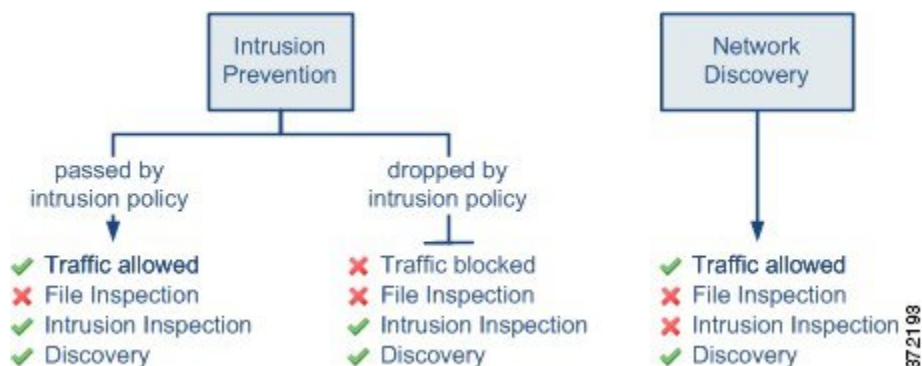
アクセスコントロールポリシーのデフォルトアクション



次の図は、[すべてのトラフィックをブロック (Block All Traffic)] および [すべてのトラフィックを信頼 (Trust All Traffic)] のデフォルトアクションを示しています。



次の図は、[侵入防御 (Intrusion Prevention)] および [ネットワーク検出のみ (Network Discovery Only)] のデフォルトアクションを説明しています。



**ヒント** [ネットワーク検出のみ (Network Discovery Only)] の目的は、検出のみの展開でパフォーマンスを向上させることです。侵入検知および防御のみを目的としている場合は、さまざまな設定でディスカバリを無効にできます。

関連トピック

- [限定的な導入のパフォーマンスに関する考慮事項 \(364 ページ\)](#)
- [ポリシーのデフォルトアクションによる接続のロギング \(2517 ページ\)](#)

## アクセスコントロールポリシーの継承

アクセス制御は、マルチテナンシーを補完する階層型ポリシーベース実装となっています。ドメイン階層を作成するのと同様に、対応するアクセスコントロールポリシーの階層を作成できます。子孫（あるいは子）アクセスコントロールポリシーは、直接の親（あるいは基本）ポリシーからルールや設定を継承します。この基本ポリシーにもさらに親ポリシーがあり、その親ポリシーにもさらに、というようにルールや設定が継承されている場合もあります。

アクセスコントロールポリシーのルールは、親ポリシーの [強制 (Mandatory)] ルールセクションと [デフォルト (Default)] のルールセクションの間にネストされています。この実装により、先祖ポリシーの [強制 (Mandatory)] ルールは実施される一方、先祖ポリシーの [デフォルト (Default)] ルールは現在のポリシーでプリエンプション処理することが可能です。

次の設定をロックすることで、すべての子孫ポリシーに設定を実行させることができます。ロック解除された設定については、子孫ポリシーによる上書きが可能です。

- セキュリティインテリジェンス：最新の IP アドレス、URL、ドメイン名レピュテーションインテリジェンスをもとに接続をブラックリストに登録（ブロック）します。
- HTTP 応答ページ：ユーザの Web サイトリクエストをブロックした際、カスタム応答ページあるいはシステム提供の応答ページを表示します。
- 詳細設定：関連するサブポリシー、ネットワーク分析設定、パフォーマンス設定、その他の一般設定オプションを指定します。

アクセスコントロールポリシーのデフォルトアクションは先祖ポリシーから継承することもできますが、継承を強制的に実施することはできません。

### ポリシーの継承とマルチテナンシー

通常マルチドメイン導入環境では、アクセスコントロールポリシーの階層がドメイン構造に対応しており、管理対象デバイスに最下位レベルのアクセスコントロールポリシーを適用します。この実装により、ドメインの上層レベルでは選択的にアクセス制御を実施しながらも、ドメインの下層レベルの管理者は展開ごとに設定を調整することが可能です（子孫ドメインの管理者を制限するには、ポリシー継承と適用だけでなく、ロールによる制限を行う必要があります）。

たとえば、所属している部門のグローバルドメイン管理者は、グローバルレベルのアクセスコントロールポリシーを作成できます。そして、そのグローバルレベルのポリシーを基本ポリシーとして、機能別にサブドメインに分けられたすべてのデバイスで使用するよう要求することが可能です。

サブドメインの管理者が Firepower Management Center にログインしてアクセス制御を設定する際、グローバルレベルのポリシーはそのまま展開できます。あるいは、グローバルレベルのポリシーの範囲内の子孫アクセスコントロールポリシーを作成、展開することも可能です。



- (注) アクセス制御の継承および適用が最も有効に実装されるのは、マルチテナンシーを補完する場合ですが、1つのドメイン内においてもアクセス制御ポリシーを階層化することが可能です。また、任意のレベルでアクセスコントロールポリシーを割り当て、展開することもできます。

#### 関連トピック

- [アクセスコントロールポリシーの継承の管理](#) (1333 ページ)
- [セキュリティインテリジェンスブラックリスト](#) (1375 ページ)
- [HTTP 応答ページとインタラクティブブロッキング](#) (1369 ページ)
- [アクセスコントロールポリシーの詳細設定](#) (1338 ページ)

## アクセスコントロールポリシーの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin Access Admin Network Admin

Firepower システムでは、システム付属のアクセスコントロールポリシーの編集と、カスタムアクセスコントロールポリシーの作成が可能です。デバイスの初期設定に応じて、システム付属のポリシーには次のものが含まれます。


- デフォルトアクセス制御：詳細な検査なしで、すべてのトラフィックをブロックします。
- デフォルト侵入防御：すべてのトラフィックを許可しますが、Balanced Security and Connectivity 侵入ポリシーおよびデフォルトの侵入変数セットを使用して検査も実行します。
- デフォルトネットワーク検出：すべてのトラフィックを許可すると同時に検出データについて検査しますが、侵入やエクスプロイトについては検査しません。





マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

#### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] を選択します。

**ステップ 2** アクセスコントロールポリシーを管理します。

- コピー：コピーアイコン () をクリックします。

- 作成：[新規ポリシー（New Policy）]をクリックします。[基本的なアクセスコントロールポリシーの作成（1329 ページ）](#)を参照してください。
- 削除：削除アイコン（)をクリックします。
- 展開：[展開（Deploy）]をクリックします（[設定変更の導入（350 ページ）](#)を参照）。
- 編集：編集アイコン（)をクリックします。次を参照してください。[アクセスコントロールポリシーの編集（1331 ページ）](#)
- 継承：子孫を持つポリシーの横にあるプラスアイコン（)をクリックすると、ポリシーの階層ビューが展開されます。
- インポート/エクスポート：[インポート/エクスポート（Import/Export）]をクリックします。[コンフィギュレーションのインポートとエクスポート（211 ページ）](#)を参照してください。
- [レポート（Report）]：レポートアイコン（)をクリックします（[現在のポリシー レポートの生成（363 ページ）](#)を参照）。

#### 関連トピック

[失効ポリシー（363 ページ）](#)

## 基本的なアクセスコントロールポリシーの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

新規アクセスコントロールポリシーを作成する場合は、少なくとも、デフォルトアクションを選択する必要があります。

ほとんどの場合、デフォルトアクションにより処理される接続のロギングは最初は無効になっています。例外は、マルチドメイン導入でサブポリシーを作成する場合です。この場合、継承されたデフォルトアクションのロギング設定に応じて、接続のロギングが有効になります。

#### 手順

**ステップ 1** [ポリシー（Policies）]>[アクセスコントロール（Access Control）]を選択します。

**ステップ 2** [新しいポリシー（New Policy）]をクリックします。

**ステップ 3** [名前（Name）]に一意の名前を入力し、オプションで[説明（Description）]を入力します。

**ステップ4** オプションで、[基本ポリシーの選択 (Select Base Policy)] ドロップダウンリストから基本ポリシーを選択します。

ドメインにアクセスコントロールポリシーが適用されている場合は、この手順はオプションではありません。適用されているポリシーまたはその子孫のいずれかを基本ポリシーとして選択する必要があります。

**ステップ5** 初期デフォルトアクションを指定します。

- 基本ポリシーを選択すると、新しいポリシーではそのデフォルトアクションが継承されません。ここで変更することはできません。
- [すべてのトラフィックをブロック (Block All Traffic)] を選択すると、[アクセスコントロール: すべてのトラフィックをブロック (Access Control: Block All Traffic)] をデフォルトアクションとするポリシーが作成されます。
- [侵入防御 (Intrusion Prevention)] を選択すると、[侵入防御: セキュリティと接続性のバランス (Intrusion Prevention: Balanced Security and Connectivity)] をデフォルトアクションとし、デフォルトの侵入変数セットが関連付けられたポリシーが作成されます。
- [ネットワーク検出 (Network Discovery)] を選択すると、[ネットワーク検出のみ (Network Discovery Only)] をデフォルトアクションとするポリシーが作成されます。

**ヒント** デフォルトですべてのトラフィックを信頼するか、基本ポリシーを選択しデフォルトアクションは継承しないようにする場合は、後でデフォルトアクションを変更できません。

**注意** アクセスコントロールポリシーによって使用される侵入ポリシーの総数の変更設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作 \(356ページ\)](#) を参照してください。現在使用されていない侵入ポリシーを追加するか、侵入ポリシーの最後のインスタンスを削除することで、侵入ポリシーの総数を変更します。アクセスコントロールルールで侵入ポリシーをデフォルトのアクションまたはデフォルトの侵入ポリシーとして使用できます。

**ステップ6** 必要に応じて、ポリシーを展開する [使用可能なデバイス (Available Devices)] を選択し、[ポリシーに追加 (Add to Policy)] をクリック (またはドラッグアンドドロップ) して、選択したデバイスを追加します。表示されるデバイスを絞り込むには、[検索 (Search)] フィールドに検索文字列を入力します。

このポリシーをすぐに展開するには、この手順を実行する必要があります。

**ステップ7** [保存 (Save)] をクリックします。

---

### 次のタスク

- 必要に応じて、[アクセスコントロールポリシーの編集 \(1331ページ\)](#) の説明に従って、さらに新しいポリシーを設定します。



- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

#### 関連トピック

[アクセスコントロールポリシーのデフォルトアクション \(1324 ページ\)](#)

[アクセスコントロールポリシーのターゲットデバイスの設定 \(1337 ページ\)](#)

## アクセスコントロールポリシーの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

ポリシーの編集は、1つのブラウザウィンドウを使用して、一度に1人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシーエディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

#### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] を選択します。




**ステップ 2** 編集するアクセスコントロールポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔒) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** アクセスコントロールポリシーを編集します。

- 名前と説明：いずれかのフィールドをクリックし、新しい情報を入力します。
- デフォルトアクション：[デフォルトアクション (Default Action)] ドロップダウンリストから値を選択します。

**注意** アクセスコントロールポリシーによって使用される侵入ポリシーの総数の変更設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。現在使用されていない侵入ポリシーを追加するか、侵入ポリシーの最後のインスタンスを削除することで、侵入ポリシーの総数を変更します。アクセスコントロールルールで侵入ポリシーをデフォルトのアクションまたはデフォルトの侵入ポリシーとして使用できます。

- デフォルトアクションの変数セット：[侵入防御（Intrusion Prevention）]のデフォルトアクションに関連付けられている変数セットを変更するには、変数アイコン（）をクリックします。表示されるポップアップウィンドウで、新しい変数セットを選択して[OK]をクリックします。また、編集アイコン（）をクリックして、選択した変数セットを新しいウィンドウで編集することもできます。詳細については、[変数の管理（460ページ）](#)を参照してください。
- デフォルトアクションのロギング：デフォルトアクションで処理される接続のロギングを設定するには、ロギングアイコン（）をクリックします。[ポリシーのデフォルトアクションによる接続のロギング（2517ページ）](#)を参照してください。
- HTTP応答：システムがWebサイトの要求をブロックする際にブラウザに表示される情報を指定するには、[HTTP応答（HTTP Responses）]タブをクリックします。[HTTP応答ページの選択（1371ページ）](#)を参照してください。
- 継承：基本ポリシーの変更：このポリシーの基本アクセスコントロールポリシーを変更するには、[継承設定（Inheritance Settings）]をクリックします。[基本アクセスコントロールポリシーの選択（1334ページ）](#)を参照してください。
- 継承：子孫での設定のロック：このポリシーの設定を子孫ポリシーに適用するには、[継承設定（Inheritance Settings）]をクリックします。[子孫アクセスコントロールポリシーのロックの設定（1335ページ）](#)を参照してください。
- ポリシー割り当て：ターゲット：このポリシーの対象となっている管理対象デバイスを特定するには、[ポリシー割り当て（Policy Assignment）]をクリックします。[アクセスコントロールポリシーのターゲットデバイスの設定（1337ページ）](#)を参照してください。
- ポリシー割り当て：ドメインで必須：このポリシーをサブドメインに適用するには、[ポリシー割り当て（Policy Assignment）]をクリックします。[ドメインでのアクセスコントロールポリシーの強制（1336ページ）](#)を参照してください。
- ルール：アクセスコントロールルールを管理し、侵入とファイルポリシーを使用して悪意のあるトラフィックを検査およびブロックするには、[ルール（Rules）]タブをクリックします。[アクセスコントロールルールの作成および編集（1350ページ）](#)を参照してください。
- セキュリティインテリジェンス：最新のレピュテーションインテリジェンスに基づいてすぐに接続をブラックリストに載せる（ブロックする）には、[セキュリティインテリジェンス（Security Intelligence）]タブをクリックします。[セキュリティインテリジェンスの設定（1378ページ）](#)を参照してください。
- 詳細オプション：前処理、SSLインスペクション、アイデンティティ、パフォーマンス、およびその他の詳細オプションを設定するには、[詳細（Advanced）]タブをクリックします。[アクセスコントロールポリシーの詳細設定（1338ページ）](#)を参照してください。
- 警告：アクセスコントロールポリシー（およびその子孫ポリシーと関連ポリシー）の警告またはエラーのリストを表示するには、[警告の表示（Show Warnings）]をクリックします。警告とエラーによって、トラフィック分析やフローに悪影響を及ぼしたり、ポリ

シーの展開を妨げたりする構成がマークされます。警告がない場合、ボタンは表示されません。

**ステップ 4** [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

- [ルールとその他のポリシーの警告 \(411 ページ\)](#)
- [ディープ インспекションについて \(1359 ページ\)](#)

## アクセスコントロールポリシーの継承の管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

#### 手順

**ステップ 1** 変更する継承設定を持つアクセスコントロールポリシーを編集します。[アクセスコントロールポリシーの編集 \(1331 ページ\)](#) を参照してください。

**ステップ 2** ポリシーの継承を管理します。

- 基本ポリシーの変更：このポリシーの基本アクセスコントロールポリシーを変更するには、[継承設定 (Inheritance Settings) ] をクリックして、[基本アクセスコントロールポリシーの選択 \(1334 ページ\)](#) で説明する手順を実行します。
- 子孫の設定のロック：このポリシーの設定を子孫ポリシーで強制適用するには、[継承設定 (Inheritance Settings) ] をクリックして、[子孫アクセスコントロールポリシーのロックの設定 \(1335 ページ\)](#) で説明する手順を実行します。
- ドメインで必須：このポリシーをサブドメインで強制適用するには、[ポリシーの割り当て (Policy Assignment) ] をクリックして、[ドメインでのアクセスコントロールポリシーの強制 \(1336 ページ\)](#) で説明する手順を実行します。
- 基本ポリシーからの設定の継承：基本アクセスコントロールポリシーから設定を継承するには、[セキュリティインテリジェンス (Security Intelligence) ] タブ、[HTTP 応答 (HTTP Responses) ] タブ、または[詳細 (Advanced) ] タブをクリックして、[基本ポリシーからのアクセスコントロールポリシー設定の継承 \(1334 ページ\)](#) で説明する手順を実行します。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 基本アクセスコントロールポリシーの選択

スマートライセンス	従来ライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

1つのアクセスコントロールポリシーを別の基本（親）として使用できます。デフォルトでは、子のポリシーが基本ポリシーから設定を継承します。ロック解除された設定を変更することも可能です。

既存のアクセスコントロールポリシーの基本ポリシーを変更すると、システムで現在のポリシー設定が新しい基本ポリシーの任意のロックされた設定に更新されます。

## 手順

- 
- ステップ 1** アクセスコントロールポリシーのエディタで、[継承設定 (Inheritance Settings)] をクリックします。
- ステップ 2** [基本ポリシーの選択 (Select Base Policy)] ドロップダウンリストからポリシーを選択します。マルチドメイン展開では、アクセスコントロールポリシーが既存のドメインで必要になることがあります。基本ポリシーとして、強制ポリシーまたはその子孫ポリシーの一つを選択できます。
- ステップ 3** [保存 (Save)] をクリックします。
- 

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 基本ポリシーからのアクセスコントロールポリシー設定の継承

スマートライセンス	従来ライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

新しい子ポリシーは、基本ポリシーから多数の設定を継承します。これらの設定は、基本ポリシーでロックされていない場合はオーバーライドできます。

基本ポリシーから後で設定を再継承すると、システムによって基本ポリシーの設定が表示され、コントロールが淡色表示されます。ただし、オーバーライドした内容はシステムによって保存され、その内容は継承を再度無効にすると復元されます。

#### 手順

- 
- ステップ 1** アクセスコントロールポリシーエディタで、[セキュリティインテリジェンス (Security Intelligence)] タブ、[HTTP 応答 (HTTP Responses)] タブまたは [詳細 (Advanced)] タブをクリックします。
- ステップ 2** 継承する設定ごとに、[基本ポリシーから継承 (Inherit from base policy)] チェックボックスをオンにします。
- コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。
- ステップ 3** [保存 (Save)] をクリックします。
- 

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 子孫アクセスコントロールポリシーのロックの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

アクセスコントロールポリシーの設定をロックして、すべての子孫ポリシーで設定を適用します。子孫ポリシーでは、ロックされていない設定をオーバーライドできます。

設定をロックするときに、すでに子孫ポリシーで実行されていたオーバーライドを保存して、設定のロックを再度解除したときにオーバーライドを復元できるようにします。

#### 手順

- 
- ステップ 1** アクセスコントロールポリシーエディタで、[設定の継承 (Inheritance Settings)] をクリックします。
- ステップ 2** [子ポリシーの継承設定 (Child Policy Inheritance Settings)] 領域で、ロックする設定をオンにします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。

**ステップ 3** [OK] をクリックして継承設定を保存します。

**ステップ 4** [保存 (Save) ] をクリックして、アクセスコントロールポリシーを保存します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ドメインでのアクセスコントロールポリシーの強制

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

ドメイン内の各デバイスが同一の基本アクセスコントロールポリシーまたは、そのポリシーの子孫ポリシーの1つを使用するように強制できます。

#### 始める前に

- 少なくとも1つのグローバルドメイン以外のドメインを設定します。

#### 手順

**ステップ 1** アクセスコントロールポリシーエディタで、[ポリシーの割り当て (Policy Assignments) ] をクリックします。

**ステップ 2** [ドメインに強制 (Required on Domains) ] タブをクリックします。

**ステップ 3** ドメインリストを作成します。

- 追加：現在のアクセスコントロールポリシーを強制適用するドメインを選択して [追加 (Add) ] をクリックするか、選択したドメインのリストにドラッグアンドドロップします。
- 削除：リーフドメインの横にある削除アイコン (🗑️) をクリックするか、先祖ドメインを右クリックして [選択項目の削除 (Delete Selected) ] を選択します。
- 検索：検索フィールドに検索文字列を入力します。クリアアイコン (✖️) をクリックして、検索をクリアします。

**ステップ 4** [OK] をクリックしてドメインに強制適用する設定を保存します。

**ステップ5** [保存 (Save) ]をクリックして、アクセスコントロールポリシーを保存します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## アクセスコントロールポリシーのターゲットデバイスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

アクセスコントロールポリシーは、それを使用するデバイスを指定します。それぞれのデバイスは、1つのアクセスコントロールポリシーのみのターゲットに設定できます。マルチドメイン展開では、ドメイン内のすべてのデバイスが同一の基本ポリシーを使用するように強制できます。

#### 手順

**ステップ1** アクセスコントロールポリシーエディタで、[ポリシーの割り当て (Policy Assignments) ]をクリックします。

**ステップ2** [ターゲットデバイス (Targeted Devices) ]タブで、ターゲットリストを作成します。

- 追加：1つ以上の [使用可能なデバイス (Available Devices) ]を選択して、[ポリシーに追加 (Add to Policy) ]をクリックするか、[選択したデバイス (Selected Devices) ]のリストにドラッグアンドドロップします。
- 削除：1つのデバイスの横にある削除アイコン (🗑️) をクリックするか、複数のデバイスを選択して、右クリックしてから [選択済み項目の削除 (Delete Selected) ]を選択します。
- 検索：検索フィールドに検索文字列を入力します。クリアアイコン (✖️) をクリックして、検索をクリアします。

[影響を受けるデバイス (Impacted Devices) ]の下に、割り当てられたアクセスコントロールポリシーが現在のポリシーの子であるデバイスが一覧表示されます。現在のポリシーを変更すると、これらのデバイスに影響します。

**ステップ3** 必要に応じて、[ドメインで強制 (Required on Domains) ]タブをクリックして、選択したサブドメイン内のすべてのデバイスが同じ基本ポリシーを使用するように強制します。[ドメインでのアクセスコントロールポリシーの強制 \(1336 ページ\)](#) を参照してください。

ステップ4 [OK] をクリックしてターゲットデバイス設定を保存します。

ステップ5 [保存 (Save) ] をクリックして、アクセスコントロールポリシーを保存します。

#### 次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

## アクセスコントロールポリシーの詳細設定

通常、アクセスコントロールポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。デフォルト設定は、ほとんどの展開環境に適しています。侵入ルールの更新 (179 ページ) で説明しているように、アクセスコントロールポリシーの前処理およびパフォーマンスの詳細オプションの多くは、ルールの更新によって変更される可能性があることに注意してください。

代わりに表示アイコン (🔒) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベースポリシーから継承する (Inherit from base policy) ] をオフにして、編集を有効にします。



**注意** Snort プロセスを再起動し、トラフィック インспекションを一時的に中断する詳細設定変更のリストについては、展開またはアクティブ化された際に Snort プロセスを再起動する設定 (357 ページ) を参照してください。この中断中にトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort® の再起動によるトラフィックの動作 (356 ページ) も参照してください。

#### 全般設定

ユーザが要求した各 URL に対して保存する文字数をカスタマイズするには、長い URL のログインの制限 (2518 ページ) を参照してください。

ユーザが最初のブロックをバイパスした後に Web サイトを再度ブロックするまでの時間間隔をカスタマイズするには、ブロックされた Web サイトのユーザバイパス タイムアウトの設定 (1373 ページ) を参照してください。

[URL キャッシュ ミス ルックアップを再試行する (Retry URL cache miss lookup) ] を無効にすると、カテゴリがキャッシュされない場合には、クラウドルックアップを使用せずに、すぐにトラフィックが URL に渡されるようにすることができます。クラウドルックアップで別のカテゴリが用意されるまで、クラウドルックアップを必要とする URL は未分類の URL として処理されます。

特定の設定で Snort プロセスを再起動する必要がない限り設定の変更を展開する場合にトラフィックを検査するには、必ず、[ポリシーの適用時にトラフィックを検査する (Inspect traffic



during policy apply) ] がデフォルト値 (有効) に設定してください。このオプションを有効にすると、リソースの需要が高まった場合にいくつかのパケットが検査なしでドロップされることがあります。詳細については、[Snort®の再起動シナリオ \(354 ページ\)](#) を参照してください。

### 関連するポリシー

詳細設定を使用して、サブポリシー (SSL、ID、プレフィルタ) をアクセス制御に関連付けます。[アクセス制御への他のポリシーの関連付け \(1340 ページ\)](#) を参照してください。

### ネットワーク分析ポリシーと侵入ポリシー

ネットワーク分析ポリシーおよび侵入ポリシーの詳細設定によって、以下が可能になります。

- システムがトラフィックを検査する方法を正確に決定する前に、最初にそのトラフィックを検査するために使用される、アクセスコントロールポリシーのデフォルトの侵入ポリシーと関連付けられている変数セットの変更。
- 多くの前処理オプションを制御する、アクセスコントロールポリシーのデフォルトネットワーク分析ポリシーの変更。
- カスタムネットワーク分析ルールおよびネットワーク分析ポリシーを使用した、特定のセキュリティゾーン、ネットワーク、および VLAN に対する前処理オプションの調整。

詳細については、[ネットワーク分析/侵入ポリシーのための高度なアクセス制御の設定 \(1837 ページ\)](#) を参照してください。

### ファイルおよびマルウェアの設定

[ファイルとマルウェアのインスペクションパフォーマンスとストレージの調整 \(1563 ページ\)](#) に、ファイル制御と AMP for Firepower のパフォーマンス オプションに関する情報が記載されています。

### インテリジェントアプリケーションバイパスの設定

インテリジェントアプリケーションバイパス (IAB) は、トラフィックがインスペクションパフォーマンスとフローしきい値の組み合わせを超過したときにバイパスするアプリケーションを指定する、または、バイパスに関するテストを行うための、エキスパートレベルの設定です。詳細については、[インテリジェントアプリケーションバイパス \(1415 ページ\)](#) を参照してください。

### トランスポート層とネットワーク層のプリプロセッサの設定

トランスポート層とネットワーク層のプリプロセッサの詳細設定は、アクセスコントロールポリシーが展開されるすべてのネットワーク、ゾーン、VLAN にグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセスコントロールポリシーで設定します。詳細については、[トランスポート/ネットワークプリプロセッサの詳細設定 \(1946 ページ\)](#) を参照してください。

### 検出拡張の設定

検出拡張の詳細設定では、次のことを実行できるようにアダプティブプロファイルを設定することができます。

- アクセス コントロール ルールでファイル ポリシーとアプリケーションを使用する。
- 侵入ルールでサービス メタデータを使用する。
- パッシブ展開で、ネットワークのホスト オペレーティング システムに基づいてパケットフラグメントと TCP ストリームのリアセンブルを向上させる。

詳細については、[適応型プロファイル \(2013 ページ\)](#) を参照してください。

### パフォーマンス設定および遅延ベースのパフォーマンス設定

[侵入防御のパフォーマンスチューニングについて \(1819 ページ\)](#) では、侵入行為についてトラフィックを分析する際にシステムのパフォーマンスを向上させるための情報を提供しています。

遅延ベースのパフォーマンス設定固有の情報については、[パケットおよび侵入ルールの遅延しきい値構成 \(1825 ページ\)](#) を参照してください。

## アクセス制御への他のポリシーの関連付け

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	機能に応じて異なる	機能に応じて異なる	任意 (Any)	Admin/Access Admin/Network Admin

次のサブポリシーのいずれかとアクセス コントロール ポリシーとを関連付けるには、アクセス コントロール ポリシーの詳細設定を使用します。

- SSL ポリシー：セキュア ソケット レイヤ (SSL) または Transport Layer Security (TLS) で暗号化されたアプリケーション層プロトコルトラフィックをモニタ、復号化、ブロック、または許可します。



**注意** SSL ポリシーを追加または削除すると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

- アイデンティティポリシー：トラフィックに関連付けられているレームと認証方式に基づいて、ユーザ認証を実行します。
- プレフィルタポリシー：（レイヤ4の）アウターヘッダによりネットワーク限定を使用した早期のトラフィック処理を実行します。

## 手順

---

**ステップ1** アクセスコントロールポリシーエディタで、[詳細 (Advanced)] タブをクリックします。

**ステップ2** 適切な [ポリシー設定 (Policy Settings)] 領域の編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔒) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベースポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。

**ステップ3** ドロップダウンリストからポリシーを選択します。

ユーザが作成したポリシーを選択する場合は、表示される編集アイコンをクリックしてポリシーを編集できます。

**ステップ4** [OK] をクリックします。

**ステップ5** [保存 (Save)] をクリックして、アクセスコントロールポリシーを保存します。

---

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 関連トピック

[Snort® の再起動シナリオ \(354 ページ\)](#)





## 第 54 章

# アクセスコントロールルール

次の各トピックでは、アクセスコントロールルールの設定方法について説明します。

- [アクセスコントロールルールの概要 \(1343 ページ\)](#)
- [アクセス制御ルール カテゴリの追加 \(1349 ページ\)](#)
- [アクセスコントロールルールの作成および編集 \(1350 ページ\)](#)
- [アクセスコントロールルールの有効化と無効化 \(1351 ページ\)](#)
- [アクセスコントロールルールの配置 \(1352 ページ\)](#)
- [アクセスコントロールルールのアクション \(1353 ページ\)](#)
- [アクセスコントロールルールのコメント \(1356 ページ\)](#)

## アクセスコントロールルールの概要

アクセスコントロールポリシー内では、アクセスコントロールルールによって複数の管理対象デバイスでネットワークトラフィックを処理するきめ細かい制御方法が提供されます。

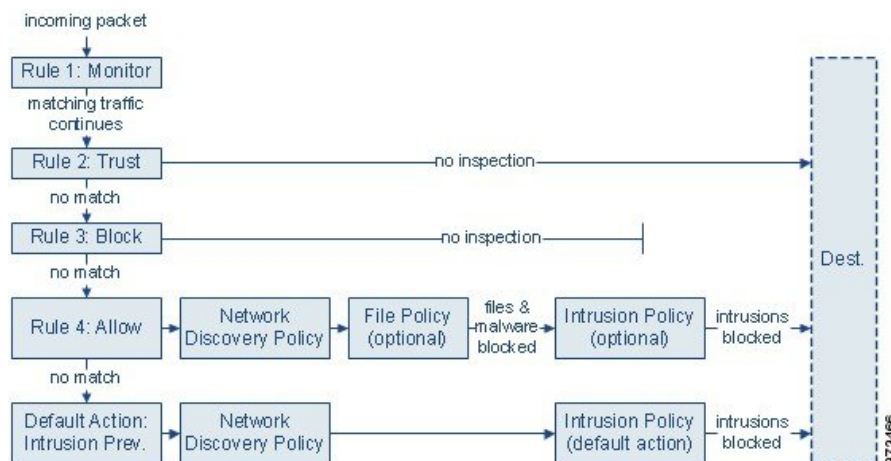


- (注) アクセスコントロールルールがネットワークトラフィックを評価する前に、8000 シリーズ高速パス、プレフィルタ評価、セキュリティインテリジェンスのフィルタリング、SSL インспекション、ユーザの識別、および一部の復号と前処理が発生します。

システムは、指定した順にアクセスコントロールルールをトラフィックと照合します。ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセスコントロールルールに従ってネットワークトラフィックを処理します。

また、各ルールにはアクションがあり、これによって一致するトラフィックをモニタ、信頼、ブロック、または許可するかを決定します。トラフィックを許可するときは、システムが侵入ポリシーまたはファイルポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、 익스プロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

次のシナリオでは、インラインの侵入防御展開環境で、アクセスコントロールルールによってトラフィックを評価できる方法を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- ルール1：モニタ**はトラフィックを最初に評価します。モニタールールはネットワークトラフィックを追跡してログに記録しますが、トラフィックフローには影響しません。システムは引き続きトラフィックを追加のルールと照合し、許可するか拒否するかを決定します。
- ルール2：信頼**はトラフィックを2番目に評価します。一致するトラフィックは追加のインスペクションなしで宛先まで通過することが許可されますが、引き続きアイデンティティの要件とレート制限の対象となります。一致しないトラフィックは、引き続き次のルールと照合されます。
- ルール3：ブロック**はトラフィックを3番目に評価します。一致するトラフィックは、追加のインスペクションなしでブロックされます。一致しないトラフィックは、引き続き最後のルールと照合されます。
- ルール4：許可**は最後のルールです。このルールの場合、一致したトラフィックは許可されますが、トラフィック内の禁止ファイル、マルウェア、侵入、エクスプロイトは検出されてブロックされます。残りの禁止されていない悪意のないトラフィックは宛先まで通過することが許可されますが、引き続きアイデンティティの要件とレート制限の対象となります。ファイルインスペクションのみを実行する、または侵入インスペクションのみを実行する、もしくは両方とも実行しない許可ルールを設定できます。
- デフォルトアクション**は、いずれのルールにも一致しないすべてのトラフィックを処理します。このシナリオでは、デフォルトアクションは、悪意のないトラフィックの通過を許可する前に侵入防御を実行します。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルトアクションを割り当てることもあります。(デフォルトアクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません。)

アクセスコントロールルールまたはデフォルトアクションによって許可したトラフィックは、自動的にホスト、アプリケーション、およびユーザーデータについてネットワーク検出ポリシーによるインスペクションの対象になります。ディスカバリを拡張することや無効化することはできますが、明示的に有効にはしません。ただし、トラフィックを許可しても、ディスカバリ

データ収集が自動的に保証されるわけではありません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、ディスクバリエーションを実行します。また、アプリケーション検出は、暗号化されたセッションに限定されます。

暗号化されたトラフィックの通過が SSL インспекション設定で許可される場合、または SSL インспекションが設定されていない場合は、そのトラフィックがアクセスコントロールルールによって処理されることに注意してください。ただし、一部のアクセスコントロールルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、システムは暗号化ペイロードの侵入およびファイルインспекションを無効にしています。これにより、侵入およびファイルインспекションが設定されたアクセスコントロールルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

## アクセスコントロールルールの管理

アクセスコントロールポリシーエディタの[ルール (Rules)]タブでは、編集中のポリシーのアクセスコントロールルールの追加、編集、分類、検索、移動、有効化、無効化、削除、その他の管理が行えます。

ポリシーエディタでは、各アクセスコントロールルールに対してルールの名前、条件の概要、ルールアクションが表示され、さらにルールのインспекションオプションや状態を示すアイコンが表示されます。各アイコンの意味は次のとおりです。

- 侵入ポリシー オプション (🛡️)
- ファイルポリシー オプション (📁)
- セーフサーチ オプション (🔒)
- YouTube EDU オプション (📺)
- ロギング オプション (📄)
- 発信元クライアント オプション (👤)
- コメント (💬)
- 警告 (⚠️)
- エラー (❗)
- 重要な情報 (ℹ️)

無効なルールはグレー表示され、ルール名の下に [ (無効) ((disabled)) ] というマークが付きます。

ルールを作成または編集するには、アクセスコントロールルールエディタを使用します。次の操作を実行できます。

- エディタの上部で、ルールの名前、状態、位置、アクションなどの基本的なプロパティを設定します。
- エディタの左下にあるタブを使用して、条件を追加します。
- インспекションおよびロギングのオプションを設定し、さらにルールにコメントを追加するには、右下にあるタブを使用します。便宜上、どのタブを表示しているかに関係なく、エディタにはルールのインспекションおよびロギングのオプションがリストされます。



(注) アクセスコントロールルールの適切な作成と順序付けは複雑なタスクですが、効果的な展開を構築するためには不可欠です。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンプレション処理したり、追加のライセンスが必要となったり、ルールに無効な設定が含まれる場合があります。システムが想定どおりにトラフィックを確実に処理できるように、アクセスコントロールポリシーインターフェイスにはルールに対する強力な警告およびエラーのフィードバックシステムがあります。

#### 関連トピック

[アクセスコントロールルールのコンポーネント](#) (1346 ページ)

[例：カスタム ユーザ ロールとアクセス制御](#) (51 ページ)

[ルールのパフォーマンスに関するガイドライン](#) (412 ページ)

## アクセスコントロール ルールのコンポーネント

一意の名前に加え、各アクセスコントロールルールには次の基本コンポーネントがあります。

### 状態 (State)

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

### 位置 (Position)

アクセスコントロールポリシー内の各ルールには、1 から始まる番号が付きます。ポリシー継承を使用する場合、ルール 1 は再外部ポリシーの 1 番目のルールです。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。モニタールールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

また、ルールはセクションおよびカテゴリに属していることがあります。これは、単に整理のためであり、ルールの位置に影響しません。ルールの位置は、すべてのセクションとカテゴリにまたがって設定されます。

### セクションおよびカテゴリ

アクセスコントロールルールの整理に役立つように、アクセスコントロールポリシーには、システムで用意されている 2 つのルールセクションとして「必須 (Mandatory)」と「デフォ



ルト (Default) 」があります。アクセスコントロールルールをさらに細かく整理するため、「必須 (Mandatory) 」セクション内と「デフォルト (Default) 」セクション内にカスタムルールカテゴリを作成することができます。

ポリシーの継承を使用する場合、現在のポリシーのルールは、その親ポリシーの「必須 (Mandatory) 」セクションと「デフォルト (Default) 」セクションの間にネストされます。

### 条件 (Conditions)

条件は、ルールが処理する特定のトラフィックを指定します。条件には単純なものと複雑なものがあり、ライセンスによって用途が異なります。

### アクション (Action)

ルールのアクションによって、一致したトラフィックの処理方法が決まります。一致したトラフィックをモニタ、信頼、ブロック、または許可 (追加のインスペクションあり/なしで) することができます。信頼できるトラフィック、ブロックされたトラフィック、または暗号化されたトラフィックに対しては、詳細な検査は実行されません。

### インスペクション (Inspection)

詳細検査オプションは、悪意のあるトラフィックをどのように検査してブロックし、それ以外のもは許可するかを決定します。ルールを使用してトラフィックを許可するときは、システムが侵入ポリシーまたはファイルポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出たりする前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

### ログ

ルールのロギング設定によって、システムが記録する処理済みトラフィックのレコードを管理します。1つのルールに一致するトラフィックのレコードを1つ保持できます。一般的に、接続の開始時または終了時 (あるいは、その両方) にセッションをログに記録できます。接続のログは、データベースの他に、システムログ (Syslog) または SNMP トラップサーバに記録できます。

### 説明

アクセスコントロールルールで変更を保存するたびに、コメントを追加できます。

### 関連トピック

- [ルールのパフォーマンスに関するガイドライン](#) (412 ページ)
- [アクセスコントロールルールの管理](#) (1345 ページ)
- [アクセスコントロールルールの作成および編集](#) (1350 ページ)
- [ルール条件タイプ](#) (371 ページ)
- [アクセスコントロールルールのアクション](#) (1353 ページ)
- [ディープインスペクションについて](#) (1359 ページ)
- [接続ロギングストラテジー](#) (2504 ページ)

[アクセスコントロール ルールのコメント](#) (1356 ページ)

## アクセスコントロール ルールの順序

アクセスコントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で先頭から順にアクセスコントロールルールをトラフィックと照合します。

ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセスコントロールルールに従ってネットワークトラフィックを処理します。モニタールール（トラフィックをログに記録するが、トラフィックフローには影響しないルール）を除き、いずれかのルールとトラフィックが一致した後、システムは優先順位の低い追加ルールに対してトラフィックの評価を継続しません。

アクセスコントロールルールの整理に役立つように、アクセスコントロールポリシーには、システムで用意されている2つのルールセクションとして「必須 (Mandatory)」と「デフォルト (Default)」があります。さらに細かく整理するため、「必須 (Mandatory)」セクション内や「デフォルト (Default)」セクション内にカスタムルールカテゴリを作成することができます。カテゴリは、作成した後に移動することはできません。ただし、カテゴリを削除または名前変更したり、ルールをカテゴリ内またはカテゴリ間で移動したりすることはできません。システムはセクションとカテゴリに横断的にルール番号を割り当てます。

ポリシーの継承を使用する場合、現在のポリシーのルールは、その親ポリシーの「必須 (Mandatory)」ルールセクションと「デフォルト (Default)」ルールセクションの間にネストされます。ルール1は、現在のポリシーではなく、最外部ポリシーの1番目のルールです。ルールの番号は、すべてのポリシー、セクション、カテゴリにまたがって割り当てられます。

アクセスコントロールポリシーの変更を許可する定義済みユーザーロールによって、ルールのカテゴリ内またはカテゴリ間でアクセスコントロールルールを移動および変更することもできます。しかし、ユーザーがルールを移動および変更することを制限するには、カスタムロールを作成できます。アクセスコントロールポリシーの変更権限が割り当てられているユーザーは、制限なく、カスタムカテゴリにルールを追加することや、カテゴリ内のルールを変更することができます。



**ヒント** アクセスコントロールルールの順序を適切に設定することで、ネットワークトラフィック処理に必要なリソースを削減して、ルールのプリエンプションを回避できます。ユーザーが作成するルールはすべての組織と展開に固有のものです。ユーザーのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

### 関連トピック

[ルールの順序指定のガイドライン](#) (413 ページ)

## アクセス制御ルール カテゴリの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

アクセス コントロール ポリシーの必須ルールセクションとデフォルトルールセクションをカスタムカテゴリに分割できます。カテゴリを作成した後は、そのカテゴリの削除と名前の変更に加え、カテゴリへのルールの挿入、ルールの削除、カテゴリ内またはカテゴリ間のルールの移動はできますが、カテゴリ自体の移動はできません。システムはセクションとカテゴリに横断的にルール番号を割り当てます。

### 手順

- ステップ 1** アクセス コントロール ポリシー エディタで、[カテゴリの追加 (Add Category)] をクリックします。
- ヒント** ポリシーにルールがすでに含まれている場合は、既存のルールの行の空白部分をクリックして、新しいカテゴリを追加する前にその位置を設定できます。既存のルールを右クリックし、[新規カテゴリの挿入 (Insert new category)] を選択することもできます。
- ステップ 2** 名前を入力します。
- ステップ 3** [挿入 (Insert)] ドロップダウン リストから、カテゴリを追加する先を選択します。
- カテゴリをセクションのすべての既存カテゴリの下に挿入するには、[必須ルール内 (Into Mandatory)] または [デフォルトルール内 (into Default)] を選択します。
  - 既存のカテゴリの上に挿入するには、[カテゴリの上 (above category)] を選択した後、カテゴリを選択します。
  - アクセス制御ルールの上または下に挿入するには、[ルールの上 (above rule)] または [ルールの下 (below rule)] を選択した後、既存のルール番号を入力します。
- ステップ 4** [OK] をクリックします。
- ステップ 5** [保存 (Save)] をクリックしてポリシーを保存します。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## アクセスコントロール ルールの作成および編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin



**注意** アクセスコントロール ポリシーによって使用される侵入ポリシーの総数の変更 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。現在使用されていない侵入ポリシーを追加するか、侵入ポリシーの最後のインスタンスを削除することで、侵入ポリシーの総数を変更します。アクセスコントロール ルールで侵入ポリシーをデフォルトのアクションまたはデフォルトの侵入ポリシーとして使用できます。

### 手順

**ステップ 1** アクセスコントロール ポリシー エディタには、以下のオプションがあります。

- 新しいルールを追加するには、[ルールの追加 (Add Rule)] をクリックします。
- 既存のルールを編集するには、編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

**ステップ 2** 名前を入力します。

**ステップ 3** 以下のルール コンポーネントを設定するか、デフォルトを受け入れます。

- [有効 (Enabled)] : ルールを有効にするかどうかを指定します。
- [位置 (Position)] : ルールの位置を指定します。[アクセスコントロール ルールの順序 \(1348 ページ\)](#) を参照してください。
- [アクション (Action)] : ルールの [アクション (Action)] を選択します。[アクセスコントロール ルールのアクション \(1353 ページ\)](#) を参照してください。
- [条件 (Conditions)] : 追加する条件に対応するタブをクリックします。詳細は、[ルール条件タイプ \(371 ページ\)](#) を参照してください。

- [ディープインスペクション (Deep Inspection)] : 許可ルールおよびインタラクティブブロッカーの場合、侵入調査アイコン (🛡️) またはファイルおよびマルウェア調査アイコン (📁) をクリックして、ルールの [インスペクション (Inspection)] オプションを設定します。アイコンが淡色表示の場合、そのタイプのポリシーがルールに選択されていません。詳細については、[侵入ポリシーとファイルポリシーを使用したアクセス制御 \(1359 ページ\)](#) を参照してください。
- [コンテンツの制限 (Content Restriction)] : セーフサーチアイコン (🔒) または YouTube EDU アイコン (🎓) をクリックして、ルールエディタの [アプリケーション (Applications)] タブでコンテンツ制限設定を行います。アイコンが淡色表示の場合、ルールに対してコンテンツ制限は無効になっています。詳細については、[コンテンツ制限について \(1425 ページ\)](#) を参照してください。
- [ロギング (Logging)] : アクティブな (青の) ロギングアイコン (📄) をクリックして、[ロギング (Logging)] オプションを指定します。アイコンが淡色表示の場合、接続ロギングがそのルールで無効になっています。詳細については、[接続ロギング戦略 \(2504 ページ\)](#) を参照してください。
- [コメント (Comments)] : コメント列の数字をクリックして、[コメント (Comments)] を追加します。数字は、ルールにすでに含まれているコメントの数を示します。詳細については、[アクセスコントロールルールのコメント \(1356 ページ\)](#) を参照してください。

**ステップ 4** ルールを保存します。

**ステップ 5** [保存 (Save)] をクリックしてポリシーを保存します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[ルールのパフォーマンスに関するガイドライン \(412 ページ\)](#)

## アクセスコントロールルールの有効化と無効化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

アクセスコントロールルールを作成すると、そのルールはデフォルトで有効になります。ルールを無効にすると、システムはネットワークトラフィックの評価にそのルールを使用せず、そ

のルールに対する警告とエラーの生成を停止します。アクセス コントロール ポリシーのルール リストを表示したときに、無効なルールはグレー表示されますが、変更は可能です。



**ヒント** また、ルール エディタを使用してアクセス コントロール ルールを有効化または無効化することもできます。

### 手順

**ステップ 1** アクセス コントロール ポリシー エディタで、ルールを右クリックし、ルールの状態を選択します。

代わりに表示アイコン (🔍) がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

**ステップ 2** [保存 (Save) ] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[アクセス コントロール ルールのコンポーネント \(1346 ページ\)](#)

## アクセス コントロール ルールの配置

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

既存のルールは、アクセス コントロール ポリシー内で移動できますが、アクセス コントロール ポリシー間では移動できません。カテゴリにルールを追加または移動すると、そのルールはシステムによってカテゴリの最後に配置されます。



**ヒント** 複数のルールを一度に移動するには、移動するルールを選択し、右クリックメニューを使用してカット アンド ペーストします。

## 手順

**ステップ 1** アクセス制御ルール エディタには、次のオプションがあります。

- 新しいルールを追加する場合は、[挿入 (Insert)] ドロップダウンリストを使用します。
- 既存のルールを編集する場合、[移動 (Move)] をクリックします。

**ステップ 2** ルールを移動またはルールを挿入する場所を選択します。

- [必須に挿入 (into Mandatory)] または [デフォルトに挿入 (into Default)] を選択します。
- [カテゴリに挿入 (into Category)] を選択して、ユーザ定義カテゴリを選択します。
- [ルールの上 (above rule)] または [ルールの下 (below rule)] を選択してから、適切なルール番号を入力します。

**ステップ 3** [保存 (Save)] をクリックします。

**ステップ 4** [保存 (Save)] をクリックしてポリシーを保存します。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

# アクセスコントロール ルールのアクション

アクセスコントロールルールには、システムが一致するトラフィックをどのように処理し、ロギングするのかを指定するアクションがあります。モニタ、信頼、ブロック、または許可 (追加のインスペクションあり/なしで) することができます。

アクセスコントロールポリシーのデフォルトアクションは、モニタ アクセスコントロールルール以外のどの条件にも一致しないトラフィックを処理します。

## アクセスコントロール ルールのモニタ アクション

**モニタ** アクションはトラフィックフローに影響を与えません。つまり、一致するトラフィックがただちに許可または拒否されることはありません。その代わりに、追加のルールに照らしてトラフィックが照合され、許可/拒否が決定されます。モニタルール以外の一致する最初のルールが、トラフィックフローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、システムはデフォルトアクションを使用します。

モニタルールの主な目的はネットワークトラフィックのトラッキングなので、システムはモニタ対象トラフィックの接続終了イベントを自動的にログに記録します。つまり、トラフィックが他のルールに一致せず、デフォルトアクションでロギングが有効になっていない場合でも、接続はログに記録されます。



- (注) ローカル内トラフィックがレイヤ3展開のモナルールに一致する場合、そのトラフィックはインスペクションをバイパスすることがあります。トラフィックのインスペクションを確実に実行するには、トラフィックをルーティングしている管理対象デバイスの詳細設定で[ローカルルータ トラフィックの検査 (Inspect Local Router Traffic)]を有効にします。

#### 関連トピック

[モニタされた監視接続のロギング](#) (2509 ページ)

## アクセスコントロールルールの信頼アクション

[信頼 (Trust)] アクションは、ディープインスペクションやネットワーク検出をせずにトラフィックを通過させます。信頼処理されたトラフィックも、ID 条件およびレート制限の対象です。

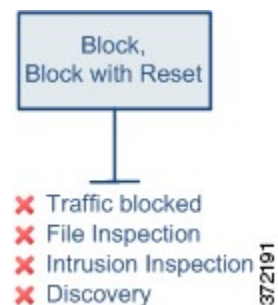


#### 関連トピック

[信頼されている接続のロギング](#) (2510 ページ)

## アクセスコントロールルールのブロックアクション

ブロックアクションおよびリセットしてブロックアクションはトラフィックを拒否し、いかなる追加のインスペクションも行われません。リセットしてブロックルールでは接続のリセットも行います。



Web リクエストをブロックした際、HTTP 応答ページを表示できます。[HTTP 応答ページとインタラクティブブロッキング](#) (1369 ページ) を参照してください。



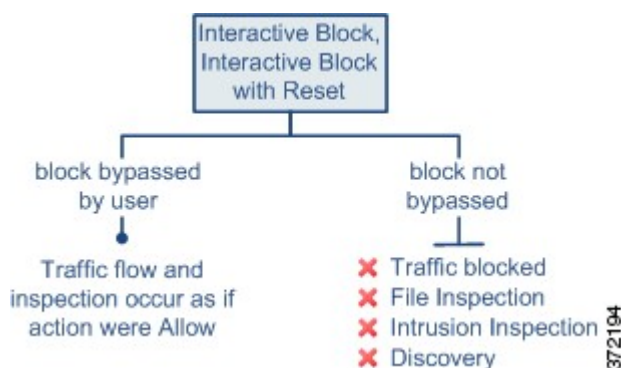
## 関連トピック

[ブロックされた接続のロギング](#) (2510 ページ)

[HTTP 応答ページについて](#) (1369 ページ)

## アクセスコントロールルールインタラクティブブロックアクション

インタラクティブブロックアクションおよびリセット付きインタラクティブブロックアクションを使用すると、ユーザはカスタマイズ可能な警告ページ (*HTTP* 応答ページと呼ばれます) をクリックスルーするか、リフレッシュすることで、Web サイトのブロックをバイパスできます。リセット付きインタラクティブブロックルールでは接続のリセットも行います。詳細については、[HTTP 応答ページとインタラクティブブロッキング](#) (1369 ページ) を参照してください。



ユーザがブロックをバイパスする場合、ルールは許可ルールを模倣します。したがって、ユーザは、どちらかのタイプのインタラクティブブロックルールをファイルポリシーと侵入ポリシーに関連付け、このユーザ許可されたトラフィックを検査できます。システムがネットワーク検出で検査することもできます。

ユーザがブロックをバイパスしない (できない) 場合は、ルールはブロックルールを模倣します。一致するトラフィックは、追加のインスペクションなしで拒否されます。

## 関連トピック

[許可された接続のロギング](#) (2512 ページ)

[SSL ルール : ブロッキングアクション](#) (1478 ページ)

## アクセスコントロールルールの許可アクション

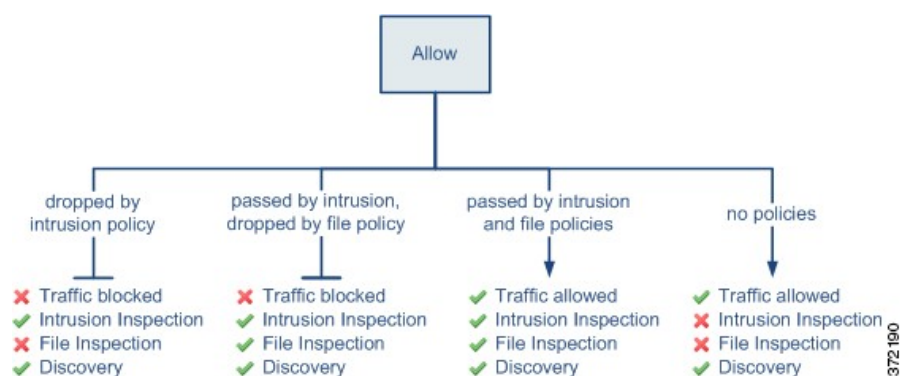
[許可 (Allow)] アクションは、一致するトラフィックを通過させます。ただし、引き続き ID 条件およびレート制限の対象となります。

任意で、ディープインスペクションを行い、トラフィックが接続先に到達する前に暗号化されていないトラフィックや復号されたトラフィックを検査、ブロックすることも可能です。

- 侵入ポリシーでは、侵入検知と防御設定に応じてネットワークトラフィックを分析し、設定内容に応じて違反パケットをドロップすることが可能です。

- ファイルポリシーでは、ファイルの制御ができます。ファイル制御により、ユーザが特定のアプリケーションプロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出およびブロックすることができます。
- ファイルポリシーでは、ネットワークベースの高度なマルウェア防御（AMP）を実行することもできます。AMP for Firepowerは設定に応じて、マルウェアがないかファイルを検査し、検出したマルウェアをブロックします。

下の図は、許可ルールの条件（またはユーザによりバイパスされるインタラクティブブロックルール）を満たすトラフィックに対して実行されるインスペクションの種類を示しています。侵入インスペクションの前にファイルインスペクションが行われることに注意してください。そこでブロックされたファイルに対しては、侵入関連の 익스プロイトについては検査されません。



シンプルにするために、この図では、侵入ポリシーとファイルポリシーの両方がアクセスコントロールルールに関連付けられている状態（またはどちらも関連付けられていない状態）のトラフィックフローを示しています。ただし、どちらか1つだけを設定することも可能です。ファイルポリシーがない場合、トラフィックフローは侵入ポリシーによって決定されます。侵入ポリシーがない場合、トラフィックフローはファイルポリシーによって決定されます。

トラフィックが侵入ポリシーとファイルポリシーのどちらかによって検査またはドロップされるかどうかに関わらず、システムはネットワーク検出を使ってトラフィックを検査できます。ただし、トラフィックを許可しても、ディスカバリ検査が自動的に保証されるわけではありません。システムは、ネットワーク検出ポリシーによって明示的にモニタされるIPアドレスを含む接続に対してのみ、ディスカバリを実行します。また、アプリケーション検出は、暗号化されたセッションに限定されます。

#### 関連トピック

[許可された接続のロギング](#) (2512 ページ)

## アクセスコントロールルールのコメント

アクセスコントロールルールを作成または編集するときは、コメントを追加できます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載するこ

とができます。あるルールの全コメントのリストを表示し、各コメントを追加したユーザやコメント追加日を確認することができます。

ルールを保存すると、最後に保存してから追加されたすべてのコメントは読み取り専用になります。

#### 関連トピック

[アクセスコントロールポリシーの設定の構成](#)

## アクセス制御ルールへのコメントの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

#### 手順

- ステップ 1 アクセスコントロールルールエディタで、[コメント (Comments)] タブをクリックします。
- ステップ 2 [New Comment] をクリックします。
- ステップ 3 コメントを入力し、[OK] をクリックします。ルールを保存するまでこのコメントを編集または削除できます。
- ステップ 4 [保存 (Save)] をクリックします。
- ステップ 5 [保存 (Save)] をクリックしてポリシーを保存します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。





## 第 55 章

# 侵入ポリシーとファイルポリシーを使用したアクセス制御

次の各トピックでは、侵入ポリシーとファイルポリシーを使用するようにアクセスコントロールポリシーを設定する方法について説明します。

- [ディープインスペクションについて \(1359 ページ\)](#)
- [アクセスコントロールトラフィック処理 \(1360 ページ\)](#)
- [ファイルインスペクションおよび侵入インスペクションの順序 \(1362 ページ\)](#)
- [ファイル制御およびマルウェア保護のためのアクセスコントロールルールの設定 \(1364 ページ\)](#)
- [侵入防御のためのアクセスコントロールルールの設定 \(1365 ページ\)](#)

## ディープインスペクションについて

侵入ポリシーとファイルポリシーは、トラフィックが宛先に対して許可される前の最後のとりでとして連携して動作します。

- 侵入ポリシーは、システムの侵入防御機能を制御します。
- ファイルポリシーは、システムのファイル制御と AMP for Firepower の機能を管理します。

アクセスコントロールはディープインスペクションの前に発生し、アクセスコントロールルールおよびアクセスコントロールのデフォルトアクションによって、侵入ポリシーおよびファイルポリシーで検査されるトラフィックが決まります。

侵入ポリシーまたはファイルポリシーをアクセスコントロールルールに関連付けることで、アクセスコントロールルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイルポリシー（またはその両方）を使ってトラフィックを検査するよう、システムに指示できます。



- (注) デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイルインスペクションは無効になっています。これにより、侵入およびファイルインスペクションが設定されたアクセスコントロールルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

システムは、AMPクラウドからエンドポイント向けAMPデータを受信し、このデータを任意のAMP for Firepowerデータと一緒に表示できます。

#### 関連トピック

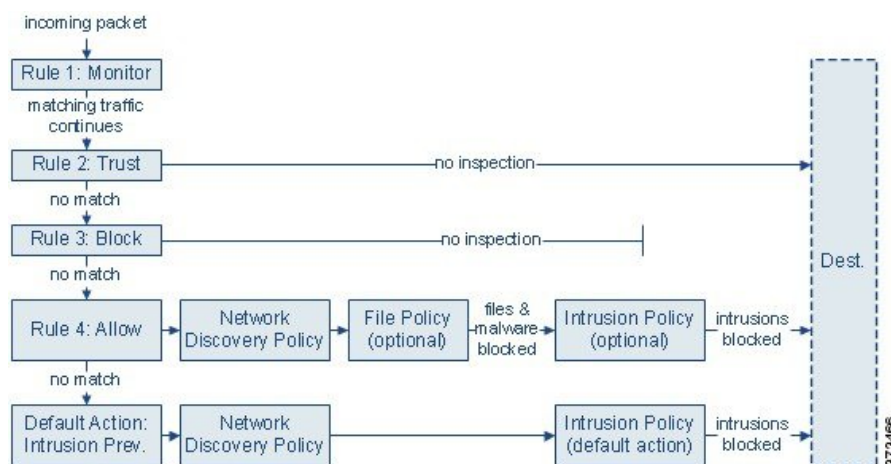
[ポリシーが侵入についてトラフィックを検査する仕組み](#) (1572 ページ)

[ファイルポリシー](#) (1535 ページ)

## アクセスコントロールトラフィック処理

アクセスコントロールルールは、複数の管理対象デバイスでネットワークトラフィックを処理する詳細な方法を提供します。システムは、指定した順にアクセスコントロールルールをトラフィックと照合します。ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセスコントロールルールに従ってネットワークトラフィックを処理します。アクセスコントロールルールのアクションによって、システムが一致するトラフィックをどのように処理するかが決まります。一致したトラフィックをモニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。

次の図は、4つの異なるタイプのアクセスコントロールルールとデフォルトアクションを含むアクセスコントロールポリシーによって制御されている、インラインの侵入防御とAMP for Firepowerの展開におけるトラフィックのフローを示します。



上記のシナリオでは、ポリシー内の最初の3つのアクセスコントロールルール（モニタ、信頼およびブロック）は一致するトラフィックを検査できません。モニタールールはネットワークトラフィックの追跡とロギングを行います。信頼ルールおよびブロックルールは、一致するトラフィックを検査し、許可または拒否を決定します。信頼ルールおよびブロックルールは、一致するトラフィックを検査し、許可または拒否を決定します。信頼ルールおよびブロックルールは、一致するトラフィックを検査し、許可または拒否を決定します。

は、どのような種類のインスペクションも追加で行うことなく一致するトラフィックを処理しますが、一致しないトラフィックは引き続き次のアクセスコントロールルールに照合されます。

ポリシー内の4番目と最後のルールである許可ルールは、次の順序で他のさまざまなポリシーを呼び出し、一致するトラフィックを検査および処理します。

- **ディスカバリ：ネットワーク検出ポリシー**：最初に、ネットワーク検出ポリシーがトラフィックのディスカバリデータの有無を検査します。ディスカバリはパッシブ分析で、トラフィックのフローに影響しません。明示的にディスカバリを有効にしなくても、それを拡張または無効にできます。ただし、トラフィックを許可しても、ディスカバリデータ収集が自動的に保証されるわけではありません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。
- **AMP for Firepower とファイル制御：ファイルポリシー**：システムは、トラフィックがディスカバリによって検査された後、トラフィックの禁止ファイルやマルウェアを検査できます。AMP for Firepower は、PDF、Microsoft Office 文書など多数のファイルタイプに潜むマルウェアを検出し、オプションでブロックできます。部門がマルウェアファイル伝送のブロックに加えて、（ファイルにマルウェアが含まれるかどうかにかかわらず）特定のタイプのすべてのファイルをブロックする必要がある場合は、ファイル制御機能により、特定のファイルタイプの伝送についてネットワークトラフィックをモニタし、ファイルをブロックまたは許可することができます。
- **侵入防御：侵入ポリシー**：ファイルインスペクションの後、システムは侵入およびエクスプロイトについてトラフィックを検査できます。侵入ポリシーは、復号されたパケットの攻撃をパターンに基づいて調査し、悪意のあるトラフィックをブロックしたり、変更したりします。侵入ポリシーは変数セットとペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映することができます。
- **接続先**：前述のすべてのチェックを通過したトラフィックは、その接続先に渡されます。

インタラクティブブロックルール（この図には表示されていません）には、許可ルールと同じインスペクションオプションがあります。これにより、あるユーザが警告ページをクリックスルーすることによってブロックされた Web サイトをバイパスした場合に、悪意のあるコンテンツがないかトラフィックを検査できます。

ポリシー内のモニタ以外のアクセスコントロールルールのいずれにも一致しないトラフィックは、デフォルトアクションによって処理されます。このシナリオでは、デフォルトアクションは侵入防御アクションとなり、トラフィックは指定された侵入ポリシーを通過する限りその最終接続先に許可されます。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルトアクションが割り当てられている場合もあります。システムはデフォルトアクションによって許可されたトラフィックに対しディスカバリデータおよび侵入の有無を検査できますが、禁止されたファイルまたはマルウェアの有無は検査できないことに注意してください。アクセスコントロールのデフォルトアクションにファイルポリシーを関連付けることはできません。



- (注) 場合によっては、接続がアクセスコントロールポリシーによって分析される場合、システムはトラフィックを処理するアクセスコントロールルール（存在する場合）を決定する前に、その接続の最初の数パケットを処理し**通過を許可する**必要があります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。

## ファイルインスペクションおよび侵入インスペクションの順序

アクセスコントロールポリシーで、複数の許可ルールとインタラクティブブロックルールを異なる侵入ポリシーおよびファイルポリシーに関連付けて、インスペクションプロファイルをさまざまなタイプのトラフィックに照合できます。



- (注) 侵入防御またはネットワーク検出のみのデフォルトアクションによって許可されたトラフィックは、検出データおよび侵入の有無について検査されますが、禁止されたファイルまたはマルウェアの有無については検査されません。アクセスコントロールのデフォルトアクションにファイルポリシーを関連付けることは**できません**。

同じルールでファイルインスペクションと侵入インスペクションの両方を実行する必要はありません。許可ルールまたはインタラクティブブロックルールに一致する接続の場合：

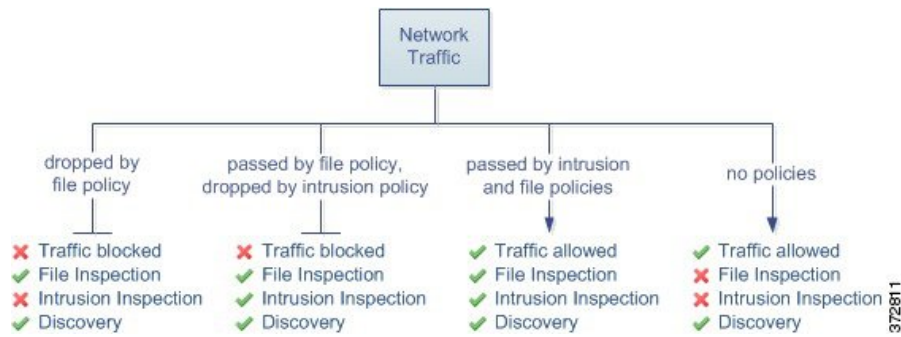
- ファイルポリシーがない場合、トラフィックフローは侵入ポリシーによって決まります
- 侵入ポリシーがない場合、トラフィックフローはファイルポリシーによって決まります
- どちらもない場合、許可されたトラフィックはネットワーク検出のみで検査されます。



- ヒント** システムは、信頼されたトラフィックに対してはどんなインスペクションも実行しません。侵入ポリシーもファイルポリシーも含めずに許可ルールを設定すると、信頼ルールの場合と同様にトラフィックが通過しますが、許可ルールでは一致するトラフィックに対して検出を実行できます。

以下の図は、「許可」アクセスコントロールルール、またはユーザによりバイパスされた「インタラクティブブロック」アクセスコントロールルールのどちらかの条件を満たすトラフィックに対して実行できるインスペクションの種類を示しています。単純化のために、侵入/ファイルポリシーの両方が1つのアクセスコントロールルールに関連付けられている（またはどちらも関連付けられていない）状態でのトラフィックフローを図に示しています。





アクセスコントロールルールによって処理される単一接続の場合、ファイルインスペクションは侵入インスペクションの前に行われます。つまり、システムは侵入のためファイルポリシーによってブロックされたファイルを検査しません。ファイルインスペクション内では、タイプによる単純なブロッキングの方が、マルウェアインスペクションおよびブロッキングよりも優先されます。

たとえば、アクセスコントロールルールで定義された特定のネットワークトラフィックを正常に許可するシナリオを考えてください。ただし、予防措置として、実行可能ファイルのダウンロードをブロックし、ダウンロードされたPDFのマルウェアインスペクションを行って検出された場合はブロックし、トラフィックに対して侵入インスペクションを実行する必要があるとします。

一時的に許可するトラフィックの特性に一致するルールを持つアクセスコントロールポリシーを作成し、それを侵入ポリシーとファイルポリシーの両方に関連付けます。ファイルポリシーはすべての実行可能ファイルのダウンロードをブロックし、マルウェアを含むPDFも検査およびブロックします。

- まず、システムはファイルポリシーで指定された単純なタイプマッチングに基づいて、すべての実行可能ファイルのダウンロードをブロックします。これはすぐにブロックされるため、これらのファイルは、マルウェアインスペクションの対象にも侵入インスペクションの対象にもなりません。
- 次に、システムは、ネットワーク上のホストにダウンロードされたPDFに対するマルウェアクラウドルックアップを実行します。マルウェアの性質を持つPDFはすべてブロックされ、侵入インスペクションの対象にはなりません。
- 最後に、システムはアクセスコントロールルールに関連付けられている侵入ポリシーを使用して、ファイルポリシーでブロックされなかったファイルを含む残りのトラフィック全体を検査します。



(注) ファイルがセッションで検出されブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

## ファイル制御およびマルウェア保護のためのアクセスコントロールルールの設定

アクセスコントロールポリシーは、複数のアクセスコントロールルールをファイルポリシーに関連付けることができます。ファイルインスペクションを許可アクセスコントロールルールまたはインタラクティブブロックアクセスコントロールルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なるファイルおよびマルウェアのインスペクションプロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムはファイルポリシーの設定に従って禁止されたファイル（マルウェアを含む）を検出すると、イベントを Firepower Management Center データベースに自動的にロギングします。ログファイルまたはマルウェア イベントが必要ない場合は、アクセスコントロールルールごとにこのロギングを無効にできます。

また、システムは、呼び出し元のアクセスコントロールルールのロギング設定にかかわらず、関連付けられた接続の終了を Firepower Management Center データベースにロギングします。

## ファイル制御および AMP を実行するアクセスコントロールルールの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (ファイル制御) マルウェア (AMP)	保護 (ファイル制御) マルウェア (AMP)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin



### 注意

[ファイルの検出 (Detect Files)] または [ファイルのブロック (Block Files)] を選択した場合、[ファイルの検出 (Detect Files)] または [ファイルのブロック (Block Files)] ルールで [ファイルの保存 (Store files)] を有効化/無効化した場合、または [マルウェアクラウドルックアップ (Malware Cloud Lookup)] または [マルウェアブロック (Block Malware)] ファイルルールアクションを分析オプション ([Spero 分析または MSEXE (Spero Analysis or MSEXE)]、[動的分析 (Dynamic Analysis)]、または [ローカルマルウェア分析 (Local Malware Analysis)] ) またはファイルの保存オプション ([マルウェア (Malware)]、[不明 (Unknown)]、[正常 (Clean)]、または [カスタム (Custom)] ) と結合する最初のファイルルールを追加または最後のファイルルールを削除した場合には、設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### 始める前に

- AMP を含むファイル制御をアクセス コントロール ルールで実行するためには、[適応型プロファイルの設定 \(2016 ページ\)](#) で説明されているように、アダプティブプロファイルを有効 (デフォルト状態) にする **必要があります**。

### 手順

- 
- ステップ 1** アクセス コントロール ルール エディタで、[許可 (Allow) ]、[インタラクティブ ブロック (Interactive Block) ]、または[リセットしてインタラクティブブロック (Interactive Block with reset) ]の[アクション (Action) ]を選択します。
- ステップ 2** [インスペクション (Inspection) ] タブをクリックします。
- ステップ 3** アクセスコントロールルールに一致するトラフィックを検査する場合は[マルウェアポリシー (Malware Policy) ] (ファイル ポリシー) を選択し、または一致するトラフィックに対するファイルインスペクションを無効にする場合は[なし (None) ]を選択します。
- ステップ 4** (オプション) [ロギング (Logging) ] タブをクリックし、[ログファイル (Log Files) ] チェックボックスをオフにして、一致する接続のファイルまたはマルウェア イベントのロギングを無効にします。
- (注) シスコでは、ファイル イベントおよびマルウェア イベントのロギングを有効のままにすることを推奨しています。
- ステップ 5** ルールを保存します。
- ステップ 6** [保存 (Save) ] をクリックしてポリシーを保存します。
- 

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

- [ファイル ポリシーの作成 \(1539 ページ\)](#)
- [Snort® の再起動シナリオ \(354 ページ\)](#)

## 侵入防御のためのアクセス コントロール ルールの設定

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールを侵入ポリシーに関連付けることができます。侵入インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なる侵入インスペクションプロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セットを使用します。セット内の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。



**ヒント** システム提供の侵入ポリシーを使用する場合であっても、正確にネットワーク環境を反映するためにシステムの侵入変数を設定することを強く推奨します。少なくとも、デフォルトセットにあるデフォルトの変数を変更します。

### システムによって提供される侵入ポリシーとカスタム侵入ポリシーについて

Firepower システムには複数の侵入ポリシーが付属しています。システム提供の侵入ポリシーを使用することで、Cisco Talos Security Intelligence and Research Group (Talos) の経験を活用できます。これらのポリシーでは、Talos が侵入ルールおよびプリプロセッサルールの状態を設定し、詳細設定の初期設定も提供します。システムによって提供されるポリシーをそのまま使用するか、またはカスタムポリシーのベースとして使用できます。カスタムポリシーを作成すれば、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。

### 接続イベントおよび侵入イベントのロギング

アクセスコントロールルールによって呼び出された侵入ポリシーが侵入を検出すると、侵入イベントを生成し、そのイベントを Firepower Management Center に保存します。また、システムはアクセスコントロールルールのロギング設定に関係なく、侵入が発生した接続の終了を Firepower Management Center データベースに自動的にロギングします。

### 関連トピック

[定義済みデフォルト変数 \(447 ページ\)](#)

## アクセスコントロールルールの設定と侵入ポリシー

ユーザが独自に作成するカスタム侵入ポリシーに加え、初期インラインポリシーと初期パッシブポリシーの2つのカスタムポリシーがシステムで用意されています。これらの2つの侵入ポリシーは、ベースとして **Balanced Security and Connectivity** 侵入ポリシーを使用します。両者の唯一の相違点は、[インライン時にドロップ (Drop When Inline)] 設定です。インラインポリシーではドロップ動作が有効化され、パッシブポリシーでは無効化されています。

1つのアクセスコントロールポリシーで使用可能な固有の侵入ポリシーの数は、ターゲットデバイスのモデルによって異なります。より強力なデバイスは、より多数のポリシーを処理できます。侵入ポリシーと変数セットの固有のペアはすべて、1つのポリシーと見なされます。異なる侵入ポリシーと変数セットのペアをそれぞれの許可ルールおよびインタラクティブブロックルール (およびデフォルトアクション) と関連付けることができますが、ターゲットデバイスが設定されたとおりに検査を実行するのに必要なリソースが不足している場合は、アクセスコントロールポリシーを展開できません。

## 侵入防御を実行するアクセスコントロールルールの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin



### 注意

アクセスコントロールポリシーによって使用される侵入ポリシーの総数の変更 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。現在使用されていない侵入ポリシーを追加するか、侵入ポリシーの最後のインスタンスを削除することで、侵入ポリシーの総数を変更します。アクセスコントロールルールで侵入ポリシーをデフォルトのアクションまたはデフォルトの侵入ポリシーとして使用できます。

### 手順

- ステップ 1** アクセスコントロールポリシーエディタで、新しいルールを作成するか、既存のルールを編集します。[アクセスコントロールルールのコンポーネント \(1346 ページ\)](#) を参照してください。
- ステップ 2** ルールアクションが [許可 (Allow) ]、[インタラクティブブロック (Interactive Block) ]、または [リセットしてインタラクティブブロック (Interactive Block with reset) ] に設定されていることを確認します。
- ステップ 3** [削除 タブ] を選択します。
- ステップ 4** システムによって提供されるまたはカスタムの侵入ポリシーを選択するか、またはアクセスコントロールルールに一致するトラフィックに対する侵入インスペクションを無効にするには [なし (None) ] を選択します。
- ステップ 5** 侵入ポリシーに関連付けられた変数セットを変更するには、[変数セット (Variable Set) ] ドロップダウンリストから値を選択します。
- ステップ 6** [保存 (Save) ] をクリックしてルールを保存します。
- ステップ 7** [保存 (Save) ] をクリックしてポリシーを保存します。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[変数セット](#) (444 ページ)

[Snort® の再起動シナリオ](#) (354 ページ)



## 第 56 章

# HTTP 応答ページとインタラクティブブロッキング

ここでは、システムが Web 要求をブロックしたときに表示されるカスタム ページの設定方法について説明します。

- [HTTP 応答ページについて \(1369 ページ\)](#)
- [HTTP 応答ページの選択 \(1371 ページ\)](#)
- [HTTP 応答ページでのインタラクティブブロッキング \(1372 ページ\)](#)

## HTTP 応答ページについて

アクセス制御の一部として、アクセスコントロールルールあるいはアクセスコントロールポリシーのデフォルトアクションを使って、システムが Web リクエストをブロックしたときに表示する *HTTP* 応答ページを設定できます。

システム提供の汎用応答ページを選択するか、カスタム HTML を入力できます。表示される応答ページはセッションのブロック方法によって異なります。

- ブロックまたはリセット付きブロックの場合、ブロックされたセッションはタイムアウトするかリセットされます。**ブロック応答ページ**により、接続が拒否されたことを示すデフォルトのブラウザ ページまたはサーバ ページは上書きされます。
- インタラクティブ ブロックまたはリセット付きインタラクティブ ブロックの場合、システムは**インタラクティブブロック応答ページ**を表示してユーザに警告しますが、ユーザはボタンをクリック (あるいはページを更新) して要求したサイトをロードできます。応答ページをバイパスした後、ロードされなかったページの要素をロードするために、ページを更新しなければならない場合があります。

システムが Web トラフィックをブロックしたときに必ず HTTP 応答ページが表示されるわけではありません。[HTTP 応答ページの制限 \(1370 ページ\)](#) を参照してください。

## HTTP 応答ページの制限

システムが Web トラフィックをブロックする場合に、常に、HTTP 応答ページが表示されるわけではありません。

### アクセスコントロールルール以外の設定

システムは、アクセスコントロールルールまたはアクセスコントロールルールのデフォルトアクションのいずれかによってブロックされた（またはインタラクティブにブロックされた）暗号化されていない接続または復号された接続の場合にのみ、応答ページを表示します。次の場合、システムは応答ページを表示しません。

- プレフィルタポリシーによってブロックされたトンネルおよびその他の接続
- セキュリティインテリジェンスによってブラックリストに載せられた接続
- SSLポリシーによってブロックされた暗号化接続

### プロモートされたアクセスコントロールルール

Web トラフィックがプロモートされたアクセスコントロールルール（単純なネットワーク条件のみの早期に適用されたブロッキングルール）の結果としてブロックされている場合、システムは応答ページを表示しません。

### URL 識別の前

システムは、システムが要求された URL を識別する前にトラフィックがブロックされた場合は、応答ページを表示しません。[URL フィルタリングの制限 \(399 ページ\)](#) を参照してください。

### 暗号化されたトラフィック

システムは、SSL ポリシーによって復号された後に、アクセスコントロールルールまたはアクセスコントロールルールのデフォルトアクションのいずれかによってブロックされた（またはインタラクティブにブロックされた）接続の場合に、応答ページを表示します。このような場合、システムは応答ページを暗号化して、再暗号化された SSL ストリームの最後にそれを送信します。

ただし、アクセスコントロールルール（または、その他の設定）によってブロックされている暗号化された接続の場合、システムは応答ページを表示しません。アクセスコントロールルールは SSL ポリシーを設定しなかった場合に暗号化された接続を評価し、それ以外の場合は、SSL ポリシーが暗号化されたトラフィックを受け渡します。

たとえば、システムは HTTP/2 または SPDY セッションを復号できません。これらのプロトコルのいずれかを使用して暗号化された Web トラフィックがアクセスコントロールルールの評価に達したが、セッションがブロックされている場合、システムは応答ページを表示しません。



## HTTP 応答ページの選択

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

HTTP 応答ページを確実に表示できるかは、ネットワーク設定、トラフィック負荷、およびページのサイズによって異なります。ページが小さいほど、正常に表示される傾向にあります。

### 手順

**ステップ 1** アクセスコントロールポリシーのエディタで、[HTTP 応答 (HTTP Responses)] タブをクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベースポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。

**ステップ 2** [応答ページをブロック (Block Response Page)] および [応答ページのインタラクティブブロック (Interactive Block Response Page)] を選択します。

- [System-provided] : 一般的な応答が表示されます。表示アイコン (🔍) をクリックすると、このページのコードが表示されます。
- [Custom] : カスタム応答ページが作成されます。ポップアップ ウィンドウが表示されます。このウィンドウに事前入力されているシステムによって提供されるコードを編集アイコン (✏️) をクリックして置換または変更できます。カウンタで使用した文字数が表示されます。
- [None] : 応答ページを無効にして、インタラクションや説明なしでセッションをブロックします。アクセスコントロールポリシー全体でインタラクティブブロッキングを無効にするには、このオプションを選択します。

**ステップ 3** [保存 (Save)] をクリックしてポリシーを保存します。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## HTTP 応答ページでのインタラクティブブロッキング

インタラクティブブロッキングを設定すると、ユーザは警告を読んだ後に当初要求したサイトを読み込むことができます。応答ページをバイパスした後、ロードされなかったページの要素をロードするために、ページを最新表示しなければならない場合があります。



**ヒント** アクセスコントロールポリシー全体に対してインタラクティブブロッキングを素早く無効にするには、システム提供のページもカスタムページも表示しないでください。そうすると、システムにより操作なしですべての接続がブロックされます。

ユーザがインタラクティブブロックをバイパスしない場合、一致するトラフィックは拒否され、追加のインスペクションは行われません。ユーザがインタラクティブブロックをバイパスするとアクセスコントロールルールはトラフィックを許可しますが、引き続きトラフィックはディープインスペクションやブロッキングの対象となる場合があります。

デフォルトでは、ユーザのバイパスは後続のアクセスで警告ページを表示することなく、10分（600秒）間有効です。期間を1年に設定したり、ユーザに毎回ブロックをバイパスするように強制できます。この制限は、ポリシー内のすべてのインタラクティブブロックルールに適用されます。ルールごとに制限を設定することはできません。

インタラクティブブロックされるトラフィックに関するロギングオプションは、許可されたトラフィックに関するオプションと同じですが、ユーザがインタラクティブブロックをバイパスしない場合、システムがログに記録できるのは接続開始イベントだけです。システムが最初にユーザに警告すると、ロギングされた接続開始イベントはシステムにより [インタラクティブブロック (Interactive Block)] または [リセットしてインタラクティブブロック (Interactive Block with reset)] アクションでマークされます。ユーザがブロックをバイパスすると、セッションが記録される追加の接続イベントに [許可 (Allow)] アクションが付きます。

## インタラクティブブロッキングの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin Access Admin Network Admin

### 手順

**ステップ1** アクセスコントロールの一部として、Webトラフィックと一致するアクセスコントロールルールを設定します。[アクセスコントロールルールの作成および編集 \(1350ページ\)](#) を参照してください。

- アクション：ルールアクションを [インタラクティブ ブロック (Interactive Block) ]、または [リセットしてインタラクティブブロック (Interactive Block with reset) ] に設定します。 [アクセスコントロールルールインタラクティブブロックアクション \(1355 ページ\)](#) を参照してください。
- 条件：URL 条件を使用して、インタラクティブにブロックする Web トラフィックを指定します。 [URL 条件 \(URL フィルタリング\) \(393 ページ\)](#) を参照してください。
- ロギング：ユーザがブロックをバイパスすると想定し、それに応じてロギングオプションを選択します。 [許可された接続のロギング \(2512 ページ\)](#) を参照してください。
- インспекション：ユーザがブロックをバイパスすると想定し、それに応じてディープインспекションオプションを選択します。 [侵入ポリシーとファイルポリシーを使用したアクセス制御 \(1359 ページ\)](#) を参照してください。

**ステップ 2** (オプション) アクセス コントロール ポリシーの [HTTP 応答 (HTTP Responses) ] タブで、カスタムインタラクティブブロックの HTTP 応答ページを選択します。 [HTTP 応答ページの選択 \(1371 ページ\)](#) を参照してください。

**ステップ 3** (オプション) アクセス コントロール ポリシーの [詳細 (Advanced) ] タブで、ユーザのバイパス タイムアウトを変更します。 [ブロックされた Web サイトのユーザバイパス タイムアウトの設定 \(1373 ページ\)](#) を参照してください。

ユーザはブロックをバイパスした後、そのページを参照でき、タイムアウト期間が経過するまで警告は表示されません。

**ステップ 4** アクセス コントロール ポリシーを保存します。

**ステップ 5** 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## ブロックされた Web サイトのユーザバイパス タイムアウトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** アクセス コントロール ポリシー エディタで、[詳細 (Advanced) ] タブをクリックします。

**ステップ 2** [全般設定 (General Settings) ] の横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する (Inherit from base policy) ] をオフにして、編集を有効にします。

**ステップ 3** [ブロックをバイパスするためのインタラクティブブロックを許可する期間 (秒) (Allow an Interactive Block to bypass blocking for (seconds)) ] フィールドに、ユーザバイパスの期限が切れるまでの経過時間を秒数で入力します。ゼロを指定すると、ユーザはブロックを毎回強制的にバイパスします。

**ステップ 4** [OK] をクリックします。

**ステップ 5** [保存 (Save) ] をクリックしてポリシーを保存します。

---

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。



## 第 57 章

# セキュリティ インテリジェンス ブラックリスト

以下のトピックでは、セキュリティインテリジェンスの概要（トラフィックのブラックリストとホワイトリストの使用、基本設定など）を示します。

- [セキュリティ インテリジェンスについて \(1375 ページ\)](#)
- [セキュリティ インテリジェンスの設定 \(1376 ページ\)](#)
- [セキュリティ インテリジェンス戦略 \(1376 ページ\)](#)
- [セキュリティ インテリジェンスの設定 \(1378 ページ\)](#)

## セキュリティ インテリジェンスについて

悪意のあるインターネットコンテンツに対する防御の前線として、セキュリティインテリジェンスは疑わしい IP アドレス、URL、ドメイン名が関連する接続をレピュテーション インテリジェンスを使用して迅速にブロックします。これは、セキュリティ インテリジェンス ブラックリスト登録と呼ばれます。

セキュリティインテリジェンスはアクセス制御の初期のフェーズであり、大量のリソースを消費する評価をシステムが実行する前に行われます。ブラックリスト登録により、インスペクションの必要がないトラフィックを迅速に除外することで、パフォーマンスが向上します。



- (注) FastPath が適用されたトラフィックをブラックリストに登録することはできません。8000 シリーズの FastPath 適用およびプレフィルタ評価は、セキュリティインテリジェンスによるフィルタリングの前に行われます。FastPath が適用されたトラフィックは、セキュリティインテリジェンスを含め、以降のすべての評価をバイパスします。

カスタムブラックリストを設定することはできますが、Cisco は定期的に更新されるインテリジェンスフィードへのアクセスを提供しています。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。

セキュリティインテリジェンスのブラックリスト登録を改良するには、ホワイトリストとモニタ専用ブラックリストを併せて使用するという方法があります。これらのメカニズムは、トラフィックをブラックリストに登録しないようにしますが、一致するトラフィックを自動的に信頼したり FastPath を適用したりすることは**しません**。ホワイトリストに登録されたトラフィックや、セキュリティインテリジェンスの段階でモニタされるトラフィックは、意図的に残りのアクセスコントロールによる分析が適用されます。

#### 関連トピック

[セキュリティインテリジェンスのリストとフィード \(464 ページ\)](#)

[設定可能な接続ロギング \(2504 ページ\)](#)

[接続およびセキュリティインテリジェンス イベント テーブルの使用 \(2548 ページ\)](#)

## セキュリティインテリジェンスの設定

特定の IP アドレス、URL、ドメイン名をホワイトリストまたはブラックリストに登録したりモニタしたりするためには、カスタムオブジェクト、リスト、またはフィードを設定する必要があります。次の選択肢があります。

- ネットワーク、URL、DNS フィールドを設定するには、[セキュリティインテリジェンス フィールドの作成 \(471 ページ\)](#) を参照してください。
- ネットワーク、URL、DNS リストを設定するには、[セキュリティインテリジェンス リストの更新 \(475 ページ\)](#) を参照してください。
- ネットワーク オブジェクトとオブジェクト グループを設定するには、[ネットワーク オブジェクトの作成 \(434 ページ\)](#) を参照してください。
- URL オブジェクトとオブジェクト グループを設定するには、[URL オブジェクトの作成 \(442 ページ\)](#) を参照してください。

DNS リストまたはフィードに基づくトラフィックのブラックリスト/ホワイトリスト登録あるいはモニタリングには、以下の条件もあります。

- DNS ポリシーを作成します。詳細については、[基本 DNS ポリシーの作成 \(1385 ページ\)](#) を参照してください。
- DNS リストまたはフィードを参照する DNS ルールを設定します。詳細については、[DNS ルールの作成および編集 \(1389 ページ\)](#) を参照してください。

DNS ポリシーはアクセスコントロールポリシーの一部として展開するため、両方のポリシーを関連付ける必要があります。詳細については、[DNS ポリシーの展開 \(1397 ページ\)](#) を参照してください。

## セキュリティインテリジェンス戦略

セキュリティインテリジェンス戦略では、次の要素を使用します。

- Cisco 提供のフィード：Cisco では、定期的に更新されるインテリジェンス フィードへのアクセスを提供しています。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。
- サードパーティのフィード：Cisco 提供のフィードをサードパーティのフィードで補完できます。これらのフィードは、Firepower Management Center が定期的にインターネットからダウンロードする動的リストです。
- グローバルおよびカスタム ブラックリスト：特定の IP アドレス、URL、ドメイン名をブラックリストに登録します。パフォーマンスを向上させるために、スパムのブラックリスト登録を電子メールトラフィックを処理するセキュリティゾーンに制限するなどして、適用対象を絞り込むこともできます。
- 誤検出をなくすためのホワイトリスト：ブラックリストの範囲が広すぎる場合、または残りのアクセスコントロールでさらに分析するトラフィックを前もってブロックしてしまう場合は、ブラックリストをカスタム ホワイトリストでオーバーライドできます。
- ブラックリスト登録に代わるモニタリング：特にパッシブ展開や、フィードを実装する前にテストする場合に有用です。違反しているセッションをブロックする代わりに単にモニタしてログに記録し、接続終了イベントを生成できます。



(注) パッシブ展開環境では、パフォーマンスを最適化するために、Cisco では常にモニタ専用の設定を使用することを推奨しています。パッシブに展開された管理対象デバイスはトラフィックフローに影響を与えることができないため、トラフィックをブロックするようにシステムを構成しても何のメリットもありません。また、ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

#### 例：ホワイトリスト登録

信頼できるフィードにより、重要なリソースへのアクセスが不適切にブロックされたものの、そのフィードが全体としては組織にとって有用である場合は、そのフィード全体をブラックリストから削除するのではなく、不適切に分類された IP アドレスだけをホワイトリストに登録するという方法を取ることができます。

#### 例：ゾーンを使用したセキュリティインテリジェンス

不適切に分類された IP アドレスをホワイトリストに登録した後、組織内でそれらの IP アドレスにアクセスする必要があるユーザが使用しているセキュリティゾーンによりホワイトリストのオブジェクトを制限するという方法が考えられます。この方法では、ビジネス ニーズを持つユーザだけが、ホワイトリストに登録された URL にアクセスできます。あるいは、サードパーティのスパムフィードを使用して、電子メールサーバのセキュリティゾーンのトラフィックをブラックリスト登録するという方法もあります。

**例：モニタ専用のブラックリスト登録**

たとえば、サードパーティのフィードを使用したブロッキングを実装する前に、そのフィードをテストする必要があるとします。フィードをモニタ専用を設定すると、ブロックされるはずの接続をシステムで詳細に分析できるだけでなく、そのような接続のそれぞれをログに記録して、評価することもできます。

## セキュリティインテリジェンスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

各アクセスコントロールポリシーには、セキュリティインテリジェンスオプションがあります。ネットワークオブジェクト、URLオブジェクトとリスト、およびセキュリティインテリジェンスフィードとリストをホワイトリストまたはブラックリストに追加でき、これらはすべてセキュリティゾーンによって制約できます。アクセスコントロールポリシーにDNSポリシーを関連付け、ドメイン名をホワイトリストまたはブラックリストに追加することもできます。

**注意**

アクセスコントロールポリシーの[セキュリティインテリジェンス (Security Intelligence)] タブからホワイトリストまたはブラックリストに複数のオブジェクトを追加したり、複数のオブジェクトを削除したりします。設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作 \(356ページ\)](#) を参照してください。Snort プロセスが再起動するかどうかは、インスペクションに使用できるメモリに応じて、デバイスごとに異なる場合がありますことに注意してください。

ホワイトリストとブラックリストには、合計255個までのネットワークオブジェクトおよび合計32767個までのURLオブジェクトとリストを追加できます。つまり、ホワイトリスト内のオブジェクトの数とブラックリスト内の数の合計が255個のネットワークオブジェクトまたは32767個のURLオブジェクトとリストを超えることはできません。

**(注)**

システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際のIPアドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。



## 始める前に

- パッシブ展開の場合、またはモニタのみにセキュリティインテリジェンスフィルタリングを設定する場合は、[ロギングを有効にします。セキュリティインテリジェンスによる接続のロギング \(2515 ページ\)](#) を参照してください。

## 手順





**ステップ 1** アクセスコントロールポリシーエディタで、[セキュリティインテリジェンス (Security Intelligence)] タブをクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベースポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。

**ステップ 2** 次の選択肢があります。

- [ネットワーク (Networks)] タブをクリックして、ネットワークオブジェクトを追加します。
- [URL (URLs)] タブをクリックして、URL オブジェクトを追加します。

**ステップ 3** ホワイトリストまたはブラックリストに追加する利用可能なオブジェクトを探します。次の選択肢があります。

- [名前または値で検索 (Search by name or value)] フィールドに入力して、利用可能なオブジェクトを検索します。[リロード (reload)] () または [クリア (clear)] () をクリックして、検索文字列をクリアします。
- 既存のリストまたはフィールドがニーズを満たしていない場合は、追加アイコン () をクリックし、[新規ネットワークリスト (New Network List)] または [新規 URL リスト (New URL List)] を選択し、[セキュリティインテリジェンス フィールドの作成 \(471 ページ\)](#) または [新しいセキュリティインテリジェンスリストの Firepower Management Center へのアップロード \(474 ページ\)](#) の説明に従って続行します。
- 既存のオブジェクトがニーズを満たしていない場合は、追加アイコン () をクリックし、[新規ネットワーク オブジェクト (New Network Object)] または [新規 URL オブジェクト (New URL Object)] を選択し、[ネットワーク オブジェクトの作成 \(434 ページ\)](#) の説明に従って続行します。

セキュリティインテリジェンスは、/0 ネットマスクを使用して、IP アドレスブロックを無視します。

**ステップ 4** 追加する 1 つ以上の利用可能なオブジェクトを選択します。

**ステップ 5** オプションで、[利用可能なゾーン (Available Zone)] を選択して、選択したオブジェクトをゾーンごとに制約します。

システムが提供するセキュリティインテリジェンスリストをゾーンで制約することはできません。

**ステップ 6** [ホワイトリストに追加 (Add to Whitelist)] または [ブラックリストに追加 (Add to Blacklist)] をクリックするか、選択したオブジェクトをクリックしていずれかのリストにドラッグします。

ホワイトリストまたはブラックリストからオブジェクトを削除するには、その削除アイコン (🗑️) をクリックします。複数のオブジェクトを削除するには、オブジェクトを選択し、右クリックして [選択項目の削除 (Delete Selected)] を選択します。

**ステップ 7** オプションで、ブラックリスト登録されたオブジェクトをモニタ専用を設定するには、[ブラックリスト (Blacklist)] にリストされている該当するオブジェクトを右クリックし、[モニタ専用 (ブロックしない) (Monitor-only (do not block))] を選択します。

システムが提供するセキュリティインテリジェンスリストをモニタ専用を設定することはできません。

**ステップ 8** [DNS ポリシー (DNS Policy)] ドロップダウンリストから DNS ポリシーを選択します。 [DNS ポリシーの概要 \(1383 ページ\)](#) を参照してください。

**ステップ 9** [保存 (Save)] をクリックします。

#### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[セキュリティインテリジェンスのリストとフィード \(464 ページ\)](#)

[Snort® の再起動シナリオ \(354 ページ\)](#)

## セキュリティインテリジェンスオプション

アクセス制御ポリシーエディタのセキュリティインテリジェンスタブを使用して、ネットワーク (IP アドレス) と URL セキュリティインテリジェンスを設定し、アクセス制御ポリシーを DNS ポリシーに関連付けます。

#### オブジェクト、ゾーン、ブラックリストアイコン

アクセス制御ポリシーエディタのセキュリティインテリジェンスタブで、オブジェクトまたはゾーンのそれぞれのタイプを別のアイコンと区別します。

ブラックリストでは、ブロックに設定したオブジェクトにはブロックアイコン (❌) を付け、監視対象のみのオブジェクトには、監視アイコン (👇) を付けます。監視のみの場合には、アクセス制御を使用して、ブラックリストの IP アドレスと URL を含む接続を処理し、ブラックリストに一致する接続をロギングします。

ホワイトリストがブラックリストをオーバーライドするため、両方のリストに同じオブジェクトを追加すると、ブラックリスト登録されたオブジェクトに取り消し線が表示されます。

### ゾーンの制約

システムが提供したグローバルリスト以外、ゾーンごとにセキュリティインテリジェンスフィルタリングを制約できます。複数のゾーンでオブジェクトのセキュリティインテリジェンスフィルタリングを適用するには、ゾーンのそれぞれについて、オブジェクトをホワイトリストまたはブラックリストに追加する必要があります。

### ログ

デフォルトで有効になっているセキュリティインテリジェンス ロギングは、アクセス制御ポリシー対象のデバイスが処理するブロックされ、監視対象である接続はすべてロギングされます。ただし、システムはホワイトリストの一致はロギングしません。ホワイトリストに登録された接続のロギングは、その接続の最終的な傾向によって異なります。ブラックリストの接続については、ブラックリスト対象のオブジェクトを監視のみに設定する前にロギングを有効にする必要があります。

### セキュリティインテリジェンス カテゴリ

セキュリティインテリジェンス カテゴリ	説明
Attacker	アクティブ スキャナと悪意のある発信アクティビティが知られているブラックリストのホスト。
Bogon	Bogon ネットワークおよび割り当てられていない IP アドレス
Bots	バイナリ マルウェア ドロップを有するサイト
CnC	botnets 用のホスト C & C サーバを有するサイト
Dga	C & C サーバのランデブーポイントとして機能するさまざまなドメイン名を生成するために使用されるマルウェア アルゴリズム
Exploitkit	クライアントのソフトウェアの脆弱性を特定するために設計されたソフトウェア キット
Malware	マルウェアバイナリまたはエクスプロイトキットを有するサイト
OpenProxy	匿名の web ブラウジングが可能な公開プロキシ
OpenRelay	スパム用に使用されることが既知のオープン メール リレー
Phishing	フィッシング ページを有するサイト
応答	悪意があるか疑わしいアクティブに積極的に参加している IP アドレスと URL
Spam	スパムを送信することが知られているメール ホスト
Suspicious	疑いがあり、既知のマルウェアと同様の特性を持つようなファイル

セキュリティインテリジェンス カテゴリ	説明
TorExitNode	Tor exit ノード

#### 関連トピック

[今すぐブラックリストに登録 (Blacklist Now) ]、[今すぐホワイトリストに登録 (Whitelist Now) ]、およびグローバルリスト (466 ページ)

セキュリティインテリジェンス リストとマルチテナンシー (468 ページ)



## 第 58 章

# DNS ポリシー

次のトピックでは、DNS ポリシーと DNS ルールについて、および管理対象デバイスに DNS ポリシーを導入する方法について説明します。

- [DNS ポリシーの概要 \(1383 ページ\)](#)
- [DNS ポリシーのコンポーネント \(1384 ページ\)](#)
- [DNS ルール \(1388 ページ\)](#)
- [DNS ポリシーの展開 \(1397 ページ\)](#)

## DNS ポリシーの概要

DNS ベースのセキュリティ インテリジェンスにより、クライアントが要求したドメイン名に基づいて、トラフィックをホワイトリスト/ブラックリストに登録できるようになります。シスコが提供するドメイン名のインテリジェンスを使用して、トラフィックをフィルタリングできます。また、環境に合わせて、ドメイン名のカスタムリストやフィードを設定することも可能です。

DNS ポリシーによってブラックリスト登録されたトラフィックは即座にブロックされるため、他のさらなるインスペクションの対象にはなりません（侵入、エクスプロイト、マルウェアなどについてだけでなくネットワーク検出についても）。ブラックリストをホワイトリストで上書きしてアクセス コントロールルールによる評価を強制することができます。また、セキュリティ インテリジェンス フィルタリングに「モニタ専用」設定を使用でき、パッシブ展開環境ではこの設定が推奨されます。この設定では、ブラックリスト登録されたであろう接続をシステムが分析できるだけでなく、ブラックリストに一致する接続がログに記録され、接続終了セキュリティ インテリジェンス イベントが生成されます。



(注) 期限切れのため、またはクライアントの DNS キャッシュやローカル DNS サーバのキャッシュがクリアされているか、期限切れであるために、DNS サーバでドメイン キャッシュが削除されない場合に、DNS ベースのセキュリティ インテリジェンスが意図したとおりに機能しないことがあります。

DNS ポリシーおよび関連付けられた DNS ルールを使用して DNS ベースのセキュリティ インテリジェンスを設定します。デバイスにこれを展開するには、アクセスコントロールポリシーに DNS ポリシーを関連付けてから管理対象デバイスに設定を展開する必要があります。

## DNS ポリシーのコンポーネント

DNS ポリシーにより、ドメイン名に基づいて、接続をホワイトリストまたはブラックリストに登録できます。次のリストに、DNS ポリシーの作成後に変更可能な設定を示します。

### 名前 (Name) と説明 (Description)

各 DNS ポリシーには固有の名前が必要です。説明は任意です。

マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

### ルール (Rule)

ルールは、ドメイン名に基づいてネットワーク トラフィックを処理する詳細な方法を提供します。DNS ポリシーのルールには1から始まる番号が付いています。システムは、ルール番号の昇順で、トラフィックを DNS ルールと上から順に照合します。

DNS ポリシーを作成すると、システムはこれをデフォルトのグローバル DNS ホワイトリストルールおよびデフォルトのグローバル DNS ブラックリストルールに入力します。両方のルールは、それぞれのカテゴリで先頭の位置に固定されます。これらのルールは変更できませんが無効にすることはできます。

マルチドメイン展開では、子孫 DNS ホワイトリストルールおよび子孫 DNS ブラックリストルールも先祖ドメインの DNS ポリシーに追加されます。これらのルールは、それぞれのカテゴリの2番目の位置に固定されます。



(注) Firepower Management Center でマルチテナンシーが有効になっている場合、システムは先祖ドメインと子孫ドメインを含むドメインの階層に編成されます。これらのドメインは、DNS 管理で使用されるドメイン名とは別になります。

子孫のリストには、Firepower システムのサブドメイン ユーザによってホワイトリストまたはブラックリストに登録されたドメインが含まれます。先祖ドメインから、子孫のリストの内容を表示することはできません。サブドメイン ユーザをホワイトリストまたはブラックリストに登録しない場合は、次を実行します。

- 子孫のリストのルールを無効にします。
- アクセス コントロール ポリシーの継承設定を使用してセキュリティ インテリジェンスを適用します。

ルールはシステムにより次の順序で評価されます。

- グローバル DNS ホワイトリスト ルール (有効な場合)
- 子孫 DNS ホワイトリスト ルール (有効な場合)
- ホワイトリスト ルール
- グローバル DNS ブラックリスト ルール (有効な場合)
- 子孫 DNS ブラックリスト ルール (有効な場合)
- ブラックリスト ルールおよびモニタ ルール

通常、システムによる DN ベースのネットワークトラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。トラフィックに一致する DNS ルールがない場合、システムは、関連付けられたアクセス コントロール ポリシー ルールに基づいてトラフィックの評価を続行します。DNS ルール条件は単純または複雑のどちらでも構いません。

## 基本 DNS ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

- ステップ 1 [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [DNS] を選択します。
- ステップ 2 [DNS ポリシーの追加 (Add DNS Policy)] をクリックします。
- ステップ 3 [名前 (Name)] に一意のポリシー名を入力し、オプションで [説明 (Description)] にポリシーの説明を入力します。
- ステップ 4 [保存 (Save)] をクリックします。

### 次のタスク

- 必要に応じて、[セキュリティインテリジェンスによる接続のロギング \(2515 ページ\)](#) の説明に従って、さらに新しいポリシーを設定します。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## DNS ポリシーの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

DNS ポリシーの編集は、1つのブラウザウィンドウを使用して、一度に1人のみで行う必要があります。複数のユーザが同じポリシーを保存を試みた場合、最初に保存された一連の変更だけが保持されます。

セッションのプライバシーを保護するために、ポリシー エディタで 30 分間操作が行われないと警告が表示されます。60 分後には、システムにより変更が破棄されます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [DNS] を選択します。

**ステップ 2** 編集する DNS ポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** DNS ポリシーを編集します。

- 名前と説明：名前または説明を変更するには、フィールドをクリックして新しい情報を入力します。
- ルール：DNS ルールを追加、分類、有効化、無効化、または管理する場合は、[ルール (Rules)] タブをクリックして、[DNS ルールの作成および編集 \(1389 ページ\)](#) の説明に従って続行します。

**ステップ 4** [保存 (Save)] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。



## DNS ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin




[DNS ポリシー (DNS Policy) ]ページ ([ポリシー (Policies) ]>[アクセスコントロール (Access Control) ]>[DNS]) を使用して、DNS のカスタム ポリシーを管理します。自分で作成したカスタム ポリシーに加えて、システムにはデフォルトの DNS ポリシーが用意されています。このポリシーは、デフォルトのブラックリストとホワイトリストを使用します。このシステム付属のカスタム ポリシーは編集して使用できます。マルチドメイン展開では、このデフォルトポリシーはデフォルトのグローバル DNS ブラックリスト、グローバル DNS ホワイトリスト、子孫 DNS ブラックリスト、および子孫 DNS ホワイトリストを使用します。また、このポリシーはグローバルドメインでのみ編集できます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

### 手順

**ステップ 1** [ポリシー (Policies) ]>[アクセスコントロール (Access Control) ]>[DNS]を選択します。

**ステップ 2** DNS ポリシーを以下のように管理します。

- 比較：DNS ポリシーを比較するには、[ポリシーの比較 (Compare Policies) ]をクリックして、[ポリシーの比較 \(361 ページ\)](#) で説明する手順を実行します。
- コピー：DNS ポリシーをコピーするには、コピーアイコン () をクリックして、[DNS ポリシーの編集 \(1386 ページ\)](#) で説明する手順を実行します。
- 作成：新しい DNS ポリシーを作成するには、[DNS ポリシーの追加 (Add DNS Policy) ]をクリックし、[基本 DNS ポリシーの作成 \(1385 ページ\)](#) で説明する手順を実行します。
- 削除：DNS ポリシーを削除するには、削除アイコン () をクリックし、ポリシーの削除を確認します。
- 編集：既存の DNS ポリシーを変更するには、編集アイコン () をクリックし、[DNS ポリシーの編集 \(1386 ページ\)](#) で説明する手順を実行します。

# DNS ルール

DNSルールは、ホストが要求するドメイン名に基づいてトラフィックを処理します。セキュリティインテリジェンスの一部として、この評価は、トラフィックの復号の後、アクセスコントロール評価の前に適用されます。

システムは指定した順序でトラフィックを DNS ルールと照合します。ほとんどの場合、システムによるネットワークトラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。DNS ルールを作成すると、システムは、モニタールールとブラックリストルールの前にホワイトリストルールを配置し、最初にホワイトリストルールに対してトラフィックを評価します。

各 DNS ルールには、一意の名前以外にも、次の基本コンポーネントがあります。

## 状態 (State)

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはネットワークトラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

## 位置 (Position)

DNSポリシーのルールには1から始まる番号が付いています。システムは、ルール番号の昇順で上から順に、トラフィックをルールと照合します。モニタールールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

## 条件 (Conditions)

条件は、ルールが処理する特定のトラフィックを指定します。DNS ルールには、DNS フィールドまたはリスト条件が含まれている必要があり、セキュリティゾーン、ネットワーク、または VLAN によってトラフィックと照合することができます。

## 操作 (Action)

ルールのアクションによって、一致したトラフィックの処理方法が決まります。

- ホワイトリストに登録されたトラフィックは許可され、アクセスコントロールによるさらなるインスペクションの対象になります。
- モニタ対象のトラフィックは、残りの DNS ブラックリストルールにより、さらなる評価の対象となります。DNS ブラックリストルールに一致しないトラフィックは、アクセスコントロールルールに検査されます。そのトラフィックのセキュリティインテリジェンスイベントは、システムにより記録されます。
- ブラックリストに登録されたトラフィックは、追加のインスペクションなしでドロップされます。[検出されないドメイン (Domain Not Found)] 応答を返すか、シンクホールサーバに DNS クエリをリダイレクトすることもできます。

## 関連トピック

[セキュリティインテリジェンスについて](#) (1375 ページ)

## DNS ルールの作成および編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

DNS ポリシーでは、ホワイトリスト ルールおよびブラックリスト ルールに合計 32767 個まで DNS リストを追加できます。つまり、DNS ポリシーのリストの数が 32767 を超えることはできません。

### 手順

**ステップ 1** DNS ポリシー エディタには、以下のオプションがあります。

- 新しいルールを追加するには、[DNS ルールの追加 (Add DNS Rule)] をクリックします。
- 既存のルールを編集するには、編集アイコン (✎) をクリックします。

**ステップ 2** 名前を入力します。

**ステップ 3** 以下のルール コンポーネントを設定するか、デフォルトを受け入れます。

- [アクション (Action)] : ルールの [アクション (Action)] を選択します。[DNS ルールのアクション \(1391 ページ\)](#) を参照してください。
- [条件 (Conditions)] : ルールの条件を設定します。[DNS ルールの条件 \(1393 ページ\)](#) を参照してください。
- [有効 (Enabled)] : ルールを有効にするかどうかを指定します。




**ステップ 4** [保存 (Save)] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## DNS ルールの管理

DNS ポリシー エディタの [ルール (Rules)] タブでは、ポリシー内の DNS ルールの追加、編集、移動、有効化、無効化、削除、その他の管理が行えます。

各ルールについて、ポリシー エディタでは、その名前、条件のサマリー、およびルールアクションが表示されます。他のアイコンにより、警告（）、エラー（）、その他の重要な情報（）が示されます。無効なルールはグレー表示され、ルール名の下に[無効 (disabled)] というマークが付きます。

## DNS ルールの有効化と無効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

作成した DNS ルールは、デフォルトで有効になっています。ルールを無効にすると、システムはネットワークトラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。DNS ポリシーのルールリストを表示すると、無効なルールはグレー表示されますが、変更は可能です。また、DNS ルールエディタを使用して DNS ルールを有効または無効にできることに注意してください。

### 手順

**ステップ 1** DNS ポリシー エディタで、ルールを右クリックしてルール状態を選択します。

**ステップ 2** [保存 (Save)] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## DNS ルールの評価順序

DNS ポリシーのルールには1から始まる番号が付いています。システムは、ルール番号の昇順で、DNS ルールを上から順にトラフィックと照合します。ほとんどの場合、システムによるネットワークトラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初のDNS ルールに従って行われます。

- モニタールールでは、システムはまずトラフィックを記録し、その後、優先順位の低いDNS ブラックリストルールに対してトラフィックの評価を続行します。
- モニタールール以外では、トラフィックがルールに一致した後、システムは優先順位の低い追加の DNS ルールに対してトラフィックの評価は続行しません。

ルールの順序については、以下の点に注意してください。

- グローバル ホワイトリストは常に先頭で、他のすべてのルールよりも優先されます。
- 子孫 DNS ホワイトリストルールは、マルチドメイン展開の非リーフドメインでのみ表示されます。これは常に2番目であり、グローバルホワイトリストを除き、他のすべてのルールよりも優先されます。
- ホワイトリストセクションはブラックリストセクションよりも優先され、ホワイトリストルールは常に他のルールよりも優先されます。
- グローバルブラックリストは常にブラックリストセクションの先頭で、他のモナールールおよびブラックリストルールよりも優先されます。
- 子孫 DNS ブラックリストルールは、マルチドメイン展開の非リーフドメインでのみ表示されます。これは常にブラックリストセクションの2番目であり、グローバルブラックリストを除き、他のすべてのモナールールおよびブラックリストルールよりも優先されます。
- ブラックリストセクションには、モナールールおよびブラックリストルールが含まれません。
- 初めて DNS ルールを作成したときは、ホワイトリストアクションを割り当てるとそれはシステムによりホワイトリストセクションの最後に配置され、他のアクションを割り当てるとブラックリストセクションの最後に配置されます。

ルールをドラッグアンドドロップして、これらの順序を変更できます。

## DNS ルールのアクション

すべての DNS ルールには、一致するトラフィックについて次のことを決定するアクションがあります。

- 処理：まずルールアクションは、システムがルールの条件に一致するトラフィックをホワイトリスト登録、モナ、またはブラックリスト登録するかどうかを制御します。
- ロギング：ルールアクションによって、一致するトラフィックの詳細をいつ、どのようにログに記録できるかが決まります。

インラインで展開されたデバイスのみがトラフィックをブラックリスト登録できることに留意してください。パッシブに展開されたデバイスまたはタップモードで展開されたデバイスは、トラフィックをホワイトリスト登録およびロギングできますが、トラフィックに影響を与えることはできません。

### [ホワイトリスト (Whitelist) ] アクション

[ホワイトリスト (Whitelist) ] アクションにより、一致するトラフィックの通過が許可されます。トラフィックをホワイトリスト登録すると、そのトラフィックは、照合するアクセスコントロールルール、またはアクセスコントロールポリシーのデフォルトアクションによるさらなるインスペクションの対象になります。

システムは、ホワイトリストの一致はロギングしません。ただし、ホワイトリストに登録された接続のロギングは、接続の最終的な傾向によって異なります。

### **[モニタ (Monitor) ]アクション**

[モニタ (Monitor) ]アクションはトラフィックフローに影響を与えません。つまり、一致するトラフィックがただちにホワイトリスト登録されたりブラックリスト登録されることはありません。その代わりに、追加のルールに照らしてトラフィックが照合され、許可/拒否が決定されます。モニタルール以外の一致する最初のDNSルールが、システムがトラフィックをブラックリスト登録するかどうかを決定します。一致する追加のルールがなければ、トラフィックはアクセスコントロール評価の対象となります。

DNS ポリシーによってモニタされる接続については、システムは、接続終了セキュリティインテリジェンスと接続イベントを Firepower Management Center データベースにロギングします。

### **[ブラックリスト (Blacklist) ]アクション**

[ブラックリスト (Blacklist) ]アクションは、いかなる種類のインスペクションなしで、トラフィックをブラックリスト登録します。

- [ドロップ (Drop) ]アクションはトラフィックをドロップします。
- [検出されないドメイン (Domain Not Found) ]アクションは、存在しないインターネットドメインの応答を DNS クエリに返し、これによりクライアントが DNS 要求を解決することを防ぎます。
- [シンクホール (Sinkhole) ]アクションは、応答内のシンクホールオブジェクトの IPv4 または IPv6 アドレスを DNS クエリに返します。シンクホールサーバは、IP アドレスへの後続の接続をロギングするか、またはロギングしてブロックすることができます。[シンクホール (Sinkhole) ]アクションを設定する場合、シンクホールオブジェクトも設定する必要があります。

[ドロップ (Drop) ]または [検出されないドメイン (Domain Not Found) ]アクションに基づいてブラックリスト登録された接続については、システムは接続開始セキュリティインテリジェンスイベントと接続イベントをロギングします。ブラックリスト登録されたトラフィックは追加のインスペクションなしですぐに拒否されるため、ログに記録できる固有の接続の終了イベントはありません。

[シンクホール (Sinkhole) ]アクションに基づいてブラックリスト登録された接続については、ロギングはシンクホールオブジェクト設定によって異なります。シンクホールオブジェクトを、シンクホール接続をロギングのみするよう設定している場合、システムは、後続の接続の接続終了イベントをロギングします。シンクホールオブジェクトを、シンクホール接続をロギングしてブロックするよう設定している場合、システムは、後続の接続の接続開始イベントをロギングし、その後、その接続をブロックします。



(注) ASA FirePOWER デバイスでシンクホールアクションを使用して DNS ルールを設定し、トラフィックがルールに一致する場合、デフォルトでは ASA によって、後続のシンクホール接続がブロックされます。回避策として、ASA コマンドラインから次のコマンドを実行します。

```
asa(config)# policy-map global_policy
asa(config-pmap)# class inspection_default
asa(config-pmap-c)# no inspect dns preset_dns_map
```

ASA が引き続き接続をブロックする場合は、サポートにお問い合わせください。

関連トピック

[アクションと接続ロギング](#) (2509 ページ)

## DNS ルールの条件

DNS ルールの条件によって、ルールが処理するトラフィックのタイプが識別されます。条件は単純または複雑のどちらでも構いません。DNS ルール内の DNS フィールドまたはリスト条件を定義する必要があります。また、必要に応じてセキュリティゾーン、ネットワーク、または VLAN によってトラフィックを制御できます。

DNS ルールに条件を追加するときは、以下に留意してください。

- ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。
- 1つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールの**すべての**条件に一致する必要があります。たとえば、DNS フィールドまたはリスト条件およびネットワーク条件を含み、VLAN タグ条件を含まないルールは、セッション中の VLAN タグに関係なく、ドメイン名と送信元または宛先に基づいてトラフィックを評価します。
- ルールの条件ごとに、最大 50 の条件を追加できます。条件の基準の**いずれか**に一致するトラフィックはその条件を満たします。たとえば、単一ルールを使用して、最大 50 の DNS リストおよびフィールドに基づいてトラフィックをブラックリスト登録できます。

## DNS およびセキュリティゾーンに基づくトラフィックの制御

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

DNS ルール内のゾーン条件によって、その送信元および宛先セキュリティゾーン別にトラフィックを制御することができます。セキュリティゾーンは、複数のデバイス間に配置されている場合がある1つ以上のインターフェイスのグループです。検出モードと呼ばれる、デバイ

その初期セットアップ時に選択するオプションによって、システムが最初にデバイスのインターフェイスをどのように設定するか、およびこれらのインターフェイスがセキュリティゾーンに属するかどうかが決まります。

### 手順

- 
- ステップ 1** DNS ルール エディタで、[ゾーン (Zones)] タブをクリックします。
- ステップ 2** [利用可能なゾーン (Available Zones)] から追加するゾーンを見つけて選択します。追加するゾーンを検索するには、[利用可能なゾーン (Available Zones)] リストの上にある [名前を検索 (Search by name)] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。
- ステップ 3** クリックして1つのゾーンを選択するか、右クリックして [すべて選択 (Select All)] を選択します。
- ステップ 4** [送信元に追加 (Add to Source)] をクリックするか、ドラッグアンドドロップします。
- ステップ 5** ルールを保存するか、編集を続けます。
- 

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## DNS およびネットワークに基づくトラフィックの制御

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

DNS ルール内のネットワーク条件によって、その送信元 IP アドレス別にトラフィックを制御することができます。制御するトラフィックに対し、明示的に送信元 IP アドレスを指定できます。

### 手順

- 
- ステップ 1** DNS ルール エディタで、[ネットワーク (Networks)] タブをクリックします。
- ステップ 2** [利用可能なネットワーク (Available Networks)] から、次のように追加するネットワークを見つけて選択します。
- ここでネットワーク オブジェクトを追加するには (後で条件に追加できます)、[利用可能なネットワーク (Available Networks)] リストの上にある追加アイコン (⊕) をクリックし、[ネットワーク オブジェクトの作成 \(434 ページ\)](#) の説明に従って進みます。



- 追加するネットワークオブジェクトを検索するには、[利用可能なネットワーク (Available Networks)] リストの上にある [名前または値で検索 (Search by name or value)] プロンプトをクリックし、オブジェクトのいずれかのコンポーネントのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

**ステップ 3** [送信元に追加 (Add to Source)] をクリックするか、ドラッグアンドドロップします。

**ステップ 4** 手動で指定する送信元 IP アドレスまたはアドレスブロックを追加します。[送信元ネットワーク (Source Networks)] リストの下にある [IP アドレスの入力 (Enter an IP address)] プロンプトをクリックし、1 つの IP アドレスまたはアドレスブロックを入力して [追加 (Add)] をクリックします。

システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

**ステップ 5** ルールを保存するか、編集を続けます。

**次のタスク**

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## DNS および VLAN に基づくトラフィックの制御

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

DNS ルールで VLAN 条件を設定すると、トラフィックの VLAN タグに応じてそのトラフィックを制御できます。システムは、最も内側の VLAN タグを使用して VLAN を基準にパケットを識別します。

VLAN ベースの DNS ルール条件を作成するときは、VLAN タグを手動で指定できます。または、VLAN タグオブジェクトを使用して VLAN 条件を設定することもできます。VLAN タグオブジェクトとは、いくつかの VLAN タグに名前を付けて再利用可能にしたものを指します。

**手順**

**ステップ 1** DNS ルールエディタで、[VLAN タグ (VLAN Tags)] タブを選択します。

**ステップ 2** [利用可能な VLAN タグ (Available VLAN Tags)] で、追加する VLAN を選択します。

- VLAN タグ オブジェクトをここで追加するには（後で条件に追加できます）、[利用可能な VLAN タグ (Available VLAN Tags) ] リストの上にある追加アイコン (+) をクリックし、[VLAN タグ オブジェクトの作成 \(440 ページ\)](#) の説明に従って進みます。
- 追加する VLAN タグ オブジェクトおよびグループを検索するには、[利用可能な VLAN タグ (Available VLAN Tags) ] リストの上にある [名前または値で検索 (Search by name or value) ] プロンプトをクリックし、オブジェクト名またはオブジェクトの VLAN タグの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

**ステップ 3** [ルールに追加 (Add to Rule) ] をクリックするか、ドラッグアンドドロップします。

**ステップ 4** 手動で指定する VLAN タグを追加します。[選択した VLAN タグ (Selected VLAN Tags) ] リストの下にある [VLAN タグの入力 (Enter a VLAN Tag) ] プロンプトをクリックし、VLAN タグまたはその範囲を入力して、[追加 (Add) ] をクリックします。1 から 4094 までの任意の VLAN タグを指定できます。VLAN タグの範囲を指定するにはハイフンを使用します。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の VLAN タグを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

**ステップ 5** ルールを保存するか、編集を続けます。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## DNS リスト、フィード、またはカテゴリに基づくトラフィックの制御

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

DNS リスト、フィード、またはカテゴリがクライアントから要求されたドメイン名を含む場合、DNS ルール内の DNS 条件によりトラフィックを制御することができます。DNS ルール内の DNS 条件を定義する必要があります。

グローバルまたはカスタムのホワイトリストまたはブラックリストを DNS 条件に追加するかどうかに関わらず、システムは設定されたルールアクションをトラフィックに適用します。たとえばルールにグローバルホワイトリストを追加し、[ドロップ (Drop) ] アクションを設定すると、システムはホワイトリスト登録されている必要があるすべてのトラフィックをブラックリスト登録します。

## 手順

**ステップ1** DNS ルール エディタで、[DNS] タブをクリックします。

**ステップ2** 次のように、[DNS リストおよびフィード (DNS Lists and Feeds) ]から追加する DNS リストおよびフィードを検索して選択します。

- DNS リストまたはフィードをここで追加するには（後で条件に追加できます）、[DNS リストおよびフィード (DNS Lists and Feeds) ]リストの上にある追加アイコン (+) をクリックし、[セキュリティインテリジェンスフィードの作成 \(471ページ\)](#) の説明に従って進みます。
- 追加する DNS リスト、フィード、またはカテゴリを検索するには、[DNS リストおよびフィード (DNS Lists and Feeds) ]リストの上にある [名前または値で検索 (Search by name or value) ]プロンプトをクリックし、オブジェクトのコンポーネントの1つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

**ステップ3** [ルールに追加 (Add to Rule) ]をクリックするか、ドラッグアンドドロップします。

**ステップ4** ルールを保存するか、編集を続けます。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350ページ\)](#) を参照してください。

## DNS ポリシーの展開

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)

DNS のポリシー設定の更新を終了した後に、アクセス コントロール設定の一部としてこれを展開する必要があります。

- [セキュリティインテリジェンスの設定 \(1378ページ\)](#) で説明されているように、DNS ポリシーをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します。[設定変更の導入 \(350ページ\)](#) を参照してください。





## 第 59 章

# プレフィルタ処理とプレフィルタポリシー

以下のトピックでは、プレフィルタを設定する方法について説明します。

- [プレフィルタの概要 \(1399 ページ\)](#)
- [プレフィルタリングとアクセスコントロール \(1400 ページ\)](#)
- [プレフィルタポリシーについて \(1404 ページ\)](#)
- [プレフィルタリングの設定 \(1405 ページ\)](#)
- [トンネルゾーンおよびプレフィルタリング \(1410 ページ\)](#)

## プレフィルタの概要

プレフィルタはアクセス制御の最初のフェーズで、システムがより大きいリソース消費の評価を実行する前に行われます。管理対象デバイスに展開されたプレフィルタポリシーは、制限付きの外側のヘッダー基準を使ってトラフィックを迅速に処理します。

内側のヘッダーを使用し、より強力なインスペクション能力を備えた他のアクセス制御とは対照的で、プレフィルタはシンプルかつ迅速で、早い段階で機能します。

プレフィルタは、以下を行う場合に設定します。

- パフォーマンスの向上：インスペクションを必要としないトラフィックの除外は、早ければ早いほど適切です。特定のタイプのプレーンテキストをファストパスまたはブロックし、カプセル化された接続を検査することなく外側のカプセル化ヘッダーに基づいてトンネルをパススルーします。早期処理のメリットがあるその他の接続についても、ファストパスやブロックをすることができます。
- カプセル化トラフィックに合わせたディープインスペクションの調整：同じ検査基準を使用してカプセル化接続を後で処理できるように、特定のタイプのトンネルを再区分できません。アクセス制御はプレフィルタ後に内側のヘッダーを使用するため、再区分は必須です。

詳細は、[プレフィルタリングとアクセスコントロール \(1400 ページ\)](#) を参照してください。

## モデル制限のプレフィルタ

Firepower システムでプレフィルタがサポートされるのは Firepower Threat Defense デバイスのみです。

クラシック デバイス（7000 および 8000 シリーズ、NGIPSv、ASA FirePOWER）にプレフィルタポリシーを展開しても、何の影響もありません。代わりに、プレフィルタとほぼ同様の機能を持つ以前から用意されてる信頼およびブロック アクセス コントロールルールを、機能の違いに留意しつつ使用してください。

以下の点にも注意してください。

- 8000 シリーズ デバイス：デバイス固有の FastPath ルールによってアクセス コントロールをバイパスできます（ただし、トラフィックをブロックすることはできません。[高速パスルールの設定（8000 シリーズ）](#)（561 ページ）を参照してください。
- クラシック デバイス：すべてのクラシック デバイスは、アクセス コントロールルールを使用して GRE でカプセル化されたトンネル全体を照合しますが、いくつかの制約事項があります。[ポートおよび ICMP コードの条件](#)（382 ページ）を参照してください。

## プレフィルタリングとアクセス コントロール

プレフィルタとアクセスコントロールポリシーのどちらを使用しても、トラフィックをブロックしたり信頼したりできますが、プレフィルタリングの「信頼」機能の方がより多くのインスペクションをスキップするため、「高速パス」と呼ばれます。次の表ではこれについて説明し、プレフィルタリングとアクセスコントロールのその他の違いを示します。これは、カスタムプレフィルタリングを設定するかどうかの決定に役立ちます。

カスタムプレフィルタリングを設定しない場合は、アクセス コントロール ポリシーに初期に配置されたブロックおよび信頼ルールにより、プレフィルタ機能に近づくことのみ可能です（複製するのではなく）。

特性	プレフィルタリング	アクセス制御	詳細
主な機能	<p>特定のタイプのプレーンテキストのパススルー トンネル（<a href="#">カプセル化の条件</a>（385 ページ）を参照）を迅速に高速パス処理またはブロックしたり、後続のインスペクションをそのカプセル化されたトラフィックに適合させたりします。</p> <p>早期処理による利点が得られる他の接続を高速パス処理またはブロックします。</p>	<p>コンテキスト情報やディープインスペクションの結果など、単純または複雑な基準を使用して、すべてのネットワークトラフィックを検査および制御します。</p>	<p><a href="#">プレフィルタの概要</a>（1399 ページ）</p>

特性	プレフィルタリング	アクセス制御	詳細
実装	<p>プレフィルタ ポリシー</p> <p>プレフィルタ ポリシーは、アクセスコントロール ポリシーによって呼び出されます。</p>	<p>アクセスコントロール ポリシー</p> <p>アクセスコントロール ポリシーは、マスター構成です。サブポリシーの呼び出しに加えて、アクセスコントロール ポリシーの独自のルールがあります。</p>	<p><a href="#">プレフィルタ ポリシーについて (1404 ページ)</a></p> <p><a href="#">アクセス制御への他のポリシーの関連付け (1340 ページ)</a></p>
アクセスコントロール内のシーケンス	<p>最初。</p> <p>トラフィックは、他のすべてのアクセスコントロール構成の前にプレフィルタ基準と照合されます。</p>	—	—
ルール アクション	<p>少ない。</p> <p>追加のインスペクションを停止したり（高速パス処理とブロック）、他のアクセスコントロールによる追加の分析を許可したり（分析）できます。</p>	<p>多い。</p> <p>アクセスコントロールルールには、モニタリング、ディープインスペクション、リセットしてブロック、インタラクティブブロッキングなどのさまざまなアクションがあります。</p>	<p><a href="#">トンネルとプレフィルタルールのコンポーネント (1408 ページ)</a></p> <p><a href="#">アクセスコントロールルールのアクション (1353 ページ)</a></p>

特性	プレフィルタリング	アクセス制御	詳細
バイパス機能	<p>高速パス ルール アクション。</p> <p>プレフィルタ段階のトラフィックの高速パス処理では、その後のすべてのインスペクションと次のような処理をバイパスします。</p> <ul style="list-style-type: none"> <li>• セキュリティインテリジェンス</li> <li>• アイデンティティポリシーによって課される認証要件</li> <li>• SSL 復号</li> <li>• アクセスコントロールルール</li> <li>• パケットペイロードのディープインスペクション</li> <li>• 検出</li> <li>• レート制限</li> </ul>	<p>信頼ルール アクション。</p> <p>アクセスコントロールルールによって信頼されるトラフィックのみがディープインスペクションとディスカバリを免除されます。</p>	<p><a href="#">アクセスコントロールルールの概要 (1343 ページ)</a></p>
ルール基準	<p>制限。</p> <p>プレフィルタポリシーのルールでは、単純なネットワーク基準、つまり IP アドレス、VLAN タグ、ポート、およびプロトコルを使用します。</p> <p>トンネルについては、トンネルエンドポイント条件によって、トンネルの両側にあるネットワーク デバイスのルーテッド インターフェイスの IP アドレスを指定します。</p>	<p>堅牢。</p> <p>アクセスコントロールルールでは、ネットワーク基準を使用しますが、パケットペイロードで利用できるユーザ、アプリケーション、要求された URL、およびその他のコンテキスト情報も使用します。</p> <p>ネットワーク条件によって、送信元と宛先ホストの IP アドレスが指定されます。</p>	<p><a href="#">トンネルとプレフィルタのルール (1407 ページ)</a></p> <p><a href="#">ルール条件タイプ (371 ページ)</a></p>



特性	プレフィルタリング	アクセス制御	詳細
IP ヘッダーの使用 (トンネル処理)	最も外側。 外部ヘッダーを使用して、プレーンテキストのパススルー トンネル全体を処理できます。 カプセル化されていないトラフィックについては、プレフィルタリングで引き続き「外部」ヘッダーが使用され、この場合は唯一のヘッダーになります。	可能な限り内側。 カプセル化されていないトンネルについては、アクセス コントロールは、トンネル全体ではなく、個々のカプセル化された接続に適用されます。	<a href="#">パススルー トンネルとアクセス制御 (1403 ページ)</a>
さらに分析するためのカプセル化された接続の再ゾーン化	トンネルされたトラフィックを再ゾーン化します。 トンネルゾーンにより、後続のインスペクションをプレフィルタされたカプセル化トラフィックに適合させることができます。	トンネルゾーンを使用。 アクセス コントロールでは、プレフィルタリング中に割り当てたトンネルゾーンを使用します。	<a href="#">トンネルゾーンおよびプレフィルタリング (1410 ページ)</a>
接続のロギング	高速パス処理およびブロックされたトラフィックのみ。許可された接続は、他の構成によってログに記録されることがあります。	任意の接続。	<a href="#">設定可能な接続ロギング (2504 ページ)</a>
サポートされるデバイス	Firepower Threat Defense のみ。	すべて。	<a href="#">モデル制限のプレフィルタ (1400 ページ)</a>

## パススルー トンネルとアクセス制御

プレーンテキスト (暗号化されていない) トンネルでは、複数の接続をカプセル化できます。これらのトンネルは、多くの場合、連続していないネットワーク間をつなぎます。したがって、IP ネットワークでカスタム プロトコルをルーティングする場合や、IPv4 ネットワークで IPv6 トラフィックをルーティングする場合などには特に役立ちます。

外側のカプセル化ヘッダーには、トンネル エンドポイント (トンネルのいずれかの側にあるネットワーク デバイスのルーテッドインターフェイス) の送信元と宛先の IP アドレスが指定されます。内側のペイロードヘッダーには、カプセル化された接続の実際のエンドポイントの送信元と宛先の IP アドレスが指定されます。

通常、ネットワーク セキュリティ デバイスは、プレーンテキスト トンネルをパススルー トラフィックとして扱います。つまり、ネットワーク セキュリティ デバイスはトンネル エンドポイントのうちの 1 つではないということです。代わりに、ネットワーク セキュリティ デバイ

スはトンネルエンドポイントの間に展開されて、それらのエンドポイント間を流れるトラフィックをモニタします。

一部のネットワークセキュリティデバイスは、外側の IP ヘッダーを使用してセキュリティポリシーを適用します。その一例は、（Firepower Threat Defense ではなく）Cisco ASA ソフトウェアを実行する Cisco ASA ファイアウォールです。プレーンテキスト トンネルの場合でも、これらのデバイスはカプセル化された個々の接続とそのペイロードを制御したりその内容を把握したりすることはできません。

それとは対照的に、Firepower システムは以下のようにアクセス制御を活用します。

- 外側のヘッダーの評価：まず、プレフィルタで外側のヘッダーを使用してトラフィックを処理します。この段階で、プレーンテキストのパススルー トンネル全体をブロックすることも、FastPath を適用することもできます。
- 内側のヘッダーの評価：次に、アクセス制御の残り（および QoS などのその他の機能）では、最も内側にあるヘッダーの検出可能レベルを使用して、可能な限り詳細なレベルでインスペクションと処理が行われるようにします。

パススルー トンネルが暗号化されていなければ、システムはこの段階で、カプセル化された個々の接続に対処します。カプセル化されたすべての接続に対処するには、トンネルの再ゾーン分割（[トンネルゾーンおよびプレフィルタリング \(1410 ページ\)](#)）を参照）を行う必要があります。

アクセス制御では、暗号化されたパススルー トンネルの内容を把握しません。たとえば、アクセス制御ルールは、パススルー VPN トンネルを 1 つの接続と見なします。システムは外側のカプセル化ヘッダーに含まれる情報だけを使用して、トンネル全体を処理します。

## プレフィルタ ポリシーについて

プレフィルタリングは、ポリシーベースの機能です。Firepower システムでは、アクセスコントロール ポリシーは、プレフィルタ ポリシーを含む、サブポリシーおよびその他の設定を呼び出すマスター設定です。

### ポリシー コンポーネント：ルールとデフォルト アクション

プレフィルタ ポリシーでは、トンネルルール、プレフィルタ ルール、デフォルトアクションに基づいてネットワーク トラフィックを処理します。

- トンネルルールとプレフィルタ ルール：最初にプレフィルタ ポリシーのルールが、指定した順序でトラフィックを処理します。トンネルルールは指定のトンネルのみを照合するもので、再ゾーニングをサポートします。プレフィルタルールはより広範囲の制約を設けるもので、再ゾーニングをサポートしていません。詳細については、[トンネルとプレフィルタのルール \(1407 ページ\)](#) を参照してください。
- デフォルトアクション（トンネルのみ）：トンネルがどのルールとも一致しない場合は、デフォルト アクションによって処理されます。デフォルト アクションは、そのトンネル

をブロックするか、あるいは個々のカプセル化された接続のアクセス制御を継続します。デフォルトアクションでトンネルの再ゾーニングを行うことはできません。

カプセル化されていないトラフィックに対するデフォルトアクションはありません。カプセル化されていない接続がどのプレフィルタルールにも一致しない場合、システムはアクセス制御を継続します。

### 接続ロギング

プレフィルタポリシーでFastPathされた接続およびブロックされた接続のログを記録することができます。[設定可能な接続ロギング \(2504 ページ\)](#) を参照してください。

接続イベントには、すべてのトンネルを含め、ロギングされる接続がプレフィルタ処理されるのかどうか、また、どのようなプレフィルタ処理を行うのかに関する情報が含まれています。この情報は、イベント表示（ワークフロー）、ダッシュボード、およびレポートで表示することができ、相関基準として使用できます。FastPathされた接続やブロックされた接続は、ディープインスペクションの対象外であるため、これらの接続に関連する接続イベントに含まれる情報は限定的となります。

### デフォルト プレフィルタ ポリシー

すべてのアクセス コントロール ポリシーにプレフィルタ ポリシーが関連付けられています。カスタム プレフィルタリングを設定しなければ、システムはデフォルト ポリシーを使用します。このシステム提供のポリシーの初期設定では、すべてのトラフィックをアクセス制御の次のフェーズに渡します。デフォルトポリシーのデフォルトアクションを変更し、ロギングのオプションを設定することはできますが、ルールの追加や削除はできません。

### プレフィルタ ポリシーの継承とマルチテナンシー

アクセス制御は、マルチテナンシーを補完する階層型実装となっています。プレフィルタポリシーの関連付けは、その他の詳細設定と同様にロックすることが可能で、これによりすべての子孫アクセス コントロール ポリシーでこの関連付けが強制的に継承されます。詳細については、[アクセス コントロール ポリシーの継承 \(1327 ページ\)](#) を参照してください。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。デフォルトプレフィルタポリシーは、グローバルドメインに属しています。

## プレフィルタリングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Admin/Access Admin/Network Admin

カスタムプレフィルタリングを実行するには、アクセスコントロールの一部として管理対象デバイスにプレフィルタポリシーを設定し、展開します。

ポリシーの編集は、1つのブラウザウィンドウを使用して、一度に1人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシーエディタが非アクティブになってから30分後に警告が表示されます。60分後には、システムにより変更が破棄されます。

## 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [プレフィルタ (Prefilter)] を選択します。

**ステップ 2** [新しいポリシー (New Policy)] をクリックして、カスタムプレフィルタポリシーを作成します。

新しいプレフィルタポリシーには、ルールや、すべてのトンネルトラフィックを分析するデフォルトアクションはありません。新しいプレフィルタポリシーでは、ロギングやトンネルの再ゾーン分割は実行されません。また、既存のポリシーをコピー (📄) したり編集 (✎) したりすることもできます。

**ステップ 3** プレフィルタポリシーのデフォルトアクションとそのロギングオプションを設定します。

- デフォルトアクション：サポートされるプレーンテキスト、パススルートンネルのデフォルトアクションを選択します。[すべてのトンネルトラフィックを分析 (Analyze all tunnel traffic)] (アクセスコントロールあり) または [すべてのトンネルトラフィックをブロック (Block all tunnel traffic)]。
- デフォルトアクションのロギング：デフォルトアクションの横にあるロギングアイコン (📄) をクリックします。[ポリシーのデフォルトアクションによる接続のロギング \(2517 ページ\)](#) を参照してください。デフォルトアクションのロギングは、ブロックされたトンネルに対してのみ設定できます。

**ステップ 4** トンネルおよびプレフィルタルールを設定します。

カスタムプレフィルタポリシーでは、両方の種類のルールを任意の順序で使用できます。照合する特定のタイプのトラフィックおよび実行するアクションまたは追加の分析に応じてルールを作成します。[トンネルとプレフィルタのルール \(1407 ページ\)](#) を参照してください。

**注意** トンネルルールを使用してトンネルゾーンを割り当てる場合は、注意してください。再ゾーン分割されたトンネルでの接続は、後の評価でセキュリティゾーンの制約に一致しない可能性があります。詳細については、[トンネルゾーンおよびプレフィルタリング \(1410 ページ\)](#) を参照してください。

ルールコンポーネントの設定の詳細については、[トンネルとプレフィルタルールのコンポーネント \(1408 ページ\)](#) および[ルール管理：共通の特性 \(369 ページ\)](#) を参照してください。

- ステップ5** ルールの順序を評価します。ルールを移動するには、クリックしてドラッグするか、または右クリックメニューを使用してカットアンドペーストを実行します。
- ルールを適切に作成して順序付けることは複雑な作業ですが、効果的な展開を構築する上で不可欠な作業です。慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、ルールに無効な設定が含まれてしまう可能性があります。詳細については、[ルールのパフォーマンスに関するガイドライン \(412 ページ\)](#) を参照してください。
- ステップ6** プレフィルタ ポリシーを保存します。
- ステップ7** トンネルゾーンの制約をサポートする設定では、再ゾーン分割されたトンネルを適切に処理します。
- トンネルゾーンを送信元ゾーンの制約として使用して、再ゾーン分割されたトンネルでの接続を照合します。[インターフェイス条件の設定 \(376 ページ\)](#) を参照してください。
- ステップ8** プレフィルタ ポリシーを管理対象デバイスに展開されたアクセス コントロール ポリシーに関連付けます。
- [アクセス制御への他のポリシーの関連付け \(1340 ページ\)](#) を参照してください。
- ステップ9** 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## トンネルとプレフィルタのルール

トンネルとプレフィルタのどちらのルールを設定するかは、照合するトラフィックのタイプと、実行するアクションや詳細な分析によって異なります。

特性	トンネル ルール	プレフィルタ ルール
主な機能	プレーンテキストのパススルー トンネルをすばやく高速パス化、ブロック、または再ゾーニングします。	初期段階の操作の影響を受ける他の接続をすばやく高速パス化またはブロックします。
カプセル化とポート/プロトコル条件	カプセル化の条件は、 <a href="#">カプセル化の条件 (385 ページ)</a> にリストされる選択済みプロトコルについて、プレーンテキスト トンネルのみと照合されます。	ポート条件では、トンネルルールより広範囲のポートおよびプロトコル制約を使用できます。 <a href="#">ポートおよび ICMP コードの条件 (382 ページ)</a> を参照してください。
ネットワーク条件	トンネルエンドポイント条件は、処理対象にするトンネルのエンドポイントを制約します。 <a href="#">トンネルエンドポイント条件 (380 ページ)</a> を参照してください。	ネットワーク条件は、各接続の送信元ホストと宛先ホストを制約します。 <a href="#">ネットワーク条件 (377 ページ)</a> を参照してください。

特性	トンネル ルール	プレフィルタ ルール
方向 (Direction)	双方向または単方向 (構成可)。 トンネルルールはデフォルトで双方向であるため、トンネルエンドポイント間のすべてのトラフィックを処理できます。	単方向のみ (構成不可)。 プレフィルタルールは、送信元から宛先へ送信されるトラフィックのみと照合されます。
詳細分析のためのセッションの再ゾーニング	トンネルゾーンを使用する場合にサポートされます。トンネルゾーンおよびプレフィルタリング (1410 ページ) を参照してください。	未サポート

## トンネルとプレフィルタ ルールのコンポーネント

### 状態 (有効/無効)

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

### 位置

ルールの番号は1から始まります。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、ルールタイプ (トンネルまたはプレフィルタ) に関係なく、そのトラフィックを処理するルールです。

### 操作

ルールのアクションによって、一致したトラフィックの処理とログ記録の方法が決まります。

- **[高速パス (Fastpath)]** : アクセス制御、ID 要件、レート制限を含む、すべての詳細な検査および制御の対象から、一致するトラフィックを除外します。トンネルを高速パス化すると、すべてのカプセル化された接続が高速パス化されます。
- **[ブロック (Block)]** : どのような種類の検査も行わずにトラフィックを照合します。トンネルをブロックすると、カプセル化されたすべての接続がブロックされます。
- **[分析 (Analyze)]** : 残りのアクセス制御で内部ヘッダーを使用して引き続きトラフィックを分析できるようにします。アクセス制御および関連するディープインスペクションによって渡された場合、このトラフィックはレート制限も行われる場合があります。トンネルルールの場合、[トンネルゾーンの割り当て (Assign Tunnel Zone)] オプションを指定して、再ゾーニングを有効にします。

### 方向 (トンネル ルールのみ)

トンネルルールの方向によって、システムの送信元と宛先の条件に従った処理方法が決まります。

- 送信元からのトンネルのみを照合します（単方向）。送信元から宛先へ送信されるトラフィックのみを照合します。一致するトラフィックは、指定された送信元インターフェイスまたはトンネルエンドポイントから発信され、宛先インターフェイスまたはトンネルエンドポイントを通過する必要があります。
- 送信元と宛先からのトンネルを照合します（双方向）。送信元から宛先へ送信されるトラフィックと宛先から送信元へ送信されるトラフィックの両方を照合します。この効果は、単方向のルールを2つ作成した場合と同じで、一方のルールがもう一方のルールのミラーとなります。

プレフィルタ ルールは常に単方向です。

### トンネル ゾーンの割り当て（トンネル ルールのみ）

トンネル ルールで、トンネル ゾーン（既存のゾーンまたはオンザフライで作成したゾーン）を割り当てると、一致するゾーンが再ゾーニングされます。再ゾーニングするには、分析アクションが必要です。

トンネルを再ゾーニングすると、アクセス制御ルールなどの他の構成で、すべてのトンネルのカプセル化された接続の所属先が同じであると認識させることができます。トンネルに割り当てられたトンネルゾーンをインターフェイスの制約として使用すると、カプセル化された接続に合わせた検査を実行することができます。詳細については、[トンネルゾーンおよびプレフィルタリング（1410 ページ）](#)を参照してください。



#### 注意

トンネル ゾーンを割り当てるときには注意が必要です。再ゾーニングされたトンネルの接続は、後から実行される評価でセキュリティゾーンの制約と一致しないことが検出される可能性があります。トンネルゾーン実装の簡単なワークスルーと、再ゾーニングするトラフィックを明示的に処理せずに再ゾーニングする理由については、[トンネルゾーンの使用（1411 ページ）](#)を参照してください。

### 条件（Conditions）

条件は、ルールが処理する特定のトラフィックを指定します。トラフィックは、ルールのすべての条件と一致し、ルールと一致する必要があります。各条件の種類には、ルールエディタ内に独自のタブがあります。

トラフィックをプレフィルタするには、次の外部ヘッダー制約を使用します。

- インターフェイス：[インターフェイス条件（374 ページ）](#)
- ネットワーク：[トンネルエンドポイント条件（380 ページ）](#) または [ネットワーク条件（377 ページ）](#)
- ポート：[カプセル化の条件（385 ページ）](#) または [ポートおよびICMP コードの条件（382 ページ）](#)
- VLAN：[VLAN 条件（382 ページ）](#)

トンネルルールは、カプセル化プロトコルで制約する必要があります。

## ログ

システムが記録する処理済みトラフィックのレコードは、ルールのロギング設定によって管理します。

トンネルとプレフィルタのルールでは、高速パスが適用されたトラフィックとブロックされたトラフィック（[高速パス（Fastpath）]と[ブロック（Block）]のアクション）をログに記録することができます。詳細分析（[分析（Analyze）]アクション）の対象となるトラフィックでは、一致する接続が他の構成で記録されている可能性があります。プレフィルタポリシーでのログ記録は無効になります。詳細については、[トンネルルールおよびプレフィルタルールによる接続のロギング（2513 ページ）](#)を参照してください。

## 説明

ルールで変更を保存するたびに、コメントを追加することができます。たとえば、他のユーザーのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。

ルールを保存した後で、これらのコメントを編集または削除することはできません。

## 関連トピック

[ルールのパフォーマンスに関するガイドライン（412 ページ）](#)

# トンネルゾーンおよびプレフィルタリング

トンネルゾーンを使用すれば、プレフィルタリングを使って後続のトラフィック処理をカプセル化された接続に合わせるすることができます。

システムは通常最も内側の検出可能なレベルのヘッダーを使用してトラフィックを処理するため、特殊なメカニズムが必要になります。これにより、可能な限りきめ細かなインスペクションが保証されます。ただし、これは、パススルートンネルが暗号化されていない場合、システムは個々のカプセル化された接続に対して処理を行うことも意味しています。[パススルートンネルとアクセス制御（1403 ページ）](#)を参照してください。

トンネルゾーンはこの問題を解決します。アクセス制御の最初のフェーズ（プレフィルタリング）で、特定のタイプのプレーンテキスト、パススルートンネルを識別するために、外側のヘッダーを使用することができます。次に、それらのトンネルは、カスタムトンネルゾーンを割り当てることで再ゾーン化できます。

トンネルを再ゾーン化すると、アクセスコントロールルールなどの他の設定で、そのトンネルのすべてのカプセル化された接続をグループとして認識できます。トンネルの割り当てられたトンネルゾーンをインターフェイスの制約として使用することで、インスペクションをそのカプセル化された接続に合わせて調整できます。

トンネルゾーンは、その名称にもかかわらず、セキュリティゾーンではありません。トンネルゾーンは、インターフェイスの一式を表すわけではありません。トンネルゾーンは、場合によっては、カプセル化された接続に関連付けられているセキュリティゾーンに置き換わるタグとして考える方がより正確です。





**注意** トンネルゾーンの制約をサポートする設定の場合、再ゾーン化されたトンネル内の各接続はセキュリティゾーンの制約とは一致しません。たとえば、トンネルを再ゾーン化した後、アクセスコントロールルールでは、そのカプセル化された各接続を、それらの新しく割り当てられたトンネルゾーンと突き合わせることはできませんが、元のセキュリティゾーンと突き合わせることはできません。

トンネルゾーンの導入の簡潔なウォークスルー、および再ゾーン化されたトラフィックを明示的に処理せずに再ゾーン化することの影響の説明については、[トンネルゾーンの使用 \(1411 ページ\)](#) を参照してください。

### トンネルゾーンの制約をサポートする設定

トンネルゾーンの制約をサポートするのは、アクセスコントロールルールだけです。

他のどの設定もトンネルゾーンの制約をサポートしません。たとえば、QoSを使用してプレーンテキスト トンネル全体をレート制限することはできず、個々のカプセル化されたセッションをレート制限できるだけです。

## トンネル ゾーンの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Firepower Threat Defense	任意 (Any)	Admin/Access Admin/Network Admin

この例の手順は、トンネルゾーンを使用してさらに分析するために GRE トンネルを再ゾーン化する方法をまとめたものです。この例で説明されている概念は、プレーンテキストのパススルー トンネルにカプセル化された接続に合わせてトラフィック インспекションを調整する必要があるシナリオにも適応できます。

組織の内部トラフィックが信頼済みセキュリティゾーンを通過する FirePOWER システムの展開について考えてみましょう。信頼済みセキュリティゾーンは、さまざまな場所に展開された複数の管理対象デバイス間における一連のセンシングインターフェイスを表します。組織のセキュリティ ポリシーでは、エクスプロイトとマルウェアのディープ インспекション後の内部トラフィックを許可する必要があります。

内部トラフィックには、特定のエンドポイント間のプレーンテキストのパススルー GRE トンネルが含まれている場合があります。このカプセル化されたトラフィックのトラフィック プロファイルは、「通常」の局間アクティビティとは異なるため（おそらく既知かつ無害）、セキュリティ ポリシーに従いながら、特定のカプセル化された接続のインспекションを制限できます。

この例では、構成の変更を展開した後、次のようになります。

- 信頼済みゾーンで検出されたプレーンテキストのパススルーGREカプセル化トンネルは、個別のカプセル化接続が1セットの侵入およびファイルポリシーによって評価されます。
- 信頼済みゾーンの他のすべてのトラフィックは、侵入およびファイルポリシーの別のセットで評価されます。

このタスクは、GREトンネルの再ゾーン化によって実行します。再ゾーン化を実行すると、アクセスコントロールによって、GREカプセル化接続が元の信頼済みセキュリティゾーンではなくカスタムトンネルゾーンに関連付けられます。再ゾーン化が必要になるのは、FirePOWERシステムとアクセスコントロールが、カプセル化されたトラフィックを処理する方法によります。パススルートンネルとアクセス制御 (1403 ページ) およびトンネルゾーンおよびプレフィルタリング (1410 ページ) を参照してください。

## 手順

- ステップ 1** カプセル化されたトラフィック向けのディープインスペクションを実行するカスタムの侵入およびファイルポリシーを設定し、カプセル化されていないトラフィックには別の侵入およびファイルポリシーのセットを設定します。
- ステップ 2** 信頼済みセキュリティゾーンを通過する GRE トンネルを再ゾーン化するようにカスタムプレフィルタリングを設定します。

カスタムプレフィルタポリシーを作成し、アクセスコントロールに関連付けます。そのカスタムプレフィルタポリシーで、トンネルルール (この例では `GRE_tunnel_rezone`) と対応するトンネルゾーン (`GRE_tunnel`) を作成します。詳細については、[プレフィルタリングの設定 \(1405 ページ\)](#) を参照してください。

表 82: `GRE_tunnel_rezone` トンネルルール

ルールコンポーネント	説明
インターフェイスオブジェクト条件	信頼済みセキュリティゾーンを送信元インターフェイスオブジェクトと宛先インターフェイスオブジェクトの両方の制約として使用して、内部のみのトンネルを照合します。
トンネルエンドポイント条件	組織で使用されている GRE トンネルの送信元と宛先のエンドポイントを指定します。  トンネルルールは、デフォルトでは双方向です。[トンネルの照合 (Match tunnels from) ] オプションを変更しない場合は、どのエンドポイントを送信元として指定し、どのエンドポイントを宛先として指定するかは重要ではありません。
カプセル化条件	GRE トラフィックを照合します。
トンネルゾーンの割り当て	<code>GRE_tunnel</code> トンネルゾーンを作成し、ルールに一致するトンネルに割り当てます。
操作	(残りのアクセスコントロールで) 分析します。

**ステップ 3** 再ゾーン化されたトンネルの接続を処理するようにアクセス コントロールを設定します。

管理対象デバイスに展開されたアクセス コントロール ポリシーでは、再ゾーン化したトラフィックを処理するルール（この例では**GRE\_inspection**）を設定します。詳細については、[アクセス コントロール ルールの作成および編集（1350 ページ）](#)を参照してください。

表 83: **GRE\_inspection** アクセス コントロール ルール

ルールコンポーネント	説明
セキュリティゾーン条件	<b>GRE_tunnel</b> セキュリティゾーンを送信元ゾーン制約として使用して、再ゾーン化されたトンネルを照合します。 <a href="#">インターフェイス条件（374 ページ）</a> を参照してください。
操作	ディープ インスペクションを有効にして許可します。 カプセル化された内部トラフィックのインスペクションを実行するように調整されたファイルおよび侵入ポリシーを選択します。

**注意** この手順をスキップすると、再ゾーン化された接続は、セキュリティゾーンによって制約されていない**任意の**アクセス コントロール ルールに一致する場合があります。再ゾーン化された接続がどのアクセス コントロール ルールにも一致しない場合は、アクセス コントロール ポリシーのデフォルト アクションによって処理されます。意図してそのようにしていることを確認してください。

**ステップ 4** 信頼済みセキュリティゾーンを通過するカプセル化されていない接続を処理するようにアクセス コントロールを設定します。

同じアクセス コントロール ポリシーで、信頼済みセキュリティゾーン内の再ゾーン化されていないトラフィックを処理するルール（この例では**internal\_default\_inspection**）を設定します。

表 84: **internal\_default\_inspection** アクセス コントロール ルール

ルールコンポーネント	説明
セキュリティゾーン条件	信頼済みセキュリティゾーンを送信元ゾーンと宛先ゾーンの両方の制約として使用して、再ゾーン化されていない内部のみのトラフィックを照合します。
操作	ディープ インスペクションを有効にして許可します。 カプセル化されていない内部トラフィックのインスペクションを実行するように適合されたファイルおよび侵入ポリシーを選択します。

**ステップ 5** 既存のルールに対して相対的な新しいアクセス コントロールルールの位置を評価します。ルールの順序を必要に応じて変更します。

2つの新しいアクセスコントロールルールを隣同士に配置した場合は、最初にどちらを配置するかは重要ではありません。GREトンネルを再ゾーン化したため、2つのルールは互いをプリエンプション処理することはできません。

**ステップ6** すべての変更された構成を保存します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## トンネルゾーンの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Admin/Access Admin/Network Admin

#### 手順

**ステップ1** [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。

**ステップ2** オブジェクトタイプのリストから [トンネルゾーン (Tunnel Zone)] を選択します。

**ステップ3** [トンネルゾーンの追加 (Add Tunnel Zone)] をクリックします。

**ステップ4** [名前 (Name)] を入力し、必要に応じて [説明 (Description)] を入力します。

**ステップ5** [保存 (Save)] をクリックします。

#### 次のタスク

- カスタム事前フィルタリングの一部として、トンネルゾーンをプレーンテキストのパススルートンネルに割り当てます。[プレフィルタリングの設定 \(1405 ページ\)](#) を参照してください。



## 第 60 章

# インテリジェント アプリケーション バイパス

次のトピックでは、インテリジェントアプリケーションバイパス (IAB) を使用するようにアクセス コントロール ポリシーを設定する方法について説明します。

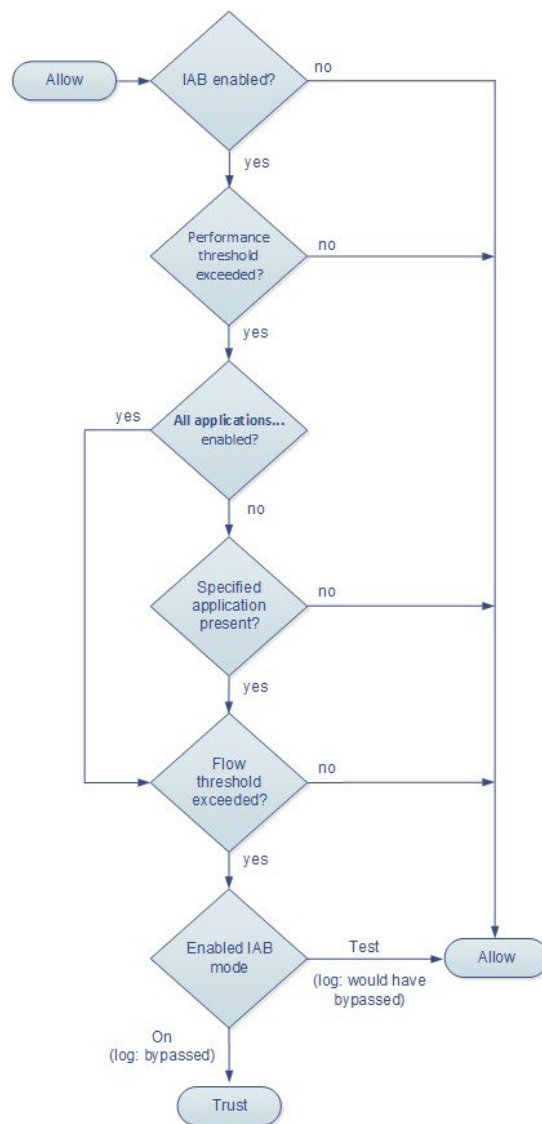
- [IAB の概要 \(1415 ページ\)](#)
- [IAB オプション \(1416 ページ\)](#)
- [IAB の設定 \(1418 ページ\)](#)
- [IAB のロギングと分析 \(1420 ページ\)](#)

## IAB の概要

IAB は、パフォーマンスとフローのしきい値を超過した場合に追加のインスペクションなしでネットワークを通過する信頼されるアプリケーションを特定します。たとえば、毎晩のバックアップがシステム パフォーマンスに大きく影響する場合、しきい値を超えてもバックアップアプリケーションが生成したトラフィックを信頼するように設定できます。オプションで、インスペクション パフォーマンスしきい値を超過したときに、IAB が、いずれかのフローバイパスしきい値を超えるすべてのトラフィックをアプリケーションのタイプに関係なく信頼するように IAB を設定できます。このオプションには、バージョン 6.1.0.3 または後続の 6.1.0.x パッチが必要です。

IAB は、アクセス コントロールルールまたはアクセス コントロールポリシーのデフォルトアクションによって許可されるトラフィックに対し、トラフィックが詳細なインスペクションの対象となる前に実行されます。テストモードでは、しきい値を超過しているかどうか判断することと、しきい値を超過している場合、IAB を実際に有効化している状態 (バイパスモードといいます) であればバイパスされたであろうアプリケーションフローを特定することが可能です。

次の図は、IAB の決定プロセスを示します。



## IAB オプション

### 状態

IAB を有効または無効にします。

### パフォーマンス サンプル インターバル (Performance Sample Interval)

システムが IAB パフォーマンスしきい値との比較のためにシステム パフォーマンス メトリックを収集する IAB パフォーマンス サンプリング スキャンの間隔を秒単位で指定します。値を 0 にすると、IAB が無効になります。

## バイパス可能なアプリケーションとフィルタ (Bypassable Applications and Filters)

この機能には、相互に排他的な、次の2つのオプションがあります。

### アプリケーション/フィルタ (Applications/Filters)

バイパス可能なアプリケーションおよびアプリケーション (フィルタ) のセットを指定できるエディタが提供されます。アプリケーション条件 (アプリケーション制御) (386ページ) を参照してください。

### 未確認アプリケーションを含むすべてのアプリケーション

インスペクションパフォーマンスしきい値を超過すると、アプリケーションのタイプに関係なく、いずれかのフローバイパスしきい値を超過するすべてのトラフィックを信頼します。このオプションを使用するにはバージョン 6.1.0.3 またはそれ以降の 6.1.0.x パッチが必要です。

## 検査パフォーマンスしきい値 (Inspection Performance Thresholds)

検査パフォーマンスしきい値は、侵入検査パフォーマンスの限界を提供し、これを超えるとフローしきい値の検査が開始されます。IAB は、0 に設定されている検査パフォーマンスしきい値を使用しません。



- (注) インスペクションパフォーマンスしきい値とフローバイパスしきい値は、デフォルトでは無効化されています。IAB がトラフィックを信頼するには、少なくともいずれか1つを有効化し、いずれか1つを超過している必要があります。インスペクションパフォーマンスしきい値またはフローバイパスしきい値を複数有効にした場合、IAB がトラフィックを信頼するには、いずれか1つのみを超過する必要があります。

## ドロップ率 (Drop Percentage)

消費が激しい侵入ルール、ファイルポリシー、圧縮解除などによってパフォーマンス過負荷となったためにパケットがドロップされた場合にドロップされたパケットが、パケット全体に占める割合の平均。侵入ルールのような通常の設定によってドロップされるパケットは含まれません。1 より大きい整数を指定すると、指定された割合のパケットがドロップされると IAB がアクティブになることに注意してください。1 を指定すると、0 ~ 1 の任意の割合によって IAB がアクティブになります。これにより、少数のパケットで IAB をアクティブにすることができます。

## プロセッサ使用率 (Processor Utilization Percentage)

プロセッサ リソースの平均使用率。

## パケット遅延 (Package Latency)

マイクロ秒単位の平均パケット遅延。

## フロー レート (Flow Rate)

1秒あたりのフロー数で測定される、システムによるフロー処理率。このオプションでは、IAB は、フローを件数ではなくレートで測定するように設定されることに注意が必要です。

### フローバイパスしきい値 (Flow Bypass Thresholds)

フローバイパスしきい値ではフロー制限が提供され、これを超えると、IAB がバイパスモードでバイパス可能なアプリケーショントラフィックを信頼するようにトリガーされるか、またはテストモードで追加の検査を受けるアプリケーショントラフィックが許可されます。IAB は、0 に設定されているフローバイパスしきい値を使用しません。



- (注) インспекションパフォーマンスしきい値とフローバイパスしきい値は、デフォルトでは無効化されています。IAB がトラフィックを信頼するには、少なくともいずれか1つを有効化し、いずれか1つを超過している必要があります。インспекションパフォーマンスしきい値またはフローバイパスしきい値を複数有効にした場合、IAB がトラフィックを信頼するには、いずれか1つのみを超過する必要があります。

#### フローあたりのバイト数

フローに含めることができる最大サイズ (KB)。

#### フローあたりのパケット数

フローに含めることができるパケットの最大個数。

#### フロー継続時間

フローをオープンのままにできる最長時間 (秒)。

#### フロー速度

最大転送速度 (KB/秒)。

## IAB の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Admin Access Admin Network Admin



- 注意** すべての展開に IAB が必要なわけではありません。IAB を使用する展開では、限定的な方法で IAB を使用する場合があります。ネットワークトラフィック (特にアプリケーショントラフィック) とシステムパフォーマンス (予測可能なパフォーマンスの問題を含む) の専門知識がある場合を除き、IAB を有効化しないでください。バイパスモードで IAB を実行する前に、指定したトラフィックを信頼してもリスクが発生しないことを確認します。



## 手順

**ステップ 1** アクセスコントロールポリシーエディタで[詳細 (Advanced)] タブをクリックし、[インテリジェントアプリケーションバイパス設定 (Intelligent Application Bypass Settings)] の横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベースポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。

**ステップ 2** IAB のオプションを設定します。

- [状態 (State)] : IAB を [オフ (Off)] または [オン (On)]、あるいは [テスト (Test)] モードで有効にします。
- パフォーマンス サンプル間隔 (Performance Sample Interval) : IAB のパフォーマンス サンプリング スキャンの間隔を秒単位で入力します。IAB を有効にした場合は、テストモードであっても、ゼロ以外の値を入力します。0 を入力すると、IAB は無効になります。
- バイパス可能なアプリケーションとフィルタ (Bypassable Applications and Filters) : 次のいずれかを実行します。
  - バイパスされるアプリケーションとフィルタの数をクリックし、トラフィックをバイパスするアプリケーションを指定します。[アプリケーション条件とフィルタの設定 \(387 ページ\)](#) を参照してください。
  - [未確認アプリケーションを含むすべてのアプリケーション (All applications including unidentified applications)] をクリックし、インスペクションパフォーマンスしきい値を超過したときに、IAB が、いずれかのフローバイパスしきい値を超えるすべてのトラフィックをアプリケーションのタイプに関係なく信頼するように設定します。このオプションを使用するにはバージョン 6.1.0.3 またはそれ以降の 6.1.0.x パッチが必要です。
- [インスペクションパフォーマンスしきい値 (Inspection Performance Thresholds)] : [設定 (Configure)] をクリックし、1 つ以上のしきい値を入力します。
- [フローバイパスしきい値 (Flow Bypass Thresholds)] : [設定 (Configure)] をクリックし、1 つ以上のしきい値を入力します。

少なくとも 1 つのインスペクションパフォーマンスしきい値と 1 つのフローバイパスしきい値を指定する必要があります。IAB がトラフィックを信頼するには、両方を超過している必要があります。各タイプに複数のしきい値を入力した場合、いずれか 1 つのタイプのみを超過する必要があります。詳細については、[IAB オプション \(1416 ページ\)](#) を参照してください。

**ステップ 3** [OK] をクリックして IAB 設定を保存します。

**ステップ 4** [保存 (Save)] をクリックしてポリシーを保存します。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

# IAB のロギングと分析

IABは、接続ロギングを有効にしたかどうかを問わず、バイパスされたフローやバイパスされることが予想されるフローをロギングする接続終了イベントを強制します。接続イベントは、バイパスモードでバイパスされたフロー、またはテストモードでバイパスされることが予想されるフローを示します。接続イベントに基づいたカスタムのダッシュボードウィジェットやレポートでは、バイパスされたフローおよびバイパスされることが予想されるフローの長期的な統計情報を表示できます。

## IAB の接続イベント

### アクション (Action)

[理由 (Reason) ]に[インテリジェントアプリケーションバイパス (Intelligent App Bypass) ]が含まれる場合：

許可 (Allow)：

適用された IAB 設定がテストモードであり、[アプリケーションプロトコル (Application Protocol) ]によって指定されたアプリケーションのトラフィックが、インスペクション用に使用可能のままであることを示します。

信頼する (Trust)：

適用された IAB 設定がバイパスモードであり、[アプリケーションプロトコル (Application Protocol) ]によって指定されたアプリケーションのトラフィックが信頼されているため、それ以上インスペクションが行われずにネットワークを通過することを示します。

### 理由 (Reason)

[インテリジェントアプリケーションバイパス (Intelligent App Bypass) ]は、IAB がバイパスモードまたはテストモードでイベントをトリガーしたことを示します。

### アプリケーションプロトコル (Application Protocol)

このフィールドには、イベントをトリガーしたアプリケーションプロトコルが表示されません。

## 例

次の省略された図では、一部のフィールドが省かれています。図は、2つの別個のアクセスコントロールポリシーの異なる IAB 設定から生成された2つの接続イベントの[アクション (Action) ]、[理由 (Reason) ]、および[アプリケーションプロトコル (Application Protocol) ]フィールドを示しています。

最初のイベントの場合、[信頼する (Trust)] アクションは、IAB がバイパス モードで有効にされており、Bonjour プロトコル トラフィックが信頼されているため、それ以上インスペクションが行われずに受け渡されることを示します。

2 番目のイベントの場合、[許可 (Allow)] アクションは、IAB がテスト モードで有効にされているため、Ubuntu Update Manager トラフィックはさらにインスペクションが行われる必要がありますが、IAB がバイパス モードであればバイパスされることが予想されることを示します。

Action ×	Reason ×	Application × Protocol
Trust	Intelligent App Bypass	<input type="checkbox"/> Bonjour
Allow	Intelligent App Bypass	<input type="checkbox"/> Ubuntu Update Manager

404483

## 例

次の省略された図では、一部のフィールドが省かれています。2 番目のイベントのフローは両方とも ([アクション (Action)]: [信頼する (Trust)], [理由 (Reason)]: [インテリジェントアプリケーションバイパス (Intelligent App Bypass)]) をバイパスし、侵入ルール ([理由 (Reason)]: [侵入モニタ (Intrusion Monitor)]) によって検査されました。[侵入モニタ (Intrusion Monitor)] の理由は、[イベントの生成 (Generate Events)] に設定された侵入ルールが検出されたが、接続時にエクスプロイトをブロックしなかったことを示しています。この例では、これはアプリケーションが検出される前に発生しました。アプリケーションが検出された後、IAB は、アプリケーションがバイパス可能であると認識し、フローを信頼しました。

Last Packet ×	Action ×	Reason ×	Application × Protocol
2015-06-12 10:53:09	Trust	Intelligent App Bypass	<input type="checkbox"/> Skype Probe
2015-06-12 10:53:08	Trust	Intelligent App Bypass, Intrusion Monitor	<input type="checkbox"/> HTTP

404541

## IAB のカスタム ダッシュボード ウィジェット

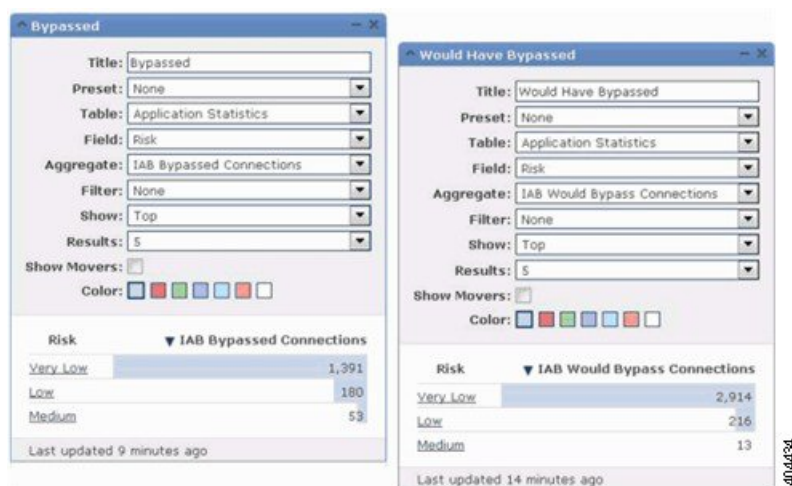
接続イベントに基づいて長期的な IAB の統計情報を表示するカスタム分析ダッシュボード ウィジェットを作成できます。ウィジェットを作成する際には、次の項目を指定します。

- プリセット (Preset) : なし (None)
- テーブル (Table) : アプリケーションの統計 (Application Statistics)
- フィールド (Field) : 任意 (any)
- 集約 (Aggregate) : 次のいずれか
  - IAB が接続をバイパスした (IAB Bypassed Connections)
  - IAB が接続をバイパスすることが予想された (IAB Would Bypass Connections)
- フィールド (Field) : 任意 (any)

## 例

次のカスタム分析ダッシュボードウィジェットの例では、次のようになっています。

- 「*Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセスコントロールポリシーにおいてバイパスモードで有効になっているためにバイパスされたアプリケーショントラフィックの統計を示しています。
- 「*Would Have Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセスコントロールポリシーにおいてテストモードで有効になっているためにバイパスされることが予想されたアプリケーショントラフィックの統計を示しています。



## IAB のカスタム レポート

接続イベントに基づいて長期的な IAB の統計情報を表示するカスタム レポートを作成できます。レポートを作成するには、次の項目を指定します。

- テーブル (Table) : アプリケーションの統計 (Application Statistics)
- プリセット (Preset) : なし (None)
- フィールド (Field) : 任意 (any)
- X 軸 (X-Axis) : 任意 (any)
- Y 軸 (Y-Axis) : 以下のいずれか
  - IAB が接続をバイパスした (IAB Bypassed Connections)
  - IAB が接続をバイパスすることが予想された (IAB Would Bypass Connections)

## 例

次の図は、2つのレポートの例の抜粋を示します。

- 「*Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセスコントロールポリシーにおいてバイパスモードで有効になっているためにバイパスされたアプリケーショントラフィックの統計を示しています。
- 「*Would Have Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセスコントロールポリシーにおいてテストモードで有効になっているためにバイパスされることが予想されたアプリケーショントラフィックの統計を示しています。



## 関連トピック

[接続およびセキュリティ インテリジェンス イベントフィールド \(2523 ページ\)](#)

[\[カスタム分析 \(Custom Analysis\) \] ウィジェット \(254 ページ\)](#)

[ダッシュボードへのウィジェットの追加 \(266 ページ\)](#)

[レポート テンプレート \(2307 ページ\)](#)





## 第 61 章

# コンテンツ制限を使用したアクセス制御

次のトピックでは、コンテンツ制限機能を使用するようにアクセス コントロール ポリシーを設定する方法について説明します。

- [コンテンツ制限について \(1425 ページ\)](#)
- [アクセス コントロール ルールを使用したコンテンツ制限の実施 \(1427 ページ\)](#)
- [DNS シンクホールを使用したコンテンツ制限の実施 \(1430 ページ\)](#)

## コンテンツ制限について

主要な検索エンジンやコンテンツ配信サービスは、検索結果と Web サイトのコンテンツを制限できる機能を提供しています。たとえば学校では、「子どもをインターネットから保護する法律」(CIPA) を順守するために、コンテンツ制限機能を使用します。

コンテンツ制限機能は、検索エンジンやコンテンツ配信サービスで実行する場合には、個々のブラウザやユーザを対象にしか実施できません。Firepower システムは、これらの機能をご使用のネットワーク全体に拡大できます。

このシステムにより、以下を実施できます。

- **セーフサーチ**：多くの主要な検索エンジンでサポートされているこのサービスは、ビジネス、行政、および教育の環境で不愉快であると分類されている、露骨なアダルト向けコンテンツを除外します。システムは、サポートされている検索エンジンのホームページへのユーザのアクセス機能は制限しません。
- **YouTube EDU**：このサービスは、教育環境向けに YouTube コンテンツをフィルタリングします。これにより学校は、教育的なコンテンツへのアクセスを設定しながら、非教育的なコンテンツへのアクセスを制限できます。YouTube EDU は YouTube 制限付きモードとは別の機能であり、Google のセーフサーチ機能の一部として YouTube 検索に対する制限を実施します。YouTube 制限付きモードは、セーフサーチのサブ機能であることに注意してください。YouTube EDU を使用すると、ユーザは標準の YouTube ホームページではなく、YouTube EDU ホームページにアクセスします。

次の 2 つの方法を使用して、これらの機能を実施するようにシステムを設定できます。

**方法：アクセスコントロールルール**

コンテンツ制限機能は、検索またはコンテンツクエリの制限状態を、要求 URI の要素、関連する Cookie、またはカスタム HTTP ヘッダー要素により通信します。システムがトラフィックを処理するときに、これらの要素を変更するためのアクセスコントロールルールを設定できます。

**方法：DNS シンクホール**

Google 検索では、セーフサーチ（YouTube 制限付きモードを含む）のフィルタを課す Google SafeSearch 仮想 IP アドレス（VIP）にトラフィックをリダイレクトするように、システムを設定できます。

次の表では、これらの実施方法の違いについて説明します。

表 85: コンテンツ制限方法の比較

属性 (Attribute)	方法：アクセスコントロールルール	方法：DNS シンクホール
サポートされるデバイス	任意 (Any)	Firepower Threat Defense のみ
[サポートされる検索エンジン (Search engines supported) ]	ルールエディタの [アプリケーション (Applications) ] タブのタグ付きのすべての safesearch supported	Google のみ
[サポートされる YouTube 制限付きモード (YouTube Restricted Mode supported) ]	○	○
[サポートされる YouTube EDU (YouTube EDU supported) ]	[はい (Yes) ]	[いいえ (No) ]
[SSL ポリシーが必要 (SSL policy required) ]	[はい (Yes) ]	[いいえ (No) ]
[ホストは IPv4 の使用が必要 (Hosts must be using IPv4) ]	なし	○
[接続イベントロギング (Connection event logging) ]	○	○

使用する方法を決定する際には、次の制限事項を考慮します。

- アクセスコントロールルール方法には SSL ポリシーが必要で、これはパフォーマンスに影響を及ぼします。
- Google セーフサーチ VIP は IPv4 トラフィックのみをサポートします。Google 検索を管理するように DNS シンクホールを設定する場合は、影響を受けるネットワークのすべてのホストが IPv4 を使用している必要があります。

接続イベントの [理由 (Reason) ] フィールドに、方法に応じて異なる値がログ記録されます。



- アクセスコントロールルール：[コンテンツの制限（Content Restriction）]
- DNS シンクホール：[DNS ブロック（DNS Block）]

## アクセスコントロールルールを使用したコンテンツ制限の実施

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin



**注意**

ルールのプリエンブションを避けるため、SSL とアクセスコントロールポリシーの両方で、YouTube EDU を制御するルールは、セーフサーチを制御するルールの上に配置します（[コンテンツ規制ルールの順序（416 ページ）](#) を参照）。

**手順**

**ステップ 1** SSL ポリシーを作成します（[基本 SSL ポリシーの作成（1462 ページ）](#) を参照）。

**ステップ 2** セーフサーチと YouTube EDU のトラフィックを処理するための SSL ルールを追加します。

- ルールの [アクション (Action)] として [復号-再署名 (Decrypt-Resign)] を選択します。システムは、コンテンツ制限処理にこれ以外のアクションをサポートしません。
- [アプリケーション (Applications)] タブで、選択内容を [選択済みのアプリケーションとフィルタ (Selected Applications and Filters)] リストに追加します。
  - YouTube EDU：YouTube と YouTube Upload アプリケーションを追加します。
  - セーフサーチ：[カテゴリ：検索エンジン (Category: search engine)] フィルタを追加します。

詳細については、[SSLルールへのアプリケーション条件の追加（1504ページ）](#) を参照してください。

**ステップ 3** 追加した SSL ルールのための、ルールの位置を設定します。クリックしてドラッグするか、または右クリックメニューを使用してカットアンドペーストを実行します。

プリエンブションを避けるため、セーフサーチルールを YouTube EDU ルールの後に配置します。

**ステップ4** アクセスコントロールポリシーを作成または編集して、SSLポリシーとアクセスコントロールポリシーを関連付けます。

詳細については、[アクセス制御への他のポリシーの関連付け \(1340ページ\)](#) を参照してください。

**ステップ5** アクセスコントロールポリシーに、セーフサーチと YouTube EDU トラフィックを処理するためのルールを追加します。

- ルールの [アクション (Action)] として [許可 (Allow)] を選択します。システムは、コンテンツ制限処理にこれ以外のアクションは許可しません。
- [アプリケーション (Applications)] タブで、セーフサーチ (🔒) または YouTube EDU (🔒) のいずれかの淡色表示されているアイコンをクリックして、関連オプションを設定します ([アクセス制御ルールのセーフサーチオプション \(1429ページ\)](#) および [アクセス制御ルールの YouTube EDU オプション \(1429ページ\)](#) を参照)。

ルールの [アクション (Action)] に [許可 (Allow)] 以外を選択すると、これらのアイコンは淡色表示されるのではなく無効になります。

同じアクセスコントロールルールに対してセーフサーチと YouTube EDU の制限を有効にすることはできません。

- [アプリケーション (Applications)] タブで、[選択済みのアプリケーションとフィルタ (Selected Applications and Filters)] リストのアプリケーション選択を絞り込みます。  
たいいていの場合、セーフサーチまたは YouTube EDU を有効にすると、[選択済みのアプリケーションとフィルタ (Selected Applications and Filters)] リストに適切な値が入力されます。セーフサーチまたは YouTube アプリケーションを有効にしたときにそれらの機能がすでにリストにある場合、システムはリストへの自動入力を行いません。予期したとおりにアプリケーションが入力を行わない場合は、それらを以下のように手動で追加します。
  - YouTube EDU : YouTube と YouTube Upload アプリケーションを追加します。
  - セーフサーチ : [カテゴリ : 検索エンジン (Category: search engine)] フィルタを追加します。

詳細については、[アプリケーション条件とフィルタの設定 \(387ページ\)](#) を参照してください。

**ステップ6** 追加したアクセスコントロールルールに対してルールの位置を設定します。クリックしてドラッグするか、または右クリックメニューを使用してカットアンドペーストを実行します。

プリエンプションを避けるため、セーフサーチルールを YouTube EDU ルールの後に配置します。

**ステップ7** システムが制限付きコンテンツをブロックするときに表示する HTTP 応答ページを設定します ([HTTP 応答ページの選択 \(1371ページ\)](#) を参照)。

**ステップ8** 設定変更を展開します。[設定変更の導入 \(350ページ\)](#) を参照してください。

## アクセス制御ルールのセーフサーチ オプション

Firepower System は、特定の検索エンジンのセーフサーチ フィルタリングにのみ対応していません。対応している検索エンジンのリストについては、アクセス制御ルールエディタの [アプリケーション (Applications) ] タブのアプリケーションにタグ付けされている safesearch supported を参照してください。対応していない検索エンジンのリストについては、アプリケーションにタグ付けされている safesearch を参照してください。

アクセス制御ルールのセーフサーチを有効にするには、次のパラメータを設定します。

### セーフサーチの有効化 (Enable Safe Search)

このルールに一致するトラフィックに対して、セーフサーチフィルタリングを有効にします。

### サポートされない検索トラフィック (Unsupported Search Traffic)

対応していない検索エンジンからのトラフィックを処理する場合は、システム上でのアクションを指定します。[ブロック (Block) ] または [リセットによるブロック (Block with Reset) ] を選択すると、いつ制限されたコンテンツをブロックするかを表示する HTTP 応答ページを設定する必要があります。[HTTP 応答ページの選択 \(1371 ページ\)](#)

## アクセス制御ルールの YouTube EDU オプション

アクセスコントロールルールに対して YouTube EDU を有効にするには、次のパラメータを設定します。

### YouTube EDU の有効化 (Enable YouTube EDU)

このルールに一致するトラフィックに対して、YouTube EDU フィルタリングを有効にします。

### カスタム ID (Custom ID)

学校または地域のネットワークを固有に識別する値を YouTube EDU イニシアチブに指定します。YouTube は、学校または地域が YouTube EDU アカウントの登録をすると、この ID を提供します。



(注) [YouTube EDU の有効化 (Enable YouTube EDU) ] をオンにした場合は、[カスタム ID (Custom ID) ] を入力する必要があります。この ID は、YouTube によって外部に定義されます。システムは、YouTube システムに対するユーザの入力内容は検証しません。無効な ID を入力すると、YouTube EDU の制限が予期したとおりに実行されない場合があります。

## DNS シンクホールを使用したコンテンツ制限の実施

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	Firepower Threat Defense	任意 (Any)	Admin/Access Admin/Network Admin

通常、DNS シンクホールは、トラフィックを特定のターゲットからそらしめます。この手順では、Google セーフサーチ仮想 IP アドレス (VIP) にトラフィックをリダイレクトする (つまり、Google と YouTube の検索結果にコンテンツフィルタを適用する) ように DNS シンクホールを設定する方法について説明します。

Google セーフサーチは VIP に単一の IPv4 アドレスを使用するため、ホストは IPv4 アドレッシングを使用する必要があります。



### 注意

ネットワークにプロキシサーバが含まれる場合、Firepower Threat Defense デバイスをプロキシサーバとインターネットの間に配置しない限り、この方法でのコンテンツ制限は効果的ではありません。

この手順では、Google 検索のみにコンテンツ制限を適用する方法について説明します。他の検索エンジンに対してコンテンツ制限を適用する場合は、[アクセスコントロールルールを使用したコンテンツ制限の実施 \(1427 ページ\)](#) を参照してください。

### 手順

**ステップ 1** 次の URL を使用して、サポートされる Google ドメインのリストを取得します。

[https://www.google.com/supported\\_domains](https://www.google.com/supported_domains)

**ステップ 2** ローカル コンピュータにカスタム DNS リストを作成し、次のエントリを追加します。

- Google セーフサーチを適用するには、サポートされる Google ドメインごとにエントリを追加します。
- YouTube 制限モードを適用するには、「youtube.com」エントリを追加します。

カスタム DNS リストは、テキストファイル (.txt) 形式にする必要があります。テキストファイルの各行に、先頭ピリオドを除いた状態で、個々のドメイン名を指定する必要があります。たとえば、サポートされるドメインが「google.com」の場合、「google.com」として指定する必要があります。

**ステップ 3** カスタム DNS リストを Firepower Management Center にアップロードします ([新しいセキュリティインテリジェンスリストの Firepower Management Center へのアップロード \(474 ページ\)](#) を参照)。

**ステップ 4** Google セーフサーチ VIP の IPv4 アドレスを判別します。たとえば、forcesafesearch.google.com で nslookup を実行します。

**ステップ 5** セーフサーチ VIP のシンクホール オブジェクトを作成します ([シンクホール オブジェクトの作成 \(476 ページ\)](#) を参照)。

このオブジェクトでは、次の値が使用されます。

- [IPv4 アドレス (IPv4 Address) ] : セーフ サーチ VIP アドレスを入力します。
- [IPv6 アドレス (IPv6 Address) ] : IPv6 ループバック アドレスを入力します (::1) 。
- [ログをシンクホールに接続する (Log Connections to Sinkhole) ] : このラジオ ボタンをクリックします。
- [タイプ (Type) ] : [なし (None) ] を選択します。

**ステップ 6** 基本 DNS ポリシーを作成します ([基本 DNS ポリシーの作成 \(1385 ページ\)](#) を参照) 。

**ステップ 7** シンクホールの DNS ルールを追加します ([DNS ルールの作成および編集 \(1389 ページ\)](#) を参照) 。

このルールでは、

- [有効 (Enabled) ] チェックボックスをオンにします。
- [アクション (Action) ] ドロップダウン リストから [シンクホール (Sinkhole) ] を選択します。
- [シンクホール (Sinkhole) ] ドロップダウン リストから、作成したシンクホール オブジェクトを選択します。
- 作成したカスタム DNS リストを [DNS] タブの [選択した項目 (Selected Items) ] リストに追加します。
- (オプション) [ネットワーク (Networks) ] タブでネットワークを選択し、コンテンツ制限を特定のユーザに限定します。たとえば、学生ユーザにコンテンツ制限を限定したい場合、学生を教員とは別のサブネットに割り当て、このルールにそのサブネットを指定します。

**ステップ 8** アクセス コントロール ポリシーと DNS ポリシーを関連付けます ([アクセス制御への他のポリシーの関連付け \(1340 ページ\)](#) を参照) 。

**ステップ 9** 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。





## 第 **XVI** 部

### 暗号化トラフィックの処理

- [トラフィック復号の概要 \(1435 ページ\)](#)
- [SSL ポリシーの使用を開始するには \(1457 ページ\)](#)
- [SSL ルールの使用を開始するには \(1467 ページ\)](#)
- [SSL ルールを使用した復号の調整 \(1489 ページ\)](#)







## 第 62 章

# トラフィック復号の概要

以下のトピックではSSLインスペクションの概要を示し、SSLインスペクション設定の前提条件と詳細な導入シナリオについて説明します。

- [トラフィックの復号の概要 \(1435 ページ\)](#)
- [SSL ハンドシェイク処理 \(1436 ページ\)](#)
- [SSL インスペクションの要件 \(1441 ページ\)](#)
- [SSL インスペクション アプライアンス導入シナリオ \(1442 ページ\)](#)

## トラフィックの復号の概要

Firepower システムは、デフォルトではセキュア ソケット レイヤ (SSL) プロトコルまたはその後継である Transport Layer Security (TLS) プロトコルで暗号化されたトラフィックを検査できません。SSL インスペクション (検査) 機能を使用すると、暗号化トラフィックのインスペクションを実行せずにブロックしたり、暗号化または復号されたトラフィックをアクセスコントロール (制御) を使用して検査したりできます。システムは、暗号化されたセッションを処理する際にトラフィックに関する詳細をログに記録します。暗号化トラフィックのインスペクションと暗号化セッションのデータ分析を組み合わせることで、ネットワーク内の暗号化されたアプリケーションやトラフィックをより詳細に把握したり制御したりできます。

SSL インスペクションは、ポリシーベースの機能です。FirePOWER システムでは、アクセスコントロールポリシーは、SSL ポリシーを含む、サブポリシーおよびその他の設定を呼び出すマスター設定です。アクセスコントロールと SSL ポリシーを関連付ければ、システムはアクセスコントロールルールで評価する前に、その SSL ポリシーを使用して暗号化セッションを処理します。SSL インスペクションを設定していない場合、またはデバイスがサポートしていない場合、アクセスコントロールルールは、すべての暗号化トラフィックを処理します。

暗号化されたトラフィックの通過が SSL インスペクション設定で許可される場合、そのトラフィックがアクセスコントロールルールによって処理されることにも注意してください。ただし、一部のアクセスコントロールルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、システムは暗号化ペイロードの侵入およびファイルインスペクションを無効にしています。これにより、侵入およびファイルインスペクションが設定されたアクセス

コントロールルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

システムで TCP 接続での SSL ハンドシェイクが検出された場合、その検出されたトラフィックを復号できるかどうか判定されます。復号できない場合は、設定されたアクションが適用されます。以下のアクションを設定できます。

- 暗号化トラフィックをブロックする
- 暗号化トラフィックをブロックし、TCP 接続をリセットする
- 暗号化されたトラフィックを復号しない

システムによるトラフィックの復号が可能な場合、システムでは、それ以上のインスペクションを行わずにトラフィックをブロックするか、復号されていないトラフィックをアクセスコントロールによって評価するか、または次のいずれかの方法を使用して復号します。

- 既知の秘密キーを使用して復号する。外部ホストがネットワーク上のサーバとの SSL ハンドシェイクを開始すると、交換されたサーバ証明書とアプライアンスにアップロード済みのサーバ証明書が照合されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号します。
- サーバ証明書の再署名によって復号する。ネットワーク上のホストが外部サーバとの SSL ハンドシェイクを開始すると、システムによって、交換されたサーバ証明書が、アップロード済みの認証局 (CA) 証明書で再署名されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号します。

復号されたトラフィックに対しては、はじめから暗号化されていないトラフィックと同じトラフィックの処理と分析 (ネットワーク、レピュテーション、およびユーザベースの各アクセスコントロール、侵入検知と防御、Cisco Advanced Malware Protection (Cisco AMP)、およびディスカバリ (検出)) が実行されます。システムで、復号されたトラフィックのポスト分析をブロックしない場合、トラフィックを再暗号化してから宛先ホストに渡します。

## SSL ハンドシェイク処理

このマニュアルでは、SSL ハンドシェイクという用語は SSL プロトコルとその後継プロトコルである TLS の両方の暗号化セッションを開始する、2 ウェイ ハンドシェイクを表します。

パッシブ展開では、FirePOWER システムはハンドシェイクのコピーを確認しますが、実際のハンドシェイクを処理しません。インライン展開では、FirePOWER システムは SSL ハンドシェイクを処理し、ClientHello メッセージを修正する可能性があり、セッションの TCP プロキシサーバとして機能します。

(正常に TCP 3 ウェイ ハンドシェイクが完了した後) クライアントがサーバとの TCP 接続を確立すると、管理対象デバイスは TCP セッションでの暗号化されたセッションの開始の試行をモニタします。SSL ハンドシェイクは、クライアントとサーバ間の特殊なパケットの交換によって、暗号化セッションを確立します。SSL と TLS プロトコルでは、これらの特殊なパケッ

トはハンドシェイク メッセージと呼ばれます。ハンドシェイク メッセージは、クライアントとサーバの両方がサポートする暗号化属性を伝えます。

- **ClientHello** : クライアントは各暗号化属性に複数のサポートされる値を指定します。
- **ServerHello** : サーバはシステムがセキュリティで保護されたセッション中に使用する暗号化方式を決定する、各暗号化属性に 1 つのサポートされる値を指定します。

セッション中に伝送されるデータは暗号化されますが、ハンドシェイク メッセージは暗号化されません。

SSL ハンドシェイクが完了すると、管理対象デバイスは暗号化セッションデータをキャッシュに保存し、それによりフルハンドシェイクを必要とせずにセッションを再開できます。管理対象デバイスもサーバ証明書データをキャッシュに保存し、それにより後続のセッションでのより速いハンドシェイクの処理が可能になります。

## ClientHello メッセージ処理

セキュアな接続が確立できる場合、クライアントはパケットの宛先として機能するサーバに ClientHello メッセージを送信します。クライアントは SSL ハンドシェイクを開始するメッセージを送信するか、または宛先サーバからの Hello Request メッセージへの応答に含めます。

SSL インспекションを設定した場合、管理対象デバイスが ClientHello メッセージを受信すると、システムはそのメッセージを [復号 - 再署名 (Decrypt - Resign) ] アクションを含む SSL ルールと照合しようとしています。照合は ClientHello メッセージからのデータとキャッシュされたサーバ証明書データからのデータに依存します。考えられるデータには次のものがあります。

表 86: SSL ルールの条件のデータの可用性

SSL ルールの条件	データの存在場所
ゾーン	ClientHello
ネットワーク	ClientHello
VLAN タグ	ClientHello
ポート	ClientHello
Users	ClientHello
アプリケーション	ClientHello (サーバ名インジケータの拡張機能)
カテゴリ	ClientHello (サーバ名インジケータの拡張機能)
証明書	サーバ証明書 (キャッシュされている可能性あり)

SSL ルールの条件	データの存在場所
識別名	サーバ証明書（キャッシュされている可能性あり）
証明書のステータス（Certificate Status）	サーバ証明書（キャッシュされている可能性あり）
暗号スイート	ServerHello
バージョン	ServerHello

ClientHello メッセージが [復号 - 再署名（Decrypt - Resign）] ルールに一致しない場合、システムはメッセージを変更しません。次に、メッセージがアクセス コントロール評価（ディープインスペクションを含めることができる）で合格するかどうかを決定します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。

メッセージが [復号 - 再署名（Decrypt - Resign）] ルールに一致したら、システムは ClientHello メッセージを次のように変更します。

- 圧縮方法：クライアントがサポートする圧縮方法を指定する、`compression_methods` 要素を削除します。Firepower システムは圧縮されたセッションを復号できません。この変更により、復号できないトラフィックの圧縮されたセッションタイプが削減されます。
- 暗号スイート：Firepower システムがサポートしない場合、`cipher_suites` 要素から暗号スイートを削除します。Firepower システムが指定した暗号スイートのいずれもサポートしない場合、システムは、元の変更されていない要素を送信します。この変更により、復号できないトラフィックの、サポートされない暗号スイートと不明な暗号スイートが削減されます。
- セッション識別子：キャッシュされたセッションデータと一致しない `SessionTicket` 拡張機能と `Session Identifier` 要素から値を削除します。ClientHello 値がキャッシュされたデータと一致した場合、一時停止したセッションは、クライアントとサーバが完全な SSL ハンドシェイクを実行せずに、中断したセッションを再開できます。この変更は、セッション再開の可能性を高め、復号できないトラフィックの、セッションが未キャッシュのタイプを削減します。
- 楕円曲線：Firepower システムがサポートしない場合、サポートされる楕円曲線拡張機能から楕円曲線を削除します。Firepower システムが指定した楕円曲線のいずれもサポートしない場合、管理対象デバイスは拡張機能を削除し、`cipher_suites` 要素から関連する暗号スイートを削除します。
- ALPN 拡張機能：Firepower システムでサポートされていないアプリケーション層プロトコルネゴシエーション（ALPN）拡張機能から値を削除します（たとえば、SPDY と HTTP/2 プロトコル）。この変更は、メッセージがコンテンツ制限機能に関連付けられた SSL ルールに一致した場合にのみ実行されます。詳細については、[コンテンツ制限について（1425 ページ）](#) を参照してください。

- 他の拡張機能：Extended Master Secret、Next Protocol Negotiation（NPN）、および TLS チャネル ID 拡張機能を削除します。



- (注) システムはデフォルトで ClientHello の変更を実行します。SSL ポリシーが正しく設定されていると、このデフォルトの動作により、トラフィックの復号がより頻繁に発生します。各ネットワークにおけるデフォルトの動作を調整するには、サポートにお問い合わせください。

システムが ClientHello メッセージを変更した後、メッセージがアクセス コントロール評価（ディープインスペクションを含めることができる）で合格するかどうかを決定します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。

メッセージを変更した後はクライアントおよびサーバで計算されたメッセージ認証コード（MAC）が一致しなくなるため、SSL ハンドシェイク時のクライアントとサーバの間の直接通信はできなくなります。すべての後続のハンドシェイクメッセージ（および一度設定された暗号化セッションに対し）、管理対象デバイスは、中間者（MITM）として機能します。ここでは 2 つの SSL セッションが作成され、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間で使用されます。その結果、暗号化セッションの詳細はセッションごとに異なります。



- (注) Firepower システムが復号できる暗号スイートは頻繁に更新されるので、SSL ルールの条件で使用可能な暗号スイートと直接対応しません。現在、復号できる暗号スイートのリストについては、サポートに連絡してください。

#### 関連トピック

[復号できないトラフィックのデフォルト処理オプション](#)（1459 ページ）

[インライン展開での暗号化トラフィックの再署名済み証明書による検査](#)（1453 ページ）

## ServerHello とサーバ証明書メッセージの処理

ServerHello メッセージは、正常な SSL ハンドシェイクの ClientHello メッセージへの応答です。

管理対象デバイスが ClientHello メッセージを処理し、宛先サーバに送信した後、サーバはクライアントがメッセージで指定した復号属性をサポートするかどうかを決定します。その属性をサポートしない場合、サーバはクライアントにハンドシェイクの失敗のアラートを送信します。その属性をサポートする場合、サーバは ServerHello メッセージを送信します。同意済みキー交換方式が認証に証明書を使用する場合、サーバ証明書メッセージはすぐに ServerHello メッセージに続きます。

管理対象デバイスがこれらのメッセージを受信すると、SSL ルールとの一致を試みます。これらのメッセージには、ClientHello メッセージまたはセッション データ キャッシュにはなかった情報が含まれます。具体的には、システムは、識別名、証明書のステータス、暗号スイート、およびバージョン条件で、これらのメッセージと一致させる可能性があります。

メッセージがSSLルールと一致しない場合、管理対象デバイスは、SSLポリシーのデフォルトのアクションを実行します。詳細については、[SSL ポリシーのデフォルトアクション \(1458 ページ\)](#) を参照してください。

メッセージがSSLルールに一致する場合、管理対象デバイスは、必要に応じて次に進みます。

#### アクション：モニタ (Monitor)

SSLハンドシェイクは完了に進みます。管理対象デバイスは追跡およびログに記録しますが、暗号化トラフィックを復号しません。

#### アクション：ブロック (Block)、またはリセットしてブロック (Block with Reset)

管理対象デバイスは、SSLセッションをブロックします。必要に応じて、TCP接続もリセットします。

#### アクション：復号しない (Do Not Decrypt)

SSLハンドシェイクは完了に進みます。管理対象デバイスは、SSLセッションの間で交換されるアプリケーションデータを復号しません。

まれに、システムではClientHelloメッセージと[復号-再署名 (Decrypt - Resign)]ルールが一致してメッセージを変更しますが、関連するServerHelloメッセージは[復号しない (Do Not Decrypt)]ルールに一致することがあります。このような場合、クライアントから更新されたハンドシェイクをトリガーするために、システムはTCP接続をリセットします。更新されたClientHelloメッセージは[復号-再署名 (Decrypt - Resign)]ルールに一致しなくなり、SSLセッションは復号せずに進みます。

#### アクション：復号 - 既知のキー (Decrypt - Known Key)

管理対象デバイスは、サーバ証明書データを以前にアップロードされたサーバ証明書と照合しようとします。

証明書が以前に生成された証明書と一致した場合、SSLハンドシェイクは完了に進みます。管理対象デバイスはアップロードされた秘密キーを使用して、SSLセッション中に交換されたアプリケーションデータを復号および再暗号化します。

まれに、システムでは、サーバ証明書メッセージが以前に生成された証明書と一致しないことがあります。たとえば、サーバはクライアントとの最初の接続と後続の接続の間に証明書を変更することがあります。この場合、システムはSSL接続をブロックし、クライアントが再接続して、システムが新しい証明書データとのハンドシェイクを処理できるようにします。

#### アクション：復号 - 再署名 (Decrypt - Resign)

管理対象デバイスは、サーバ証明書メッセージを処理し、以前にアップロードされた認証局 (CA) 証明書で交換されるサーバ証明書を再署名します。SSLハンドシェイクは完了に進みます。管理対象デバイスはアップロードされた秘密キーを使用して、SSLセッション中に交換されたアプリケーションデータを復号および再暗号化します。

ServerHello および証明書メッセージの処理中、管理対象デバイスは識別名と証明書データをキャッシュし、再確立されたセッションと、後続のSSLセッションの両方でハンドシェイクが高速で処理されるようにします。

## SSL インспекションの要件

構成時の設定やライセンスに加え、アプライアンスをネットワーク上にどのように展開しているかにより、暗号化トラフィックの制御や復号化に適用できるアクションが異なります。最適な展開タイプを決定するときは、マッピングされたアクション、既存のネットワーク展開、および全体的な要件のリストを確認してください。

インライン、ルーティング、スイッチド、またはハイブリッドのインターフェイスで設定および展開されたデバイスでは、トラフィックフローの変更が可能です。これらのデバイスでは、着信および発信トラフィックのモニタリング、ブロック、許可、および復号を行うことができます。

パッシブまたはインライン（タップモード）のインターフェイスで設定および展開されたデバイスでは、トラフィックフローを変更することはできません。これらのデバイスで行えるのは、着信トラフィックのモニタリング、許可、および復号だけです。パッシブ展開では、一時 Diffie-Hellman（DHE）および楕円曲線 Diffie-Hellman（ECDHE）の暗号スイートを使用した暗号化トラフィックの復号はサポートされません。

SSL インспекションの一部の機能では、公開キー証明書と秘密キーのペアが必要です。暗号化セッションの特性に応じてトラフィックを復号したり制御したりするためには、証明書および秘密キーのペアを Firepower Management Center にアップロードする必要があります。

## SSL ルール設定の前提条件に関する情報

SSL インспекションは、サポートする公開キーインフラストラクチャ（PKI）の多くの情報に依存しています。照合ルールの条件を設定するときは、その組織におけるトラフィックパターンについて検討する必要があります。

表 87: SSL ルール条件の設定に必要な情報

一致対象	必要な情報
自己署名サーバ証明書を含む、検出されたサーバ証明書	サーバ証明書
信頼できるサーバ証明書	CA 証明書
検出されたサーバ証明書のサブジェクトまたは発行元	サーバ証明書のサブジェクト DN または発行元 DN

ルールの適用先となる暗号化トラフィックの復号、ブロック、モニタリングが不要かどうか、または復号が必要かどうかについて検討します。その結果を、SSL ルールのアクション、復号できないトラフィックのアクション、および SSL ポリシーのデフォルトアクションに反映させます。

表 88: SSL 復号に必要な情報

復号の対象	必要な情報
制御対象のサーバへの着信トラフィック	サーバ証明書のファイルと秘密キー ファイルのペア
外部サーバへの発信トラフィック	CA 証明書のファイルと秘密キー ファイルのペア CA 証明書と秘密キーを生成することもできます。

これらの情報を収集したら、システムにアップロードして、再利用可能なオブジェクトを設定します。

#### 関連トピック

[識別名オブジェクト](#) (484 ページ)

[PKI オブジェクト](#) (487 ページ)

## SSL インспекション アプライアンス 導入シナリオ

ここでは Life Insurance Example, Inc. (LifeIns) という架空の生命保険会社で使われる複数のシナリオを例にして、同社のプロセス監査で利用されている暗号化トラフィックの SSL インспекションについて解説します。LifeIns はそのビジネス プロセスに基づいて、以下の展開を計画しています。

- カスタマー サービス部門では、単一の 7000 または 8000 シリーズ デバイスをパッシブ展開する
- 契約審査部門では、単一の 7000 または 8000 シリーズ デバイスをインライン展開する
- 上記の両方のデバイスを単一の Firepower Management Center で管理する

#### カスタマー サービスのビジネス プロセス

LifeIns はすでに顧客対応用の Web サイトを構築済みです。LifeIns は、保険契約に関する見込み顧客からの暗号化された質問や要求を、Web サイトや電子メールで受け取ります。LifeIns のカスタマー サービスは、これらの要求を処理して 24 時間以内に必要な情報を返信しなければなりません。カスタマー サービスでは、着信するコンタクトメトリックのコレクションを拡張したいと思っています。LifeIns では、すでにカスタマー サービスに対する内部監査用のレビューが確立されています。

また、LifeIns は暗号化された申請書もオンラインで受信します。カスタマー サービス部門は申請書を 24 時間以内に処理し、申請書類のファイルを契約審査部門に送信しなければなりません。カスタマー サービスでは、オンラインフォームからの不正な申請をすべて除外するようにしていますが、この作業が同部門での作業のかなりの部分を占めています。



## 契約審査部門のビジネス プロセス

LifeIns の契約審査担当者は、Medical Repository Example, LLC (MedRepo) という医療データリポジトリに、オンラインで暗号化された医療情報要求を送信します。MedRepo はこれらの要求を評価し、LifeIns に暗号化されたレコードを 72 時間以内に送信します。その後は契約審査担当者が申請書類を査定し、保険契約および保険料に関連する判定を送信します。契約審査部門では、そのメトリック コレクションを拡張したいと思っています。

最近、不明な送信元からのスプーフィング (なりすまし) 応答が LifeIns に送られてくるようになりました。LifeIns の契約審査担当者はインターネット使用に関する適切なトレーニングを受けていますが、LifeIns の IT 部門はまず、医療応答の形式で送られてくる暗号化トラフィックをすべて分析し、すべてのスプーフィング行為をブロックしたいと考えています。

LifeIns では、経験の浅い契約審査担当者に対して 6 ヶ月のトレーニング期間を設けています。最近、こうした契約審査担当者が MedRepo のカスタマー サービス部門への暗号化された医療規制リクエストの送信を正しく行わない事例がありました。そのため MedRepo から LifeIns に複数の苦情が提出されています。LifeIns は、新任の契約審査担当者用のトレーニング期間を延長し、契約審査担当者から MedRepo への要求についても監査を入れることを計画しています。

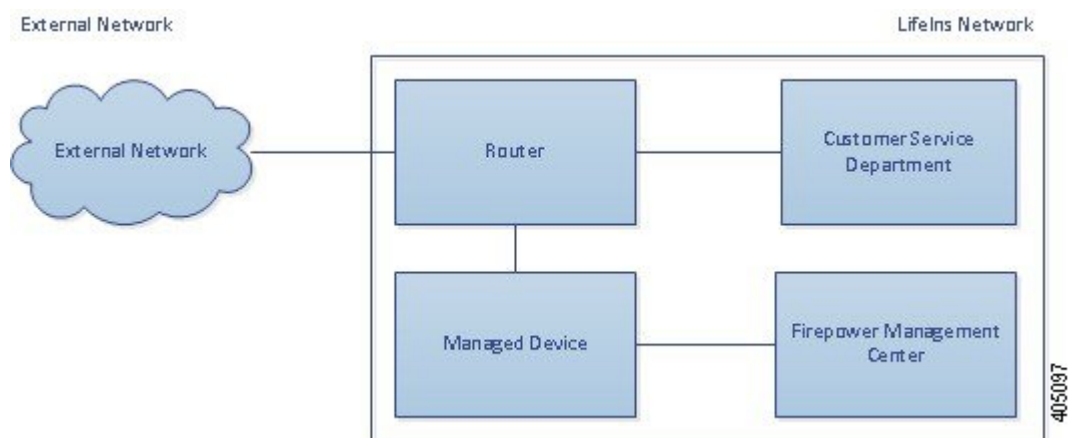
## パッシブ展開でのトラフィックの復号

LifeIns のビジネス要件では、カスタマー サービスに次の要求をしています。

- すべての要求と申請書類を 24 時間以内に処理する
- 着信するコンタクトメトリックのコレクションプロセスを改善する
- 着信した不正な申請書類を特定して廃棄する

カスタマー サービス部門では、追加の監査用レビューを必要としません。

LifeIns ではカスタマー サービスの管理対象デバイスのパッシブ展開を計画しています。



外部ネットワークからのトラフィックはLifeInsのルータに送信されます。ルータはトラフィックをカスタマーサービス部門にルーティングし、検査用にトラフィックのコピーを管理対象デバイスにミラーリングします。

管理元の Firepower Management Center で、[アクセス コントロール (Access Control) ] および [SSL エディタ (SSL Editor) ] のカスタム ロールを持つユーザが、SSL インスペクションの設定を次のように行います。

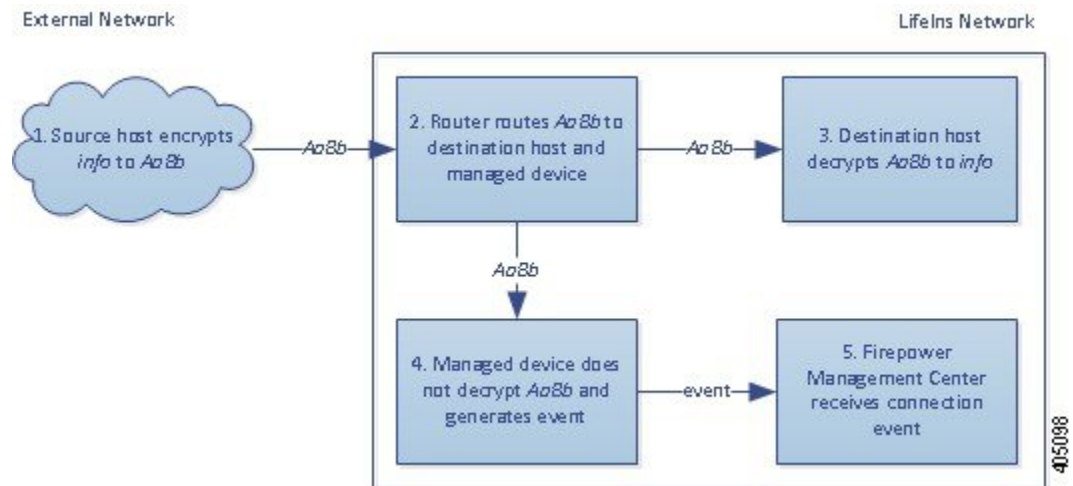
- カスタマー サービス部門に送信された暗号化トラフィックをすべてログに記録する
- オンラインの申請フォームからカスタマー サービスに送信された暗号化トラフィックを復号する
- カスタマー サービスに送信された他の暗号化トラフィックは、オンライン リクエスト フォームからのトラフィックも含め、すべて復号しない

さらに、復号された申請フォームトラフィック中に偽の申請データが含まれていないかを確認し、検出された場合はログに記録するためのアクセス コントロールも設定します。

次のシナリオでは、ユーザからカスタマー サービスにオンライン フォームが送信されます。ユーザのブラウザは、サーバとの TCP 接続を確立してから、SSL ハンドシェイクを開始します。管理対象デバイスが、このトラフィックのコピーを受信します。クライアントとサーバが SSL ハンドシェイクを完了することで、暗号化されたセッションが確立されます。システムは、ハンドシェイクと接続の詳細に応じて、接続のログを記録し、暗号化トラフィックのコピーを処理します。

## パッシブ展開での暗号化トラフィック モニタリング

管理対象デバイスは、カスタマー サービスに送信されるすべての SSL 暗号化トラフィックについて、接続のログを記録します。



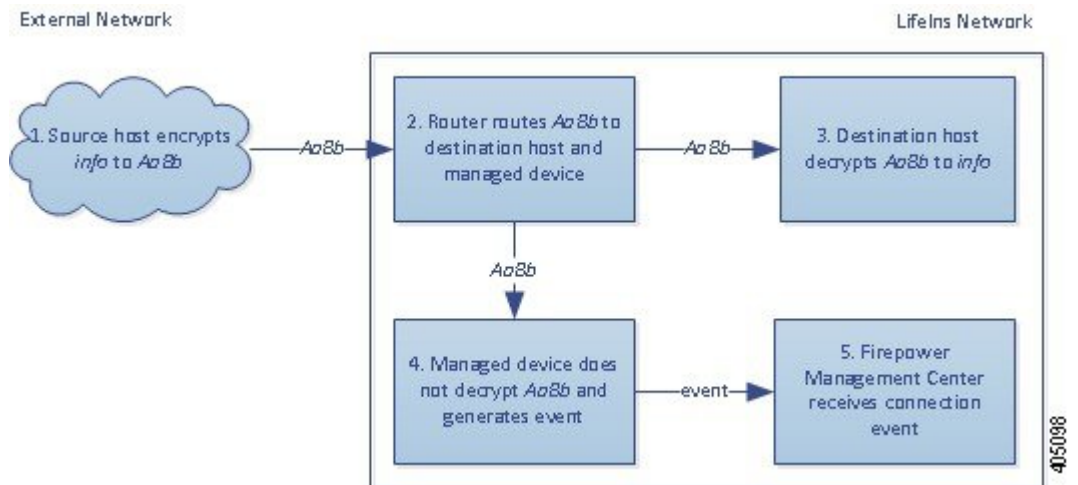
次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (info) を送信します。クライアントがこれを暗号化 (AaBb) し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。

3. カスタマーサービス部門のサーバが、暗号化された情報の要求 (AaBb) を受信し、これをプレーンテキスト (info) に復号します。
4. 管理対象デバイスはトラフィックを復号しません。  
アクセスコントロールポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、デバイスは接続イベントを生成します。
5. Firepower Management Centerが接続イベントを受信します。

## パッシブ展開での復号されていない暗号化トラフィック

保険契約に関する要求を含むすべてのSSL暗号化トラフィックについては、管理対象デバイスはそのトラフィックを復号せずに許可し、接続のログを記録します。



次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (info) を送信します。クライアントがこれを暗号化 (AaBb) し、カスタマーサービスに暗号化トラフィックを送信します。
2. LifeInsのルータが暗号化トラフィックを受信し、カスタマーサービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。
3. カスタマーサービス部門のサーバが、暗号化された情報の要求 (AaBb) を受信し、これをプレーンテキスト (info) に復号します。
4. 管理対象デバイスはトラフィックを復号しません。  
アクセスコントロールポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、デバイスは接続イベントを生成します。
5. Firepower Management Centerが接続イベントを受信します。

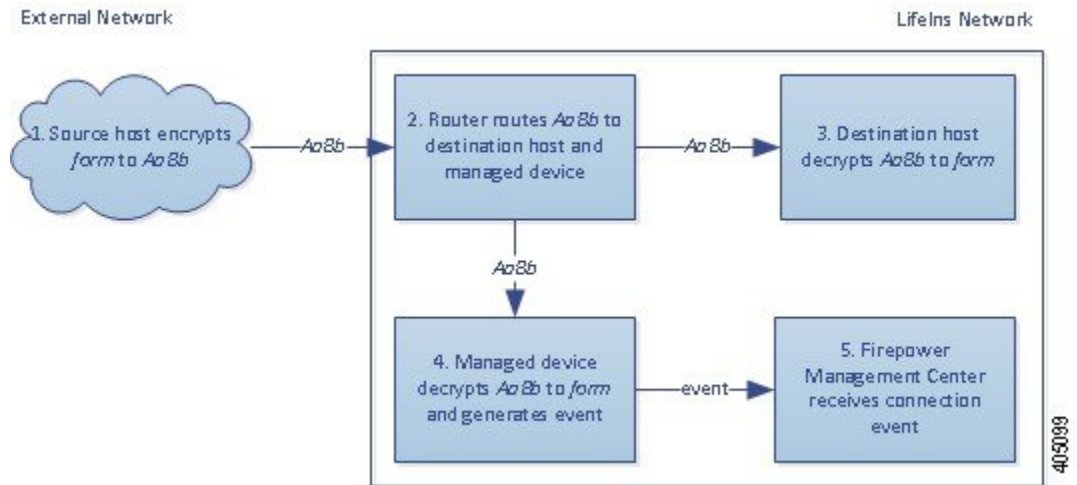
## パッシブ展開での暗号化トラフィックの秘密キーによる検査

申請フォームのデータを含むすべてのSSL暗号化トラフィックは復号され、接続のログが記録されます。



(注) パッシブ展開の場合、DHEまたはECDHE暗号スイートで暗号化されたトラフィックは、既知の秘密キーを使って復号することはできません。

有効な申請フォームの情報を含むトラフィックについては、接続のログが記録されます。



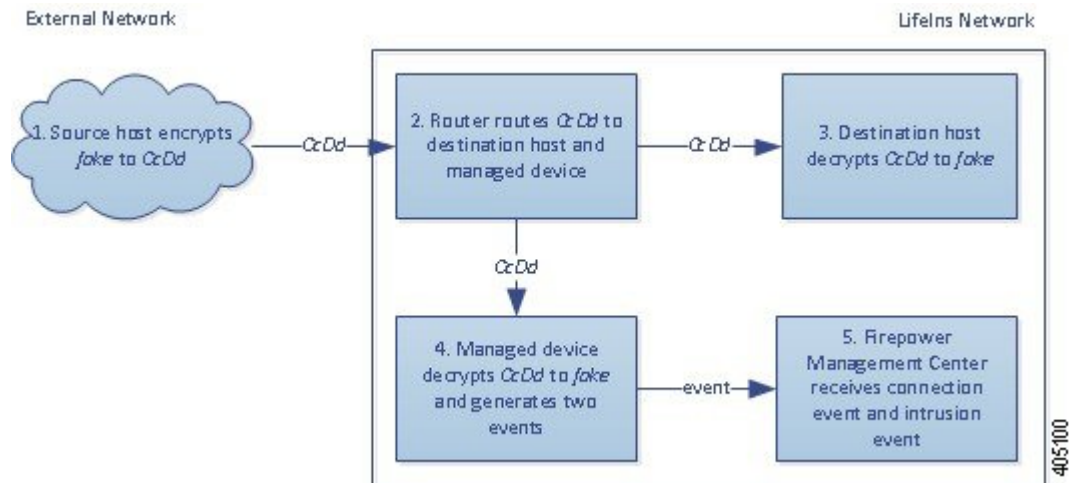
次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (form) を送信します。クライアントがこれを暗号化 (AaBb) し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求 (AaBb) を受信し、これをプレーンテキスト (form) に復号します。
4. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッションキーを使用して、暗号化トラフィックをプレーンテキスト (form) に復号化します。

アクセス コントロール ポリシーは、復号されたトラフィックの処理を継続します。偽の申請書であることを示す情報は検出されません。セッション終了後、デバイスは接続イベントを生成します。

5. Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、復号されたトラフィックに偽の申請データが含まれていた場合、接続および偽のデータについてのログが記録されます。



次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (*fake*) を送信します。クライアントがこれを暗号化 (*CcDd*) し、カスタマーサービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマーサービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。
3. カスタマーサービス部門のサーバが、暗号化された情報の要求 (*CcDd*) を受信し、これをプレーンテキスト (*fake*) に復号します。
4. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッションキーを使用して、暗号化トラフィックをプレーンテキスト (*fake*) に復号します。  
アクセスコントロールポリシーは、復号されたトラフィックの処理を継続して、偽の申請書であることを示す情報を検出します。デバイスが侵入イベントを生成します。セッション終了後、デバイスは接続イベントを生成します。
5. Firepower Management Center は、暗号化および復号されたトラフィックの情報とともに、接続イベントおよび偽の申請データの侵入イベントを受信します。

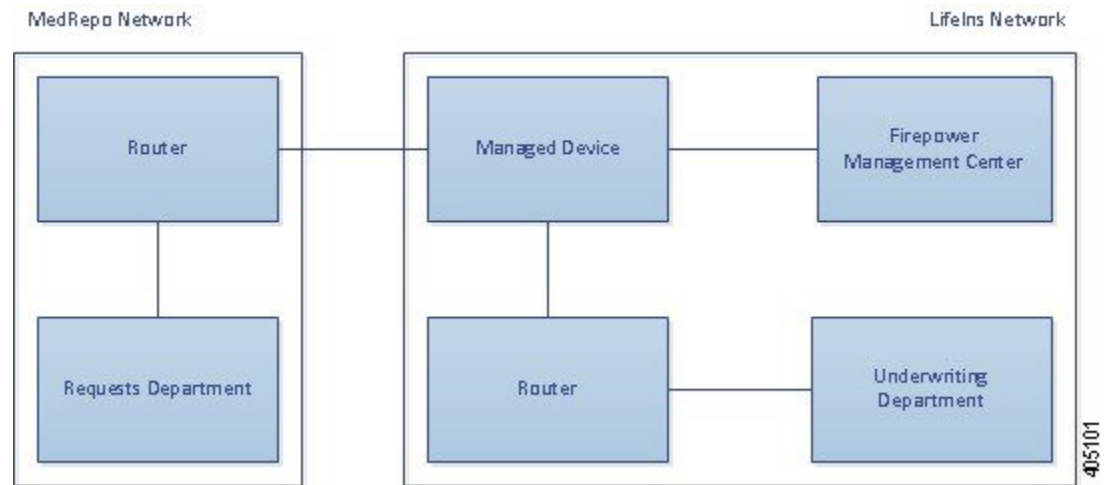
## インライン展開でのトラフィックの復号

LifeIns のビジネス要件では、契約審査部門に次の要求をしています。

- 新採用および経験の浅い契約審査担当者を監査し、MedRepo への情報要求が適切なすべての規則に準じていることを検証する
- その契約審査によるメトリックコレクションプロセスを改善する
- MedRepo が送信元と思われるすべての要求を調査し、スプーフィング行為を排除する
- 契約審査部門から MedRepo のカスタマーサービス部門へのすべての不適切な規制要求を排除する

- 経験豊富な契約審査担当者は監査しない

LifeIns の契約審査部門では、デバイスのインライン展開を計画しています。



MedRepo のネットワークからのトラフィックは、MedRepo のルータに流されます。そこから LifeIns のネットワークにトラフィックがルーティングされます。管理対象デバイスがそのトラフィックを受信し、許可されたトラフィックを LifeIns のルータに転送し、また管理元の Firepower Management Center にイベントを送信します。LifeIns のルータは、トラフィックを宛先ホストにルーティングします。

管理元の Firepower Management Center で、[アクセスコントロール (Access Control)] および [SSL エディタ (SSL Editor)] のカスタムロールを持つユーザが、SSL アクセスコントロールロールの設定を次のように行います。

- 契約審査部門に送信された暗号化トラフィックをすべてログに記録する
- LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信された暗号化トラフィックをすべてブロックする
- MedRepo から LifeIns の契約審査部門宛て、および LifeIns の経験の浅い契約審査担当者から MedRepo のリクエスト部門宛てに送信される暗号化トラフィックをすべて復号する
- 経験豊富な契約審査担当者から送信される暗号化トラフィックは復号しない

さらに、カスタムの侵入ポリシーと以下の設定を使用して、復号トラフィックを検査するアクセスコントロールを設定します。

- 復号トラフィックでスプーフィング行為が検出された場合はそのトラフィックをブロックし、スプーフィング行為をログに記録する
- 規制に準拠しない情報を含んでいる復号トラフィックをブロックし、不適切な情報をログに記録する
- 他の暗号化および復号されたトラフィックをすべて許可する

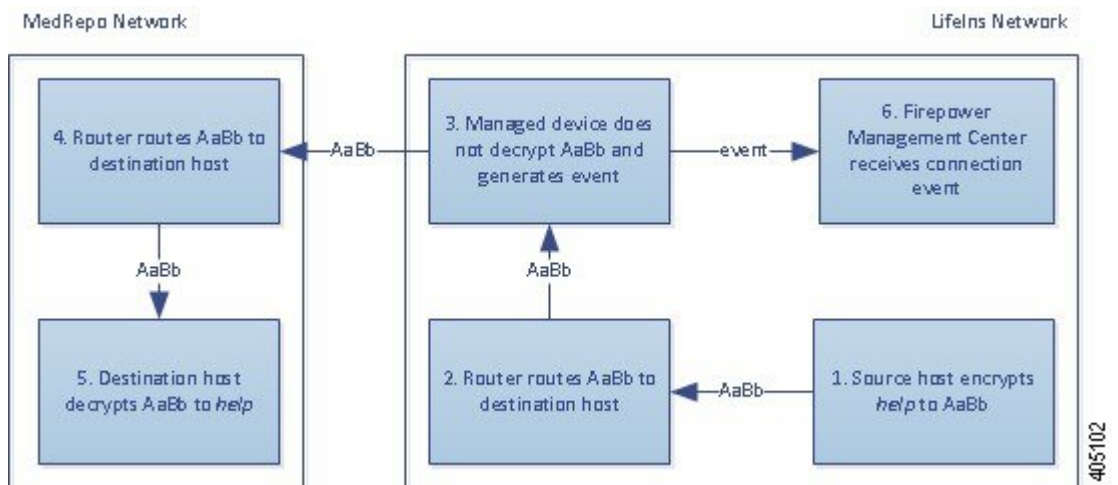
許可された復号トラフィックは、再暗号化されて宛先ホストに転送されます。

また、SSL アクセスコントロールルールを使用して、[復号 - 再署名 (Decrypt - Resign)] アクションでシステムにトラフィックを復号化して再署名させることもできます。トラフィックが SSL ルールに一致する場合、システムは ClientHello メッセージを変更した後、メッセージがアクセスコントロール評価 (ディープインスペクションを含めることができる) に合格するかどうかを判断します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。詳細については、次を参照してください。 [ClientHello メッセージ処理 \(1437 ページ\)](#)

次のシナリオでは、ユーザが情報をオンラインでリモートサーバに送信します。ユーザのブラウザは、サーバとの TCP 接続を確立してから、SSL ハンドシェイクを開始します。管理対象デバイスがこのトラフィックを受信し、ハンドシェイクと接続の詳細に基づいて、システムが接続のログへの記録とトラフィックの処理を行います。システムがトラフィックをブロックした場合、TCP 接続も切断されます。トラフィックがブロックされない場合、クライアントとサーバが SSL ハンドシェイクを完了することで、暗号化されたセッションが確立されます。

## インライン展開での暗号化トラフィック モニタリング

契約審査部門で送受信されるすべての SSL 暗号化トラフィックについて、接続のログが記録されます。



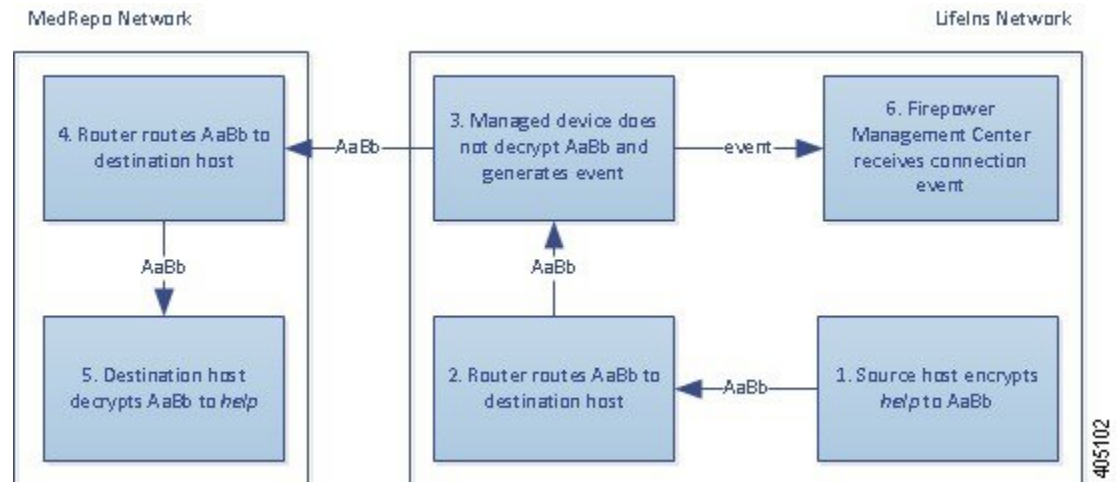
次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (help) を送信します。クライアントがこれを暗号化 (AaBb) し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. 管理対象デバイスはトラフィックを復号しません。  
アクセスコントロールポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。

5. 契約審査部門のサーバは、暗号化された情報の要求 (AaBb) を受信し、これをプレーンテキスト (help) に復号します。
6. Firepower Management Centerが接続イベントを受信します。

## インライン展開での復号されていない暗号化トラフィック

経験豊富な契約審査担当者から送信されるすべてのSSL暗号化トラフィックについては、管理対象デバイスはそのトラフィックを復号せずに許可し、接続のログを記録します。



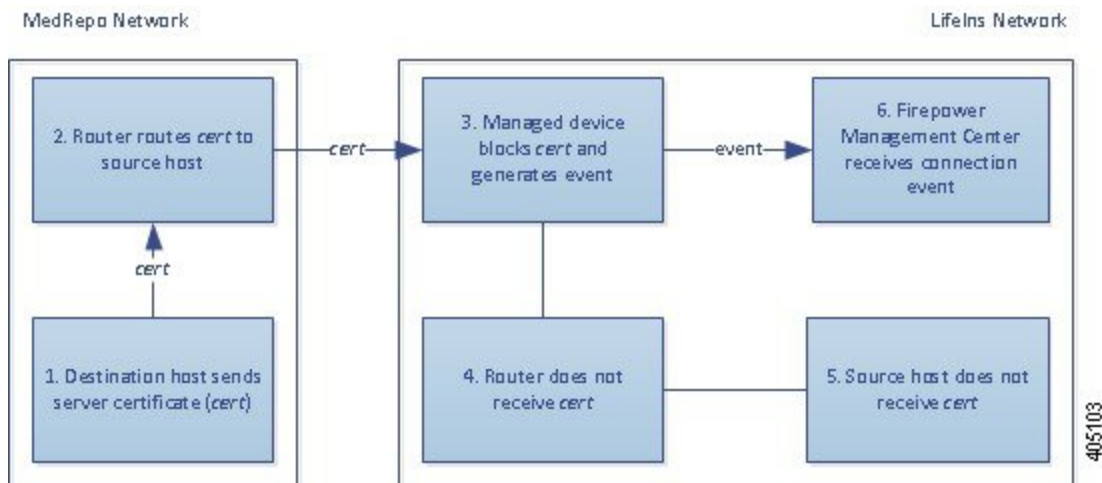
次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (help) を送信します。クライアントがこれを暗号化 (AaBb) し、MedRepoのリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeInsのルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. 管理対象デバイスはこのトラフィックを復号しません。  
アクセスコントロールポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. リクエスト部門のサーバは、暗号化された情報の要求 (AaBb) を受信し、これをプレーンテキスト (help) に復号します。
6. Firepower Management Centerが接続イベントを受信します。



## インライン展開での暗号化トラフィックのブロック

LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信されるすべての SMTPS 電子メールトラフィックは SSL ハンドシェイク時にブロックされ、追加の検査なしで接続のログが記録されます。

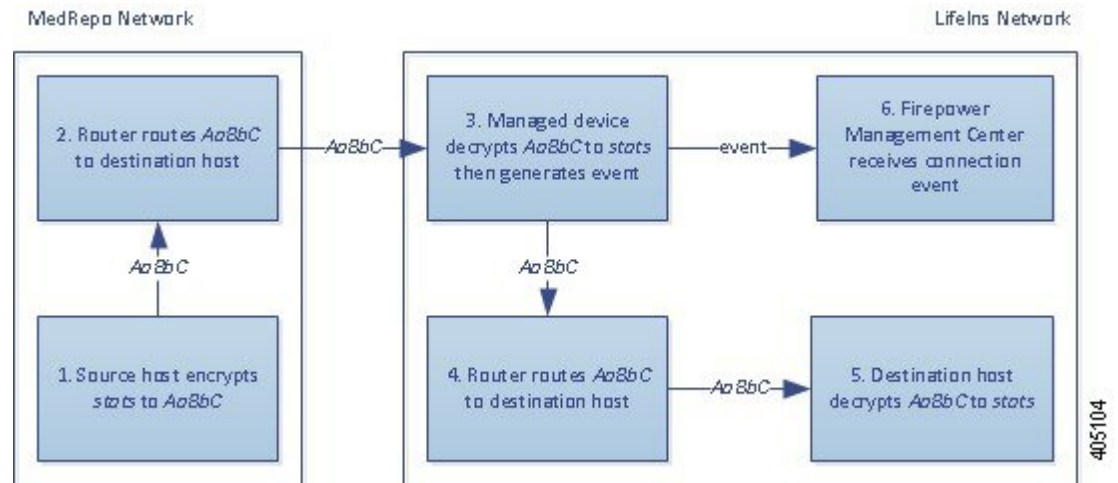


次のステップが実行されます。

1. カスタマー サービス部門のサーバは、クライアントブラウザから SSL ハンドシェイクの確立要求を受信すると、SSL ハンドシェイクの次のステップとして、サーバ証明書 (cert) を LifeIns の契約審査担当者に送信します。
2. MedRepo のルータが証明書を受信し、これを LifeIns の契約審査担当者にルーティングします。
3. 管理対象デバイスは追加の検査を行わずにトラフィックをブロックし、TCP 接続を終了します。これにより、接続イベントが生成されます。
4. 内部ルータは、ブロックされたトラフィックを受信しません。
5. 契約審査担当者は、ブロックされたトラフィックを受信しません。
6. Firepower Management Center が接続イベントを受信します。

## インライン展開での暗号化トラフィックの秘密キーによる検査

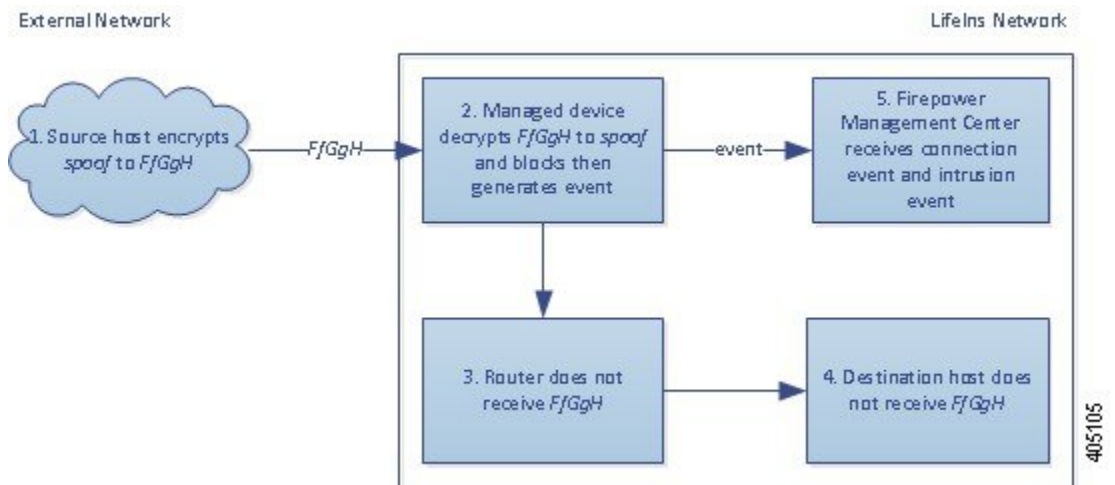
MedRepo から LifeIns の契約審査部門に送信されるすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。復号には、アップロードされたサーバ秘密キーを使って取得されたセッションキーが使用されます。正規のトラフィックは許可され、再暗号化されて契約審査部門に送信されます。



次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (stats) を送信します。クライアントがこれを暗号化 (AaBbC) し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. 外部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
3. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッションキーを使用して、このトラフィックをプレーンテキスト (stats) に復号します。  
アクセスコントロールポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続します。スプーフィング行為は検出されません。デバイスは暗号化トラフィック (AaBbC) を転送し、セッション終了後に接続イベントを生成します。
4. 内部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
5. 契約審査部門のサーバは、暗号化された情報 (AaBbC) を受信し、これをプレーンテキスト (stats) に復号します。
6. Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、スプーフィング行為の復号トラフィックはすべてドロップされ、接続およびスプーフィング行為についてのログが記録されます。



次のステップが実行されます。

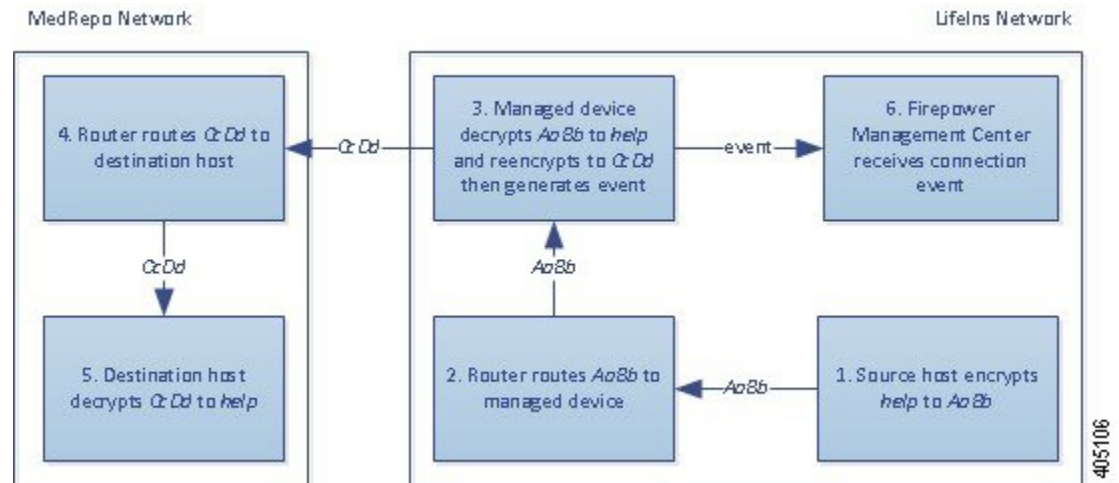
1. ユーザがプレーンテキストの要求 (spoof) を送信しますが、このトラフィックは変更されており、発信元が MedRepo, LLC であるかのように偽装されています。クライアントがこれを暗号化 (FfGgH) し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッションキーを使用して、このトラフィックをプレーンテキスト (spoof) に復号します。  
アクセスコントロールポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続し、スプーフィング行為を検出します。デバイスはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。
3. 内部ルータは、ブロックされたトラフィックを受信しません。
4. 契約審査部門のサーバは、ブロックされたトラフィックを受信しません。
5. Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントおよびスプーフィング行為の侵入イベントを受信します。

## インライン展開での暗号化トラフィックの再署名済み証明書による検査

新任および経験の浅い契約審査担当者から MedRepo のリクエスト部門に送信されるすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。復号には、再署名されたサーバ証明書を使って取得されたセッションキーが使用されます。正規のトラフィックは許可され、再暗号化されて MedRepo に送信されます。



- (注) インライン展開においてサーバ証明書の再署名によりトラフィックを復号化する場合、デバイスは中間者 (man-in-the-middle) として機能します。ここでは2つの SSL セッションが作成され、1つはクライアントと管理対象デバイスの間、もう1つは管理対象デバイスとサーバの間で使用されます。その結果、暗号セッションの詳細はセッションごとに異なります。



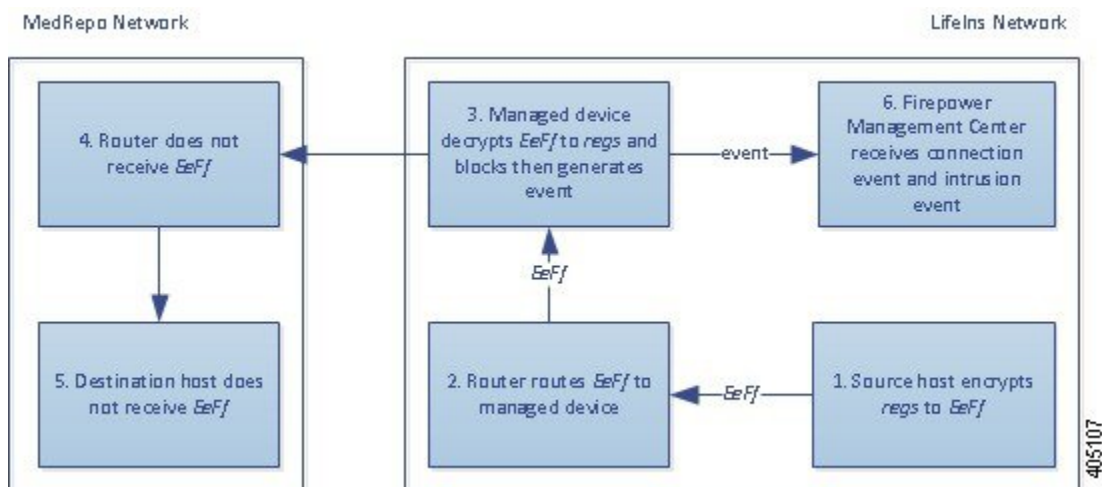
次のステップが実行されます。

1. ユーザがプレーンテキストの要求 (help) を送信します。クライアントがこれを暗号化 (AaBb) し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. 管理対象デバイスは、再署名されたサーバ証明書と秘密キーで取得したセッションキーを使用して、このトラフィックをプレーンテキスト (help) に復号します。  
アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続します。不適切な要求は検出されません。デバイスはトラフィックを再暗号化 (CcDd) して、送信を許可します。セッション終了後、接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. リクエスト部門のサーバは、暗号化された情報 (CcDd) を受信し、これをプレーンテキスト (help) に復号します。
6. Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。



- (注) 再署名されたサーバ証明書で暗号化されたトラフィックにより、信頼できない証明書についての警告がクライアントのブラウザに表示されます。この問題を避けるには、組織のドメインルートにある信頼できる証明書ストアまたはクライアントの信頼できる証明書ストアにCA証明書を追加します。

これに対し、規制要件を満たさない情報を含んでいる復号トラフィックは、すべてドロップされます。接続および非準拠情報についてのログが記録されます。



次のステップが実行されます。

1. ユーザが規制要件に準拠していない要求をプレーンテキスト (regs) で送信します。クライアントがこれを暗号化 (EeFf) し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. 管理対象デバイスは、再署名されたサーバ証明書と秘密キーで取得したセッションキーを使用して、このトラフィックをプレーンテキスト (regs) に復号します。  
アクセスコントロールポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続し、不適切な要求を検出します。デバイスはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。
4. 外部ルータは、ブロックされたトラフィックを受信しません。
5. リクエスト部門のサーバは、ブロックされたトラフィックを受信しません。
6. Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントおよび不適切な要求の侵入イベントを受信します。





## 第 63 章

# SSL ポリシーの使用を開始するには

ここでは、SSL ポリシーの作成、設定、管理、およびロギングの概要を示します。

- [SSL ポリシーの概要 \(1457 ページ\)](#)
- [SSL ポリシーのデフォルトアクション \(1458 ページ\)](#)
- [復号できないトラフィックのデフォルト処理オプション \(1459 ページ\)](#)
- [SSL ポリシーの管理 \(1460 ページ\)](#)
- [基本 SSL ポリシーの作成 \(1462 ページ\)](#)
- [復号できないトラフィックのデフォルト処理の設定 \(1463 ページ\)](#)
- [SSL ポリシーの編集 \(1464 ページ\)](#)

## SSL ポリシーの概要

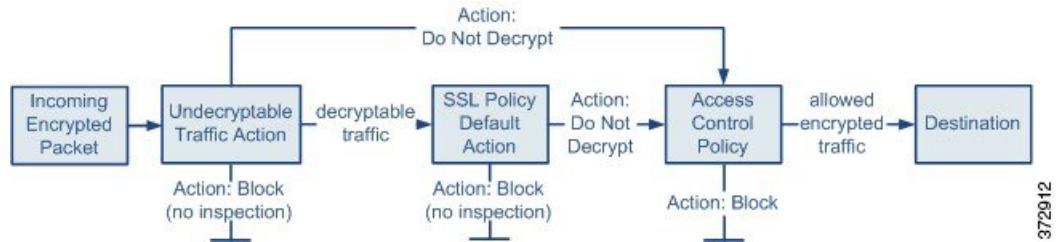
SSL ポリシーは、ネットワーク上の暗号化トラフィックをシステムがどのように処理するかを決定します。SSL ポリシーを、1 つまたは複数設定できます。SSL ポリシーをアクセス コントロール ポリシーに関連付け、そのアクセス コントロール ポリシーを管理対象デバイスに展開します。デバイスで TCP ハンドシェイクが検出されると、アクセス コントロール ポリシーは最初にトラフィックを処理して検査します。次に TCP 接続上で SSL 暗号化セッションが識別された場合は、SSL ポリシーが引き継いで、暗号化トラフィックの処理および復号を行います。



**注意** SSL ポリシーを追加または削除すると設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

最も単純な SSL ポリシーは、次の図のように、単一のデフォルトアクションで暗号化トラフィックを処理するように展開先のデバイスに指示します。デフォルトアクションの設定では、それ以上のインスペクションなしで復号可能トラフィックをブロックするか、復号されていない復号可能トラフィックをアクセスコントロールで検査するように指定できます。システ

ムは、暗号化されたトラフィックを許可するか、またはブロックできます。デバイスは復号できないトラフィックを検出すると、トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号しないままにして、アクセスコントロールによる検査を行います。



より複雑な SSL ポリシーでは、各種の復号できないトラフィックをさまざまなアクションで処理できます。また、認証局 (CA) が証明書を発行したか、または暗号化証明書を信頼するかどうかに応じてトラフィックを制御したり、SSL ルールを使ってきめ細かな暗号化トラフィックの制御およびログの記録を行ったりできます。これらのルールには、単純なものや複雑なものがあり、複数の基準を使用して暗号化トラフィックの照合および検査を行います。

#### 関連トピック

[SSL ルールの条件](#) (1474 ページ)

## SSL ポリシーのデフォルトアクション

SSL ポリシーのデフォルトアクションは、ポリシーのモニタ以外のルールと一致しない復号可能な暗号化トラフィックについてシステムがどのように処理するかを決定します。SSL ルールがまったく含まれない SSL ポリシーを適用する場合、ネットワーク上のすべての復号可能トラフィックの処理方法を、デフォルトアクションが決定します。デフォルトアクションでブロックされた暗号化トラフィックに対しては、システムはいかなる種類のインスペクションも行わないことに注意してください。

表 89: SSL ポリシーのデフォルトアクション

デフォルトアクション	暗号化トラフィックに対して行う処理
ブロック (Block)	それ以上のインスペクションは行わずに SSL セッションをブロックする
リセットしてブロック (Block with reset)	それ以上のインスペクションは行わずに SSL セッションをブロックし、TCP 接続をリセットする
復号しない (Do not decrypt)	アクセスコントロールを使用して暗号化トラフィックを検査する



# 復号できないトラフィックのデフォルト処理オプション

表 90: 復号できないトラフィック タイプ

タイプ (Type)	説明	デフォルト アクション	使用可能なアクション
圧縮されたセッション (Compressed Session)	SSLセッションはデータ圧縮メソッドを適用します。	デフォルト アクションを継承する (Inherit default action)	復号しない (Do not decrypt) ブロック (Block) リセットしてブロック (Block with reset) デフォルト アクションを継承する (Inherit default action)
SSLv2 セッション (SSLv2 Session)	セッションは SSL バージョン 2 で暗号化されます。 トラフィックが復号可能となるのは、ClientHello メッセージが SSL 2.0 で、送信トラフィックの残りが SSL 3.0 であることに注意してください。	デフォルト アクションを継承する (Inherit default action)	復号しない (Do not decrypt) ブロック (Block) リセットしてブロック (Block with reset) デフォルト アクションを継承する (Inherit default action)
不明な暗号スイート (Unknown Cipher Suite)	システムが認識できない暗号スイートです。	デフォルト アクションを継承する (Inherit default action)	復号しない (Do not decrypt) ブロック (Block) リセットしてブロック (Block with reset) デフォルト アクションを継承する (Inherit default action)
サポートされていない暗号スイート (Unsupported Cipher Suite)	検出された暗号スイートに基づく復号を、システムはサポートしていません。	デフォルト アクションを継承する (Inherit default action)	復号しない (Do not decrypt) ブロック (Block) リセットしてブロック (Block with reset) デフォルト アクションを継承する (Inherit default action)

タイプ (Type)	説明	デフォルト アクション	使用可能なアクション
セッションが未キャッシュ (Session not cached)	SSLセッションでセッションの再利用が有効化されており、クライアントとサーバがセッションIDを使ってセッションを再確立しているが、システムでセッションIDがキャッシュされていません。	デフォルトアクションを継承する (Inherit default action)	復号しない (Do not decrypt) ブロック (Block) リセットしてブロック (Block with reset) デフォルトアクションを継承する (Inherit default action)
ハンドシェイク エラー (Handshake Errors)	SSLハンドシェイクのネゴシエーション中にエラーが発生しました。	デフォルトアクションを継承する (Inherit default action)	復号しない (Do not decrypt) ブロック (Block) リセットしてブロック (Block with reset) デフォルトアクションを継承する (Inherit default action)
復号エラー (Decryption Errors)	トラフィックの復号中にエラーが発生しました。	ブロック (Block)	ブロック (Block) リセットしてブロック (Block With Reset)

SSL ポリシーを最初に作成する場合、デフォルトアクションによって処理される接続のログは、デフォルトでは無効化されています。復号できないトラフィックの処理ではデフォルトアクションのログ設定も適用されるため、復号できないトラフィックのアクションで処理される接続のログは、デフォルトでは無効化されています。

ブラウザが証明書ピンングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号できないことに注意してください。このトラフィックはアクセスコントロールを使用して引き続き検査できるため、復号できないトラフィックアクションでは処理されません。このトラフィックを許可するには、サーバ証明書の共通名または識別名と一致させるために、[復号しない (Do not decrypt)] アクションを使用して SSL ルールを設定します。

## SSL ポリシーの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

SSL ポリシー エディタでは、次の操作を実行できます。






- ポリシーを設定する
- SSL ルールを追加、編集、削除、有効化、無効化、および編成する
- 信頼できる CA 証明書を追加する
- システムが復号できない暗号化トラフィックに対する処理を決定する
- デフォルトアクションおよび復号できないトラフィック アクションで処理されるトラフィックのログを記録する

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

## 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [SSL] を選択します。

**ステップ 2** SSL ポリシーを管理します。

- 関連付け：アクセス コントロール ポリシーに SSL ポリシーを関連付ける場合は、[アクセス制御への他のポリシーの関連付け \(1340 ページ\)](#) を参照してください。
- [比較 (Compare)]：[ポリシーの比較 (Compare Policies)] をクリックします ([ポリシーの比較 \(361 ページ\)](#) を参照)。
- コピー：コピーアイコン () をクリックします。
- 作成：[新規ポリシー (New Policy)] をクリックします。[基本 SSL ポリシーの作成 \(1462 ページ\)](#) を参照してください。
- 削除：削除アイコン () をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 展開：[展開 (Deploy)] をクリックします ([設定変更の導入 \(350 ページ\)](#) を参照)。
- 編集：編集アイコン () をクリックします。[SSL ポリシーの編集 \(1464 ページ\)](#) を参照してください。代わりに表示アイコン () が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- インポート/エクスポート：[コンフィギュレーションのインポート/エクスポートについて \(211 ページ\)](#) を参照してください。
- [レポート (Report)]：レポートアイコン () をクリックします ([現在のポリシー レポートの生成 \(363 ページ\)](#) を参照)。

## 基本 SSL ポリシーの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

SSL ポリシーの設定では、ポリシーに一意の名前を付け、デフォルトアクションを指定する必要があります。

### 手順

- ステップ 1 [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [SSL] を選択します。
- ステップ 2 [新しいポリシー (New Policy)] をクリックします。
- ステップ 3 [名前 (Name)] に一意のポリシー名を入力し、オプションで [説明 (Description)] にポリシーの説明を入力します。
- ステップ 4 [デフォルトアクション (Default Action)] を指定します。 [SSL ポリシーのデフォルトアクション \(1458 ページ\)](#) を参照してください。
- ステップ 5 [ポリシーのデフォルトアクションによる接続のロギング \(2517 ページ\)](#) の説明に従って、デフォルトアクションのロギング オプションを設定します。
- ステップ 6 [保存 (Save)] をクリックします。

### 次の作業

- SSL ポリシーに追加するルールを設定します。 [SSL ルールの作成および変更 \(1472 ページ\)](#) を参照してください。
- 復号化できないトラフィックのデフォルト処理を設定します。 [復号できないトラフィックのデフォルト処理の設定 \(1463 ページ\)](#) を参照してください。
- 復号化できないトラフィックのデフォルト処理のロギング オプションを設定します。 [ポリシーのデフォルトアクションによる接続のロギング \(2517 ページ\)](#) を参照してください。
- [アクセス制御への他のポリシーの関連付け \(1340 ページ\)](#) の説明に従って、SSL ポリシーをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## 復号できないトラフィックのデフォルト処理の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

システムによる復号や検査ができない特定タイプの暗号化トラフィックの処理については、SSLポリシーレベルで、復号できないトラフィックのアクションを設定できます。SSLルールがまったく含まれないSSLポリシーを展開する場合、ネットワーク上のすべての復号できない暗号化トラフィックの処理方法は、復号できないトラフィックのアクションによって決定されます。

復号できないトラフィックのタイプによって、次の選択ができます。

- 接続をブロックする
- 接続をブロックした後でリセットする
- アクセスコントロールを使用して暗号化トラフィックを検査する
- SSLポリシーのデフォルトアクションを継承する

### 手順

- ステップ 1** SSLポリシーエディタで、[復号できないアクション (Undecryptable Actions)] タブをクリックします。
- ステップ 2** 各フィールドで、SSLポリシーのデフォルトアクションを選択するか、復号できないタイプのトラフィックに対して実行する別のアクションを選択します。詳細については、[復号できないトラフィックのデフォルト処理オプション \(1459 ページ\)](#) と [SSLポリシーのデフォルトアクション \(1458 ページ\)](#) を参照してください。
- ステップ 3** [保存 (Save)] をクリックしてポリシーを保存します。

### 次のタスク

- 復号できないトラフィックのアクションで処理される接続に関するデフォルトロギングを設定します。[ポリシーのデフォルトアクションによる接続のロギング \(2517 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## SSL ポリシーの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

ポリシーの編集は、1つのブラウザウィンドウを使用して、一度に1人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシーエディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [SSL] を選択します。

**ステップ 2** 設定する SSL ポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** SSL ポリシーを設定します。

- 説明：SSL ポリシーの説明を更新するには、[説明 (Description)] フィールドをクリックし、新しい説明を入力します。
- ログ：復号できないトラフィックの処理および SSL ルールに一致しないトラフィックについて接続を記録するには、[ポリシーのデフォルトアクションによる接続のロギング \(2517 ページ\)](#) を参照してください。
- 名前の変更：SSL ポリシーの名前を変更するには、[名前 (Name)] フィールドをクリックし、新しい名前を入力します。
- デフォルト アクションの設定：SSL ポリシーが SSL ルールに一致しないトラフィックをどのように処理するかを設定するには、[SSL ポリシーのデフォルトアクション \(1458 ページ\)](#) を参照してください。
- 復号できないトラフィックのデフォルトアクションの設定：SSL ポリシーが復号できないトラフィックをどのように処理するかを設定するには、[復号できないトラフィックのデフォルト処理の設定 \(1463 ページ\)](#) を参照してください。
- 信頼：SSL ポリシーに信頼された CA 証明書を追加するには、[外部認証局の信頼 \(1515 ページ\)](#) を参照してください。

#### ステップ4 SSL ポリシー内のルールを編集します。

- 追加：ルールを追加するには、[ルールの追加 (Add Rule)] をクリックします。
- コピー：ルールをコピーするには、選択したルールを右クリックして、[コピー (Copy)] を選択します。
- 切り取り：ルールを切り取るには、選択したルールを右クリックして、[切り取り (Cut)] を選択します。
- 削除：ルールを削除するには、ルールの横にある削除アイコン (🗑️) をクリックして、[OK] をクリックします。
- 無効化：有効なルールを無効にするには、選択したルールを右クリックして、[状態 (State)] を選択し、[無効 (Disable)] を選択します。
- 表示：特定のルール属性の設定ページを表示するには、ルールの行にある条件の列で名前、値、またはアイコンをクリックします。たとえば、[送信元ネットワーク (Source Networks)] カラムに示されている名前または値をクリックすると、選択したルールの [ネットワーク (Networks)] ページが表示されます。詳細については、[ネットワークベースの SSL ルールの条件 \(1490 ページ\)](#) を参照してください。
- 編集：ルールを編集するには、ルールの横にある編集アイコン (✎) をクリックします。
- 有効化：無効なルールを有効にするには、選択したルールを右クリックして、[状態 (State)] を選択し、[有効 (Enable)] を選択します。無効なルールはグレー表示され、ルール名の下に [ (無効) ((disabled)) ] というマークが付きます。
- 貼り付け：切り取られたルールまたはコピーされたルールを貼り付けるには、選択したルールを右クリックして、[上に貼り付け (Paste above)] または [下に貼り付け (Paste below)] を選択します。

#### ステップ5 設定を保存または廃棄します。

- 変更を保存し、編集を続行する場合は、[保存 (Save)] をクリックします。
- 変更を廃棄する場合は、[キャンセル (Cancel)] をクリックし、プロンプトが出たら [OK] をクリックします。

---

#### 次のタスク

- SSL ポリシーがアクセス コントロール ポリシーにまだ関連付けられていない場合は、[アクセス制御への他のポリシーの関連付け \(1340 ページ\)](#) の説明に従って関連付けます。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[SSL ルールの作成および変更 \(1472 ページ\)](#)







## 第 64 章

# SSL ルールの使用を開始するには

ここでは、SSL ルールの作成、設定、管理、トラブルシューティングの概要を示します。

- [SSL ルールの概要 \(1467 ページ\)](#)
- [SSL ルールのトラフィック処理 \(1467 ページ\)](#)
- [SSL ルールの条件 \(1474 ページ\)](#)
- [SSL ルールのアクション \(1477 ページ\)](#)
- [SSL ルールの管理 \(1484 ページ\)](#)
- [SSL ルールのトラブルシューティング \(1487 ページ\)](#)

## SSL ルールの概要

SSL ポリシー内に各種の SSL ルールを設定することで、それ以上のインスペクションなしでトラフィックをブロックする、トラフィックを復号せずにアクセスコントロールで検査する、あるいはアクセスコントロールの分析用にトラフィックを復号するなど、複数の管理対象デバイスをカバーしたきめ細かな暗号化トラフィックの処理メソッドを構築できます。

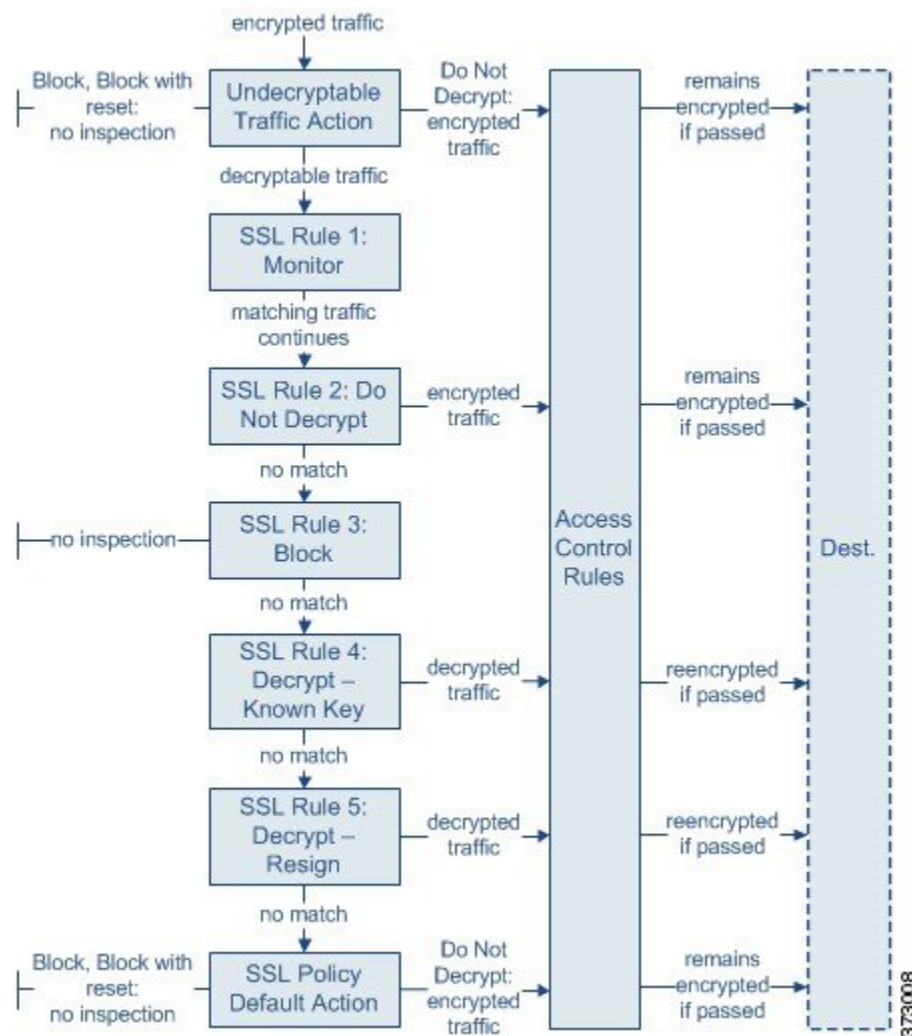
## SSL ルールのトラフィック処理

システムは指定した順序で SSL ルールをトラフィックと照合します。ほとんどの場合、システムによる暗号化トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の SSL ルールに従って行われます。こうした条件には、単純なものと複雑なものがあります。セキュリティゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書の識別名、証明書ステータス、暗号スイート、暗号化プロトコルバージョンなどによってトラフィックを制御できます。

各ルールにはアクションも設定されます。アクションにより、アクセス制御と一致する暗号化または復号化トラフィックに対してモニタ、ブロック、検査のいずれを行うかが決まります。システムがブロックした暗号化トラフィックは、それ以上のインスペクションが行われないことに注意してください。暗号化されたトラフィックおよび復号できないトラフィックは、アクセスコントロールを使用して検査します。ただし、一部のアクセスコントロールルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致

するルール数が少なくなる場合があります。またデフォルトでは、システムは暗号化ペイロードの侵入およびファイルインスペクションを無効にしています。

次のシナリオは、インライン展開での SSL ルールによるトラフィックの処理を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **復号できないトラフィックアクション (Undecryptable Traffic Action)** は、暗号化されたトラフィックを最初に評価します。復号できないトラフィックについては、システムはそれ以上のインスペクションを行わないでブロックするか、あるいはアクセス制御による検査に渡します。一致しなかった暗号化トラフィックは、次のルールへと進められます。
- **SSL ルール 1 : モニタ (SSL Rule 1: Monitor)** は、暗号化トラフィックを次に評価します。モニタールールは、暗号化トラフィックのログ記録と追跡を行います。トラフィックフローには影響しません。システムは引き続きトラフィックを追加のルールと照合し、許可するか拒否するかを決定します。

- **SSL ルール 2：復号しない (SSL Rule 2: Do Not Decrypt)** は、暗号化トラフィックを 3 番目に評価します。一致したトラフィックは復号されません。システムはこのトラフィックをアクセスコントロールにより検査しますが、ファイルや侵入インспекションは行いません。一致しないトラフィックは、引き続き次のルールと照合されます。
- **SSL ルール 3：ブロック (SSL Rule 3: Block)** は、暗号化トラフィックを 4 番目に評価します。一致するトラフィックは、追加のインспекションなしでブロックされます。一致しないトラフィックは、引き続き次のルールと照合されます。
- **SSL ルール 4：復号 - 既知のキー (SSL Rule 4: Decrypt - Known Key)** は、暗号化トラフィックを 5 番目に評価します。ネットワークへの着信トラフィックで一致したものは、ユーザのアップロードする秘密キーを使用して復号されます。復号トラフィックはその後、アクセスコントロールルールで評価されます。アクセスコントロールルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ルール 5：復号 - 再署名 (SSL Rule 5: Decrypt - Resign)** は、最後のルールです。トラフィックがこのルールに一致した場合、システムはアップロードされた CA 証明書を使用してサーバ証明書を再署名してから、中間者 (man-in-the-middle) としてトラフィックを復号します。復号トラフィックはその後、アクセスコントロールルールで評価されます。アクセスコントロールルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ポリシーのデフォルト アクション (SSL Policy Default Action)** は、どの SSL ルールにも一致しなかったすべてのトラフィックを処理します。デフォルトアクションでは、暗号化トラフィックをそれ以上のインспекションなしでブロックするか、あるいは復号しないで、アクセスコントロールによる検査を行います。

## 暗号化トラフィック インспекションの設定

暗号化セッションの特性に基づいた暗号化トラフィックの制御および暗号化トラフィックの復号には、再利用可能な公開キー インフラストラクチャ (PKI) オブジェクトの作成が必要です。この情報の追加は、信頼できる認証局 (CA) の証明書の SSL ポリシーへのアップロード時、SSL ルール条件の作成時、およびプロセスでの関連オブジェクトの作成時に、臨機応変に実行できます。ただし、これらのオブジェクトを事前に設定しておく、不適切なオブジェクトが作成される可能性を抑制できます。

### 証明書とキー ペアによる暗号化トラフィックの復号

セッション暗号化に使用するサーバ証明書と秘密キーをアップロードして内部証明書オブジェクトを設定しておく、システムは着信する暗号化トラフィックを復号化できます。[復号-既

知のキー (Decrypt - Known Key) ] アクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、システムはアップロードされた秘密キーを使用してセッションを復号化します。

CA 証明書と秘密キーをアップロードして内部 CA オブジェクトを設定した場合、システムは発信トラフィックの復号化もできます。[復号 - 再署名 (Decrypt - Resign) ] アクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、システムはクライアント ブラウザに渡されたサーバ証明書を再署名した後、中間者 (man-in-the-middle) としてセッションを復号します。オプションで、証明書全体ではなく自己署名証明書キーのみを置き換えることができます。この場合、ユーザはブラウザで自己署名証明書キー通知を確認します。

### 暗号化セッションの特性に基づいたトラフィック制御

システムによる暗号化トラフィックの制御は、セッションネゴシエートに使用されたサーバ証明書または暗号スイートに基づいて実行できます。複数の異なる再利用可能オブジェクトの 1 つを設定し、SSL ルール条件でオブジェクトを参照してトラフィックを照合することができます。次の表に、設定できる再利用可能なオブジェクトのタイプを示します。

設定する内容	暗号化トラフィック制御に使用する条件
1 つまたは複数の暗号スイートが含まれる暗号スイートのリスト	暗号化セッションのネゴシエートに使用される暗号スイートが、暗号スイート リストにある暗号スイートのいずれかに一致する。
組織が信頼する CA 証明書のアップロードによる信頼できる CA オブジェクト	この信頼できる CA は、次のいずれかにより、セッションの暗号化に使用されたサーバ証明書を信頼する。 <ul style="list-style-type: none"> <li>• CA が証明書を直接発行した。</li> <li>• サーバ証明書を発行した中間 CA に CA が証明書を発行した。</li> </ul>
サーバ証明書のアップロードによる外部証明書オブジェクト	セッションの暗号化に使用されたサーバ証明書が、アップロードされたサーバ証明書と一致する。
発行元の識別名または証明書サブジェクトを含む識別名オブジェクト	セッション暗号化に使用された証明書で、サブジェクトまたは発行元の共通名、国、組織、組織単位のいずれかが、設定された識別名と一致する。

### 関連トピック

[暗号スイート リスト](#) (483 ページ)

[識別名オブジェクト](#) (484 ページ)

[PKI オブジェクト](#) (487 ページ)

## SSL ルールのコンポーネント

各 SSL ルールには、一意の名前以外にも、次の基本コンポーネントがあります。

### 状態 (State)

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはネットワークトラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

### 位置 (Position)

SSL ポリシーのルールには1から始まる番号が付いています。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。モニタールールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

### 条件 (Conditions)

条件は、ルールが処理する特定のトラフィックを指定します。こうした条件では、セキュリティゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書のサブジェクトまたは発行元、証明書ステータス、暗号スイート、暗号化プロトコルバージョンなどによってトラフィックを照合できます。使用する条件は、ターゲット デバイスのライセンスによって異なります。

### 操作 (Action)

ルールのアクションによって、一致したトラフィックの処理方法が決まります。暗号化された一致したトラフィックは、モニタ、許可、ブロック、または復号できます。復号および許可された暗号化トラフィックは、さらなる検査の影響下に置かれます。システムは、ブロックされた暗号化トラフィックに対してはインスペクションを実行しないことに注意してください。

### ログ

ルールのロギング設定によって、システムが記録する処理済みトラフィックのレコードを管理します。1つのルールに一致するトラフィックのレコードを1つ保持できます。SSL ポリシーでの設定に従って、システムが暗号化セッションをブロックするか、あるいは復号なしで渡すことを許可するときに、その接続をログに記録できます。アクセスコントロールルールに従ってより詳細な評価のために復号化した場合の接続ログを記録するようにシステムを強制することも可能で、これはその後でどのような処理やトラフィックの検査がされるかとは無関係です。接続のログは、Firepower Management Center のデータベースの他に、システムログ (Syslog) または SNMP トラップ サーバに記録できます。



#### ヒント

SSL ルールを適切に作成し順序付けするのは複雑なタスクです。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、追加のライセンスが必要となったり、ルールに無効な設定が含まれる場合があります。予期したとおりにトラフィックが確実に処理されるようにするために、SSL ポリシーインターフェイスには、ルールに関する強力な警告およびエラーのフィードバック システムが用意されています。

#### 関連トピック

[インターフェイス条件](#) (374 ページ)

- [ネットワーク条件](#) (377 ページ)
- [VLAN 条件](#) (382 ページ)
- [ポートおよび ICMP コードの条件](#) (382 ページ)
- [アプリケーション条件 \(アプリケーション制御\)](#) (386 ページ)
- [URL 条件 \(URL フィルタリング\)](#) (393 ページ)
- [ユーザ条件、レルム条件、および ISE 属性条件 \(ユーザ制御\)](#) (401 ページ)
- [ルールのパフォーマンスに関するガイドライン](#) (412 ページ)
- [SSL ルールのトラブルシューティング](#) (1487 ページ)

## SSL ルールの作成および変更

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス ( <b>Access</b> )
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [SSL] を選択します。

**ステップ 2** SSL ポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** 次の選択肢があります。

- 新しいルールを追加するには、[ルールの追加 (Add Rule)] をクリックします。
- 既存のルールを編集するには、編集アイコン (✎) をクリックします。

**ステップ 4** 名前を入力します。

**ステップ 5** 上記に要約されるようにルールコンポーネントを設定します。次の設定をするか、デフォルト設定をそのまま使用することができます。

- ルールを**有効**にするかどうかを指定します。
- ルールの位置を指定します。[SSL ルールの順序の評価 \(1473 ページ\)](#) を参照してください。
- [アクション (Action)] で、ルールのアクションを選択します。[SSL ルールアクションの設定 \(1482 ページ\)](#) を参照してください。
- ルールの条件を設定します。[SSL ルールの条件タイプ \(1475 ページ\)](#) を参照してください。

- [ログ (Logging) ] オプションを指定します。 [SSL ルールによる復号可能接続のロギング \(2514 ページ\)](#) を参照してください。

ステップ 6 [保存 (Save) ] をクリックします。

#### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## SSL ルールの順序の評価

SSL ルールを最初に作成するときに、ルールエディタの [挿入 (Insert) ] ドロップダウンリストを使用して、その位置を指定します。SSL ポリシーの SSL ルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、SSL ルールを上から順にトラフィックと照合します。

ほとんどの場合、システムによるネットワークトラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の SSL ルールに従って行われます。モニタールール (トラフィックをログに記録するがトラフィックフローには影響しないルール) の場合を除き、システムは、そのトラフィックがルールに一致した後、追加の優先順位の低いルールに対してトラフィックを評価し続けることはありません。



#### ヒント

適切な SSL ルールの順序を指定することで、ネットワークトラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

番号ごとのルールの順序付けに加えて、カテゴリ別にルールをグループ化できます。デフォルトでは、3つのカテゴリ (管理者、標準、ルート) があります。カスタムカテゴリを追加できますが、システム提供のカテゴリを削除したり、それらの順序を変更したりすることはできません。

#### 関連トピック

[ルールのパフォーマンスに関するガイドライン \(412 ページ\)](#)

## ルールカテゴリへの SSL ルールの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

## 手順

**ステップ1** SSL ルールエディタの [挿入 (Insert) ] ドロップダウンリストで [カテゴリ (Into Category) ] を選択し、使用するカテゴリを選択します。

**ステップ2** [保存 (Save) ] をクリックします。

ヒント ルールを保存すると、そのカテゴリの最後に配置されます。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 番号による SSL ルールの配置

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

## 手順

**ステップ1** SSL ルールエディタの [挿入 (Insert) ] ドロップダウンリストで、[ルールの上 (above rule) ] または [ルールの下 (below rule) ] を選択して、適切なルール番号を入力します。

**ステップ2** [保存 (Save) ] をクリックします。

ヒント ルールを保存すると、指定した場所に配置されます。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## SSL ルールの条件

SSL ルールの条件は、ルールで処理する暗号化トラフィックのタイプを特定します。条件には、単純なものと複雑なものがあり、ルールごとに複数の条件タイプを指定できます。トラフィックにルールが適用されるのは、トラフィックがルールの条件をすべて満たしている場合だけです。



ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。たとえば、証明書の条件が設定され、バージョンの条件が設定されていないルールは、セッションSSLまたはTLSのバージョンにかかわらず、セッションのネゴシエーションに使用されるサーバ証明書に基づいてトラフィックを評価します。

すべてのSSLルールには、一致する暗号化トラフィックに対して次の判定をする関連アクションがあります。

- 処理：まず第一に、ルールアクションはルールの条件に一致する暗号化トラフィックに対して、モニタ、信頼、ブロック、または復号化を行うかどうかを判定します。
- ロギング：ルールアクションは一致する暗号化トラフィックの詳細をいつ、どのようにログに記録するかを判定します。

SSLインスペクション設定では、次のように復号されたトラフィックの処理、検査、ログ記録を行います。

- SSLポリシーの復号できないアクションは、システムが復号できないトラフィックを処理します。
- ポリシーのデフォルトアクションは、モニタ以外のどのSSLルールの条件にも一致しないトラフィックを処理します。

システムが暗号化セッションを信頼またはブロックしたときに、接続イベントをログに記録できます。アクセスコントロールルールに従ってより詳細な評価のために復号した場合の接続ログを記録するようにシステムを強制することも可能で、これはその後でどのような処理やトラフィックの検査がされるかとは無関係です。暗号化セッションの接続ログには、セッションの暗号化に使用される証明書など、暗号化の詳細が含まれます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続 ([ブロック (Block) ], [リセットしてブロック (Block with reset) ]) の場合、システムは即座にセッションを終了し、イベントを生成します。
- 信頼された接続 (Do not decrypt) の場合、システムはセッション終了時にイベントを生成します。

## SSL ルールの条件タイプ

SSLルールを追加および編集するときは、ルールエディタ下部の左側にあるタブを使用して、ルール条件の追加と編集を行います。

表 91: SSL ルールの条件タイプ

条件	一致する暗号化トラフィック	詳細 (Details)
ゾーン	特定のセキュリティゾーンでインターフェイスを介したデバイスへの着信またはデバイスからの発信	セキュリティゾーンは、ご使用の導入ポリシーおよびセキュリティポリシーに準じた1つ以上のインターフェイスの論理グループです。ゾーン内のインターフェイスは、複数のデバイスにまたがって配置される場合があります。
ネットワーク	その送信元または宛先 IP アドレス、国、または大陸による	IP アドレスを明示的に指定できます。位置情報機能を使用して、その送信元または宛先の国または大陸に基づいてトラフィックを制御できます。
VLAN タグ	VLAN のタグ	システムは、最も内側の VLAN タグを使用して VLAN を基準にパケットを識別します。
ポート	その送信元または宛先ポートによる	TCP ポートに基づいて暗号化トラフィックを制御できます。
Users	セッションに関与するユーザによる	暗号化されたモニタ対象セッションの関連ホストにログインしている LDAP ユーザに基づいて暗号化トラフィックを制御できます。Microsoft Active Directory サーバから取得された個別ユーザまたはグループに基づいてトラフィックを制御できます。
アプリケーション	セッションで検出されたアプリケーションによる	タイプ、リスク、ビジネスとの関連性、カテゴリの基本的な特性に従って、フィルタ アクセスまたは暗号化セッションの各アプリケーションへのアクセスを制御できます。
カテゴリ	証明書サブジェクトの識別名に基づいてセッションで要求される URL	URL の一般分類とリスク レベルに基づいて、ネットワークのユーザがアクセスできる Web サイトを制限できます。
識別名	暗号化セッションのネゴシエートに使用されたサーバ証明書のサブジェクトまたは発行元の識別名	サーバ証明書を発行した CA またはサーバ証明書ホルダーに基づいて、暗号化トラフィックを制御できます。

条件	一致する暗号化トラフィック	詳細 (Details)
証明書 (Certificates)	暗号化セッションのネゴシエートに使用されるサーバ証明書	暗号化セッションのネゴシエート用にユーザのブラウザに渡されるサーバ証明書に基づいて、暗号化されたトラフィックを制御できます。
証明書のステータス (Certificate Status)	暗号化セッションのネゴシエートに使用されるサーバ証明書のプロパティ	サーバ証明書のステータスに基づいて、暗号化トラフィックを制御できます。
暗号スイート	暗号化セッションのネゴシエートに使用する暗号スイート	暗号化セッションのネゴシエート用にサーバで選択された暗号スイートに基づいて、暗号化トラフィックを制御できます。
バージョン	セッションの暗号化に使用される SSL または TLS のバージョン	セッションの暗号化に使用される SSL または TLS のバージョンに基づいて、暗号化トラフィックを制御できます。

#### 関連トピック

[ネットワーク ベースの SSL ルールの条件](#) (1490 ページ)

[ユーザベースの SSL ルールの条件](#) (1498 ページ)

[暗号化トラフィックでのレピュテーションベースの URL ブロッキング](#) (1506 ページ)

[サーバ証明書ベースの SSL ルール条件](#) (1508 ページ)

[ClientHello メッセージ処理](#) (1437 ページ)

## SSL ルールのアクション

### SSL ルール : モニタ アクション

[ モニタ (Monitor) ] アクションは暗号化トラフィック フローに影響を与えません。つまり、一致するトラフィックがただちに許可または拒否されることはありません。その代わりに、追加のルールが存在する場合はそのルールに照らしてトラフィックが照合され、信頼するか、ブロックするか、復号するかが決定されます。モニタールール以外の一致する最初のルールが、トラフィック フローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、システムはデフォルト アクションを使用します。

モニタールールの主要な目的はネットワーク トラフィックを追跡することであるため、ルールのロギング設定や、あとで接続を処理するデフォルトのアクションにかかわらず、システムはモニター対象トラフィックの接続終了イベントを自動的に Firepower Management Center データベースに記録します。

## SSL ルール：復号しないアクション

[復号しない (Do not decrypt) ]アクションは、アクセス コントロール ポリシーのルールおよびデフォルトアクションに従って暗号化トラフィックを評価するため転送します。一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、こうしたトラフィックに一致するルール数が少なくなる場合があります。暗号化トラフィックに対しては、侵入やファイル インスペクションなどのディープ インスペクションを行うことはできません。

[復号しない (Do not decrypt) ]ルールの一般的な理由は、以下のとおりです。

- SSL トラフィックの復号が法律によって禁止されている。
- 信頼できると判明しているサイトである。
- トラフィックを調べることによって中断できるサイト (Windows Update など) である。

詳細については、次を参照してください。 [復号できないトラフィックのデフォルト処理オプション \(1459 ページ\)](#)

## SSL ルール：ブロッキングアクション

[ブロック (Block) ]および[リセットしてブロック (Block with reset) ]アクションは、アクセス コントロール ルールの [ブロック (Block) ]と [リセットしてブロック (Block with reset) ]アクションに類似しています。これらのアクションは、クライアントとサーバによる SSL 暗号化セッションの確立と暗号化トラフィックの転送を防止します。リセット付きブロックルールでは接続のリセットも行います。

ブロックされた暗号化トラフィックについては、設定された応答ページが表示されないのに注意してください。その代わりに、ユーザの要求する禁止された URL の接続は、リセットされるか、またはタイムアウトになります。



### ヒント

パッシブまたはインライン (タップモード) 展開では、デバイスがトラフィックを直接検査しないので、[ブロック (Block) ]と [リセットしてブロック (Block with reset) ]アクションを使用できないことに注意してください。パッシブまたはインライン (タップモード) インターフェイスを含むセキュリティゾーン条件内で、[ブロック (Block) ]と [リセットしてブロック (Block with reset) ]アクションを使用したルールを作成すると、ポリシー エディタでルールの横に警告アイコン (⚠) が表示されます。

### 関連トピック

[HTTP 応答ページについて \(1369 ページ\)](#)

## SSL ルール : 復号アクション

[復号 - 既知のキー (Decrypt - Known Key) ]および[復号 - 再署名 (Decrypt - Resign) ]アクションは、暗号化トラフィックを復号します。復号されたトラフィックは、アクセス制御を使用して検査されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。ここではデータの確認に加えて、侵入、禁止ファイル、マルウェアを検出およびブロックできます。システムは、許可されたトラフィックを再暗号化してから宛先に渡します。

### SSL ルールの復号メカニズムとガイドライン

[復号 - 既知のキー (Decrypt - Known Key) ]アクションを設定した場合は、1つまたは複数のサーバ証明書と秘密キーペアをアクションに関連付けることができます。トラフィックがルールに一致して、トラフィックの暗号化に使用された証明書とアクションに関連付けられた証明書が一致した場合、システムは適切な秘密キーを使用してセッションの暗号化と復号キーを取得します。秘密キーへのアクセスが必要なため、このアクションが最も適しているのは、組織の管理下にあるサーバへの入力トラフィックを復号する場合です。






同様に [復号 - 再署名 (Decrypt - Resign) ]アクションには、1つの認証局証明書と秘密キーを関連付けることができます。トラフィックがこのルールに一致した場合、システムはCA 証明書を使用してサーバ証明書を再署名してから、中間者 (man-in-the-middle) として機能します。ここでは2つのSSLセッションが作成され、1つはクライアントと管理対象デバイスの間、もう1つは管理対象デバイスとサーバの間で使用されます。各セッションにはさまざまな暗号セッションの詳細が含まれており、システムはこれを使用することでトラフィックの復号化と再暗号化が行えます。このアクションは、証明書の秘密キーを各自の管理下にあるキーに置き換えてセッション キーを取得するため、発信トラフィックに適しています。

サーバ証明書の再署名では、証明書の公開キーをCA 証明書の公開キーに置き換えるか、あるいは証明書全体が置き換えられます。通常、サーバ証明書全体を置き換える場合は、SSL接続が確立された時点で、証明書が信頼できる認証局によって署名されていないことがクライアントブラウザで警告されます。ただし、そのCA をクライアントブラウザで信頼できることがポリシーに設定されている場合、ブラウザは証明書が信頼できないことについて警告しません。オリジナルのサーバ証明書が自己署名の場合、システムは証明書全体を置き換えて再署名するCA を信頼しますが、ユーザのブラウザは証明書が自己署名されていることを警告しません。この場合、サーバ証明書の公開キーを交換するだけで、クライアントブラウザは証明書が自己署名であることを警告します。

[復号 - 再署名 (Decrypt - Resign) ]アクションをルールに設定すると、ルールによるトラフィックの照合は、設定されている他のルール条件に加えて、参照する内部CA 証明書の署名アルゴリズムタイプに基づいて実施されます。各 [復号 - 再署名 (Decrypt - Resign) ]アクションにはそれぞれ1つのCA 証明書が関連付けられるので、異なる署名アルゴリズムで暗号化された複数のタイプの発信トラフィックを復号化するSSLルールは作成できません。また、ルールに追加する暗号スイートと外部証明書のオブジェクトのすべては、関連するCA 証明書の暗号化アルゴリズムタイプに一致する必要があります。オプションで、証明書全体ではなく自己署名証明書キーのみを置き換えることができます。この場合、ユーザはブラウザで自己署名証明書キー通知を確認します。

たとえば、楕円曲線暗号 (EC) アルゴリズムで暗号化された発信トラフィックが [復号 - 再署名 (Decrypt - Resign)] ルールに一致するのは、アクションが EC ベースの CA 証明書を参照している場合だけです。証明書と暗号スイートのルール条件を作成する場合は、EC ベースの外部証明書と暗号スイートをルールに追加する必要があります。同様に、RSA ベースの CA 証明書を参照する [復号 - 再署名 (Decrypt - Resign)] ルールは、RSA アルゴリズムで暗号化された発信トラフィックとのみ一致します。EC アルゴリズムで暗号化された発信トラフィックは、設定されている他のルール条件がすべて一致したとしても、このルールには一致しません。

次の点に注意してください。

- SSL 接続の確立に使用される暗号スイートが Diffie-Hellman Ephemeral (DHE) または楕円曲線 Diffie-Hellman Ephemeral (ECDHE) キー交換アルゴリズムを適用している場合、パッシブ展開では [復号 - 既知のキー (Decrypt - Known Key)] アクションを使用できません。SSL ポリシーのターゲットデバイスにパッシブまたはインライン (タップモード) インターフェイスがあり、そこに含まれる [復号 - 既知のキー (Decrypt - Known Key)] ルールで DHE または ECDHE の暗号スイート条件が使われている場合、ルールの横に情報アイコン ([)] が表示されます。パッシブまたはインライン (タップモード) インターフェイスを含む SSL ルールに後からゾーン条件を追加すると、警告アイコン ([)] が表示されます。
- デバイスはトラフィックを直接検査しないため、パッシブまたはインライン (タップモード) 展開では [復号 - 再署名 (Decrypt - Resign)] アクションを使用できません。セキュリティゾーン内にパッシブまたはインライン (タップモード) インターフェイスを含む [復号 - 再署名 (Decrypt - Resign)] アクションを指定してルールを作成すると、ポリシーエディタでルールの横に警告アイコン () が表示されます。SSL ポリシーのターゲットデバイスにパッシブまたはインライン (タップモード) インターフェイスがあり、[復号 - 再署名 (Decrypt - Resign)] ルールが含まれる場合、ルールの横に情報アイコン ([)] が表示されます。パッシブまたはインライン (タップモード) インターフェイスを含む SSL ルールに後からゾーン条件を追加すると、警告アイコン ([)] が表示されます。パッシブまたはインライン (タップモード) インターフェイスを含むデバイスに、[復号 - 再署名 (Decrypt - Resign)] ルールを含む SSL ポリシーを適用した場合、このルールに一致する SSL セッションはすべて失敗します。
- サーバ証明書の再署名に使用する CA をクライアントが信頼していない場合、証明書が信頼できないという警告がユーザに出されます。これを防ぐには、クライアントの信頼できる CA ストアに CA 証明書をインポートします。または、組織にプライベート PKI がある場合は、組織の全クライアントにより自動的に信頼されるルート CA が署名する中間 CA 証明書を発行して、その CA 証明書をデバイスにアップロードすることもできます。
- SSL ルールの暗号スイート条件に匿名の暗号スイートを追加できますが、次の点に注意してください。
  - システムは ClientHello 処理中に自動的に匿名の暗号スイートを削除します。ルールを使用するシステムでは、ClientHello の処理を防止するために SSL ルールも設定する必要があります。詳細については、[SSL ルールの順序 \(416 ページ\)](#) を参照してください。

- システムは匿名の暗号スイートで暗号化されたトラフィックを復号化できないため、ルールで[復号-再署名 (Decrypt-Resign) ]または[復号-既知のキー (Decrypt-Known Key) ]アクションは使用できません。
- クライアントと管理対象デバイスの中に HTTP プロキシがあって、クライアントとサーバが CONNECT HTTP メソッドを使用してトンネル SSL 接続を確立する場合、システムはトラフィックを復号化できません。システムによるこのトラフィックの処理法は、ハンドシェイクエラー (**Handshake Errors**) の復号できないアクションが決定します。
- システムは、管理対象デバイス上のキャプティブポータルユーザの Web ブラウザとキャプティブポータルのデーモン間のキャプティブポータルの認証接続でトラフィックを復号化できません。
- [復号-既知のキー (Decrypt-Known Key) ]アクションを指定して SSL ルールを作成した場合は、[識別名 (Distinguished Name) ]や[証明書 (Certificate) ]条件による照合はできません。ここでの前提は、このルールがトラフィックと一致する場合、証明書、サブジェクト DN、および発行元 DN は、ルールに関連付けられた証明書とすでに一致済みであることです。
- 内部 CA オブジェクトを作成して証明書署名要求 (CSR) の生成を選択した場合は、オブジェクトに署名付き証明書をアップロードするまで、この CA を [復号-再署名 (Decrypt-Resign) ]アクションに使用できません。
- [復号-再署名 (Decrypt-Resign) ]アクションをルールに設定し、1 つまたは複数の外部証明書オブジェクトまたは暗号スイートで署名アルゴリズムタイプの不一致が生じた場合、ポリシーエディタでルールの横に情報アイコン (i) が表示されます。すべての外部証明書オブジェクトまたはすべての暗号スイートで署名アルゴリズムタイプの不一致が生じた場合、ポリシーのルールの横には警告アイコン ([!]) が表示され、SSL ポリシーに関連付けたアクセスコントロールポリシーは適用できなくなります。
- ブラウザが証明書ピンングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号化できません。このトラフィックを許可するには、サーバ証明書の共通名または識別名と一致させるために、[復号しない (Do not decrypt) ]アクションを使用して SSL ルールを設定します。
- [インタラクティブブロック (Interactive Block) ]または[リセット付きインタラクティブブロック (Interactive Block with reset) ]アクション付きのアクセスコントロールルールと復号化トラフィックが一致する場合、システムは応答ページを表示します。
- インライン正規化プリプロセッサで[余剰ペイロードの正規化 (Normalize Excess Payload) ]オプションを有効にすると、プリプロセッサによる復号トラフィックの標準化時に、パケットがドロップされてトリミングされたパケットに置き換えられる場合があります。これにより SSL セッションは終了しません。トラフィックが許可された場合、トリミングされたパケットは SSL セッションの一部として暗号化されます。

## 関連トピック

[PKI オブジェクト](#) (487 ページ)

## SSL ルールアクションの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** SSL ポリシー エディタには、次のオプションがあります。

- 新しいルールを追加するには、[ルールを追加 (Add Rule)] をクリックします。
- 既存のルールを編集するには、編集アイコン (✎) をクリックします。

**ステップ 2** [アクション (Action)] ドロップダウン リストからルールアクションを選択します。

- 暗号化トラフィックをブロックするには、[ブロック (Block)] を選択します。
- 暗号化トラフィックをブロックし、接続をリセットするには、[リセットでブロック (Block with reset)] を選択します。
- 着信トラフィックの復号の詳細については、[復号 - 既知のキーアクションの設定 \(1483 ページ\)](#) を参照してください。
- 発信トラフィックの復号の詳細については、[復号 - 再署名アクションの設定 \(1483 ページ\)](#) を参照してください。
- 暗号化トラフィックを記録するには、[モニタ (Monitor)] を選択します。
- 暗号化トラフィックを復号しない場合は、[復号化しない (Do Not Decrypt)] を選択します。

**ステップ 3** [追加 (Add)] をクリックします。

### 次のタスク

- [ネットワークベースの SSL ルールの条件 \(1490 ページ\)](#)、[ユーザベースの SSL ルールの条件 \(1498 ページ\)](#)、[レピュテーションベースの SSL ルール条件 \(1499 ページ\)](#)、および [サーバ証明書ベースの SSL ルール条件 \(1508 ページ\)](#) の説明に従ってルール条件を設定します。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。



## 復号 - 再署名アクションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

- ステップ 1 SSL ルール エディタで、[アクション (Action)] リストから [復号 - 再署名 (Decrypt-Resign)] を選択します。
- ステップ 2 リストから内部 CA 証明書のオブジェクトを選択します。
- ステップ 3 証明書全体ではなく証明書公開キーのみを置き換えるには、[キー置換 (Replace Key)] [キー置換のみ (Replace Key Only)] をオンにする必要があります。公開キーのみを置き換えようとしているため、自己署名証明書の通知がユーザのブラウザに表示されます。
- ステップ 4 [追加 (Add)] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 復号 - 既知のキー アクションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

- ステップ 1 SSL ルール エディタで、[アクション (Action)] ドロップダウン リストから、[復号 - 既知のキー (Decrypt - Known Key)] を選択します。
- ステップ 2 [クリックして復号証明書を選択 (Click to select decryption certs)] フィールドをクリックします。
- ステップ 3 [使用可能な証明書 (Available Certificates)] リストの 1 つ以上の内部証明書のオブジェクトを選択し、[ルールに追加 (Add to Rule)] をクリックします。
- ステップ 4 [OK] をクリックします。

ステップ 5 [追加 (Add)] をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## SSL ルールの管理

SSL ポリシー エディタの [ルール (Rules)] タブでは、ポリシー内の SSL ルールの追加、編集、検索、移動、有効化、無効化、削除、およびその他の管理を行うことができます。

### SSL ルール検索

スペースおよび印刷可能な特殊文字を含む英数字文字列を使用して、SSL ルールのリストで一致する値を検索できます。この検索では、ルール名およびルールに追加したルール条件が検索されます。ルール条件の場合は、条件タイプ（ゾーン、ネットワーク、アプリケーションなど）ごとに追加できる任意の名前または値が検索照合されます。これには、個々のオブジェクト名または値、グループオブジェクト名、グループ内の個々のオブジェクト名または値、およびリテラル値が含まれます。

検索文字列のすべてまたは一部を使用できます。照合ルールごとに、一致する値のカラムが強調表示されます。たとえば、100Bao という文字列のすべてまたは一部を基準に検索すると、少なくとも、100Bao アプリケーションが追加された各ルールの [アプリケーション (Applications)] 列が強調表示されます。100Bao という名前のルールもある場合は、[名前 (Name)] 列と [アプリケーション (Applications)] 列の両方が強調表示されます。

1つ前または次の照合ルールに移動することができます。ステータスメッセージには、現行の一致および合計一致数が表示されます。

複数ページのルールリストでは、どのページでも一致が検出される可能性があります。最初の一致が検出されたのが最初のページではない場合は、最初の一致が検出されたページが表示されます。最後の一致が現行の一致となっている場合、次の一致を選択すると、最初の一致が表示されます。また、最初の一致が現行の一致となっている場合、前の一致を選択すると、最後の一致が表示されます。

### SSL ルールの検索

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

## 手順

**ステップ1** SSL ポリシー エディタで、[検索ルール (Search Rules) ] プロンプトをクリックし、検索文字列を入力してから Enter キーを押します。

**ヒント** 一致する値を含むルールのカラムが強調表示されます。表示されている (最初の) 一致は、他とは区別できるように強調表示されます。

**ステップ2** 目的のルールを見つけます。

- 照合ルールの間を移動する場合は、次の一致アイコン (▼) または前の一致アイコン (▲) をクリックします。
- ページを更新し、検索文字列および強調表示をクリアするには、クリア アイコン (✖) をクリックします。

## SSL ルールの有効化と無効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

作成した SSL ルールは、デフォルトで有効になっています。ルールを無効にすると、システムはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。SSL ポリシーのルールリストを表示すると、無効なルールはグレー表示されますが、変更は可能です。またはルール エディタを使用して SSL ルールを有効または無効にできることに注意してください。

## 手順

**ステップ1** SSL ポリシー エディタで、ルールを右クリックしてルール状態を選択します。

**ステップ2** [保存 (Save) ] をクリックします。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## SSL ルールの移動

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** SSL ポリシー エディタで、各ルール of 空白部分をクリックしてルールを選択します。

**ステップ 2** ルールを右クリックして、[切り取り (Cut)] を選択します。

**ステップ 3** 切り取ったルールを貼り付けたい位置に隣接するルールの空白部分を右クリックし、[上に貼り付け (Paste above)] または [下に貼り付け (Paste below)] を選択します。

**ヒント** 2つの異なる SSL ポリシーの間では、SSL ルールのコピー アンド ペーストはできません。

**ステップ 4** [保存 (Save)] をクリックします。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 新しい SSL ルール カテゴリの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

余計なポリシーを作成することなくルールをさらに整理するため、標準ルールとルートルールのカテゴリの間にカスタムカテゴリを作成できます。追加したカテゴリは、名前変更と削除ができます。これらのカテゴリの移動はできませんが、ルールのカテゴリ間およびカテゴリ内外への移動は可能です。

### 手順

**ステップ 1** SSL ポリシー エディタで、[カテゴリの追加 (Add Category)] をクリックします。

**ヒント** ポリシーにルールがすでに含まれている場合は、既存のルールの行の空白部分をクリックして、新しいカテゴリを追加する前にその位置を設定できます。既存のルールを右クリックし、[新規カテゴリの挿入 (Insert new category)] を選択することもできます。

**ステップ 2** [名前 (Name)] を入力します。

**ステップ 3** 次の選択肢があります。

- 最初の [挿入 (Insert)] ドロップダウンリストから [カテゴリの上 (above Category)] を選択した後、2 番目のドロップダウンリストからカテゴリを選択します。ここで選択したカテゴリの上にルールが配置されます。
- ドロップダウンリストから [ルールの下 (below rule)] を選択し、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。
- ドロップダウンリストから [ルールの上 (above rule)] を選択し、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

**ステップ 4** [OK] をクリックします。

**ヒント** 削除するカテゴリに含まれるルールは、その上にあるカテゴリに追加されます。

**ステップ 5** [保存 (Save)] をクリックします。

## SSL ルールのトラブルシューティング

SSL ルールを適切に設定するのは複雑なタスクですが、暗号化トラフィックを処理する有効な導入には不可欠のタスクです。ルールが互いをプリエンプトしたり、追加ライセンスが必要になったりすることがあります。また、ルールに無効な設定が含まれる可能性もあります。慎重に設定された SSL ルールは、ネットワークトラフィックの処理に必要なリソースの軽減にも寄与します。あまりにも複雑なルールを作成したり、ルールの順番が不適切であったりすると、パフォーマンスに影響する可能性があります。詳細については、[ルールのパフォーマンスに関するガイドライン \(412 ページ\)](#) を参照してください。

### SSL ルールの無効な設定に対する警告

SSL ポリシーが依存する外部の設定は変更される可能性があるため、有効であった SSL ポリシー設定が無効になる場合があります。次の例について考えてみます。

- URL カテゴリ条件を含むルールで、それまで有効であったものが、URL フィルタリングライセンスを持たないデバイスをターゲットにすることで無効になる場合があります。その時点で、ルールの横にエラーアイコンが表示され、ポリシーをそのデバイスに展開でき

なくなります。展開可能にするには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、または適切なライセンスを有効にする必要があります。

- [復号 - 再署名 (Decrypt-Resign) ]ルールを作成し、後でパッシブ インターフェイスでセキュリティゾーンを条件として追加した場合、ルールの横に警告アイコンが表示されます。パッシブ展開では証明書の再署名によるトラフィックの復号はできないので、パッシブインターフェイスをルールから削除するか、またはルールアクションを変更するまで、このルールには効果がありません。
- ルールにレلمまたはユーザを追加した後、そのレلمまたはユーザを除外するようにレلمの設定を変更すると、ルールは適用されなくなります。
- ServerHello またはサーバ証明書条件（証明書、識別名、証明書のステータス、暗号スイート、バージョン）と一致する [復号しない (Do not decrypt) ]ルールを、ClientHello 条件（ゾーン、ネットワーク、VLAN タグ、ポート、ユーザ、アプリケーション、カテゴリ）で照合する [復号 - 再署名 (Decrypt-Resign) ]ルールの前に配置する場合、ClientHello の変更をプリエンプトして、復号されないセッションの数を増やすことができます。システムがこの準最適な設定に含まれるルールを識別すると、ServerHello またはサーバ証明書条件を使用するルールの横に警告アイコンが表示されます。

#### 関連トピック

[ルールとその他のポリシーの警告](#) (411 ページ)

[ルールのパフォーマンスに関するガイドライン](#) (412 ページ)



## 第 65 章

# SSL ルールを使用した復号の調整

次のトピックでは、SSL ルール条件を設定する方法の概要を示します。

- [SSL ルール条件の概要 \(1489 ページ\)](#)
- [ネットワーク ベースの SSL ルールの条件 \(1490 ページ\)](#)
- [ユーザベースの SSL ルールの条件 \(1498 ページ\)](#)
- [レピュテーション ベースの SSL ルール条件 \(1499 ページ\)](#)
- [サーバ証明書ベースの SSL ルール条件 \(1508 ページ\)](#)

## SSL ルール条件の概要

デバイスで検査されるすべての暗号化トラフィックには、基本的な SSL ルールに基づいたアクションが適用されます。暗号化トラフィックをより詳細に復号および制御するには、特定タイプのトラフィックの処理およびログ記録を制御するルール条件を設定します。各 SSL ルールには 0 個、1 個、または複数の条件を設定できますが、トラフィックに SSL ルールが適用されるのは、そのルールのすべての条件にトラフィックが一致する場合のみです。



(注) トラフィックがルールに一致すると、デバイスは設定されたルールアクションをトラフィックに適用します。ログの記録が指定されている場合、接続が終了した時点でトラフィックに関するログが記録されます。

各ルール条件には、照合するトラフィックのプロパティを 1 つまたは複数指定できます。たとえば、以下のプロパティを指定できます。

- 通過するセキュリティゾーン、IP アドレスおよびポート、送信元または宛先の国、送信元または宛先の VLAN などのトラフィックフロー
- 検出された IP アドレスに関連付けられたユーザ
- トラフィックで検出されたアプリケーションなどのトラフィックペイロード
- 接続の暗号化に使用された SSL/TLS プロトコルバージョン、暗号スイート、サーバ証明書などの接続暗号化

- サーバ証明書の識別名に指定された URL のカテゴリおよびレピュテーション

## ネットワーク ベースの SSL ルールの条件

SSL ポリシーに追加する SSL ルールにより、暗号化トラフィックの処理やログ記録を詳細に制御できます。ネットワークベースの条件を使用して、ネットワークを通過する暗号化トラフィックを管理できます。以下の条件を使用できます。

- SSL ルールでゾーン条件を設定すると、暗号化トラフィックの送信元および宛先のセキュリティゾーンに応じてそのトラフィックを制御できます。セキュリティゾーンとは、1つ以上のインターフェイスの論理グループを指します。ゾーン内のインターフェイスが複数のデバイス間に配置される場合もあります。検出モードと呼ばれる、デバイスの初期セットアップ時に選択するオプションによって、システムが最初にデバイスのインターフェイスをどのように設定するか、およびこれらのインターフェイスがセキュリティゾーンに属するかどうかが決まります。
- SSL ルールでネットワーク条件を設定すると、暗号化トラフィックの送信元および宛先の IP アドレスに応じてそのトラフィックを制御および復号できます。制御対象とする暗号化トラフィックの送信元と宛先の IP アドレスを明示的に指定するか、地理位置情報機能を使用することができます。地理位置情報機能では、IP アドレスを地理的位置に関連付けて、暗号化トラフィックをその送信元または宛先の国や大陸に基づいて制御できます。
- SSL ルールで VLAN 条件を設定すると、トラフィックの VLAN タグに応じてそのトラフィックを制御できます。システムは、最も内側の VLAN タグを使用して VLAN を基準にパケットを識別します。
- SSL ルールでポート条件を設定すると、暗号化トラフィックの送信元および宛先の TCP ポートに応じてそのトラフィックを制御できます。

ネットワークベースの複数の条件を組み合わせたり、他のタイプの条件と組み合わせたりして、SSL ルールを作成できます。これらの SSL ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。

### 関連トピック

[Firepower システムの IP アドレス表記法](#) (14 ページ)

## ネットワーク ゾーン SSL ルールの条件

1 つのゾーン条件で [送信元ゾーン (Sources Zones)] および [宛先ゾーン (Destination Zones)] それぞれに対し、最大 50 のゾーンを追加できます。

- 特定のゾーンのインターフェイスからデバイスを離れる暗号化トラフィックを照合するには、そのゾーンを [宛先ゾーン (Destination Zones)] に追加します。

パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブなインターフェイスで構成されるゾーンを [宛先ゾーン (Destination Zones)] 条件で使用することはできません。



- 特定のゾーンのインターフェイスからデバイスに入る暗号化トラフィックを照合するには、そのゾーンを [送信元ゾーン (Source Zones) ] に追加します。

送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの1つから発生し、宛先ゾーンの1つを通して出力する必要があります。

ゾーン内のすべてのインターフェイスが同じタイプ (インライン、パッシブ、スイッチド、またはルーテッド) である必要があるため、SSLルールのゾーン条件で使用されているすべてのゾーンが同じタイプでなければならないことに注意してください。つまり、異なるタイプのゾーンを送信元/宛先とする暗号化トラフィックを照合する単一ルールを定義することはできません。

ゾーンにインターフェイスが含まれていないなど、無効な設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

## ネットワークゾーンによる暗号化トラフィックの制御

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

- ステップ 1** SSL ルール エディタで、[ゾーン (Zones) ] タブを選択します。
- ステップ 2** [利用可能なゾーン (Available Zones) ] から追加するゾーンを見つけます。追加するゾーンを検索するには、[利用可能なゾーン (Available Zones) ] リストの上にある [名前を検索 (Search by name) ] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。
- ステップ 3** クリックすると、ゾーンを選択できます。すべてのゾーンを選択するには、右クリックして [すべて選択 (Select All) ] を選択します。
- ステップ 4** [送信元に追加 (Add to Source) ] または [宛先に追加 (Add to Destination) ] をクリックします。  
ヒント 選択したゾーンをドラッグアンドドロップすることもできます。
- ステップ 5** ルールを保存するか、編集を続けます。

### 例

単純な例として、インライン検出モードを選択したデバイスでは、Firepower Management Centerにより内部と外部の2つのゾーンが作成され、そのデバイスの最初のインター

フェイスのペアがそれらのゾーンに割り当てられます。内部側のネットワークに接続されたホストは、保護されている資産を表します。

このシナリオを拡張すると、同等に設定された追加デバイス（同じFirepower Management Centerによって管理されるもの）を展開して、複数の異なるロケーションで同様のリソースを保護できます。最初のデバイスと同様に、これらのデバイスも内部セキュリティゾーンのアセットを保護します。



- (注) 内部（または外部）のすべてのインターフェイスを1つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティポリシーが意味をなすグループ化を選択します。

この展開では、これらのホストにインターネットへの無制限アクセスを提供できますが、着信する暗号化トラフィックを復号および検査してホストを保護しなければなりません。

これを実現するには、[宛先ゾーン (Destination Zone)] が [内部 (Internal)] に設定されたゾーン条件を持つ SSL ルールを設定します。この単純な SSL ルールでは、内部ゾーンのいずれかのインターフェイスからデバイスを離れるトラフィックが照合されます。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[インターフェイスオブジェクト：インターフェイスグループとセキュリティゾーン \(437 ページ\)](#)

## ネットワークまたは地理位置情報 SSL ルールの条件

ネットワークベースの SSL ルールの条件を作成する場合、IP アドレスと地理的位置を手動で指定できます。または、再利用可能で名前を1つ以上の IP アドレス、アドレスブロック、国、大陸などに関連付けるネットワークオブジェクトおよび位置情報オブジェクトを使用してネットワーク条件を設定できます。



- (注) 地理的位置別にトラフィックを制御するルールを作成して、確実に最新の位置情報データを使用してトラフィックをフィルタ処理する場合は、シスコは Firepower Management Center の位置情報データベース (GeoDB) を定期的に更新することを強く推奨しています。

1つのネットワーク条件で [送信元ネットワーク (Source Networks)] および [宛先ネットワーク (Destination Networks)] それぞれに対し、最大 50 の項目を追加でき、ネットワークベースの設定と位置情報ベースの設定を組み合わせることができます。

- 特定の IP アドレスまたは地理的位置からの暗号化トラフィックを照合するには、[送信元ネットワーク (Source Networks) ]を設定します。
- 特定の IP アドレスまたは地理的位置への暗号化トラフィックを照合するには、[宛先ネットワーク (Destination Networks) ]を設定します。

送信元 (Source) ネットワーク条件と宛先 (Destination) ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信される暗号化トラフィックの照合を行う必要があります。

ネットワーク条件を作成する際、警告アイコンは無効な設定を示します。アイコンの上にポインタを置くと詳細が表示されます。

### 関連トピック

[Firepower システムの IP アドレス表記法](#) (14 ページ)

## ネットワークまたは地理位置情報による暗号化トラフィックの制御

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 始める前に

- [地理位置情報データベースの更新](#) (192 ページ) の説明に従って、Firepower Management Center で地理位置情報データベース (GeoDB) を更新します。

### 手順

**ステップ 1** SSL ルール エディタで、[ネットワーク (Networks) ] タブを選択します。

**ステップ 2** [利用可能なネットワーク (Available Networks) ] から、次のように追加するネットワークを見つけてみます。

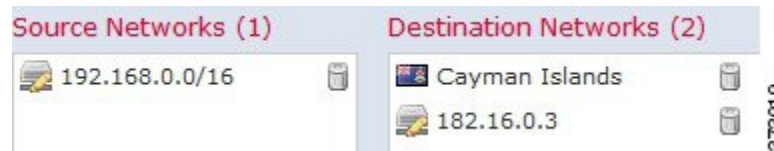
- 追加するネットワーク オブジェクトとグループを表示するには [ネットワーク (Networks) ] タブをクリックします。位置情報オブジェクトを表示するには [位置情報 (Geolocation) ] タブをクリックします。
- ネットワーク オブジェクトをオンザフライで追加するには (後で条件に追加できます) 、 [利用可能なネットワーク (Available Networks) ] リストの上にある追加アイコン (+) をクリックします。
- 追加するネットワーク オブジェクトまたは位置情報オブジェクトを検索するには、適切なタブを選択し、[利用可能なネットワーク (Available Networks) ] リストの上にある [名前または値で検索 (Search by name or value) ] プロンプトをクリックして、オブジェクトの

コンポーネントの1つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

- ステップ 3** オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択 (Select All)] を選択します。
- ステップ 4** [送信元に追加 (Add to Source)] または [宛先に追加 (Add to Destination)] をクリックします。  
ヒント 選択したオブジェクトをドラッグアンドドロップすることもできます。
- ステップ 5** 手動で指定する送信元または宛先 IP アドレスまたはアドレスブロックを追加します。[送信元ネットワーク (Source Networks)] リストまたは [宛先ネットワーク (Destination Networks)] リストの下にある [IP アドレスの入力 (Enter an IP address)] プロンプトをクリックし、1つの IP アドレスまたはアドレスブロックを入力して [追加 (Add)] をクリックします。
- ステップ 6** ルールを保存するか、編集を続けます。

### 例

次の図は、内部ネットワークから発信され、ケイマン諸島 (Cayman Islands) または海外にある持ち株会社のサーバ (182.16.0.3) のリソースにアクセスしようとする暗号化接続をブロックする SSL ルールのネットワーク条件を示しています。



この例では、持ち株会社のサーバの IP アドレスを手動で指定し、ケイマン諸島の IP アドレスを表すシステム提供の地理位置情報オブジェクト Cayman Islands を使用しています。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

- [ネットワーク オブジェクト \(433 ページ\)](#)
- [Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## VLAN SSL ルールの条件

VLAN ベースの SSL ルール条件を作成するときは、1 ~ 4094 の VLAN タグを手動で指定できます。または、VLAN タグ オブジェクトを使用して VLAN 条件を設定することもできます。VLAN タグ オブジェクトとは、いくつかの VLAN タグに名前を付けて再利用可能にしたものを指します。



**ヒント** VLAN タグ オブジェクトを作成しておく、それを使用して SSL ルールを作成したり、Web インターフェイスのさまざまな場所で VLAN タグを表すオブジェクトとして使用したりできます。VLAN タグ オブジェクトはオブジェクト マネージャを使用して作成できます。また、アクセス コントロール ルールの設定時に作成することもできます。

1 つの VLAN タグ条件で、[選択済み VLAN タグ (Selected VLAN Tags)] に最大 50 の項目を追加できます。無効な VLAN タグ条件設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

## 暗号化された VLAN トラフィックの制御

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** SSL ルール エディタで、[VLAN タグ (VLAN Tags)] タブを選択します。

**ステップ 2** [利用可能な VLAN タグ (Available VLAN Tags)] で、次のように追加する VLAN を見つけます。

- VLAN タグ オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[利用可能な VLAN タグ (Available VLAN Tags)] リストの上にある追加アイコン (+) をクリックします。
- 追加する VLAN タグ オブジェクトおよびグループを検索するには、[利用可能な VLAN タグ (Available VLAN Tags)] リストの上にある [名前または値で検索 (Search by name or value)] プロンプトをクリックし、オブジェクト名またはオブジェクトの VLAN タグの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

**ステップ 3** オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択 (Select All)] を選択します。

**ステップ 4** [ルールに追加 (Add to Rule)] をクリックします。

**ヒント** 選択したオブジェクトをドラッグアンドドロップすることもできます。

**ステップ 5** 手動で指定する VLAN タグを追加します。[選択した VLAN タグ (Selected VLAN Tags)] リストの下にある [VLAN タグの入力 (Enter a VLAN Tag)] プロンプトをクリックし、VLAN タグまたはその範囲を入力して、[追加 (Add)] をクリックします。1 から 4094 までの任意の VLAN タグを指定できます。VLAN タグの範囲を指定するにはハイフンを使用します。

**ステップ 6** ルールを保存するか、編集を続けます。

#### 例

次の図は、特定の公開 VLAN（VLAN タグ オブジェクトグループで指定）および手動で追加した VLAN 「42」 上の暗号化トラフィックに一致する SSL ルールの VLAN タグ条件を示しています。



#### 次のタスク

- 設定変更を展開します。[設定変更の導入（350 ページ）](#) を参照してください。

#### 関連トピック

[VLAN タグ オブジェクト（440 ページ）](#)

## ポート SSL ルールの条件

ポートベースの SSL ルールの条件を作成するときは、手動で TCP ポートを指定できます。または、再利用可能で名前を1つ以上のポートに関連付けるポートオブジェクトを使用してポート条件を設定できます。

1つのネットワーク条件で[選択した送信元ポート（Selected Source Ports）]および[選択した宛先ポート（Selected Destination Ports）]それぞれに対し、最大 50 の項目を追加できます。

- 特定の TCP ポートからの暗号化トラフィックを照合するには、[選択した送信元ポート（Selected Source Ports）]を設定します。
- 特定の TCP ポートへの暗号化トラフィックを照合するには、[選択した宛先ポート（Selected Destination Ports）]を設定します。
- TCP [選択した送信元ポート（Selected Source Ports）] から送信された暗号化トラフィックと TCP [選択した宛先ポート（Selected Destination Ports）] に送信した暗号化トラフィックを双方とも照合するには、それぞれのポートを設定します。

[選択した送信元ポート (Selected Source Ports)] および [選択した宛先ポート (Selected Destination Ports)] リストで設定できるのは TCP ポートだけです。非 TCP ポートを含むポート オブジェクトは、[使用可能ポート (Available Ports)] リストではグレイで表示されます。

ポート条件を作成する際、警告アイコンは無効な設定を示します。たとえば、オブジェクトマネージャを使用して使用中のポート オブジェクトを編集し、それらのオブジェクト グループを使用するルールを無効にできます。アイコンの上にポインタを置くと詳細が表示されます。

## ポートによる暗号化トラフィックの制御

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** SSL ルール エディタで、[ポート (Ports)] タブを選択します。

**ステップ 2** [利用可能なポート (Available Ports)] から追加する TCP ポートを次のように探します。

- TCP ポート オブジェクトをオンザフライで追加するには (後で条件に追加できます)、[利用可能なポート (Available Ports)] リストの上にある追加アイコン (🟢) をクリックします。
- 追加する TCP ベースのポート オブジェクトおよびグループを検索するには、[利用可能なポート (Available Ports)] リストの上にある [名前または値で検索 (Search by name or value)] プロンプトをクリックし、オブジェクトの名前またはオブジェクトのポートの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。たとえば、「443」と入力すると、システム提供の HTTPS ポート オブジェクトが Firepower Management Center に表示されます。

**ステップ 3** TCP ベースのポート オブジェクトを 1 つ選択するには、クリックします。TCP ベースのポート オブジェクトをすべて選択するには、右クリックして [すべて選択 (Select All)] を選択します。非 TCP ベースのポートを含んでいるオブジェクトは、ポート条件に追加できません。

**ステップ 4** [送信元に追加 (Add to Source)] または [宛先に追加 (Add to Destination)] をクリックします。

**ヒント** 選択したオブジェクトをドラッグアンドドロップすることもできます。

**ステップ 5** 送信元または宛先のポートを手動で指定するには、[選択した送信元ポート (Selected Source Ports)] または [選択した宛先ポート (Selected Destination Ports)] リストの下にある [ポート (Port)] にポート番号を入力します。0 ~ 65535 の値を持つ 1 つのポートを指定できます。

**ステップ 6** [追加 (Add)] をクリックします。

(注) Firepower Management Center では、無効なポート設定はルール条件に追加されません。

**ステップ 1** ルールを保存するか、編集を続けます。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[ポート オブジェクト \(435 ページ\)](#)

## ユーザベースの SSL ルールの条件

レルム、グループ、またはユーザに基づいてトラフィックと照合するように SSL ルールを設定することができます。SSL ルールのレルム、グループ、およびユーザの条件では、ユーザ制御を実行して、権威のあるユーザを IP アドレスに関連付けることにより、ネットワークを通過できるトラフィックを管理することができます。

ユーザ条件を設定した SSL ルールとトラフィックを一致させるには、モニタ対象のセッションにおける送信元または宛先ホストの IP アドレスと、ログインする権威のあるユーザを関連付ける必要があります。レルム、個々のユーザ、またはユーザが属しているグループに基づいてトラフィックを制御できます。

## ユーザベースの暗号化トラフィックの制御

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

#### 始める前に

- [ユーザ アイデンティティ ソース \(2121 ページ\)](#) の説明に従って、1 つ以上の権限のあるユーザ アイデンティティ ソースを設定します。
- [レルムの作成 \(2185 ページ\)](#) の説明に従って、レルムを設定します。

#### 手順

**ステップ 1** SSL ルール エディタで、[ユーザ (Users) ] タブを選択します。

**ステップ 2** [使用可能なレルム (Available Realms) ] リストで名前または値で検索してレルムを選択します。



**ステップ3** [使用可能なユーザ (AvailableUsers) ] リストで名前または値で検索してレムを選択します。

**ステップ4** [ルールに追加 (Add to Rule) ] をクリックします。

ヒント 選択したユーザおよびグループをドラッグアンドドロップすることもできます。

**ステップ5** ルールを保存するか、編集を続けます。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## レピュテーションベースの SSL ルール条件

SSL ルールでレピュテーションベース条件を設定すると、ネットワークトラフィックをコンテキスト化して状況に応じて制限することで、ネットワーク通過を許可する暗号化トラフィックを管理できます。SSLルールでのレピュテーションベースの制御には、以下のタイプがあります。

- アプリケーション条件によりアプリケーション制御を実行できます。このシステムが暗号化された IP トラフィックを分析するときに、ネットワーク上で一般的に使用されている暗号化アプリケーションを識別および分類してから暗号化セッションを復号します。このシステムでは、こうした検出ベースのアプリケーション認識機能を使用して、ネットワーク上の暗号化されたアプリケーショントラフィックを制御できます。

1つのSSLルールにおいて、カスタムアプリケーションなどの個々のアプリケーションを選択できます。システムにより提供されたアプリケーションフィルタを使用できます。これは、アプリケーションの基本的な特性 (タイプ、リスク、ビジネスとの関連性、およびカテゴリ) に応じて構成された名前付きのアプリケーションセットです。

- URL 条件では、Web サイトに割り当てられたカテゴリおよびレピュテーションに基づいて Web トラフィックを制御できます。

## SSL ルールの選択されたアプリケーションとフィルタ

シスコは、システムおよび脆弱性データベース (VDB) の更新を通じて頻繁にディテクタを更新し追加しています。独自のディテクタを作成し、そのディテクタが検出するアプリケーションに特性 (リスク、関連性など) を割り当てることもできます。アプリケーションの特性に基づいたフィルタを使用することで、システムは最新のディテクタを使用してアプリケーショントラフィックをモニタします。

アプリケーション条件を設定した SSL ルールとトラフィックを一致させるには、[選択済みのアプリケーションとフィルタ (Selected Applications and Filters) ] リストに追加したいいずれかのアプリケーションまたはフィルタにトラフィックが一致する必要があります。



- (注) アクセスコントロールルールを使用してアプリケーショントラフィックをフィルタ処理する場合、フィルタ条件としてアプリケーションタグを使用できます。ただし、暗号化トラフィックはアプリケーションタグでフィルタ処理できません。そのことには意味がないからです。暗号化トラフィックのすべてのアプリケーションを検出するにはタグ付きの **SSL プロトコル** である必要があり、このタグが付けられていないアプリケーションは、非暗号化トラフィックまたは復号化されたトラフィックでしか検出できません。

1つのアプリケーション条件において、最大 50 の項目を [選択済みのアプリケーションとフィルタ (Selected Applications and Filters) ] リストに追加できます。以下はそれぞれ 1つの項目としてカウントされます。

- 個別またはカスタムな組み合わせの、[アプリケーションフィルタ (Application Filters) ] リストからの 1つ以上のフィルタ。この項目は、特性によってグループ化されたアプリケーションのセットを表します。
- [使用可能なアプリケーション (Available Applications) ] リストにあるアプリケーションの検索結果を保存することで作成されたフィルタ。この項目は、部分文字列の一致によってグループ化されたアプリケーションのセットを表します。
- [使用可能なアプリケーション (Available Applications) ] リストからの個々のアプリケーション。

Web インターフェイスでは、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられません。

SSL ポリシーの展開時には、一致する固有のアプリケーションのリストが、アプリケーションの条件を設定したルールごとに生成されます。つまり、完全なカバレッジを確保するために、重複フィルタおよび個々に指定されたアプリケーションを使用できます。

## SSL ルールのアプリケーション フィルタ

SSL ルールのアプリケーション条件を作成するには、[アプリケーションフィルタ (Application Filters) ] リストを使用して、照合するトラフィックの特性を基にアプリケーションをグループ化します。

ユーザの利便性のため、各アプリケーションの特性がタイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグによって判別されます。これらの基準をフィルタとして使用したり、フィルタのカスタムな組み合わせを作成してアプリケーション制御を実行したりできます。

SSL ルールにおけるアプリケーションフィルタのメカニズムは、オブジェクトマネージャを使用して再利用可能なカスタムアプリケーションフィルタを作成する場合と同じです。また、オンザフライで作成した多数のフィルタを、アクセスコントロールルールに新規の再利用可能なフィルタとして保存できます。ユーザが作成したフィルタはネストすることができないため、別のユーザが作成したフィルタを含むフィルタは保存できません。

## フィルタの組み合わせ方について

フィルタを単独または組み合わせて選択すると、[使用可能なアプリケーション (Available Applications)] リストが更新され、条件を満たすアプリケーションのみが表示されます。システムによって提供されるフィルタは組み合わせて選択できますが、カスタムフィルタはできません。

システムは、OR 演算を使用して同じフィルタ タイプの複数のフィルタをリンクします。たとえば、Risks (リスク) タイプの下の Medium (中) および High (高) フィルタを選択すると、結果として次のようなフィルタになります。

Risk: Medium OR High

[中 (Medium)] フィルタに 110 個のアプリケーション、[高 (High)] フィルタに 82 個のアプリケーションが該当する場合は、それら 192 個のアプリケーションすべてが [使用可能なアプリケーション (Available Applications)] リストに表示されます。

システムは、AND 演算を使用して異なるタイプのフィルタをリンクします。たとえば Risks (リスク) タイプで Medium (中) および High (高) フィルタを選択し、Business Relevance (ビジネスとの関連性) タイプで Medium (中) および High (高) フィルタを選択した場合、結果として次のようなフィルタになります。

Risk: Medium OR High  
AND  
Business Relevance: Medium OR High

この場合、システムは [中 (Medium)] または [高 (High)] の [リスク (Risk)] タイプと [中 (Medium)] または [高 (High)] の [ビジネスとの関連性 (Business Relevance)] タイプの両方に含まれるアプリケーションだけを表示します。

## フィルタの検索および選択

フィルタを選択するには、フィルタタイプの横にある矢印をクリックしてそれを展開し、アプリケーションを表示/非表示にする各フィルタの横のチェック ボックスを選択/選択解除します。また、Cisco 提供のフィルタ タイプ ([リスク (Risks)]、[ビジネスとの関連性 (Business Relevance)]、[タイプ (Types)]、または[カテゴリ (Categories)]) を右クリックして、[すべて選択 (Check All)] または [すべて選択解除 (Uncheck All)] を選択することもできます。

フィルタを検索するには、[使用可能なフィルタ (Available Filters)] リストの上にある [名前で検索 (Search by name)] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するフィルタが表示されます。

フィルタを選択したら、[使用可能なアプリケーション (Available Applications)] リストを使用して、それらのフィルタをルールに追加します。

## 関連トピック

[アプリケーション フィルタ \(439 ページ\)](#)

## SSL ルールで使用可能なアプリケーション

SSL ルールのアプリケーション条件を作成するには、[使用可能なアプリケーション (Available Applications)] リストを使用して、照合するトラフィックのアプリケーションを選択します。

### アプリケーションのリストの参照

条件の作成を初めて開始するときは、リストは制約されておらず、システムが検出するすべてのアプリケーションを一度に 100 個ずつ表示します。

- アプリケーションを確認していくには、リストの下にある矢印をクリックします。
- アプリケーションの特性に関する概要情報と参照可能なインターネット検索リンクを含むポップアップ ウィンドウを表示するには、アプリケーションの横にある情報アイコン (ℹ) をクリックします。

### 一致するアプリケーションの検索

照合するアプリケーションを見つけやすくするために、[使用可能なアプリケーション (Available Applications)] リストを次のように制約できます。

- アプリケーションを検索するには、リスト上部にある [名前を検索 (Search by name)] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するアプリケーションが表示されます。
- フィルタを適用してアプリケーションを制約するには、[アプリケーション フィルタ (Application Filters)] リストを使用します。フィルタを適用すると、[使用可能なアプリケーション (Available Applications)] リストが更新されます。

制約されると、[フィルタに一致するすべてのアプリケーション (All apps matching the filter)] オプションが [使用可能なアプリケーション (Available Applications)] リストの上部に表示されます。



- (注) [アプリケーション フィルタ (Application Filters)] リストで 1 つ以上のフィルタを選択し、さらに [使用可能なアプリケーション (Available Applications)] リストも検索すると、選択内容と検索フィルタ適用後の [使用可能なアプリケーション (Available Applications)] リストが AND 演算を使用して結合されます。つまり [フィルタに一致するすべてのアプリケーション (All apps matching the filter)] 条件には、[使用可能なアプリケーション (Available Applications)] リストに現在表示されている個々のすべての条件と、[使用可能なアプリケーション (Available Applications)] リストの上で入力された検索文字列が含まれます。

### 条件内で照合する単一アプリケーションの選択

照合するアプリケーションを検索したら、それをクリックして選択します。現在制約されているビューですべてのアプリケーションを選択するには、右クリックして [すべて選択 (Select All)] を選択します。

1つのアプリケーション条件において、アプリケーションの個別選択で追加できる最大数は50です。50を超えるアプリケーションを追加するには、複数の SSL ルールを作成するか、フィルタを使用してアプリケーションをグループ化する必要があります。

### 条件のフィルタに一致するすべてのアプリケーションの選択

[アプリケーションフィルタ (Application Filters) ] リストで検索またはフィルタを使用して制約されると、[フィルタに一致するすべてのアプリケーション (All apps matching the filter) ] オプションが [使用可能なアプリケーション (Available Applications) ] リストの上部に表示されます。

このオプションを使用して、制約された [使用可能なアプリケーション (Available Applications) ] リスト内のアプリケーションのセット全体を [選択済みのアプリケーションとフィルタ (Selected Applications and Filters) ] リストに同時に追加できます。アプリケーションを個別に追加するのとは対照的に、このアプリケーションのセットを追加すると、そのセットを構成する個々のアプリケーションの数にかかわらず、最大 50 のアプリケーションに対してただ 1 つのアイテムとしてカウントされます。

このようにアプリケーション条件を作成するときは、[選択済みのアプリケーションとフィルタ (Selected Applications and Filters) ] リストに追加するフィルタの名前は、フィルタに表されているフィルタタイプ+各タイプの最大3つのフィルタの名前を連結させたものとなります。同じタイプのフィルタが3個を超える場合は、その後に省略記号 (...) が表示されます。たとえば次のフィルタ名には、Risks (リスク) タイプの2つのフィルタと Business Relevance (ビジネスとの関連性) タイプの4つのフィルタが含まれています。

Risks: Medium, High Business Relevance: Low, Medium, High, ...

[フィルタに一致するすべてのアプリケーション (All apps matching the filter) ] で追加するフィルタに表されないフィルタタイプは、追加するフィルタの名前に含まれません。[選択済みのアプリケーションとフィルタ (Selected Applications and Filters) ] リスト内のフィルタ名の上にポインタを置いたときに表示される説明テキストは、これらのフィルタタイプが [任意 (any) ] に設定されていることを示します。つまり、これらのフィルタタイプはフィルタを制約しないので、任意の値が許可されます。

[フィルタに一致するすべてのアプリケーション (All apps matching the filter) ] の複数のインスタンスをアプリケーション条件に追加でき、各インスタンスは [選択済みのアプリケーションとフィルタ (Selected Applications and Filters) ] リストで個別の項目としてカウントされます。たとえば、リスクが高いすべてのアプリケーションを1つの項目として追加し、選択内容をクリアしてから、ビジネスとの関連性が低いすべてのアプリケーションを別の項目として追加できます。このアプリケーション条件は、リスクが高いアプリケーションまたはビジネスとの関連性が低いアプリケーションに一致します。

## アプリケーションベースの SSL ルール条件の要件

アプリケーション条件を設定した SSL ルールと暗号化トラフィックを一致させるには、[選択済みのアプリケーションとフィルタ (Selected Applications and Filters) ] リストに追加したいいずれかのアプリケーションまたはフィルタにトラフィックが一致する必要があります。

1条件ごとに最大50の項目を追加でき、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。アプリケーション条件を作成する際、警告アイコンは無効な設定を示します。アイコンの上にポインタを置くと詳細が表示されます。

## SSL ルールへのアプリケーション条件の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

- ステップ 1** SSL ルール エディタで、[アプリケーション (Applications)] タブを選択します。
- ステップ 2** [使用可能なアプリケーション (Available Applications)] リストに表示されるアプリケーションのリストをフィルタするには、[アプリケーション フィルタ (Application Filters)] リストにあるフィルタを1つまたは複数選択します。詳細については、[SSL ルールのアプリケーション フィルタ \(1500 ページ\)](#) を参照してください。
- ステップ 3** [使用可能なアプリケーション (Available Applications)] リストから追加するアプリケーションを見つけて選択します。個々のアプリケーションを検索して選択するか、またはリストが制約されている場合は、[フィルタに一致するすべてのアプリケーション (All apps matching the filter)] を選択できます。詳細については、[SSL ルールで使用可能なアプリケーション \(1502 ページ\)](#) を参照してください。
- ステップ 4** [ルールに追加 (Add to Rule)] をクリックします。
 

**ヒント** [すべてのフィルタをクリア (Clear All Filters)] をクリックして既存の選択をクリアします。選択したアプリケーションとフィルタをドラッグアンドドロップすることもできます。
- ステップ 5** ルールを保存するか、編集を続けます。

### 例

次の図は、MyCompanyのアプリケーション、リスクが高くビジネスとの関連性の低いすべてのアプリケーション、ゲームアプリケーション、およびいくつかの指定アプリケーションからなるカスタム グループを復号する、SSL ルールのアプリケーション条件を示しています。



### 次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

## 暗号化されたアプリケーションの制御に対する制限

### 暗号化されたアプリケーションの識別

このシステムでは、StartTLS を使用して暗号化される非暗号化アプリケーションを識別できません。これには、SMTPS、POPS、FTPS、TelnetS、IMAPS などのアプリケーションが含まれます。また、TLS ClientHello メッセージ内の Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。

### アプリケーション識別の速度

暗号化トラフィックのアプリケーション制御は、以下のすべての処理が完了するまで実行されません。

- 暗号化された接続がクライアントとサーバ間で確立される。
- 暗号化セッション内のアプリケーションがシステムにより識別される。

この識別が行われるのは、サーバ証明書が交換された後です。SSL ハンドシェイク中に交換されるトラフィックでアプリケーションの識別が完了する前に、アプリケーション条件を含んでいる SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。この動作により、ハンドシェイクが完了し、アプリケーションを識別できるようになります。便宜を図るため、影響を受けるルールは情報アイコン (i) でマークされます。

システムによる識別が完了すると、アプリケーション条件に一致する残りのセッショントラフィックに SSL ルールのアクションが適用されます。

### アプリケーションディテクタの自動有効化

ポリシーのアプリケーションルール条件ごとに、少なくとも1つのディテクタが有効にされている必要があります。有効になっているディテクタがないアプリケーションについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザ定義ディテクタが有効になります。

#### 関連トピック

[ディテクタのアクティブおよび非アクティブの設定](#) (2118 ページ)

## 暗号化トラフィックでのレピュテーションベースの URL ブロッキング

URL フィルタリング ライセンスでは、SSL ルールに設定した URL 条件により、要求された URL のカテゴリおよびレピュテーションに基づいて暗号化 Web サイトへのアクセスを制御できます。詳細については、[URL 条件 \(URL フィルタリング\)](#) (393 ページ) を参照してください。



**ヒント** SSL ルールで使用する URL 条件は、手動による URL フィルタリングをサポートしていません。代わりに、サブジェクト共通名を照合する識別名条件を使用してください。

### レピュテーションベースの URL ブロッキングの実行

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
URL フィルタリング (URL Filtering)	URL フィルタリング (URL Filtering)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

#### 手順

**ステップ 1** SSL ルール エディタで、[カテゴリ (Category)] タブを選択します。

**ステップ 2** [カテゴリ (Categories)] リストで、追加する URL カテゴリを見つけます。カテゴリを指定せずにすべての暗号化 Web トラフィックと一致させるには、[任意 (Any)] カテゴリを選択します。追加可能なカテゴリを検索するには、[カテゴリ (Categories)] リストの上にある [名前または値で検索 (Search by name or value)] プロンプトをクリックし、カテゴリ名を入力します。入力すると、リストが更新されて一致するカテゴリが表示されます。

**ステップ 3** カテゴリを選択するには、そのカテゴリをクリックします。

**ヒント** 右クリックで表示される [すべて選択 (Select All)] も利用できますが、この方法ですべてのカテゴリを追加すると、SSL ルールの最大項目数 50 を超えてしまいます。代わりに [任意 (Any)] を使用してください。



**ステップ 4** カテゴリの選択を限定する場合は、[レピュテーション (Reputations)] リストからレピュテーション レベルをクリックする必要があります。選択できるレピュテーション レベルは 1 つだけです。レピュテーション レベルを指定しない場合、システムはデフォルトとして [任意 (Any)] (つまりすべてのレベル) を設定します。

- ルールで Web アクセスのブロックまたはトラフィックの復号を行う場合 (ルールアクションが、[ブロック (Block)]、[リセットしてブロック (Block with reset)]、[復号 - 既知のキー (Decrypt - Known Key)]、[復号 - 再署名 (Decrypt - Resign)]、または [モニタ (Monitor)] の場合)、選択したレピュテーション レベルよりも厳しいすべてのレピュテーション も自動的に選択されます。たとえば **疑わしいサイト (Suspicious sites)** (レベル 2) をブロックするようルールを設定した場合、**高リスク (High Risk)** (レベル 1) のサイトも自動的にブロックされます。
- ルールで Web アクセスを許可して、アクセスコントロールに従わせる場合 (ルールアクションが [復号しない (Do not decrypt)] の場合)、選択したレピュテーション レベルよりも厳しくないすべてのレピュテーション も自動的に選択されます。たとえば **無害なサイト (Benign sites)** (レベル 4) を許可するようルールを設定した場合、**有名 (Wellknown)** (レベル 5) サイトもまた自動的に許可されます。

(注) ルールのアクションを変更した場合、システムは、上記の点に従って URL 条件のレピュテーション レベルを自動的に変更します。

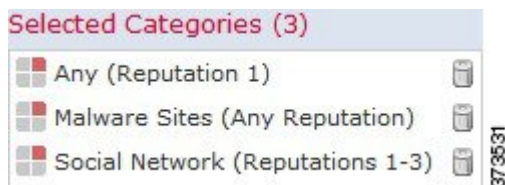
**ステップ 5** [ルールに追加 (Add to Rule)] をクリックして、選択した項目を [選択したカテゴリ (Selected Categories)] リストに追加します。

ヒント 選択した項目をドラッグアンドドロップすることもできます。

**ステップ 6** ルールを保存するか、編集を続けます。

### 例

次の図は、すべてのマルウェアサイト、すべてのリスクの高いサイト、およびすべての安全でないソーシャルネットワーキングサイトをブロックするアクセスコントロールルール例の URL 条件を示しています。



次の表では、前の図で示した条件を作成する方法を要約します。

表 92: 例 : URL 条件の作成

ブロックする対象	選択するカテゴリまたは URL オブジェクト	選択するレピュテーション
マルウェア サイト (レピュテーションに関係なく)	マルウェア サイト (Malware Sites)	任意 (Any)
高リスクの URL (レベル 1)	任意 (Any)	1 - 高リスク (High Risk)
無害 (benign) よりも大きいリスクがあるソーシャルネットワークワーキング サイト (レベル 1 ~ 3)	ソーシャル ネットワーク (Social Network)	3 - セキュリティリスクのある無害なサイト (Benign sites with security risks)

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## サーバ証明書ベースの SSL ルール条件

SSL ルールでは、サーバ証明書の特性に基づいて暗号化トラフィックを処理および復号できます。SSL ルールは、以下のサーバ証明書属性に基づいて設定することができます。

- 識別名条件を設定すると、証明書所有者またはサーバ証明書の発行元 CA に応じて暗号化トラフィックを処理および検査できます。発行元の識別名を基準にすると、サイトのサーバ証明書を発行した CA に基づいてトラフィックを処理できます。
- SSL ルールで証明書条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書に応じて暗号化トラフィックを処理および検査できます。1つの条件に1つまたは複数の証明書を設定でき、トラフィックの証明書がいずれかの条件の証明書と一致するとそのルールが適用されます。
- SSL ルールの証明書ステータス条件では、トラフィックの暗号化に使用されたサーバ証明書のステータスに基づいて暗号化されたトラフィックを処理して、証明書が有効か、失効しているか、期限切れか、まだ有効でないか、自己署名済みか、信頼できる CA によって署名済みか、証明書失効リスト (CRL) が有効かどうか、証明書のサーバ名指定 (SNI) が要求内のサーバと一致するかどうかなどの検査を行うことができます。
- SSL ルールで暗号スイート条件を設定すると、暗号化セッションのネゴシエートに使用される暗号スイートに応じて暗号化トラフィックを処理および検査できます。
- SSL ルールでセッション条件を設定すると、トラフィックの暗号化に使用されている SSL または TLS のバージョンに応じて暗号化トラフィックを検査できます。

複数の暗号スイートを1つのルールで検出したり、証明書の発行元や証明書ホルダーを検出したりする場合は、再利用可能な暗号スイートのリストおよび識別名オブジェクトを作成して

ルールに追加できます。サーバ証明書および特定の証明書ステータスを検出するには、ルール用の外部証明書と外部 CA オブジェクトの作成が必要です。

## 証明書の識別名の SSL ルール条件

ルール条件を設定する場合は、手動でリテラル値を指定するか、識別名オブジェクトを参照するか、または複数のオブジェクトを含んでいる識別名グループを参照できます。



- (注) [復号 - 既知のキー (Decrypt - Known Key)] アクションを選択した場合、識別名条件を設定することはできません。このアクションでは、トラフィック復号用のサーバ証明書の選択が必要であるため、トラフィックの照合はすでにこの証明書で行われています。

複数のサブジェクトおよび発行元の識別名との照合を単一の証明書ステータスのルール条件で行うことも可能ですが、ルールとの照合で一致する必要があるのは1つの共通名または識別名だけです。

識別名を手動で追加する場合、共通名属性 (CN) を含めることができます。CN= なしで共通名を追加すると、オブジェクトを保存する前に CN= が追加されます。

また、以降の属性ごとに1つずつ識別名をカンマで区切って追加することができます。たとえば、**C, CN, O, OU** というようにします。

1つの識別名条件で、[サブジェクト DN (Subject DNs)] リストおよび [発行元 DN (Issuer DNs)] リストにそれぞれ最大 50 のリテラル値および識別名オブジェクトを追加できます。

システム提供の識別名オブジェクトグループである Cisco-Undecryptable-Sites には、システムで復号できないトラフィックの Web サイトが含まれます。このグループを識別名条件に追加すると、該当する Web サイトとのトラフィックがブロックしたり復号を無効にしたりでき、これらのトラフィックの復号に使用されるシステムリソースの浪費を回避できます。グループ内の各エントリは変更できますが、このグループを削除することはできません。システムによる更新によってこのリストのエントリが変更されることがありますが、ユーザによる変更は保持されます。

システムが新しいサーバへの暗号化セッションを最初に検出したときは、DNデータを ClientHello の処理には使用できません。これは復号されていない最初のセッションとなる可能性があります。最初のセッションの後に、管理対象デバイスは、サーバの証明書メッセージからのデータをキャッシュします。同じクライアントからの後続の接続で、システムは識別名条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

## 証明書の識別名による暗号化トラフィックの制御

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** SSL ルール エディタで、[DN] タブを選択します。

**ステップ 2** [使用可能な DN (Available DN)] で、追加する識別名を探します。

- ここで識別名オブジェクトを作成してリストに追加するには (後で条件に追加できます)、[使用可能な DN (Available DN)] リストの上にある追加アイコン (+) をクリックします。
- 追加する識別名オブジェクトおよびグループを検索するには、[使用可能な DN (Available DN)] リストの上にある [名前または値で検索 (Search by name or value)] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

**ステップ 3** オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択 (Select All)] を選択します。

**ステップ 4** [サブジェクトに追加 (Add to Subject)] または [発行元に追加 (Add to Issuer)] をクリックします。

ヒント 選択したオブジェクトをドラッグアンドドロップすることもできます。

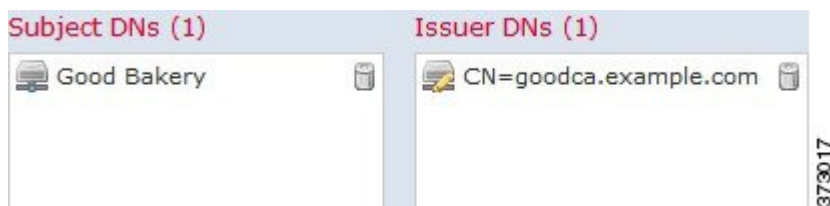
**ステップ 5** 手動で指定するリテラル共通名または識別名がある場合は、それらを追加します。[サブジェクト DN (Subject DN)] または [発行元 DN (Issuer DN)] リストの下にある [DN または CN の入力 (Enter DN or CN)] プロンプトをクリックし、共通名または識別名を入力して [追加 (Add)] をクリックします。

**ステップ 6** ルールを追加するか、編集を続けます。

### 例

### 例

次の図は、goodbakery.example.com に対して発行された証明書および goodca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。これらの証明書で暗号化されたトラフィックは許可され、アクセスコントロールにより制御されます。



次の図は、badbakery.example.com および関連ドメインに対して発行された証明書およびbadca.example.comによって発行された証明書を検索する識別名ルール条件を示しています。これらの証明書で暗号化されたトラフィックは、再署名された証明書を使用して復号されます。



#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

- [識別名オブジェクト \(484 ページ\)](#)

## 証明書の SSL ルール条件

証明書ベースの SSL ルール条件を作成するときにサーバ証明書をアップロードしたり、再利用可能な外部証明書オブジェクトとして保存してサーバ証明書の名前を関連付けたりできます。また、既存の外部証明書オブジェクトやオブジェクトグループを使用して証明書条件を設定することもできます。

ルール条件の [使用可能な証明書 (Available Certificates)] フィールドでは、外部証明書オブジェクトやオブジェクトグループを証明書の識別名に関する以下の特性に基づいて検索できません。

- サブジェクトまたは発行元の共通名 (CN)
- サブジェクトまたは発行元の組織 (O)
- サブジェクトまたは発行元の組織単位 (OU)

1 つの証明書のルール条件で複数の証明書を照合することもでき、トラフィックの暗号化に使用されている証明書がアップロードされた証明書のいずれかと一致した場合、その暗号化トラフィックはルールに一致したと判定されます。

1 つの証明書条件で、[選択した証明書 (Selected Certificates)] リストに最大 50 の外部証明書オブジェクトおよび外部証明書オブジェクトグループを追加できます。

次の点に注意してください。

- [復号 - 既知のキー (Decrypt - Known Key) ]アクションも選択すると、証明書条件を設定できなくなります。このアクションでは、トラフィック復号用のサーバ証明書の選択が必要であるため、トラフィックの照合はすでにこの証明書で行われていることとなります。
- 証明書条件に外部証明書オブジェクトを設定する場合、暗号スイート条件に追加する暗号スイートまたは [復号 - 再署名 (Decrypt - Resign) ]アクションに関連付ける内部 CA オブジェクトのいずれかが、外部証明書の署名アルゴリズム タイプと一致する必要があります。たとえば、ルール of 証明書条件で EC ベースのサーバ証明書を参照する場合は、追加する暗号スイート、または [復号 - 再署名 (Decrypt - Resign) ]アクションに関連付ける CA 証明書も EC ベースでなければなりません。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。
- システムが新しいサーバへの暗号化セッションを最初に検出したときは、証明書データを ClientHello の処理には使用できません。これは復号されていない最初のセッションとなる可能性があります。最初のセッション後に、管理対象デバイスは、サーバの証明書メッセージからのデータをキャッシュします。同じクライアントからの後続の接続で、システムは証明書条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

## 証明書による暗号化トラフィックの制御

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** SSL ルール エディタで、[証明書 (Certificate) ] タブを選択します。

**ステップ 2** [使用可能な証明書 (Available Certificates) ] で、追加するサーバ証明書を探します。

- ここで外部証明書オブジェクトを作成してリストに追加するには (後で条件に追加できます)、[使用可能な証明書 (Available Certificates) ] リストの上にある追加アイコン (+) をクリックします。
- 追加する証明書オブジェクトおよびグループを検索するには、[使用可能な証明書 (Available Certificates) ] リストの上にある [名前または値で検索 (Search by name or value) ] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

**ステップ 3** オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択 (Select All) ] を選択します。

**ステップ 4** [ルールに追加 (Add to Rule) ] をクリックします。

ヒント 選択したオブジェクトをドラッグアンドドロップすることもできます。

**ステップ 5** ルールを追加するか、編集を続けます。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[外部証明書オブジェクト \(497 ページ\)](#)

## 証明書ステータスの SSL ルール条件

証明書ステータスの SSL ルール条件では、各ステータスの有無を基準にしたトラフィックの照合ができます。1 つのルール条件で複数のステータスを選択でき、いずれかのステータスと証明書が一致すれば、ルールとトラフィックが一致したと判定されます。

複数の証明書ステータスの有無を単一の証明書ステータスルール条件で照合するように選択できます (いずれか 1 つの基準に一致するだけで、その証明書はルールに一致します)。

次の表は、暗号化用のサーバ証明書のステータスを基準に、システムが暗号化トラフィックを評価する方法を示しています。

表 93: 証明書ステータスのルール条件の基準

ステータスの確認	[はい (Yes) ] を設定	[いいえ (No) ] を設定
失効 (Revoked)	ポリシーは、サーバ証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれています。	ポリシーは、サーバ証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれていません。
自己署名 (Self-signed)	検出されたサーバ証明書が、同じサブジェクトと発行元の識別名を含んでいます。	検出されたサーバ証明書が、異なるサブジェクトと発行元の識別名を含んでいます。

ステータスの確認	[はい (Yes) ]を設定	[いいえ (No) ]を設定
有効 (Valid)	<p>以下のすべてを満たしています。</p> <ul style="list-style-type: none"> <li>• 証明書を発行した CA をポリシーが信頼しています。</li> <li>• 署名が有効です。</li> <li>• 発行元が有効です。</li> <li>• ポリシーの信頼できる CA のいずれも証明書を失効させていません。</li> <li>• 現在の日付が証明書の有効期間の開始日と終了日の範囲内にあります。</li> </ul>	<p>以下の 1 つ以上を満たしています。</p> <ul style="list-style-type: none"> <li>• 証明書を発行した CA をポリシーが信頼していません。</li> <li>• 署名が無効です。</li> <li>• 発行元が無効です。</li> <li>• ポリシーの信頼できる CA の 1 つが証明書を失効させています。</li> <li>• 現在の日付が証明書の有効期間の開始日より前です。</li> <li>• 現在の日付が証明書の有効期限の終了日より後です。</li> </ul>
署名が無効 (Invalid signature)	証明書の内容に対して証明書の署名が適切に検証されません。	証明書の内容に対して証明書の署名が適切に検証されます。
発行元が無効 (Invalid issuer)	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されていません。	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されています。
期限切れ	現在の日付が証明書の有効期限の終了日より後です。	現在の日付が証明書の有効期限の終了日であるかそれより前です。
まだ無効 (Not yet valid)	現在の日付が証明書の有効期間の開始日より前です。	現在の日付が証明書の有効期間の開始日であるかそれより後です。
サーバの不一致	サーバ名がサーバの <b>サーバ名指定 (SNI)</b> 名と一致しません。これは、サーバ名を偽装しようとする試みを示している可能性があります。	サーバ名は、クライアントがアクセスを要求しているサーバの SNI 名と一致します。



1つの証明書が複数のステータスに一致する場合でも、ルールがトラフィックに行うアクションは一度に1つだけであることを注意してください。

CA が証明書を発行したか失効したかを確認するには、ルートおよび中間 CA 証明書とその関連 CRL をオブジェクトとしてアップロードする必要があります。その後で SSL ポリシーの信頼できる CA 証明書のリストに、これらの信頼できる CA のオブジェクトを追加します。

システムが新しいサーバへの暗号化セッションを最初に検出したときは、証明書ステータスを ClientHello の処理には使用できません。これは復号されていない最初のセッションとなる可能性があります。最初のセッションの後に、管理対象デバイスは、サーバの証明書メッセージからのデータをキャッシュします。同じクライアントからの後続の接続で、システムは証明書ステータス条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

## 外部認証局の信頼

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

SSL ポリシーでルートおよび中間 CA 証明書を追加することで信頼できる CA が設定され、トラフィックの暗号化に使用されているサーバ証明書の検証に、これらの信頼できる CA を使用できるようになります。

信頼できる CA 証明書の中にアップロードされた証明書失効リスト (CRL) が含まれている場合は、信頼できる CA により、暗号化証明書が失効されているかどうかを確認できます。

### 手順

- ステップ 1** SSLルールエディタで、[信頼できる CA 証明書 (Trusted CA Certificates)] タブを選択します。
- ステップ 2** 次のように、[使用可能な信頼できる CA (Available Trusted CAs)] で追加する信頼できる CA を見つけます。
  - ここで信頼できる CA のオブジェクトを作成してリストに追加するには、[使用可能な信頼できる CA (Available Trusted CAs)] リストの上にある追加アイコン (+) をクリックします。
  - 追加する信頼できる CA オブジェクトおよびグループを検索するには、[使用可能な信頼できる CA (Available Trusted CAs)] リストの上にある [名前または値で検索 (Search by name or value)] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。
- ステップ 3** オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択 (Select All)] を選択します。
- ステップ 4** [ルールに追加 (Add to Rule)] をクリックします。

ヒント 選択したオブジェクトをドラッグアンドドロップすることもできます。

ステップ5 ルールを追加するか、編集を続けます。

#### 次のタスク

- SSLルールに証明書ステータスのSSLルール条件を追加します。詳細については、[証明書ステータスでのトラフィックの照合 \(1516 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[信頼できる認証局オブジェクト \(494 ページ\)](#)

### 信頼できる外部認証局の設定

検証されたサーバ証明書には、信頼できる CA によって署名された証明書が含まれます。SSL ポリシーに信頼できる CA 証明書を追加した後は、トラフィックと照合する証明書ステータス条件を SSL ルールに設定することができます。



ヒント 信頼できるルート CA の信頼チェーン内にあるすべての証明書を、信頼できる CA 証明書のリストにアップロードしますが、これにはルート CA 証明書およびすべての中間 CA 証明書が含まれます。これを行わないと、中間 CA から発行された信頼できる証明書の検出が困難になります。また、ルート発行者 CA に基づいてトラフィックを信頼するように証明書ステータス条件を設定する場合、信頼できる CA の信頼チェーン内のすべてのトラフィックは、復号する必要はなく、復号せずに許可することができます。

SSL ポリシーを作成すると、[信頼できる CA 証明書 (Trusted CA Certificates)] タブにデフォルトの信頼できる CA オブジェクト グループ Cisco Trusted Authorities が入力されます。

このグループ内の各エントリは変更が可能で、SSL ポリシーにこのグループを含めるかどうかを選択できます。このグループを削除することはできません。システムによる更新によりこのリストのエントリが変更されることがありますが、ユーザによる変更は保持されます。

## 証明書ステータスでのトラフィックの照合

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

## 始める前に

- 信頼できる CA オブジェクトまたはグループを SSL ポリシーに追加します。詳細については、[外部認証局の信頼 \(1515 ページ\)](#) を参照してください。

## 手順

- 
- ステップ 1** Firepower Management Center で、[ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [SSL] を選択します。
- ステップ 2** 新しいポリシーを追加するか、既存のポリシーを編集します。
- ステップ 3** 新しい SSL ルールを追加するか、既存のルールを編集します。
- ステップ 4** [ルールの追加 (Add Rule)] または [ルールの編集 (Editing Rule)] ダイアログボックスで [証明書ステータス (Cert Status)] タブを選択します。
- ステップ 5** 各証明書ステータスには次のオプションがあります。
- 該当する証明書ステータスが存在するときに照合する場合は、[はい (Yes)] を選択します。
  - 該当する証明書ステータスが存在しないときに照合する場合は、[いいえ (No)] を選択します。
  - ルールが一致する場合、[任意 (Any)] を選択して条件をスキップします。つまり、[任意 (Any)] を選択すると、証明書ステータスの有無に関わらずルールは一致します。
- ステップ 6** ルールを追加するか、編集を続けます。
- 

## 例

組織は Verified Authority という認証局を信頼しています。組織は Spammer Authority という認証局を信頼していません。システム管理者は、Verified Authority の証明書および、Verified Authority の発行した中間 CA 証明書をアップロードします。Verified Authority が以前に発行した証明書の 1 つを失効させたため、システム管理者は Verified Authority から提供された CRL をアップロードします。

次の図は、有効な証明書をチェックする証明書ステータスのルール条件を示しています。これにより、Verified Authority から発行されたが CRL には登録されておらず、現状で有効期間の開始日と終了日の範囲内にあるかどうかチェックされます。この設定では、これらの証明書で暗号化されたトラフィックはアクセスコントロールにより復号および検査されません。

Revoked:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Self Signed:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Valid:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Invalid Signature:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Invalid Issuer:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Expired:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Not Yet Valid:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Invalid Certificate:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Invalid CRL:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Server Mismatch:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any

次の図は、ステータスが存在しないことをチェックする証明書ステータスのルール条件を示しています。この設定では、期限切れになっていない証明書を使用して暗号化されたトラフィックと照合し、そのトラフィックをモニタします。

Revoked:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Self Signed:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Valid:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Invalid Signature:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Invalid Issuer:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Expired:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Not Yet Valid:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Invalid Certificate:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Invalid CRL:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Server Mismatch:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any

次の図は、さまざまなステータスの有無に一致する証明書ステータスのルール条件を示しています。この設定でルールが一致するのは、着信トラフィックを暗号化した証明書が無効なユーザが発行元、自己署名、無効、または期限切れであった場合で、そうしたトラフィックを既知のキーで復号します。

Revoked:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Self Signed:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Valid:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Invalid Signature:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Invalid Issuer:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Expired:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Not Yet Valid:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Invalid Certificate:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Invalid CRL:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Server Mismatch:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any

次の図は、要求のSNIがサーバ名に一致する、またはCRLが有効でない場合に一致する証明書ステータスのルール条件を示しています。この設定のため、ルールがいずれかの条件に一致する場合に、トラフィックがブロックされます。

Revoked:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Self Signed:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Valid:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Invalid Signature:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Invalid Issuer:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Expired:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Not Yet Valid:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Invalid Certificate:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any
Invalid CRL:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any	Server Mismatch:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Any

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 暗号スイート SSL ルール条件

Cisco では、暗号スイートのルール条件に追加できる事前定義の暗号スイートを提供しています。複数の暗号スイートを含む、暗号スイートのリストのオブジェクトを追加することもできます。



(注) 新しい暗号スイートを追加することはできません。定義済みの暗号スイートは変更も削除もできません。

1つの暗号スイート条件で、[選択した暗号スイート (Selected Cipher Suites)] リストに最大50の暗号スイートおよび暗号スイートリストを追加できます。暗号スイート条件に追加できる暗号スイートとして、次のものがサポートされています。

- SSL\_RSA\_FIPS\_WITH\_3DES\_EDE\_CBC\_SHA
- SSL\_RSA\_FIPS\_WITH\_DES\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_DES\_CBC\_SHA
- TLS\_DH\_Anon\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DH\_Anon\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_DH\_Anon\_WITH\_CAMELLIA\_128\_CBC\_SHA
- TLS\_DH\_anon\_WITH\_CAMELLIA\_128\_CBC\_SHA256
- TLS\_DH\_Anon\_WITH\_CAMELLIA\_256\_CBC\_SHA
- TLS\_DH\_anon\_WITH\_CAMELLIA\_256\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_NULL\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA
- TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_NULL\_SHA
- TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA
- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA256
- TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA
- TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA256
- TLS\_RSA\_WITH\_DES\_CBC\_SHA
- TLS\_RSA\_WITH\_NULL\_MD5
- TLS\_RSA\_WITH\_NULL\_SHA
- TLS\_RSA\_WITH\_RC4\_128\_MD5
- TLS\_RSA\_WITH\_RC4\_128\_SHA

次の点に注意してください。

- 展開でサポートされていない暗号スイートを追加すると、設定を展開できません。たとえば、パッシブ展開では、一時 Diffie-Hellman (DHE) および一時的楕円曲線 Diffie-Hellman (ECDHE) 暗号スイートを使用したトラフィックの復号がサポートされません。それらの暗号スイートを使用してルールを作成すると、アクセス コントロール ポリシーを展開できなくなります。
- 暗号スイート条件に暗号スイートを設定する場合は、証明書条件に追加する外部証明書オブジェクト、または [復号 - 再署名 (Decrypt - Resign) ] アクションに関連付ける内部 CA オブジェクトが、暗号スイートの署名アルゴリズム タイプと一致している必要があります。たとえば、ルールの暗号スイート条件で EC ベースの暗号スイートを参照する場合、追加するサーバ証明書または [復号 - 再署名 (Decrypt - Resign) ] アクションに関連付ける

CA 証明書も EC ベースである必要があります。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。

- SSL ルールの暗号スイート条件に匿名の暗号スイートを追加できますが、次の点に注意してください。
  - システムは ClientHello 処理中に自動的に匿名の暗号スイートを削除します。ルールを使用するシステムでは、ClientHello の処理を防止するために SSL ルールも設定する必要があります。詳細については、[SSL ルールの順序 \(416 ページ\)](#) を参照してください。
  - システムでは、匿名の暗号スイートで暗号化されたトラフィックは復号できないため、ルールに [復号 - 再署名 (Decrypt - Resign) ] または [復号 - 既知のキー (Decrypt - Known Key) ] アクションを使用できません。
- 暗号スイートをルール条件として指定する際、ルールを ClientHello メッセージで指定された暗号スイートの完全なリストではなく、ServerHello メッセージのネゴシエートされた暗号スイートと照合することを検討してください。ClientHello の処理中に、管理対象デバイスは ClientHello メッセージからサポートされていない暗号スイートを削除します。ただし、これにより指定されたすべての暗号スイートが削除されることになる場合、システムでは元のリストを保持します。システムがサポートされていない暗号スイートを保持する場合、後続の評価は復号化されないセッションになります。

## 暗号スイートによる暗号化トラフィックの制御

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** SSL ルール エディタで、[暗号スイート (Cipher Suite) ] タブを選択します。

**ステップ 2** [使用可能な暗号スイート (Available Cipher Suites) ] で、追加する暗号スイートを探します。

- ここで暗号スイートリストを作成してリストに追加するには (後で条件に追加できます) 、[使用可能な暗号スイート (Available Cipher Suites) ] リストの上にある追加アイコン (+) をクリックします。
- 追加する暗号スイートおよびリストを検索するには、[使用可能な暗号スイート (Available Cipher Suites) ] リストの上にある [名前または値で検索 (Search by name or value) ] プロンプトをクリックし、暗号スイートの名前または暗号スイートの値を入力します。入力を開始するとリストが更新され、一致する暗号スイートが表示されます。

**ステップ3** 暗号スイートをクリックして選択します。すべての暗号スイートを選択するには、右クリックして [すべて選択 (Select All)] を選択します。

**ステップ4** [ルールに追加 (Add to Rule)] をクリックします。

ヒント 選択した暗号スイートをドラッグアンドドロップでリストに追加することもできます。

**ステップ5** ルールを追加するか、編集を続けます。

#### 次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

#### 関連トピック

[暗号スイート リスト](#) (483 ページ)

## 暗号化プロトコルバージョンの SSL ルール条件

SSL バージョン 3.0 または TLS バージョン 1.0、1.1、1.2 のいずれかで暗号化されたトラフィックとの照合を選択できます。デフォルトでは、ルールの作成時にすべてのプロトコルのバージョンが選択されます。複数のバージョンが選択されている場合、いずれかのバージョンと一致する暗号化トラフィックがルールに一致したと判定されます。ルール条件を保存するには、最低 1 つのプロトコルバージョンを選択する必要があります。

バージョンのルール条件で SSL バージョン 2.0 を選択することはできません。これは、SSL バージョン 2.0 で暗号化されたトラフィックの復号化がサポートされていないためです。復号できないアクションを設定すれば、それ以上のインスペクションなしで、これらのトラフィックを許可またはブロックできます。

## 暗号化プロトコルのバージョンによるトラフィックの制御

スマートライセンス	従来ライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

#### 手順

**ステップ1** SSL ルールエディタで、[バージョン (Version)] タブを選択します。

**ステップ2** 照合するプロトコルバージョンを選択します。



**ステップ3** ルールを追加するか、編集を続けます。

---

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。





## 第 **XVII** 部

# 高度なマルウェア防御（AMP）とファイル制御

- [ファイルポリシーと AMP for Firepower](#)（1527 ページ）
- [ファイルとマルウェアのインスペクションパフォーマンスとストレージの調整](#)（1563 ページ）





## 第 66 章

# ファイルポリシーと AMP for Firepower

次のトピックでは、ファイル制御、ファイルポリシー、ファイルルール、AMPクラウド接続、および動的分析接続の概要を示します。

- [ファイルポリシーと AMP for Firepower について \(1527 ページ\)](#)
- [ファイル制御および Cisco AMP の基本 \(1528 ページ\)](#)
- [ファイルポリシー \(1535 ページ\)](#)
- [ファイルルール \(1542 ページ\)](#)
- [クラウド接続 \(1549 ページ\)](#)
- [集合型セキュリティ インテリジェンス通信の設定 \(1559 ページ\)](#)

## ファイルポリシーと AMP for Firepower について

悪意のあるソフトウェア、つまりマルウェアは、複数のルートで組織のネットワークに入る可能性があります。マルウェアの影響を特定して軽減しやすくするため、Firepower システムの *Advanced Malware Protection for Firepower* (AMP for Firepower) の機能によって、ネットワークトラフィックでのマルウェアの伝送を検出、追跡、保存、分析、および必要に応じてブロックできます。

AMP for Firepower およびファイル制御（ファイルにマルウェアが含まれているかどうかにかかわらず、特定のタイプのすべてのファイルを制御できる）をアクセス制御設定全体の一部として設定します。作成してアクセスコントロールルールに関連付けたファイルポリシーは、ルールに一致するネットワークトラフィックを処理します。そのトラフィックで検出されたファイルをダウンロードし、ローカルマルウェア分析を実行して、ファイルにマルウェアが含まれているかどうかを判断できます。また、ファイルを動的分析のために AMP Threat Grid クラウドに送信して、そのファイルがマルウェアを表しているかどうかを判断できます。

アクティブファイルポリシーのファイルイベント、マルウェアイベント、および取得されたファイルロギングが自動的に有効になります。また、ファイルポリシーでファイルイベントまたはマルウェアイベントが生成されるか、ファイルがキャプチャされると、システムは関連する接続の終了を Firepower Management Center データベースに自動的に記録します。



- (注) NetBIOS-ssn (SMB) トラフィックのインスペクションによって生成されるファイルイベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。システムはクライアントまたはサーバがセッションを終了した後に接続イベントを生成します。

分析のターゲットをさらに絞り込むために、マルウェア ファイルの [ネットワーク ファイル トrajекトリ (network file trajectory) ] ページを使用して、ホスト間での個々の脅威の広がりを時系列で追跡できます。これにより、最も効果的なアウトブレイク制御と防止対策に集中できます。



- ヒント 組織で AMP for Endpoints を使用している場合は、システムで、AMP for Firepower によって収集されたデータとともにエンドポイントベースのデータをインポートして表示できます。このデータのインポートには、ライセンスは必要ありません。

組織で追加のセキュリティが必要であるか、外部接続を制限する場合は、Cisco AMP プライベートクラウド仮想アプライアンス (AMPv) を使用します。AMPv は個別に AMP for Endpoints イベントを収集し、Firepower Management Center に転送します。

## ファイル制御および Cisco AMP の基本

### AMP for Firepower

AMP for Firepower では、インライン展開された管理対象デバイスを使用して、ネットワーク上のマルウェアを検出、保存、トラッキング、分析、およびブロックできます。AMP for Firepower は、PDF、Microsoft Office ドキュメントを含め、多くのタイプのマルウェアファイルをブロックできます。

#### ファイルの検出と保存

AMP for Firepower により、管理対象デバイスは、特定のファイル タイプの送信のネットワーク トラフィックをモニタします。

デバイスが対象のファイルを検出すると、ファイルの SHA-256 ハッシュ値を Firepower Management Center に送信します。Firepower Management Center は、マルウェア クラウドルックアップを実行し、AMP クラウドでファイルの性質をクエリします。デバイスは、ファイル ストレージ機能を使用して、ハードドライブまたはマルウェアのストレージパックに対象ファイルを保存できます。イベント ビューアのキャプチャ ファイル情報を表示したり、オフライン分析のためにコピーをダウンロードしたりできます。

## ファイル分析

システムでは、ファイルにマルウェアが含まれるかどうかを判断するために、ファイルインスペクションと分析のいくつかの方法が適用されます。



- (注) 設定に応じて、システムがファイルを初めて検出したときに、そのファイルを検査してクラウドルックアップの結果を待機するか、または、クラウドルックアップの結果を待機せずにファイルを通過させることができます。

ファイルルールでオプションを有効にするかどうかに基づいて、システムは次の順序でファイルを検査します。

### Spero 分析

ファイルが対象の実行可能ファイルの場合、デバイスはファイル構造を分析し、結果として得られた Spero シグネチャを AMP Threat Grid クラウドに送信できます。クラウドは、このシグネチャを使用して、ファイルにマルウェアが含まれるかを判断します。

### ローカル マルウェア分析

ローカル マルウェア インスペクション エンジンを使用して、デバイスは対象ファイルを調べ、ファイルにマルウェアが含まれる場合、ファイルルールでそのように設定されていればこのファイルをブロックし、マルウェア イベントを生成します。

また、デバイスにより、ファイルプロパティ、組み込みオブジェクト、および可能性のあるマルウェアの詳細情報を含むファイル構成レポートが生成されます。

### 動的分析

デバイスが、マルウェアの可能性があるととしてファイルを事前分類している場合、デバイスがファイルを保存するかどうかに関係なく、これらのファイルを AMP Threat Grid クラウドまたは AMP Threat Grid オンプレミス アプライアンスに動的分析のために送信します。

AMP Threat Grid クラウドまたはオンプレミスの AMP Threat Grid アプライアンスは、悪意のあるファイルかどうかを判断するためにサンドボックス環境でファイルを実行し、ファイルにマルウェアが含まれる可能性を示す脅威スコアを返します。脅威スコアから、クラウドが脅威スコアを割り当てた理由を詳細に説明する動的分析のサマリー レポートを表示できます。

### ファイルとマルウェア イベント、およびキャプチャ ファイル

ファイル分析結果に基づいて、イベント ビューアからのキャプチャ ファイル、生成されたマルウェアとファイルイベントを確認できます。使用可能な場合は、ファイルの構成、性質、脅威スコア、動的分析のサマリー レポートを調べ、マルウェア分析をさらに詳細に把握できます。また、ファイルがネットワークをどのように通過するか (ホストを通過するか) を示すマップ、およびさまざまなファイルプロパティを表示する、ネットワーク ファイル トラジェクトリにアクセスできます。

### アーカイブ ファイル

システムは、ファイルがアーカイブ (.rar または .zip アーカイブ ファイルなど) の場合、一番外側のアーカイブ ファイル (レベル 0) の下の最大 3 レベルのネストされたファイルを検査できます。ブロック アクションを含むファイル ルールにいずれかの個別ファイルが一致する場合は、その個別ファイルだけでなくアーカイブ全体がブロックされます。また、指定したネストのレベルを超えるアーカイブ、またはそのコンテンツが暗号化されているか検査できないアーカイブも、ブロックされることがあります。

### ファイル トラッキング

AMP クラウドにあるファイルの性質が不正確だとわかっている場合、次のようにして、ファイルの SHA-256 値をファイル リストに追加できます。

- AMP クラウドがクリーンの性質を割り当てた場合と同じ方法でファイルを扱うには、クリーン リストにファイルを追加します。
- AMP クラウドがマルウェアの性質を割り当てた場合と同じ方法でファイルを扱うには、カスタム検出リストにファイルを追加します。

これ以降に検出された場合、デバイスでは、ファイルの性質を再評価せずに許可またはブロックできます。ファイル ポリシーに応じてクリーン リストまたはカスタム検出リストを使用できます。



- (注) ファイル ポリシーで、マルウェア クラウド ルックアップを実行するか、一致ファイルでマルウェアをブロックしてファイルの SHA-256 値を計算するルールを設定する必要があります。

### 関連トピック

[ファイル リスト](#) (476 ページ)

## マルウェアの性質

システムは、AMP クラウドから返される性質に基づいてファイルの性質を決定します。パフォーマンスを改善するために、SHA-256 値に基づいてファイルの性質がシステムですでにわかっている場合、Firepower Management Center は AMP クラウドでクエリを行う代わりに、キャッシュ済みの性質を使用します。システムは、ファイルの性質に基づいてファイルをブロックすることもできます。アーカイブ ファイル内にネストされているファイルが 1 つでもブロックされる場合、システムはアーカイブ ファイル全体をブロックします。

ファイル リストへの追加操作の結果、または脅威スコアに応じて、ファイルの性質は次のいずれかになります。

- マルウェア (Malware) : ファイルが AMP クラウドでマルウェアと分類されていること、ローカルマルウェア分析でマルウェアとして識別されたこと、またはファイルの脅威スコアがファイル ポリシーに定義されたマルウェアのしきい値を超えたこと示します。
- [クリーン (Clean) ] : AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。



- 不明 (Unknown) : システムはAMPクラウドでファイルの性質をクエリしましたが、ファイルには性質が割り当てられていませんでした。言い換えると、AMPクラウドがファイルを分類できませんでした。
- カスタム検出 (Custom Detection) : ユーザがカスタム検出リストにファイルを追加したことを示します。
- 利用不可 (Unavailable) : システムがAMPクラウドでクエリを行えなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。

アーカイブ ファイルの性質は、アーカイブ内部のファイルに割り当てられた性質に基づきます。識別されたマルウェアファイルを含んでいるすべてのアーカイブは、マルウェア (Malware) の性質になります。識別されたマルウェアファイルを含んでいないアーカイブの場合、不明なファイルが1つでも含まれていれば不明 (Unknown) の性質、クリーンファイルのみが含まれていればクリーン (Clean) の性質になります。

表 94: 内容に基づくアーカイブ ファイルの性質

アーカイブ ファイルの性質	不明なファイルの数	クリーン ファイルの数	マルウェア ファイルの数
不明	1 つ以上	任意 (Any)	[0]
クリーン (Clean)	[0]	1 つ以上	[0]
マルウェア (Malware)	任意 (Any)	任意 (Any)	1 つ以上

他のファイルと同様に、アーカイブファイルにも、該当する性質に関する条件が適用される場合はカスタム検出 (Custom Detection) または利用不可 (Unavailable) の性質が割り当てられます。



**ヒント** 短時間で利用不可 (Unavailable) マルウェア イベントが連続して発生した場合は、Firepower Management Center が AMP クラウドに接続できることを確認してください。

ファイルの性質は変更される可能性があることに注意してください。たとえば、AMPクラウドによる判定の結果、以前はクリーンであると考えられていたファイルが今はマルウェアとして識別されるようになったり、その逆、つまりマルウェアと識別されたファイルが実際にはクリーンであったりする可能性があります。前の週にクエリを行ったファイルの性質が変更された場合、AMPクラウドはシステムに通知して、システムが次回そのファイルの送信を検出した際に自動的にアクションをとれるようにします。変更された性質は、レトロスペクティブな性質と呼ばれます。

AMPクラウドのクエリから返された、脅威スコアに関連付けられた性質、およびローカルマルウェア分析によって割り当てられた性質には、存続可能時間 (TTL) が設定されます。性質が更新されないまま、TTL値で指定された期間にわたって保持された後は、キャッシュ情報が消去されます。性質および関連する脅威スコアには次の TTL 値が割り当てられます。

- クリーン : 4 時間

- 不明 : 1 時間
- マルウェア : 1 時間

このキャッシュに対するクエリで、キャッシュされた性質がタイムアウトになったことが識別された場合、システムは AMP クラウドに新しい性質を再びクエリします。

## AMP for Firepower を使用しないファイル制御

マルウェアファイル伝送のブロックに加えて、(マルウェアを含むかどうかにかかわらず) 特定のタイプのすべてのファイルをブロックする必要がある場合は、ファイル制御機能により防御網を広げることができます。AMP for Firepower の場合と同様に、管理対象デバイスはネットワーク トラフィック内で特定のファイルタイプの伝送をモニタし、そのファイルをブロックまたは許可します。

システムでマルウェアを検出できるすべてのファイルタイプだけでなく、さらに多数のファイルタイプに対するファイル制御がサポートされています。これらのファイルタイプは、マルチメディア (swf、mp3)、実行可能ファイル (exe、トレント)、PDF などの基本的なカテゴリにグループ分けされます。ファイル制御は AMP for Firepower とは異なり、AMP クラウドへの照会を必要としないことに注意してください。

## エンドポイント向け AMP

エンドポイント向け AMP は、シスコのエンタープライズクラスの高度なマルウェア防御ソリューションです。高度なマルウェアの発生、高度で継続的な脅威、およびターゲット型攻撃を検出、分析、ブロックします。次の図に、エンドポイント向け AMP を使用した場合の一般的な情報フローを示します。



所属部門がエンドポイント向け AMP を使用している場合、個々のユーザはエンドポイント (つまり、コンピュータやモバイルデバイス) に軽量コネクタをインストールします。コネクタは、ファイルのアップロード、ダウンロード、実行、開く、コピー、移動などの操作を行う際にファイルを検査します。コネクタは AMP クラウドと通信して、検査対象のファイルにマルウェアが含まれるかどうかを判断します。

ファイルがマルウェアとして特定された場合、AMP クラウドは特定した脅威の情報を Firepower Management Center に送ります。さらに AMP クラウドは、スキャン、検疫、実行のブロック、クラウドリコールなど、他の種類のデータを Firepower Management Center に送信すること

もできます。Firepower Management Center はこれらの情報をマルウェア イベントとしてログに記録します。

エンドポイント向け AMP は、ホストのセキュリティに感染の疑いがある場合、侵害の兆候 (IOC) を生成することができます。Firepower システムでは、モニタ対象ホストの IOC 情報が表示できます。シスコでは折にふれて、エンドポイントベースのマルウェア イベントに対応する新しい IOC タイプの開発を行っており、システムにより自動的にダウンロードされます。

エンドポイント向け AMP では、マルウェア イベントに基づいて Management Center で開始される修復やアラートを設定できるだけでなく、エンドポイント向け AMP 管理コンソールを使ってマルウェアの影響を軽減することもできます。管理コンソールの堅牢かつ柔軟な Web インターフェイスを使用すると、エンドポイント向け AMP 展開のあらゆる側面を制御し、アウトブレイクのすべての段階を管理できます。次の操作を実行できます。

- 部門全体のためにカスタム マルウェア検出ポリシーとプロファイルを設定し、すべてのユーザのファイルに対してフラッシュ スキャンおよび完全スキャンを実行する
- マルウェア分析の実行：ヒートマップ、詳細なファイル情報、ネットワーク ファイルトラジェクトリ、脅威の根本原因の表示など
- アウトブレイクコントロールのさまざまな要素を設定する：自動検疫、検疫されていない実行可能ファイルの実行を停止するアプリケーションブロッキング、除外リストなど
- カスタム保護の作成、グループポリシーに基づく特定のアプリケーションの実行ブロッキング、およびカスタム ホワイトリストの作成



**ヒント** エンドポイント向け AMP の詳細については『AMP for Endpoints management console』を参照してください。

## AMP for Firepower とエンドポイント向け AMP の比較

Firepower システムは、AMP for Firepower およびエンドポイント向け AMP のどちらのデータも使用できます。

管理対象デバイスはネットワークトラフィックのマルウェアを検出しますが、エンドポイント向け AMP のマルウェア検出はダウンロード時または実行時にエンドポイントで行われるため、この 2 種類のマルウェア イベントの情報は異なります。たとえば、エンドポイントベースのマルウェア イベントには、ファイルパス、呼び出し元クライアントアプリケーションなどの情報が含まれるのに対して、ネットワークトラフィックでのマルウェア検出には、ファイル伝送に使われた接続のポート、アプリケーションプロトコル、発信元 IP アドレス情報が含まれます。

別の例としては、ネットワークベースのマルウェア イベントの場合、ユーザ情報は、ネットワーク検出で判別された、マルウェアの送信先であるホストに最後にログインしたユーザを示すことが挙げられます。一方、エンドポイント向け AMP で報告されるユーザは、マルウェアが検出されたエンドポイントに現在ログインしているユーザを示します。



(注) 展開によっては、AMP for Endpoints がモニタするエンドポイントは、AMP for Firepower がモニタしているものと同じホストではない場合があります。このため、エンドポイントベースのマルウェア イベントは、ネットワーク マップにホストを追加しません。ただし、システムは IP アドレスおよび MAC アドレスのデータを使用して、AMP for Endpoints の展開から取得した侵害の兆候をモニタ対象のホストにタグ付けします。異なる AMP ソリューションによってモニタされる2つの異なるホストが同じ IP アドレスと MAC アドレスを持っている場合、システムは AMP for Endpoints の IOC をモニタ対象のホストに誤ってタグ付けする場合があります。

次の表に、2つの戦略の違いをまとめます。

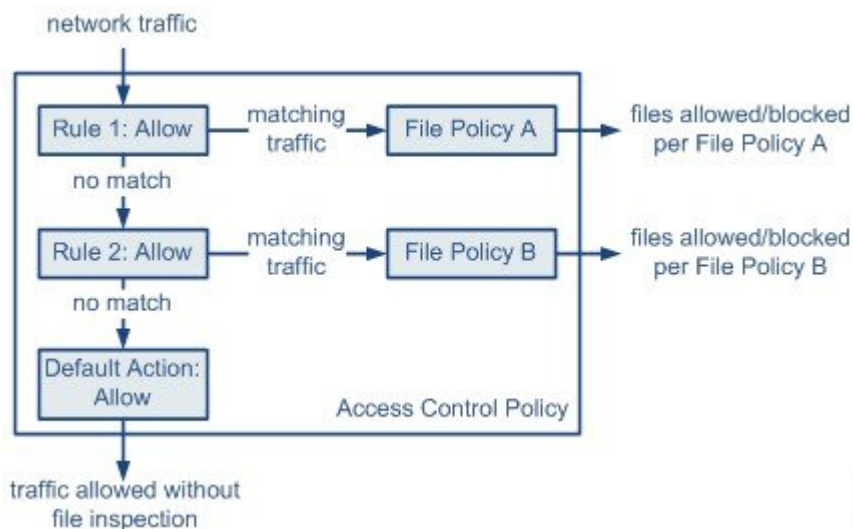
表 95: ネットワークベースとエンドポイントベースの高度なマルウェア防御戦略の比較

機能	AMP for Firepower	エンドポイント向け AMP
ファイルタイプの検出とブロックングの方法 (ファイル制御)	ネットワークトラフィックで、アクセスコントロールポリシーとファイルポリシーを使用	未サポート
マルウェアの検出とブロックングの方法	ネットワークトラフィックで、アクセスコントロールポリシーとファイルポリシーを使用	個々のエンドポイントで、AMPクラウドとの通信を行うコネクタを使用
ネットワークトラフィックを検査	管理対象デバイスを通るトラフィック	なし (エンドポイントにインストールされたコネクタがファイルを直接検査する)
マルウェア検出の堅牢性	限定されたファイルタイプ	すべてのファイルタイプ
マルウェア分析の選択肢	Management Center ベース、および AMP クラウドでの分析	Management Center ベース、およびエンドポイント向け AMP 管理コンソールの追加オプション
マルウェアの影響軽減	ネットワークトラフィックでのマルウェアブロックング、Management Center が開始する修復	エンドポイント向け AMP ベースの検疫およびアウトブレイクコントロールオプション、Management Center が開始する修復
生成されるイベント	ファイルイベント、キャプチャされたファイル、マルウェアイベント、およびレトロスペクティブマルウェアイベント	マルウェア イベント
マルウェア イベントに含まれる情報	基本的なマルウェアイベント情報、および接続データ (IP アドレス、ポート、アプリケーションプロトコル)	詳細なマルウェアイベント情報 (接続データなし)

機能	AMP for Firepower	エンドポイント向け AMP
ネットワーク ファイル トラジェクトリ	Management Center ベース	Management Center ベース、およびエンドポイント向け AMP 管理コンソールの追加オプション
必要なライセンスまたはサブスクリプション	ファイル制御および AMP for Firepower の実行に必要なライセンス	エンドポイント向け AMP サブスクリプション (ライセンスベースではありません)

## ファイルポリシー

ファイルポリシーは、いくつかの設定からなるセットです。システムは全体的なアクセス制御設定の一部としてこれを使用して、AMP for Firepower とファイル制御を実行できます。この関連付けにより、アクセス コントロール ルールの条件と一致するトラフィック内のファイルを通させる前に、システムは必ずファイルを検査するようになります。次の図のような、インライン展開での単純なアクセス コントロール ポリシーがあるとします。



371859

このポリシーには2つのアクセス コントロール ルールがあり、両方とも許可アクションを使用し、ファイル ポリシーに関連付けられています。このポリシーのデフォルトアクションもまた「トラフィックの許可」ですが、ファイル ポリシー インспекションはありません。このシナリオでは、トラフィックは次のように処理されます。

- ルール 1 に一致するトラフィックはファイル ポリシー A で検査されます。
- ルール 1 に一致しないトラフィックはルール 2 に照らして評価されます。ルール 2 に一致するトラフィックはファイル ポリシー B で検査されます。
- どちらのルールにも一致しないトラフィックは許可されます。デフォルトアクションにファイル ポリシーを関連付けることはできません。

1つのファイルポリシーを、[許可 (Allow)]、[インタラクティブブロック (Interactive Block)]、または[リセットしてインタラクティブブロック (Interactive Block with reset)]アクションを含むアクセスコントロールルールに関連付けることができます。その後、システムはそのファイルポリシーを使用して、アクセスコントロールルールの条件を満たすネットワークトラフィックを検査します。

異なるファイルポリシーを個々のアクセスコントロールルールに関連付けることにより、ネットワークで伝送されるファイルを識別/ブロックする方法をきめ細かく制御できます。ただし、アクセスコントロールのデフォルトアクションによって処理されるトラフィックを検査するためにファイルポリシーを使用できないことに注意してください。

## ファイルポリシーの詳細設定

### 詳細なファイルインスペクションの設定に関する注意事項

ファイルポリシーでは、詳細なオプションを設定して、カスタム検出リストのファイルのブロック、クリーンリストのファイルの許可、およびファイルがマルウェアと見なされる脅威スコアのしきい値の設定を行うことができます。

また、組織のニーズに合わせてアーカイブファイルを分析し、ブロックできるように、アーカイブファイルの内容を検査するようにファイルポリシーを設定できます。圧縮解除されたファイルに適用できるすべての機能（動的分析やファイルストレージなど）は、アーカイブファイル内のネストされたファイルに使用可能です。

### アーカイブファイルのインスペクションに関する注意事項

一部のアーカイブファイルには、追加のアーカイブファイル（など）が含まれています。ファイルがネストされるレベルは、そのアーカイブファイルの深さです。トップレベルのアーカイブファイルは深さの数で考慮されないことに注意してください。深さは最初にネストされたファイルで1から始まります。

システムでは、ネストされたアーカイブファイルを最大3レベルまでしか検査できませんが、その深さ（または指定したそれより低い最大深さ）を超えるアーカイブファイルをブロックするようファイルポリシーを設定できます。ネストされたアーカイブをさらに制限する場合は、2または1のより低い最大ファイル深さを設定するオプションがあります。

最大アーカイブファイルの深さ3を超えるファイルをブロックしないよう選択した場合、抽出可能な内容と深さ3以上でネストされた内容を含むアーカイブファイルがモニタ対象のトラフィックに現れると、システムは検査可能だったファイルについてのみデータを検査して報告します。



- (注) アーカイブファイルを含むトラフィックがセキュリティインテリジェンスによってブラックリスト登録またはホワイトリスト登録された場合、またはトップレベルのアーカイブファイルの SHA-256 値がカスタム検出リストにある場合、システムはアーカイブファイルの内容を検査しません。ネストされたファイルがブラックリスト登録された場合、アーカイブ全体がブロックされます。しかし、ネストされたファイルがホワイトリスト登録された場合、アーカイブは自動的に渡されません (他のネストされたファイルおよび特性による)。

アーカイブファイルの内容を検査するようにファイルポリシーが設定されている場合は、イベントビューアのコンテキストメニューおよびネットワークファイルトラジェクトリビューアを使用して、アーカイブファイルがファイルイベント、マルウェアイベントに現れた場合、またはキャプチャされたファイルとして現れた場合に、アーカイブ内のファイルに関する情報を表示できます。

アーカイブのすべてのファイルコンテンツは表形式でリストされます。そのリストには、名前、SHA-256ハッシュ値、タイプ、カテゴリ、およびアーカイブの深さといった関連情報の概略が含まれています。ネットワークファイルトラジェクトリアイコンはファイルごとに表示されます。そのアイコンをクリックすることで、特定のファイルに関する詳細な情報を表示することができます。

#### ファイルポリシー設定に関する注意事項と制約事項

- 新しいポリシーの場合、ポリシーが使用中でないことが Web インターフェイスに示されます。使用中のファイルポリシーを編集している場合は、そのファイルポリシーを使用しているアクセスコントロールポリシーの数が Web インターフェイスに示されます。どちらの場合も、テキストをクリックすると [アクセスコントロールポリシー (Access Control Policies)] ページに移動できます。
- FTP に関する [マルウェアブロック (Block Malware)] ルールを持つファイルポリシーを使用するアクセスコントロールポリシーでは、[インライン時にドロップ (Drop when Inline)] を無効にした侵入ポリシーをデフォルトアクションに設定した場合、システムはルールに一致するファイルやマルウェアの検出でイベントを生成しますが、ファイルをドロップしません。FTPファイア転送をブロックし、ファイルポリシーを選択するアクセスコントロールポリシーのデフォルトアクションとして侵入ポリシーを使用するには、[インライン時にドロップ (Drop when Inline)] を有効にした侵入ポリシーを選択する必要があります。

## ファイルポリシーの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
Threat (ファイル制御) マルウェア (AMP for Firepower)	Protection (ファイル制御) マルウェア (AMP for Firepower)	任意 (Any)	任意 (Any)	Admin/Access Admin

[ファイルポリシー (File Policies)] ページには、既存のファイルポリシーが最終更新日とともに表示されます。このページは、ファイルポリシーの管理に使用できます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。






- (注) 動的分析の対象になるファイルタイプのリストが更新されたかどうか検査するために、システムは AMP クラウドをチェックします (多くても 1 日に 1 回)。対象になるファイルタイプのリストが変更された場合、これはファイルポリシーの変更を意味します。このファイルポリシーを使用するアクセスコントロールポリシーがいずれかのデバイスに展開されている場合、そのアクセスコントロールポリシーには失効マークが付けられます。更新したファイルポリシーがデバイスで有効になるには、まず、ポリシーを展開しておく必要があります。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [マルウェアとファイル (Malware & File)] を選択します。

**ステップ 2** ファイルポリシーを管理します。

- [比較 (Compare)] : [ポリシーの比較 (Compare Policies)] をクリックします ([ポリシーの比較 \(361 ページ\)](#) を参照)。
- 作成 : ファイルポリシーを作成するには、[新規ファイルポリシー (New File Policy)] をクリックし、[ファイルポリシーの作成 \(1539 ページ\)](#) で説明する手順を実行します。
- コピー : ファイルポリシーをコピーするには、コピーアイコン () をクリックします。  
代わりに表示アイコン () が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 削除 : ファイルポリシーを削除するには、削除アイコン () をクリックし、プロンプトが表示されたら [はい (Yes)] と [OK] をクリックします。



コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- 展開: [展開 (Deploy)] をクリックします ([設定変更の導入 \(350 ページ\)](#) を参照)。
- 編集: 既存のファイルポリシーを変更するには、編集アイコン (✎) をクリックします。
- [レポート (Report)]: レポートアイコン (📄) をクリックします ([現在のポリシー レポートの生成 \(363 ページ\)](#) を参照)。

## ファイルポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
Threat (ファイル制御) マルウェア (AMP for Firepower)	Protection (ファイル制御) マルウェア (AMP for Firepower)	任意 (Any)	任意 (Any)	Admin/Access Admin

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [マルウェアとファイル (Malware & File)] を選択します。

**ヒント** 既存のファイルポリシーのコピーを作成するには、コピーアイコン (📄) をクリックして、表示されるダイアログボックスで新しいポリシーの固有名を入力します。その後、そのコピーを変更できます。

**ステップ 2** [新しいファイルポリシー (New File Policy)] をクリックします。

**ステップ 3** 新しいポリシーの [名前 (Name)] とオプションの [説明 (Description)] を入力します。

**ステップ 4** [保存 (Save)] をクリックします。

**ステップ 5** [ファイルルールの作成 \(1548 ページ\)](#) の説明に従って、ファイルポリシーに1つ以上のルールを追加します。

**ステップ 6** 必要に応じて、[詳細 (Advanced)] タブを選択し、[詳細オプションおよびアーカイブファイル 検査オプション \(1540 ページ\)](#) の説明に従って詳細オプションを設定します。

**ステップ 7** ファイルポリシーを保存します。

### 次のタスク

- [ファイル制御およびマルウェア保護のためのアクセスコントロールルールの設定 \(1364 ページ\)](#) の説明に従って、アクセスコントロールルールにファイルポリシーを追加します。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 詳細オプションおよびアーカイブファイル検査オプション

ファイルポリシーエディターの [詳細設定 (Advanced)] タブには、次の一般オプションがあります。

- [初回ファイル分析 (First Time File Analysis)] : システムで初めて検出するファイル分析のためのファイルを送信します。ファイルは、マルウェアクラウドルックアップと Spero 分析、ローカルマルウェア分析、またはダイナミック分析を実行するように設定されているルールに一致する必要があります。このオプションを無効にすると、初めて検出されたファイルの性質が「不明 (Unknown)」になります。
- [カスタム検出リストを有効にする (Enable Custom Detection List)] : カスタム検出リストにあるファイルをブロックします。
- [クリーンリストを有効にする (Enable Clean List)] : クリーンリストにあるファイルを許可します。
- [ダイナミック分析の脅威スコアに基づいてマルウェアとしてファイルをマークする (Mark files as malware based on dynamic analysis threat score)] : しきい値の脅威スコアを設定します。スコアがしきい値以上のファイルはマルウェアと見なされます。

しきい値に低い値を選択すると、マルウェアとして扱われるファイルの数が増えます。ファイルポリシーで選択したアクションによっては、その結果、ブロックされるファイルの数が増える可能性があります。

ファイルポリシーエディターの [詳細設定 (Advanced)] タブには、次のアーカイブファイル検査オプションがあります。

- [アーカイブを検査する (Inspect Archives)] : アーカイブファイルの内容を検査します。



#### 注意

[アーカイブを検査する (Inspect Archives)] を有効化または無効化 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

- [暗号化されているアーカイブをブロックする (Block Encrypted Archives) ] : 暗号化されている内容を含むアーカイブ ファイルをブロックします。
- [検査できないアーカイブをブロックする (Block Uninspectable Archives) ] : 暗号化以外の理由で検査できない内容を含むアーカイブ ファイルをブロックします。これは、通常、破損したファイル、または指定されているアーカイブの最大の深さを超えるファイルに適用されます。
- [アーカイブの最大の深さ (Max Archive Depth) ] : 指定されている深さを超えてネストされているアーカイブをブロックします。最上位のアーカイブ ファイルはこの数に含まれず、深さは最初のネスト ファイルを 1 として始まります。

### 関連トピック

[Snort® の再起動シナリオ](#) (354 ページ)

## ファイルポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
Threat (ファイル制御) マルウェア (AMP for Firepower)	Protection (ファイル制御) マルウェア (AMP for Firepower)	任意 (Any)	任意 (Any)	Admin/Access Admin

### 手順

- ステップ 1** [ポリシー (Policies) ] > [アクセス コントロール (Access Control) ] > [マルウェアとファイル (Malware & File) ] を選択します。
- ステップ 2** 編集するファイル ポリシーの横にある編集アイコン (✎) をクリックします。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3** 次の選択肢があります。
  - [ファイルルールの追加 (Add File Rule) ] を選択して、ファイルルールを追加します。詳細については、[ファイルルール \(1542 ページ\)](#) を参照してください。
  - 既存のファイルルールを編集するには、そのルールの横にある編集アイコン (✎) をクリックします。
  - [詳細オプションおよびアーカイブファイル検査オプション \(1540 ページ\)](#) の説明に従って詳細オプションを設定します。

- (注) ファイルポリシーエディタに、現在編集集中のファイルポリシーを使用しているアクセスコントロールポリシーの数が表示されます。この通知をクリックすると、親ポリシーのリストが表示され、オプションで[アクセスコントロールポリシー (Access Control Policies)] ページに進むことができます。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ファイルルール

ファイルのポリシーには、その親であるアクセスコントロールポリシーと同様に、各ルールの条件に一致したファイルをシステムがどのように処理するかを決定するルールが含まれています。ファイルタイプ、アプリケーションプロトコル、転送方向の違いに応じて異なるアクションを実行する別個のファイルルールを設定できます。

ファイルがルールに一致すると、ルールは以下を実行できます。

- 単純なファイルタイプ照合に基づいてファイルを許可またはブロックする
- 性質に基づいてファイルをブロックする
- キャプチャされたファイルをデバイスに保存する
- ローカルマルウェア分析、Spero 分析、または動的分析のために、キャプチャしたファイルを送信する。

さらに、ファイルポリシーによって以下を実行できます。

- クリーンリストまたはカスタム検出リストのエントリに基づいて、ファイルがクリーンまたはマルウェアである場合と同じ方法で自動的にファイルを扱う
- ファイルの脅威スコアが、設定可能なしきい値を超えた場合、マルウェアと同じ方法でファイルを扱う
- アーカイブファイル (.zip や .rar など) の内容を検査する
- アーカイブファイルの内容が暗号化されている場合、アーカイブのネストレベルが最大レベル指定値より深い場合、あるいはその反対で検査できない場合、アーカイブファイルをブロックする

## ファイル ルールのコンポーネント

表 96: ファイル ルールのコンポーネント

ファイル ルールのコンポーネント	説明
アプリケーション プロトコル	システムは、FTP、HTTP、SMTP、IMAP、POP3、および NetBIOS-ssn (SMB) を介して伝送されるファイルを検出し、検査できます。デフォルトの [任意 (Any)] は、HTTP、SMTP、IMAP、POP3、FTP、および NetBIOS-ssn (SMB) トラフィック内のファイルを検出します。パフォーマンスを向上させるには、ファイルルールごとに、これらのアプリケーション プロトコルのうち 1 つだけでファイルを検出するよう限定できます。
転送の方向	ダウンロードされるファイルに対して、FTP、HTTP、IMAP、POP3、および NetBIOS-ssn (SMB) の着信トラフィックを検査できます。アップロードされるファイルに対しては、FTP、HTTP、SMTP、および NetBIOS-ssn (SMB) の発信トラフィックを検査できます。  <b>ヒント</b> [任意 (Any)] を使用すると、ユーザが送信しているか受信しているかには関係なく、多数のアプリケーション プロトコルを介したファイルが検出されます。
ファイルのカテゴリとタイプ	システムは、さまざまなタイプのファイルを検出できます。これらのファイルタイプは、マルチメディア (swf、mp3)、実行可能ファイル (exe、トレント)、PDF などの基本的なカテゴリにグループ分けされます。個々のファイルタイプを検出したり、ファイルタイプカテゴリ全体を検出したりするよう、ファイルルールを設定できます。  たとえば、すべてのマルチメディア ファイルをブロックしたり、ShockWave Flash (swf) ファイルのみをブロックしたりできます。または、ユーザが BitTorrent (torrent) ファイルをダウンロードしたときにアラートを出すよう、システムを設定できます。  (注) 頻繁にトリガーされるファイルルールは、システム パフォーマンスに影響を与える可能性があります。たとえば、HTTP トラフィックでマルチメディア ファイルを検出しようとする (たとえば YouTube は多量の Flash コンテンツを伝送します)、膨大な数のイベントが生成される可能性があります。

ファイルルールのコンポーネント	説明
ファイルルールアクション	<p>ファイルルールのアクションによって、ルールの条件に一致したトラフィックをシステムが処理する方法が決定されます。</p> <p>選択したアクションに応じて、システムでファイルを保存するか、ファイルに対して Spero 分析、ローカルマルウェア分析、または動的分析を実行するかを設定できます。[ブロック (Block)] アクションを選択すると、システムでブロックされた接続をリセットするかどうかも設定できます。</p> <p>(注) ファイルルールは数値上の順番ではなく、ルールアクションの順番で評価されます。</p>

## ファイルルールアクションと評価順序

効果を発揮するには、ファイルポリシーに1つ以上のルールが含まれている必要があります。ファイルルールを使用すると、ロギング、ブロック、またはマルウェア スキャンの対象となるファイルタイプを詳細に制御できます。

各ファイルルールには、ルールの条件に一致するトラフィックがシステムによってどのように処理されるかを決定する1つのアクションが関連付けられます。1つのファイルポリシー内に、ファイルタイプ、アプリケーションプロトコル、転送方向の違いに応じて異なるアクションを実行する別々のルールを設定できます。(優先度の高い順に) 単純なブロッキング、次にマルウェアインスペクションとブロッキング、さらにその次に単純な検出とロギングとなります。

複数のファイルルールアクションは、以下のようなルールアクション順になります。

- [ファイルブロック (Block Files)] ルールを使用すると、特定のファイルタイプをブロックできます。ファイル転送がブロックされたときに接続をリセットするオプション、およびキャプチャされたファイルを管理対象デバイスに保存するオプションを設定できます。
- [マルウェアブロック (Block Malware)] ルールを使用すると、特定のファイルタイプの SHA-256 ハッシュ値を計算した後、AMP クラウドを照会して、ネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示すファイルをブロックできます。
- [マルウェアクラウドルックアップ (Malware Cloud Lookup)] ルールを使用すると、ネットワークを通過するファイルの性質を取得して記録したうえでその伝送を許可できます。
- [ファイル検出 (Detect Files)] ルールを使用すると、ファイルの伝送を許可しながら、特定のファイルタイプの検出をデータベースに記録できます。



## 注意

[ファイルの検出 (Detect Files) ] または [ファイルのブロック (Block Files) ] を選択、[ファイルの検出 (Detect Files) ] または [ファイルのブロック (Block Files) ] ルールで [ファイルの保存 (Store files) ] または無効化、または [マルウェア クラウドルックアップ (Malware Cloud Lookup) ] または [マルウェア ブロック (Block Malware) ] ファイルルールアクションを分析オプション ([Spero 分析または MSEXE (Spero Analysis or MSEXE) ]、[動的分析 (Dynamic Analysis) ]、または [ローカル マルウェア分析 (Local Malware Analysis) ]) またはファイルの保存オプション ([マルウェア (Malware) ]、[不明 (Unknown) ]、[正常 (Clean) ]、または [カスタム (Custom) ]) と結合する最初のファイルルールを追加または最後のファイルルールを削除すると、設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

ファイルルールアクションに応じて、ファイル転送がブロックされたときに接続をリセットするオプション、管理対象デバイスに取得したファイルを保存するオプション、ファイルでマルウェアをローカルで分析するオプション、取得したファイルを動的分析および Spero 分析のために AMP クラウドに送信するオプション、および後で送信するためにクラウドに現在送信できないファイルを保存するオプションを設定できます。

表 97: ファイルルールアクション

ファイルルールアクションのオプション	ファイルのブロックが可能か	マルウェアのブロックが可能か	ファイルの検出が可能か	マルウェア クラウドルックアップが可能か
MSEXE 用の Spero 分析 (Spero Analysis for MSEXE)	No	はい: 実行可能 ファイルを送信できます	No	はい: 実行可能 ファイルを送信できます
動的分析 (Dynamic Analysis)	No	はい: 不明なファイルの性質の実行可能ファイルを送信できます	No	はい: 不明なファイルの性質の実行可能ファイルを送信できます
容量処理 (Capacity Handling)	No	Yes	No	Yes
ローカル マルウェア分析 (Local Malware Analysis)	No	Yes	No	Yes

ファイルルールアクションのオプション	ファイルのブロックが可能か	マルウェアのブロックが可能か	ファイルの検出が可能か	マルウェアクラウドルックアップが可能か
接続のリセット (Reset Connection)	はい (推奨)	はい (推奨)	No	No
ファイルの保存 (Store files)	はい: 一致するすべてのファイルを保存できます	はい: 選択したファイルの性質に一致するファイルタイプを保存できます	はい: 一致するすべてのファイルを保存できます	はい: 選択したファイルの性質に一致するファイルタイプを保存できます

## ファイルポリシーの注意事項と制約事項

### ファイルルール設定に関する注意事項と制約事項

- パッシブ展開でファイルをブロックするよう設定されたルールは、一致するファイルをブロックしません。接続ではファイル伝送が続行されるため、接続の開始をログに記録するルールを設定した場合、この接続に関して複数のイベントが記録されることがあります。
- [マルウェアクラウドルックアップ (Malware Cloud Lookup)] アクションまたは [マルウェアブロック (Block Malware)] アクションを使ってファイルルールが設定されている場合、Firepower Management Center が AMP クラウドとの接続を確立できないと、接続が復元されるまで、システムは設定済みルールアクションオプションを実行できません。
- シスコでは、[ファイルブロック (Block Files)] アクションと [マルウェアブロック (Block Malware)] アクションで [接続のリセット (Reset Connection)] を有効にすることを推奨しています。これにより、ブロックされたアプリケーションセッションが TCP 接続リセットまで開いたままになることを防止できます。接続をリセットしない場合、TCP 接続が自身をリセットするまで、クライアントセッションが開いたままになります。
- 大量のトラフィックをモニタしている場合、キャプチャしたすべてのファイルを保存したり、動的分析用に送信したりしないでください。そのようにすると、システムパフォーマンスに悪影響が及ぶことがあります。
- システムで検出されるすべてのファイルタイプに対してマルウェア分析を実行できるわけではありません。[アプリケーションプロトコル (Application Protocol)]、[転送の方向 (Direction of Transfer)]、および [アクション (Action)] ドロップダウンリストで値を選択すると、システムはファイルタイプのリストを限定します。

### ファイル検出に関する注意事項と制約事項

- アダプティブプロファイリングが有効でなければ、アクセスコントロールルールは、AMP を含め、ファイルの制御を実行できません。



- ファイルがアプリケーション プロトコル条件を持つルールに一致する場合、ファイル イベントの生成は、システムがファイルのアプリケーションプロトコルを正常に識別した後に行われます。識別されていないファイルは、ファイル イベントを生成しません。
- FTP は、さまざまなチャネルを介してコマンドおよびデータを転送します。パッシブまたはインライン タップ モードの展開では、FTP データ セッションとその制御セッションからのトラフィックは同じ内部リソースに負荷分散されない場合があります。
- POP3、POP、SMTP、または IMAP セッションでのすべてのファイル名の合計バイト数が 1024 を超えると、セッションのファイル イベントでは、ファイル名バッファがいっぱいになった後で検出されたファイルの名前が正しく反映されないことがあります。
- SMTP 経由でテキストベースのファイルを送信すると、一部のメールクライアントは改行を CRLF 改行文字標準に変換します。MAC ベースのホストはキャリッジリターン (CR) 文字を使用し、UNIX/Linux ベースのホストはライン フィード (LF) 文字を使用するので、メールクライアントによる改行変換によってファイルのサイズが変更される場合があります。一部のメールクライアントは、認識できないファイルタイプを処理する際に改行変換を行うようデフォルト設定されていることに注意してください。

## ファイル ブロックに関する注意事項と制約事項

- ファイルの終わりを示す End of File マーカーが検出されない場合、転送プロトコルとは無関係に、そのファイルはマルウェア ブロック ルールでもカスタム検出リストでもブロックされません。システムは、End of File マーカーで示されるファイル全体の受信が完了するまでファイルのブロックを待機し、このマーカーが検出された後にファイルをブロックします。
- FTP ファイル転送で End of File マーカーが最終データ セグメントとは別に伝送される場合、マーカーがブロックされ、ファイル転送失敗が FTP クライアントに表示されますが、実際にはそのファイルは完全にディスクに転送されます。
- [ファイルブロック (Block Files) ] アクションおよび [マルウェア ブロック (Block Malware) ] アクションを持つファイルルールでは、最初のファイル転送試行後 24 時間で検出される、同じファイル、URL、サーバ、クライアントアプリケーションを使った新しいセッションをブロックすることにより、HTTP 経由のファイルダウンロードの自動再開をブロックします。
- まれに、HTTP アップロードセッションからのトラフィックが不適切である場合、システムはトラフィックを正しく再構築できなくなり、トラフィックのブロックやファイル イベントの生成を行いません。
- [ファイルブロック (Block Files) ] ルールでブロックされる NetBIOS-ssn 経由ファイル転送 (SMB ファイル転送など) の場合、宛先ホストでファイルが見つかることがあります。ただし、ダウンロード開始後にファイルがブロックされ、結果としてファイル転送が不完全になるため、そのファイルは使用できません。
- (SMB ファイル転送など) NetBIOS-ssn 経由で転送されるファイルを検出またはブロックするファイルルールを作成した場合、ファイル ポリシーを呼び出すアクセス コントロール ポリシーの展開前に開始された、確立済み TCP または SMB セッションで転送される

ファイルに対しては、検査が行われません。このため、これらのファイルは検出/ブロックされません。

- Firepower Threat Defense のハイ アベイラビリティを設定したときに、元のアクティブなデバイスがファイルを識別している間にフェイル オーバーが発生した場合、ファイル タイプは同期されません。ファイル ポリシーでそのファイル タイプがブロックされている場合でも、新しいアクティブ デバイスはファイルをダウンロードします。

## ファイル ルールの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
Threat (ファイル制御)	Protection (ファイル制御)	任意 (Any)	任意 (Any)	Admin/Access Admin
Malware (AMP for Firepower)	Malware (AMP for Firepower)			



**注意** [ファイルの検出 (Detect Files) ]または[ファイルのブロック (Block Files) ]を選択した場合、[ファイルの検出 (Detect Files) ]または[ファイルのブロック (Block Files) ]ルールで[ファイルの保存 (Store files) ]を有効化/無効化した場合、または[マルウェアクラウドルックアップ (Malware Cloud Lookup) ]または[マルウェアブロック (Block Malware) ]ファイルルールアクションを分析オプション ([Spero 分析または MSEXE (Spero Analysis or MSEXE) ]、[動的分析 (Dynamic Analysis) ]、または[ローカル マルウェア分析 (Local Malware Analysis) ]) またはファイルの保存オプション ([マルウェア (Malware) ]、[不明 (Unknown) ]、[正常 (Clean) ]、または[カスタム (Custom) ]) と結合する最初のファイルルールを追加または最後のファイルルールを削除した場合には、設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### 手順

- ステップ 1** ファイルポリシーエディタで、[ファイルルールの追加 (Add File Rule) ]をクリックします。
- ステップ 2** [ファイルルールのコンポーネント \(1543 ページ\)](#) の説明に従って、[アプリケーションプロトコル (Application Protocol) ]および[転送の宛先 (Direction of Transfer) ]を選択します。
- ステップ 3** [ファイルタイプ (File Types) ]を1つ以上選択します。ファイルタイプのリストを、次のようにフィルタ処理できます。

- 1つ以上の [ファイルタイプカテゴリ (File Type Categories)] を選択し、[選択したカテゴリのすべてのタイプ (All types in selected Categories)] をクリックします。
- 名前または説明でファイルタイプを検索します。たとえば、Microsoft Windows 固有のファイルのリストを表示するには、[名前および説明の検索 (Search name and description)] フィールドに **Windows** と入力します。

ヒント ファイルタイプの上にポインタを移動すると、説明が表示されます。

**ステップ 4** [ファイルルールアクションと評価順序 \(1544 ページ\)](#) の説明に従って、ファイルルールの [アクション (Action)] を選択します。

**ステップ 5** 選択したアクションに応じて、以下を実行するかどうかを設定します。

- ファイルのブロック後に接続をリセットする
- 一致するファイルを保存する
- Spero 分析を有効にする
- ローカル マルウェア分析を有効にする
- ダイナミック分析およびキャパシティの処理を有効にする

[ファイルルールアクションと評価順序 \(1544 ページ\)](#) の説明を参照してください。

**ステップ 6** [追加 (Add)] をクリックします。

**ステップ 7** [保存 (Save)] をクリックしてポリシーを保存します。

---

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[Snort® の再起動シナリオ \(354 ページ\)](#)

## クラウド接続

Firepower システムでは Cisco Advanced Malware Protection (AMP) を実施するため、次のパブリック クラウドベースのサーバへの接続を行います。

- AMP クラウド : AMP for Firepower のマルウェア判定結果と更新、エンドポイント向け AMP のスキャンレコード、マルウェア検出、検疫、侵害の兆候 (IOC) を取得できます。
- AMP Threat Grid クラウド : AMP for Firepower ダイナミック分析に利用可能なファイルの送信、脅威スコアやダイナミック分析レポートの取得ができます。

部門のプライバシー、セキュリティ保護のニーズに応じて、プライベートクラウドサーバを導入することもできます。

- AMPプライベートクラウド仮想アプライアンス (AMPv) は、圧縮型、オンプレミスAMPクラウドおよびパブリックAMPクラウドに接続するための匿名プロキシとして機能します。
- AMP Threat Grid アプライアンスはパブリックAMP Threat Gridクラウドとは連絡しないオンプレミスAMP Threat Gridクラウドとして機能します。

## AMP クラウド接続

高度なマルウェア防御 (AMP) クラウドは、ビッグデータ分析や連続分析によりネットワーク上のマルウェアを検出およびブロックするシスコホステッドサーバです。次の2つのシスコAMPソリューションはどちらもAMPクラウドを使用します。

- AMP for Firepower は、管理対象デバイスがネットワークトラフィックから検出した潜在的なマルウェアの性質を取得し、ローカルマルウェア分析とファイルの事前分類の更新を取得するためにAMPクラウドを使用します。
- エンドポイント向けAMPは、シスコのエンタープライズクラスのAMPソリューションです。ユーザはそれぞれ、AMPクラウドと通信するコンピュータやモバイルデバイスに軽量コネクタをインストールします。次にFirepower Management Centerがスキャン、マルウェア検出、隔離、および侵害の兆候 (IOC) のレコードをインポートします。

展開によっては、AMP for Endpoints がモニタするエンドポイントは、AMP for Firepower がモニタしているものと同じホストではない場合があります。このため、エンドポイントベースのマルウェアイベントは、ネットワークマップにホストを追加しません。ただし、システムはIPアドレスおよびMACアドレスのデータを使用して、AMP for Endpoints の展開から取得した侵害の兆候をモニタ対象のホストにタグ付けします。異なるAMPソリューションによってモニタされる2つの異なるホストが同じIPアドレスとMACアドレスを持っている場合、システムはAMP for Endpoints のIOCをモニタ対象のホストに誤ってタグ付けする場合があります。

[AMP管理 (AMP Management) ]ページ ([AMP]>[AMP管理 (AMP Management) ]) でAMPクラウドとの接続を管理します。AMP for Firepower では、デフォルトで米国 (US) AMPパブリッククラウドへの接続が設定され、有効になっています。AMP for Firepowerクラウド接続の削除や無効化はできませんが、欧州連合 (EU) および米国 (US) AMPクラウドの切り替え、またはプライベートクラウド (AMPv) の接続の設定が可能です。

エンドポイントに独自のFireAMP接続を追加するには、FireAMPポータルのアカウントが必要です。ポータルに登録されていないエンドポイント向けAMP接続では、AMP for Firepowerは無効になりません。

### AMPクラウド接続要件

- AMP for Networks : パブリックまたはプライベートいずれのAMPクラウドを使用している場合、ポート443を使ってAMP for Networksのマルウェアクラウドルックアップを行い

ます。Firepower Management Center からの通信を行うため、このポートをアウトバウンドに開く必要があります。

- エンドポイント向け AMP : エンドポイントベースのマルウェア イベントを受信するために、システムはポート 443/HTTPS を使用してシスコクラウド (パブリックまたはプライベート) に接続します。Firepower Management Center との通信を行うため、このポートをインバウンドとアウトバウンドの両方に開く必要があります。また、Firepower Management Center はインターネットに直接アクセスできる必要があります。デフォルトの正常性ポリシーに含まれる AMP ステータス モニタは、Firepower Management Center からクラウドへの最初の接続が成功した後で接続できなくなった場合、または AMP ポータルを使って接続が登録解除された場合に警告を出します。

AMP の通信にレガシーポートを使用するには [集合型セキュリティインテリジェンスの通信設定オプション \(1559 ページ\)](#) を参照してください。

### AMP とハイ アベイラビリティ

ハイ アベイラビリティ ペアの Firepower Management Center はファイル ポリシーおよび関連する設定を共有しますが、クラウド接続、キャプチャされたファイル、ファイルイベント、マルウェア イベントを共有することはありません。運用の継続性を確保し、検出されたファイルのマルウェア処理が両方の Firepower Management Center で同じであるようにするためには、アクティブとスタンバイ両方の Firepower Management Center がクラウドにアクセスできる必要があります。

ハイアベイラビリティの設定では、Firepower Management Center のアクティブインスタンスとスタンバイインスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。

これらの要件は、パブリック、プライベート両方の AMP クラウドに適用されます。

### AMP クラウド接続とマルチテナンシー

マルチドメイン導入環境では、AMP for Firepower 接続はグローバルレベルでのみ設定します。各 Firepower Management Center で可能な AMP for Firepower 接続数は 1 接続のみです。エンドポイント向け AMP 接続は、どのドメインレベルでも設定可能です。ただし、各接続にそれぞれ個別のエンドポイント向け AMP アカウントを使用する必要があります。たとえば、MSSP の各クライアントは、それぞれ独自のエンドポイント向け AMP を展開している場合があります。



#### 注意

特にリーフドメインに重複する IP スペースがある場合、エンドポイント向け AMP 接続はリーフレベルのみで設定することを強く推奨します。複数のサブドメインに同じ IP-MAC アドレスペアを持つホストが存在する場合、誤ったリーフドメインにエンドポイントベースのマルウェア イベントを保存したり、誤ったホストに IOC を関連付けたりする可能性があります。

## AMP for Endpoints クラウド接続の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

組織で AMP for Endpoints が展開されると、脅威の識別、侵害の兆候 (IOC)、およびその他のマルウェア関連の情報を AMP クラウドからシステムにインポートできます。AMP for Firepower 接続がすでに設定されている場合にも、AMP for Endpoints 接続を設定する必要があります。



**注意** マルチドメイン展開では、特にリーフドメインに重複する IP スペースがある場合は、AMP for Endpoints 接続をリーフレベルのみで設定することを強くお勧めします。複数のサブドメインに同じ IP-MAC アドレスペアを持つホストがある場合、システムが誤ったリーフドメインにエンドポイントベースのマルウェアイベントを保存したり、誤ったホストに IOC を関連付けたりする可能性があります。

### 始める前に

- Firepower Management Center を工場出荷時の初期状態に復元した後、または以前のバージョンに戻した後、AMP クラウドに接続している場合は、AMP for Endpoints 管理コンソールを使用して以前の接続を削除します。

### 手順

**ステップ 1** [AMP] > [AMP 管理 (AMP Management)] を選択します。

**ステップ 2** [AMP クラウド接続の作成 (Create AMP Cloud Connection)] をクリックします。

**ステップ 3** [クラウド名 (Cloud Name)] ドロップダウンリストから、使用するクラウドを選択します。

- 欧州連合 AMP クラウドの場合、[EU クラウド (EU Cloud)] を選択します。
- 米国 AMP クラウドの場合、[US クラウド (US Cloud)] を選択します。
- AMPv の場合、[プライベートクラウド (Private Cloud)] を選択し、[Cisco AMP プライベートクラウド \(1553 ページ\)](#) の説明に従って続行します。

**ステップ 4** このクラウドを AMP for Firepower と AMP for Endpoints に使用する場合は、[AMP for Firepower に使用 (Use for AMP for Firepower)] チェックボックスをオンにします。

マルチドメイン展開では、このチェックボックスはグローバルドメインにのみ表示されます。各 Firepower Management Center には、AMP for Firepower 接続を 1 つだけ設定できます。

**ステップ 5** [登録 (Register)] をクリックします。

回転状態のアイコンは、たとえば、Firepower Management Center で接続を設定した後、AMP for Endpoints 管理コンソールの使用を許可する前に、接続が保留中であることを示します。失敗または拒否を示すアイコン (❌) は、クラウドが接続を拒否したこと、または他の理由で接続が失敗したことを示します。

- ステップ 6** AMP for Endpoints 管理コンソールを続行することを確認し、管理コンソールにログインします。
- ステップ 7** 管理コンソールを使用して、AMP for Endpoints データを Firepower Management Center に送信することを AMP クラウドに許可します。
- ステップ 8** 受信するデータを制限する場合は、情報を受け取る組織内の特定のグループを選択します。
- デフォルトでは、AMP クラウドはすべてのグループのデータを送信します。グループを管理するには、AMP for Endpoints 管理コンソールで **[管理 (Management)]** > **[グループ (Groups)]** を選択します。詳細については、管理コンソールのオンラインヘルプを参照してください。
- ステップ 9** **[許可 (Allow)]** をクリックして接続を有効にして、データの転送を開始します。

**[拒否 (Deny)]** をクリックすると Firepower Management Center に戻りますが、接続には拒否マークが付きます。接続を拒否/許可しないまま AMP for Endpoints 管理コンソールの **[アプリケーション (Applications)]** ページから別のページに移動した場合、Firepower Management Center の Web インターフェイスでは接続に保留中のマークが付きます。これらのいずれの状況でも、ヘルスマニタは失敗した接続のアラートを生成しません。後で AMP クラウドに接続するには、失敗した接続または保留中の接続を削除してから再作成します。

AMP for Endpoints 接続の登録が未完了であっても、AMP for Firepower 接続は無効になりません。

---

### 次のタスク

ハイアベイラビリティの設定では、Firepower Management Center のアクティブインスタンスとスタンバイインスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。

## Cisco AMP プライベート クラウド

Cisco AMP プライベート クラウド仮想アプライアンス (AMPv) を構成することで、ネットワーク上の AMP エンドポイントデータを収集することができます。AMPv は、AMP クラウドの圧縮型、オンプレミスバージョンとして機能する、シスコ独自の仮想マシンです。

エンドポイント向け AMP のすべてのコネクタが AMPv にデータを送信し、AMPv は Firepower Management Center にデータを転送します。AMPv は、エンドポイントデータを外部接続では一切共有しません。Firepower Management Center は AMP クラウドに接続し、ネットワークトラフィックで検出されたファイルの判定結果をクエリしたり、レトロスペクティブマルウェアイベントを受信したりします。

部門のプライバシーやセキュリティ保護の観点から、モニタ対象ネットワークと AMP クラウドとの間で頻繁にあるいは直接接続することが困難、または不可能な場合があります。こうし

た状況で、Cisco AMP プライベート クラウド仮想アプライアンス (AMPv) を構成することができます。AMPv は、AMP クラウドの圧縮型、オンプレミスバージョンとして機能する、シスコ独自の仮想マシンであり、ユーザのネットワークと AMP クラウドの安全なメディアータです。Firepower Management Center を AMPv に接続すると、AMP クラウドとの既存の直接接続は無効化されます。

AMP クラウドとのすべての接続 (AMP for Firepower でもエンドポイント向け AMP でも) が AMPv に集約され、AMPv は、管理対象ネットワークのセキュリティとプライバシーを確保するための匿名プロキシとして機能します。ネットワークトラフィックで検出されたファイルの判定結果のクエリ、レトロスペクティブ マルウェア イベントの受信、エンドポイント向け AMP データのインポートなどを行います。AMPv は、エンドポイントデータを外部接続では一切共有しません。

各プライベートクラウドは、エンドポイント向け AMP コネクタを最大 10,000 までサポート可能で、複数のプライベートクラウドを設定できます。

[AMP 管理 (AMP Management) ] ページ ([AMP] > [AMP 管理 (AMP Management) ]) を使って、Firepower Management Center から AMPv との接続を制御します。



- (注) AMP for Firepower のコンポーネントであるダイナミック分析では、管理対象デバイスがポート 443 から AMP Threat Grid クラウドまたはオンプレミス AMP Threat Grid アプライアンスに、直接あるいはプロキシを介してアクセスできる必要があります。AMPv はダイナミック分析をサポートしていません。また、シスコ集合型セキュリティインテリジェンス (CSI) に依存するその他の機能 (URL フィルタリングやセキュリティインテリジェンス フィルタリングなど) のための脅威インテリジェンスの匿名での取得もサポートしていません。

## AMPv への接続

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア (AMP for Firepower)	マルウェア (AMP for Firepower)	任意 (Any)	任意 (Any)	Admin
任意 (AMP for Endpoints)	任意 (AMP for Endpoints)			

### 始める前に

- AMPv のマニュアルの指示に従って、Cisco AMP プライベートクラウドまたはクラウドを設定します。設定時に、プライベートクラウドのホスト名をメモしてください。このホスト名は、後で Firepower Management Center で接続を設定するときに必要なになります。
- Firepower Management Center が AMPv と通信できることを確認し、AMPv がインターネットにアクセスでき、AMP クラウドと通信できることを確認します。



## 手順

- 
- ステップ 1** [AMP] > [AMP 管理 (AMP Management)] を選択します。
- ステップ 2** [AMP クラウド接続の作成 (Create AMP Cloud Connection)] をクリックします。
- ステップ 3** [クラウド名 (CloudName)] ドロップダウンリストから [プライベートクラウド (Private Cloud)] を選択します。
- ステップ 4** 名前を入力します。
- この情報は、AMPv によって生成または送信されるマルウェア イベントに表示されます。
- ステップ 5** [ホスト (Host)] フィールドに、AMPv の設定時に設定したプライベートクラウドのホスト名を入力します。
- ステップ 6** [証明書アップロードパス (Certificate Upload Path)] フィールドの横にある [参照 (Browse)] をクリックして、AMPv の有効な TLS または SSL 暗号化証明書の場所を参照します。詳細については、AMPv のマニュアルを参照してください。
- ステップ 7** このプライベートクラウドを AMP for Firepower および AMP for Endpoints に使用する場合は、[AMP for Firepower に使用 (Use for AMP for Firepower)] チェックボックスをオンにします。
- AMP for Firepower 通信を処理する別のプライベートクラウドを設定した場合は、このチェックボックスをオフにすることができます。これが唯一の AMPv 接続の場合は、オフにできません。
- マルチドメイン展開では、このチェックボックスはグローバルドメインにのみ表示されます。各 Firepower Management Center には、AMP for Firepower 接続を 1 つだけ設定できます。
- ステップ 8** プロキシを使用して AMPv と通信するには、[接続にプロキシを使用 (Use Proxy for Connection)] チェックボックスをオンにします。
- ステップ 9** [登録 (Register)] をクリックし、AMP クラウドへの既存の直接接続を無効にすることを確認し、最後に AMPv 管理コンソールを続行して登録を完了することを確認します。
- ステップ 10** 管理コンソールにログインして登録プロセスを完了します。手順の詳細については、AMPv のマニュアルを参照してください。
- 

## 次のタスク

ハイアベイラビリティの設定では、Firepower Management Center のアクティブインスタンスとスタンバイインスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。

## AMP クラウドおよび AMPv 接続の管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア (AMP for Firepower)	マルウェア (AMP for Firepower)	任意 (Any)	任意 (Any)	Admin
任意 (AMP for Endpoints)	任意 (AMP for Endpoints)			

クラウドからマルウェア関連の情報を受信する必要がなくなったら、Firepower Management Center を使用して AMP クラウドまたは AMPv 接続を削除します。AMP for Endpoints または AMPv 管理コンソールを使用して接続の登録を解除しても、システムから接続を削除することにはならない点に注意してください。登録解除した接続は、Firepower Management Center の Web インターフェイスに障害発生状態で表されます。

また、接続は一時的に無効にすることもできます。クラウド接続を再度有効化すると、クラウドは、無効化されていた期間にキューに保持していたデータを含めて、システムへのデータ送信を再開します。



**注意** 無効化された接続に対して、AMP クラウドおよび AMPv は、接続を再有効化するまでマルウェア イベントや侵害の兆候などを保存できます。まれに、イベント レートが非常に高い場合や接続が長期間無効になっていた場合など、接続無効中に生成されたすべての情報をクラウドで保存できないことがあります。

マルチドメイン展開では、現在のドメインで作成された接続が表示されます。これは、管理が可能な接続です。また、先祖ドメインで作成した接続も表示されますが、この接続は管理できません。下位ドメインの接続を管理するには、そのドメインに切り替えます。各 Firepower Management Center は、グローバルドメインに属する AMP for Firepower 接続を 1 つのみ保持できます。

### 手順

**ステップ 1** [AMP] > [AMP 管理 (AMP Management)] を選択します。

**ステップ 2** AMP クラウド接続を管理します。

- 削除：削除アイコン (🗑️) をクリックして、選択内容を確認します。
- 有効化または無効化：スライダをクリックして、選択内容を確認します。

### 次のタスク

ハイアベイラビリティの設定では、Firepower Management Center のアクティブインスタンスとスタンバイインスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。

## 動的分析接続

AMP Threat Grid クラウドでは、ファイルがサンドボックス環境で実行されます。AMP for Firepower ではクラウドを使用して、動的分析送信ファイルの脅威スコアと動的分析レポートを取得します。適切なライセンスを使用して、システムが自動的にクラウドにアクセスします。

組織のセキュリティポリシーが Firepower システムによるネットワーク外部へのファイルの送信を許可しない場合は、オンプレミスの AMP Threat Grid アプライアンスを設定できます。詳細については、『Cisco AMP Threat Grid Appliance Setup and Configuration Guide』を参照してください。

Firepower Management Center の [ダイナミック分析接続 (Dynamic Analysis Connections)] ページ ([AMP] > [ダイナミック分析接続 (Dynamic Analysis Connections)]) を使用して、AMP Threat Grid クラウドへのパブリック動的分析接続およびオンプレミスの AMP Threat Grid アプライアンスへのプライベート動的分析接続を管理します。

### デフォルトの動的分析接続の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア	マルウェア	任意 (Any)	グローバルだけ	Admin/Access Admin/Network Admin

デフォルトで、Firepower Management Center は、ファイルを送信したり、レポートを取得したりするために、パブリック AMP Threat Grid クラウドに接続できます。この接続は、設定したり、削除したりすることはできません。

### 手順

**ステップ 1** [AMP] > [ダイナミック分析接続 (Dynamic Analysis Connections)] を選択します。

**ステップ 2** 編集アイコン (✎) をクリックします。

## Threat Grid のオンプレミス アプライアンス

組織にパブリックの AMP Threat Grid クラウドへのファイルの送信に関してプライバシーまたはセキュリティ上の懸念がある場合、オンプレミスの AMP Threat Grid アプライアンスを展開

することができます。このオンプレミス アプライアンスは、パブリック クラウドと同様に適切なファイルをサンドボックス環境で実行し、脅威スコアと動的分析レポートを Firepower システムに戻します。ただし、このオンプレミス アプライアンスは、ご使用のネットワークの外部にあるパブリック クラウドや他のすべてのシステムとは通信しません。

1 台のオンプレミス AMP Threat Grid アプライアンスを Firepower Management Center に接続できます。詳細については、『Cisco AMP Threat Grid アプライアンスセットアップおよび構成ガイド』を参照してください。

このオンプレミス アプライアンスへの動的分析接続を設定した場合、システムではパブリックの AMP クラウドを使用してマルウェアクラウドルックアップを実行し、またファイルが以前に動的分析用に送信されていないことを確認します。

システムでは、パブリック レポートの取得に AMP クラウドへのデフォルトのパブリック動的分析接続も使用します。オンプレミス アプライアンスがファイル用の動的分析レポートを生成しなかった場合、システムはこの動的分析レポートについてパブリックの AMP クラウドに問い合わせます。組織がファイルを送信していない限り、表示できるのは、限られたデータが含まれた、スクラビング処理が実行されたレポートだけです。

## オンプレミスの動的分析接続の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア	マルウェア	任意 (Any)	グローバルだけ	Admin/Access Admin/Network Admin

ネットワークでオンプレミスの AMP Threat Grid アプライアンスをインストールする場合は、動的分析接続を設定して、ファイルを送信し、アプライアンスからレポートを取得できます。オンプレミスのアプライアンスの動的分析接続を設定するには、オンプレミスのアプライアンスに Firepower Management Center を登録します。

### 始める前に

- オンプレミスの AMP Threat Grid アプライアンスを設定します。『Cisco AMP Threat Grid Appliance Setup and Configuration Guide』を参照してください。
- ログインに使用する公開キー証明書を AMP Threat Grid アプライアンスからオンプレミスのアプライアンスにダウンロードします。『Cisco AMP Threat Grid Appliance Administrator's Guide』を参照してください。
- プロキシを使用してオンプレミスのアプライアンスに接続する場合は、プロキシを設定します。[Firepower Management Center 管理インターフェイスの設定 \(937 ページ\)](#) を参照してください。

## 手順

- ステップ 1 [AMP] > [ダイナミック分析接続 (Dynamic Analysis Connections)] を選択します。
- ステップ 2 [新しい接続を追加 (Add New Connection)] をクリックします。
- ステップ 3 名前を入力します。
- ステップ 4 [ホスト URL (Host URL)] を入力します。
- ステップ 5 [証明書のアップロード (Certificate Upload)] の横にある [参照 (Browse)] をクリックして、オンプレミスのアプライアンスとの接続を確立するために使用する公開キー証明書をアップロードします。
- ステップ 6 設定されているプロキシを使用して接続を確立する場合は、[可能な場合はプロキシを使用 (Use Proxy When Available)] を選択します。
- ステップ 7 [登録 (Register)] をクリックします。
- ステップ 8 [はい (Yes)] をクリックして、オンプレミスの AMP Threat Grid アプライアンスのログインページを表示します。
- ステップ 9 オンプレミスの AMP Threat Grid アプライアンスにユーザ名とパスワードを入力します。
- ステップ 10 [サインイン (Sign in)] をクリックします。
- ステップ 11 次の選択肢があります。
  - 以前にオンプレミスのアプライアンスに Firepower Management Center を登録した場合は、[戻る (Return)] をクリックします。
  - Firepower Management Center を登録していない場合は、[アクティブ化 (Activate)] をクリックします。

## 集合型セキュリティ インテリジェンス通信の設定

Firepower システムは、レピュテーション、リスク、脅威インテリジェンスに関して、シスコ 集合型セキュリティ インテリジェンス (CSI) を使用します。適正なライセンスがあれば、URL フィルタリングおよび AMP for Firepower 機能の通信オプションを指定できます。

## 集合型セキュリティ インテリジェンスの通信設定オプション

### Enable URL Filtering

Web サイトの一般的な分類、カテゴリ、リスク レベル、またはレピュテーションに基づくトラフィックのフィルタリングを可能にします。URL フィルタリング ライセンスが自動的に追加されるようにして、[URL フィルタリングを有効にする (Enable URL Filtering)] および [自動更新を有効にする (Enable Automatic Updates)] を有効にします。URL フィルタリングは、他の URL フィルタリング オプションを選択する前に有効にする必要があります。

URL フィルタリングを有効にする場合は、URL フィルタリングが最後に有効になってから経過した時間に応じて、または URL フィルタリングを今回初めて有効にするかどうかに応じて、Firepower Management Center が Cisco CSI から URL データを取得します。

メモリの制約上、一部のモデルでは、小規模でそれほど細分化されていないカテゴリとレピュテーションによってほとんどの URL フィルタリングが実行されます。たとえば、親 URL のサブサイトがそれぞれ異なる URL カテゴリとレピュテーションを持っている場合でも、一部のデバイスでは、親 URL のデータのみが保存される場合があります。これらのデバイスによって処理される Web トラフィックの場合、システムはクラウドルックアップを実行して、ローカルデータベースにないサイトのカテゴリとレピュテーションを判断できます。

メモリが少ないデバイスには、7100 ファミリと次の ASA モデルが含まれます：ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X。NGIPSv で、カテゴリおよびレピュテーションベースの URL フィルタリングを実行するための正しいメモリ量を割り当てる方法について、詳しくは *Firepower System Virtual Installation Guide* を参照してください。

### 自動更新を有効にする (Enable Automatic Updates)

Firepower Management Center で展開環境の URL データが自動的に更新されるようにします。一般的に、URL データは 1 日 1 回更新されますが、自動更新を有効にすると、30 分ごとに Firepower Management Center が確認するようになります。通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

システムが外部リソースと通信するタイミングを厳格に制御する必要がある場合は、自動更新を無効にし、代わりにスケジューラを使用します。



(注) Cisco では、自動更新を有効にするか、またはスケジューラを使用して更新をスケジュールすることを推奨しています。[今すぐ更新する (Update Now)] をクリックして手動でオンデマンド更新を実行できますが、プロセスを自動化すると、最新の関連データを使用できるようになります。更新がすでに進行中である場合は、オンデマンド更新を開始できません。

### 不明 URL を Cisco CSI に問い合わせる (Query Cisco CSI for Unknown URL)

カテゴリとレピュテーションがローカルデータセットにない Web サイトをユーザが閲覧するときに URL が脅威インテリジェンス評価のために送信されるようにします。プライバシー上の理由などで未分類の URL を送信したくない場合は、このオプションを無効にしてください。

未分類の URL への接続は、カテゴリまたはレピュテーションベースの URL 条件を含むルールに一致しません。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

### ローカル マルウェア検出の自動更新を有効にする (Enable Automatic Local Malware Detection Updates)

ローカル マルウェア検出エンジンは、Cisco が提供する署名を使用して統計的にファイルを分析し、事前に分類します。このオプションを有効にすると、Firepower Management Center が 30 分ごとに署名の更新を確認します。

### マルウェア イベントの URL を Cisco と共有する (Share URI from Malware Events with Cisco)

ネットワーク トラフィックで検出されたファイルに関する情報を AMP クラウドに送信することができます。この情報には、検出されたファイルに関連する URI 情報と SHA-256 ハッシュ値が含まれます。共有はオプトインですが、この情報を Cisco に送信すると、マルウェアを識別して追跡する今後の取り組みに役立ちます。

### レガシー ポート 32137 を AMP for Firepower に使用する (Use Legacy Port 32137 for AMP for Firepower)

デフォルトでは、AMP for Firepower はポート 443/HTTPS を使用して AMP クラウド (または AMPv) と通信します。このオプションは、AMP for Firepower によるポート 32137 の使用を許可します。システムを以前のバージョンから更新する場合は、このオプションを有効にすることができます。

#### 関連トピック

[通信ポートの要件](#) (2787 ページ)

## 集合型セキュリティ インテリジェンスとの通信の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
URL フィルタリング (URL フィルタリング) マルウェア (AMP for Firepower)	URL フィルタリング (URL フィルタリング) マルウェア (AMP for Firepower)	任意 (Any)	任意 (Any)	Admin

#### 手順

- ステップ 1 [システム (System)] > [統合 (Integration)] を選択します。
- ステップ 2 [Cisco CSI] タブをクリックします。
- ステップ 3 [集合型セキュリティ インテリジェンスの通信設定オプション](#) (1559 ページ) の説明に従って Cisco CSI 通信を設定します。

ステップ 4 [保存 (Save) ] をクリックします。

---





## 第 67 章

# ファイルとマルウェアのインスペクション パフォーマンスとストレージの調整

次のトピックでは、ファイルとマルウェアのインスペクションパフォーマンスとストレージを設定する方法について説明します。

- [ファイルおよびマルウェアのインスペクションのパフォーマンスとストレージの調整について \(1563 ページ\)](#)
- [ファイルおよびマルウェアのインスペクションパフォーマンスとストレージのオプション \(1564 ページ\)](#)
- [ファイルおよびマルウェアのインスペクションパフォーマンスおよびストレージの調整 \(1568 ページ\)](#)

## ファイルおよびマルウェアのインスペクションのパフォーマンスとストレージの調整について

ファイル制御を実行するか、AMP for Firepowerを使用する場合は、次の詳細設定ファイルとマルウェア インスペクション機能のオプションを設定できます。

- ファイルタイプを検出したときに検査されるバイト数を制限する。
- マルウェア ブロック ルールがキャッシュされた性質のないファイルと一致し、性質を取得せずに経過した時間が長すぎる場合は、ファイルの通過を許可する。
- 特定のサイズよりも大きい場合は、ファイルの保存、ファイルでのマルウェア クラウド ルックアップの実行、またはカスタム検出リストでのファイルのブロックを回避する。
- 保存する最小ファイル サイズと最大ファイル サイズを指定する。
- 動的分析に送信する最小ファイル サイズと最大ファイル サイズを指定する。

これらのオプションはシステム パフォーマンスおよびファイル ストレージに影響を与える可能性があります。

# ファイルおよびマルウェアのインスペクションパフォーマンスとストレージのオプション

ファイルサイズを増やすと、システムのパフォーマンスに影響を与える可能性があります。



**注意** [ファイルおよびマルウェアの設定 (File and Malware Settings)] でデフォルト以外の値を設定します。設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

表 98: アクセスコントロール ファイルおよび AMP for Firepower の詳細オプション

フィールド	説明	使用可能な値	注記 (Notes)
ファイルタイプを検知する前に検閲するバイト数制限 (Limit the number of bytes inspected when doing file type detection)	ファイルタイプを検出するときに検査するバイト数を指定します。	0 ~ 4294967295 (4GB)	制限を取り除くには、0 を入力します。  デフォルト値は、TCP パケットの最大セグメントサイズです。ほとんどの場合、システムは最初のパケットによって、一般的なファイルタイプを特定できます。
ファイルを許可するのにかかるマルウェアブロックのクラウドルックアップの制限時間 (秒) (Allow file if cloud lookup for Block Malware takes longer than (seconds))	マルウェアクラウドルックアップの実行中に、システムが [マルウェアブロック (Block Malware)] ルールに一致し、性質がキャッシュに入っていないファイルの最後のバイトを保持する期間を指定します。システムが性質を取得する前にこの期間が満了すると、ファイルが渡されます。「使用不可」の性質はキャッシュに入れられません。	0 ~ 30 秒	シスコは、接続の障害によってトラフィックのブロックを防ぐために、デフォルト値を使用することをお勧めします。サポートに連絡することなくこのオプションを 0 に設定しないでください。

フィールド	説明	使用可能な値	注記 (Notes)
SHA-256 ハッシュ値を計算するファイルの上限サイズ (バイト) (Do not calculate SHA-256 hash values for files larger than (in bytes))	システムが特定のサイズを超えるファイルを保管すること、ファイルでマルウェアクラウドルックアップを実行すること、またはカスタム検出リストに追加されたファイルをブロックすることを防止します。	0 ~ 4294967295 (4GB)	制限を取り除くには、0を入力します。  この値は、[保存する最大ファイルサイズ (バイト) (Maximum file size to store (bytes))] および [動的分析テストの最大ファイルサイズ (バイト) (Maximum file size for dynamic analysis testing (bytes))] の値以上に設定する必要があります。
保存する最小ファイルサイズ (バイト) (Minimum file size to store (bytes))	システムがファイルルールを使用して保管できるファイルの最小サイズを指定します。	0 ~ 10485760 (10MB)	ファイルストレージを無効にするには、0を入力します。  このフィールドは、[保存する最大ファイルサイズ (バイト) (Maximum file size to store (bytes))] および [SHA-256 ハッシュ値を計算するファイルの上限サイズ (バイト) (Maximum file size to store (bytes))] の値以下に設定する必要があります。
保存する最大ファイルサイズ (バイト) (Maximum file size to store (bytes))	システムがファイルルールを使用して保管できるファイルの最大サイズを指定します。	0 ~ 10485760 (10MB)	ファイルストレージを無効にするには、0を入力します。  このフィールドは、[保存する最小ファイルサイズ (バイト) (Minimum file size to store (bytes))] の値以上、および [SHA-256 ハッシュ値を計算するファイルの上限サイズ (バイト) (Do not calculate SHA-256 hash values for files larger than (in bytes))] の値以下に設定する必要があります。

フィールド	説明	使用可能な値	注記 (Notes)
ダイナミック分析の最小ファイルサイズ (バイト) (Minimum file size for dynamic analysis testing (bytes))	システムが AMP クラウドに動的な分析対象として送信できるファイルの最小サイズを指定します。	0 ~ 104857600 (100 MB)	<p>このフィールドは、[動的な分析テストの最大ファイルサイズ (バイト) (Maximum file size for dynamic analysis testing (bytes)) ] および [SHA-256 ハッシュ値を計算するファイルの上限サイズ (バイト) (Do not calculate SHA-256 hash values for files larger than (in bytes)) ] の値以下に設定する必要があります。</p> <p>バージョン 5.x の Firepower システムを実行するデバイスにアクセス コントロール ポリシーを展開した場合、システムは 15360 より小さい値をすべて 15360 に変更します。</p> <p>システムは AMP クラウドをチェックして、送信可能なファイルの最小サイズが更新されているかどうかを調べます (最大で 1 日 1 回)。新しい最小サイズが現在の値より大きい場合、現在の値が新しい最小サイズに更新され、ポリシーは古いポリシーとしてマークされます。</p>

フィールド	説明	使用可能な値	注記 (Notes)
ダイナミック分析の最大ファイルサイズ(バイト) (Maximum file size for dynamic analysis testing (bytes))	システムが AMP クラウドに動的な分析対象として送信できるファイルの最大サイズを指定します。	0 ~ 104857600 (100 MB)	<p>このフィールドは、[M ダイナミック分析の最小ファイルサイズ (バイト) (Minimum file size for dynamic analysis testing (bytes)) ] の値以上、[SHA-256 ハッシュ値を計算するファイルの上限サイズ (バイト) (Do not calculate SHA-256 hash values for files larger than (in bytes)) ] の値以下に設定する必要があります。</p> <p>バージョン 5.x の Firepower システムを実行するデバイスにアクセス コントロール ポリシーを展開した場合、システムは 2097152 より大きい値をすべて 2097152 に変更します。</p> <p>システムは AMP クラウドをチェックして、送信可能なファイルの最大サイズが更新されているかどうかを調べます (最大で1日1回)。新しい最大サイズが現在の値より小さい場合、現在の値が新しい最大サイズに更新され、ポリシーは古いポリシーとしてマークされます。</p>

# ファイルおよびマルウェアのインスペクションパフォーマンスおよびストレージの調整

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (ファイル制御) マルウェア (AMP)	保護 (ファイル制御) マルウェア (AMP)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin



**注意** [ファイルおよびマルウェアの設定 (Files and Malware Settings)] にデフォルト以外の値を設定することによって、設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

## 手順

- ステップ 1** アクセス コントロール ポリシー エディタで、[詳細 (Advanced)] タブをクリックします。
- ステップ 2** [ファイルおよびマルウェアの設定 (Files and Malware Settings)] の横にある編集アイコン (✎) をクリックします。
- 代わりに表示アイコン (🔍) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。
- ステップ 3** [ファイルおよびマルウェアのインスペクションパフォーマンスとストレージのオプション \(1564 ページ\)](#) で説明されている任意のオプションを設定します。
- ステップ 4** [OK] をクリックします。
- ステップ 5** [保存 (Save)] をクリックしてポリシーを保存します。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 関連トピック

- [Snort® の再起動シナリオ \(354 ページ\)](#)



## 第 XVIII 部

### 侵入検知と防御

- ネットワーク分析ポリシーと侵入ポリシーの概要 (1571 ページ)
- 侵入ポリシーおよびネットワーク分析ポリシーのレイヤ (1591 ページ)
- 侵入ポリシーの使用を開始するには (1609 ページ)
- ルールを使用した侵入ポリシーの調整 (1619 ページ)
- ネットワーク資産に応じた侵入防御の調整 (1655 ページ)
- 機密データの検出 (1661 ページ)
- 侵入イベント ログイングのグローバル制限 (1677 ページ)
- 侵入ルール エディタ (1685 ページ)
- 侵入防御パフォーマンスの調整 (1819 ページ)







## 第 68 章

# ネットワーク分析ポリシーと侵入ポリシーの概要

以下のトピックでは、ネットワーク分析ポリシーと侵入ポリシーの概要を示します。

- ネットワーク分析ポリシーと侵入ポリシーの基本 (1571 ページ)
- ポリシーが侵入についてトラフィックを検査する仕組み (1572 ページ)
- システム提供およびカスタムのネットワーク分析ポリシーと侵入ポリシー (1578 ページ)
- ナビゲーション ウィンドウ: ネットワーク分析と侵入ポリシー (1586 ページ)
- 競合と変更: ネットワーク分析ポリシーと侵入ポリシー (1587 ページ)

## ネットワーク分析ポリシーと侵入ポリシーの基本

ネットワーク分析ポリシーと侵入ポリシーは、Firepower システムの侵入検知および防御機能の一部として連携して動作します。侵入検知という用語は、一般に、ネットワークトラフィックへの侵入の可能性を受動的に分析し、セキュリティ分析用に攻撃データを保存するプロセスを指します。侵入防御という用語には、侵入検知の概念が含まれますが、さらにネットワークを通過中の悪意のあるトラフィックをブロックしたり変更したりする機能も追加されます。

侵入防御の展開では、システムがパケットを検査するときに次のことが行われます。

- ネットワーク分析ポリシーは、トラフィックのデコードと前処理の方法を管理し、特に、侵入を試みている兆候がある異常なトラフィックについて、さらに評価できるようにします。
- 侵入ポリシーでは侵入およびプリプロセッサルール（総称的に「侵入ルール」とも呼ばれる）を使用し、パターンに基づき、デコードされたパケットを検査して攻撃の可能性を調べます。侵入ポリシーは変数セットとペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映することができます。

ネットワーク分析ポリシーと侵入ポリシーは、どちらも親のアクセスコントロールポリシーによって呼び出されますが、呼び出されるタイミングが異なります。システムでトラフィックが分析される際には、侵入防御（追加の前処理と侵入ルール）フェーズよりも前に、別途ネットワーク分析（デコードと前処理）フェーズが実行されます。ネットワーク分析ポリシーと侵

入ポリシーと一緒に使用すると、広範囲で詳細なパケットインスペクションを行うことができます。このポリシーは、ホストとそのデータの可用性、整合性、機密性を脅かす可能性のあるネットワークトラフィックの検知、通知および防御に役立ちます。

Firepower システムには、同様の名前（Balanced Security and Connectivity など）が付いた複数のネットワーク分析ポリシーと侵入ポリシーが付属しており、それらは相互に補完して連携します。システム付属のポリシーを使用することで、Cisco Talos Security Intelligence and Research Group（Talos）の経験を活用できます。これらのポリシーでは、Talos は侵入ルールおよびプリプロセッサルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。

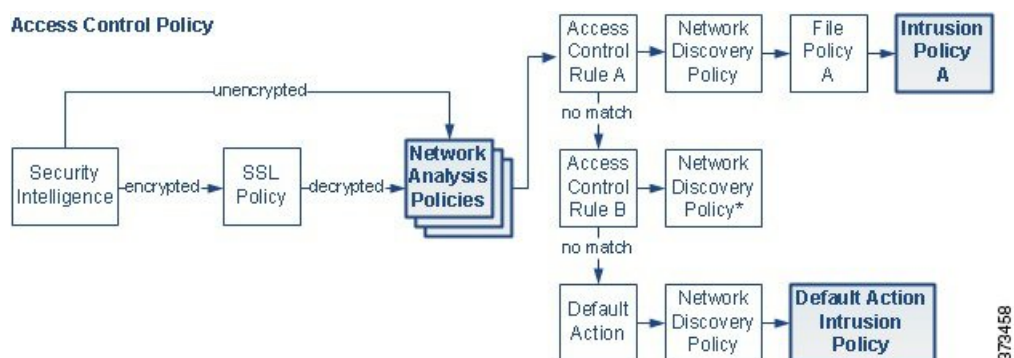
また、カスタムのネットワーク分析ポリシーや侵入ポリシーも作成できます。カスタムポリシーの設定を調整することで、各自にもっとも役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

Web インターフェイスで同様のポリシーエディタを使用し、ネットワーク分析ポリシーや侵入ポリシーを作成、編集、保存、管理します。いずれかのタイプのポリシーを編集するときには、Web インターフェイスの左側にナビゲーションパネルが表示され、右側にさまざまな設定ページが表示されます。

## ポリシーが侵入についてトラフィックを検査する仕組み

アクセスコントロールの展開の一部としてシステムがトラフィックを分析すると、ネットワーク分析（復号化と前処理）フェーズが侵入防御（侵入ルールおよび詳細設定）フェーズとは別にその前に実行されます。

次の図は、インラインの侵入防御および AMP for Firepower 展開におけるトラフィック分析の順序を簡略化して示しています。アクセスコントロールポリシーが他のポリシーを呼び出してトラフィックを検査するしくみ、およびそれらのポリシーが呼び出される順序が示されています。ネットワーク分析ポリシーおよび侵入ポリシーの選択フェーズが強調表示されています。



インライン展開（つまり、ルーテッド、スイッチド、トランスペアレントインターフェイスまたはインラインインターフェイスのペアを使用して関連設定がデバイスに展開される展開）では、システムは上図のプロセスのほぼすべての段階において、追加のインスペクションなしで

トラフィックをブロックすることができます。セキュリティインテリジェンス、SSLポリシー、ネットワーク分析ポリシー、ファイルポリシー、および侵入ポリシーのすべてで、トラフィックをドロップまたは変更できます。唯一の例外として、パケットをパッシブに検査するネットワーク検出ポリシーは、トラフィックフローに影響を与えることができません。

同様に、プロセスの各ステップで、パケットによってシステムがイベントを生成する場合があります。侵入イベントおよびプリプロセッサイベント（まとめて侵入イベントと呼ばれることもあります）は、パケットまたはその内容がセキュリティリスクを表す可能性があることを示すものです。



#### ヒント

この図では、SSLインスペクションの設定で暗号化トラフィックの通過が許可されている場合や、SSLインスペクションが設定されていない場合については、アクセスコントロールルールによる暗号化トラフィックの処理を反映していません。デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイルインスペクションは無効になっています。これにより、侵入およびファイルインスペクションが設定されたアクセスコントロールルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

単一の接続の場合は、図に示すように、アクセスコントロールルールよりも前にネットワーク分析ポリシーが選択されますが、一部の前処理（特にアプリケーション層の前処理）はアクセスコントロールルールの選択後に実行されます。これは、カスタムネットワーク分析ポリシーでの前処理の設定には影響しません。

## 復号化、正規化、前処理：ネットワーク分析ポリシー

デコードと前処理を実行しないと、プロトコルの相違によりパターンマッチングを行えなくなるので、侵入についてトラフィックを適切に評価できません。これらのトラフィック処理タスクは、以下のタイミングでネットワーク分析ポリシーによる処理の対象となります。

- 暗号化トラフィックがセキュリティインテリジェンスによってフィルタリングされた後
- 暗号化トラフィックがオプションのSSLポリシーによって復号化された後
- ファイルポリシーまたは侵入ポリシーによってトラフィックを検査できるようになる前

ネットワーク分析ポリシーは、フェーズでのパケット処理を制御します。最初に、システムは最初の3つのTCP/IP層を通ったパケットを復号化し、次にプロトコル異常の正規化、前処理、および検出に進みます。

- パケットデコーダは、パケットヘッダーとペイロードを、プリプロセッサや以降の侵入ルールで簡単に使用できる形式に変換します。TCP/IPスタックの各レイヤのデコードは、データリンク層から開始され、ネットワーク層、トランスポート層へと順番に行われます。パケットデコーダは、パケットヘッダーのさまざまな異常動作も検出します。
- インライン展開では、インライン正規化プリプロセッサは、攻撃者が検出を免れる可能性を最小限にするために、トラフィックを再フォーマット（正規化）します。その他のプリプロセッサや侵入ルールによる検査用にパケットを準備し、システムで処理されるパケットがネットワーク上のホストで受信されるパケットと同じものになるようにします。



(注) パッシブな展開の場合、シスコでは、ネットワーク分析レベルでインライン正規化を行うのではなく、アクセスコントロールポリシーレベルでアダプティブプロファイルの更新を有効にすることを推奨しています。

- ネットワーク層とトランスポート層のさまざまなプリプロセッサは、IPフラグメントを悪用する攻撃を検出したり、チェックサム検証を実行したり、TCP および UDP セッションの前処理を実行したりします。

トランスポートおよびネットワーク プリプロセッサの一部の詳細設定は、アクセスコントロールポリシーのターゲットデバイスで処理されるすべてのトラフィックにグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセスコントロールポリシーで設定します。

- 各種のアプリケーション層プロトコル デコーダは、特定タイプのパケットデータを侵入ルールエンジンで分析可能な形式に正規化します。アプリケーション層プロトコルのエンコードを正規化することにより、システムはデータ表現が異なるパケットに同じコンテンツ関連の侵入ルールを効果的に適用し、大きな結果を得ることができます。
- Modbus と DNP3 SCADA のプリプロセッサは、トラフィックの異常を検出し、データを侵入ルールに提供します。Supervisory Control and Data Acquisition (SCADA) プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャプロセス、および設備プロセスからのデータをモニタ、制御、取得します。
- 一部のプリプロセッサでは、Back Orifice、ポートスキャン、SYNフラッドおよび他のレートベース攻撃など、特定の脅威を検出できます。

侵入ポリシーで、ASCII テキストのクレジットカード番号や社会保障番号などの機密データを検出する機密データ プリプロセッサを設定することに注意してください。

新たに作成されたアクセスコントロールポリシーでは、1つのデフォルト ネットワーク分析ポリシーが、同じ親アクセスコントロールポリシーによって呼び出されるすべての侵入ポリシー向けのすべてのトラフィックの前処理を制御します。初期段階では、デフォルトで [バランスの取れたセキュリティと接続 (Balanced Security and Connectivity)] ネットワーク分析ポリシーが使用されますが、別のシステム付属ポリシーやカスタム ネットワーク分析ポリシーに変更できます。より複雑な展開では、上級ユーザは、一致するトラフィックの前処理にさまざまなカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティゾーン、ネットワーク、VLAN に合わせてトラフィックの前処理オプションを調整できます。

## アクセスコントロールルール：侵入ポリシーの選択

最初の前処理の後、トラフィックはアクセスコントロールルール (設定されている場合) によって評価されます。ほとんどの場合、パケットが一致する最初のアクセスコントロールルールがそのトラフィックを処理するルールとなります。一致するトラフィックをモニタ、信頼、ブロック、または許可できます。

アクセスコントロールルールでトラフィックを許可すると、ディスカバリ データ、マルウェア、禁止ファイル、侵入について、この順序でトラフィックを検査できます。アクセスコントロールルールに一致しないトラフィックは、アクセスコントロールポリシーのデフォルトアクションによって処理されます。デフォルトアクションでは、ディスカバリ データと侵入についても検査できます。



(注) どのネットワーク分析ポリシーによって前処理されるかに関わらず、すべてのパケットは、設定されているアクセスコントロールルールと上から順に照合されます（したがって、侵入ポリシーによる検査の対象となります）。

[ポリシーが侵入についてトラフィックを検査する仕組み \(1572ページ\)](#) の図では、インラインの侵入防御と AMP for Firepower の展開における、デバイスを経由したトラフィック フローを示しています。

- アクセスコントロールルール A により、一致したトラフィックの通過が許可されます。次にトラフィックは、ネットワーク検出ポリシーによるディスカバリデータの検査、ファイルポリシー A による禁止ファイルおよびマルウェアの検査、侵入ポリシー A による侵入の検査を受けます。
- アクセスコントロールルール B も一致したトラフィックを許可します。ただし、このシナリオでは、トラフィックは侵入（あるいはファイルまたはマルウェア）について検査されないため、ルールに関連付けられている侵入ポリシーやファイルポリシーはありません。通過を許可されたトラフィックは、デフォルトでネットワーク検出ポリシーによって検査されます。したがって、この設定を行う必要はありません。
- このシナリオでは、アクセスコントロールポリシーのデフォルトアクションで、一致したトラフィックを許可しています。次に、トラフィックはネットワーク検出ポリシー、さらにその後侵入ポリシーによって検査されます。アクセスコントロールルールまたはデフォルトのアクションに侵入ポリシーを関連付けるときは、異なる侵入ポリシーを使用できます（ただし必須ではありません）。

ブロックされたトラフィックや信頼済みトラフィックは検査されないため、図の例には、ブロックルールや信頼ルールは含まれていません。

## 侵入インスペクション：侵入ポリシー、ルール、変数セット

トラフィックが宛先に向かうことを許可する前に、システムの最終防御ラインとして侵入防御を使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーの主な機能は、どの侵入ルールおよびプリプロセッサルールを有効にすることでどのように設定するかを管理することです。

## 侵入ルールおよびプリプロセッサルール

侵入ルールはキーワードと引数のセットとして指定され、ネットワーク上の脆弱性を悪用する試みを検出します。システムは侵入ルールを使用してネットワークトラフィックを分析し、トラフィックがルールの条件に合致しているかどうかをチェックします。システムは各ルールで指定された条件をパケットに照らし合わせます。ルールで指定されたすべての条件にパケットデータが一致する場合、ルールがトリガーされます。

システムには、Cisco Talos Security Intelligence and Research Group (Talos) によって作成された次のタイプのルールが含まれています。

- 共有オブジェクト侵入ルール：コンパイルされており、変更できません（ただし、送信元と宛先のポートや IP アドレスなどのルールヘッダー情報を除く）
- 標準テキスト侵入ルール：ルールの新しいカスタムインスタンスとして保存および変更できます。
- プリプロセッサルール：ネットワーク分析ポリシーのプリプロセッサおよびパケットデコード検出オプションに関連付けられています。プリプロセッサルールはコピーまたは編集できません。ほとんどのプリプロセッサルールはデフォルトで無効になっています。プリプロセッサを使用してイベントを生成し、インライン展開では、違反パケットをドロップします。するにはそれらを有効にする必要があります。

システムで侵入ポリシーに従ってパケットを処理する際には、最初にルール最適化が、基準（トランスポート層、アプリケーションプロトコル、保護されたネットワークへの入出力方向など）に基づいて、サブセット内のすべてのアクティブなルールを分類します。次に、侵入ルールエンジンが、各パケットに適用する適切なルールのサブセットを選択します。最後に、マルチルール検索エンジンが3種類の検索を実行して、トラフィックがルールに一致するかどうかを検査します。

- プロトコルフィールド検索は、アプリケーションプロトコル内の特定のフィールドでの一致を検索します。
- 汎用コンテンツ検索は、パケットペイロードの ASCII またはバイナリバイトでの一致を検索します。
- パケット異常検索では、特定のコンテンツが含まれているかどうかではなく、確立されたプロトコルに違反しているパケットヘッダーやペイロードが検索されます。

カスタム侵入ポリシーでは、ルールを有効化および無効化し、独自の標準テキストルールを記述および追加することで、検出を調整できます。Firepower 推奨機能を使用して、ネットワーク上で検出されたオペレーティングシステム、サーバ、およびクライアントアプリケーションプロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます。

## 変数セット

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セットを使用します。セット内の大部分の変数は、侵入ルールで一般的に使用される値を表し、送信元および

び宛先の IP アドレスとポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

システムには、定義済みのデフォルト変数から構成される1つのデフォルト変数セットが含まれています。システム提供の共有オブジェクトルールと標準テキストルールは、これらの定義済みのデフォルト変数を使用してネットワークおよびポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 `$HOME_NET` を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 `$EXTERNAL_NET` を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Web サーバに対するエクスプロイトを検出するルールは、`$HTTP_SERVERS` 変数および `$HTTP_PORTS` 変数を使用します。



#### ヒント

システム提供の侵入ポリシーを使用する場合でも、シスコでは、デフォルトセットの主要なデフォルト変数を変更すること強く推奨します。ネットワーク環境を正確に反映する変数を使用すると、処理が最適化され、システムによって疑わしいアクティビティに関連するシステムをモニタできます。高度なユーザは、1つ以上のカスタム侵入ポリシーとペアリングするために、カスタム変数セットを作成して使用できます。

#### 関連トピック

[定義済みデフォルト変数](#) (447 ページ)

## 侵入イベントの生成

侵入されている可能性を特定すると、システムは侵入イベントまたはプリプロセッサイベント（まとめて侵入イベントと呼ばれることもあります）を生成します。管理対象デバイスは、**Firepower Management Center** にイベントを送信します。ここで、集約データを確認し、ネットワークアセットに対する攻撃を的確に把握できます。インライン展開では、管理対象デバイスは、有害であると判明しているパケットをドロップまたは置き換えることができます。

データベース内の各侵入イベントにはイベントヘッダーがあり、イベント名と分類、送信元と宛先の IP アドレス、ポート、イベントを生成したプロセス、およびイベントの日時に関する情報、さらに攻撃の送信元とそのターゲットに関するコンテキスト情報が含まれています。パケットベースのイベントの場合、システムは復号化されたパケットヘッダーとイベントをトリガーしたパケット（複数の場合あり）のペイロードのコピーもログに記録します。

パケットデコーダ、プリプロセッサ、および侵入ルールエンジンはすべて、システムによるイベントの生成を引き起こします。次に例を示します。

- (ネットワーク分析ポリシーで設定された) パケットデコーダが 20 バイト (オプションやペイロードのない IP データグラムのサイズ) 未満の IP パケットを受け取った場合、デコーダはこれを異常なトラフィックと解釈します。パケットを検査する侵入ポリシー内の付随するデコーダルールが有効な場合、システムは後でプリプロセッサ イベントを生成します。

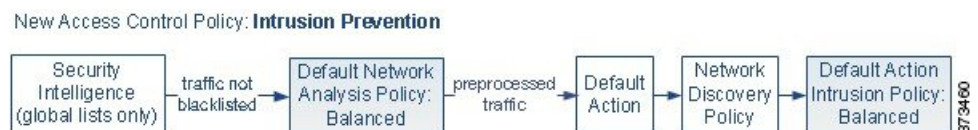
- IP最適化プリプロセッサが重複する一連のIPフラグメントを検出した場合、プリプロセッサはこれを潜在的な攻撃と解釈して、付随するプリプロセッサルールが有効な場合、システムはプリプロセッサ イベントを生成します。
- 侵入ルールエンジン内では、ほとんどの標準テキストルールおよび共有オブジェクトルールはパケットによってトリガーされた場合に侵入イベントを生成するように記述されます。

データベースに侵入イベントが蓄積されると、ユーザは攻撃の可能性について分析を開始できます。システムは、ユーザが侵入イベントを確認し、ネットワーク環境とセキュリティポリシーのコンテキストでそのイベントが重要であるかどうかを評価するために必要なツールを提供します。

## システム提供およびカスタムのネットワーク分析ポリシーと侵入ポリシー

Firepower システムを使用してトラフィック フローを管理する最初のステップの1つは、新しいアクセス コントロール ポリシーを作成することです。デフォルトでは、新しく作成されたアクセス コントロール ポリシーは、システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーを呼び出してトラフィックを検査します。

次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理および侵入防御のフェーズが強調表示されています。



以下の点に注意してください。

- デフォルトのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が制御されます。初期段階では、システムによって提供される *Balanced Security and Connectivity* ネットワーク分析ポリシーがデフォルトです。
- アクセス コントロール ポリシーのデフォルトアクションがシステムによって提供される *Balanced Security and Connectivity* 侵入ポリシーで指定された通りに悪意のないすべてのトラフィックを許可する。デフォルトアクションはトラフィックの通過を許可するので、侵入ポリシーが悪意のあるトラフィックを検査して潜在的にブロックする前に、検出機能によって、ホスト、アプリケーション、ユーザ データについてトラフィックを検査できます。
- ポリシーは、デフォルトのセキュリティ インテリジェンス オプション（グローバルなホワイトリストとブラックリストのみ）を使用し、SSLポリシーによる暗号化トラフィック



の復号や、アクセスコントロールルールによるネットワークトラフィックの特別な処理や検査を実行しません。

侵入防御展開を調整するために実行できるシンプルなステップは、システム付属のネットワーク分析ポリシーと侵入ポリシーの別のセットをデフォルトとして使用することです。Firepower システムには、これらのポリシーの複数のペアが提供されています。

または、カスタムポリシーを作成して使用することで、侵入防御展開を調整できます。それらのポリシーに設定されているプリプロセッサオプション、侵入ルール、およびその他の詳細設定が、ネットワークのセキュリティニーズに適合しない場合があります。設定できるネットワーク分析ポリシーおよび侵入ポリシーを調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

## システム提供のネットワーク分析ポリシーと侵入ポリシー

Firepower システムには、ネットワーク分析ポリシーと侵入ポリシーのペアがいくつか付属しています。システム提供のネットワーク分析ポリシーおよび侵入ポリシーを使用して、Cisco Talos Security Intelligence and Research Group (Talos) のエクスペリエンスを活用することができます。これらのポリシーでは、Talos が侵入ルールおよびプリプロセッサルールの状態、ならびにプリプロセッサおよび他の詳細設定の初期設定も指定しています。

システム提供のポリシーはいずれも、あらゆるネットワークプロファイル、トラフィックの混合、防御ポスチャを網羅しているわけではありません。それぞれのポリシーは、十分に調整した防御ポリシーを作成するための出発点となるように、共通のケースとネットワーク設定をカバーしています。システム提供のポリシーをそのまま使用することもできますが、カスタムポリシーのベースとして使用して、ネットワークに応じて調整することを強くお勧めします。



### ヒント

システム付属のネットワーク分析ポリシーと侵入ポリシーを使用する場合でも、ネットワーク環境が正確に反映されるように、システムの侵入変数を設定する必要があります。少なくとも、デフォルトのセットにある主要なデフォルトの変数を変更します。

新たな脆弱性が発見されると、Talos は侵入ルールの更新をリリースします。これらのルール更新により、システム付属のネットワーク分析ポリシーや侵入ポリシーが変更され、侵入ルールやプリプロセッサルールの新規作成または更新、既存ルールのステータスの変更、デフォルトのポリシー設定の変更が実施されます。ルールの更新では、システムによって提供されるポリシーからのルールが削除されたり、新しいルールカテゴリの提供やデフォルトの変数セットの変更が行われることがあります。

ルール更新によって展開が影響を受けると、Web インターフェイスは影響を受けた侵入ポリシーやネットワーク分析ポリシー、およびそれらの親のアクセスコントロールポリシーを失効したものとして扱います。変更を有効にするには、更新されたポリシーを再展開する必要があります。

必要に応じて、影響を受けた侵入ポリシーを（単独で、または影響を受けたアクセスコントロールポリシーと組み合わせて）自動的に再展開するように、ルールの更新を設定できます。

これにより、新たに検出されたエクスプロイトおよび侵入から保護するために展開環境を容易に自動的に最新に維持することができます。

前処理の設定を最新の状態に保つには、アクセス コントロール ポリシーを再展開する**必要があります**。これにより、現在実行されているものとは異なる、関連する SSL ポリシー、ネットワーク分析ポリシー、ファイルポリシーが再展開され、前処理とパフォーマンスの詳細設定オプションのデフォルト値も更新できるようになります。

Firepower システムに付属しているネットワーク分析ポリシーと侵入ポリシーのペアは以下のとおりです。

### **Balanced Security and Connectivity ネットワーク分析ポリシーおよび侵入ポリシー**

これらのポリシーは、速度と検出の両方を目的として作成されています。一緒に使用すると、ほとんどの組織および展開タイプにとって最適な出発点となります。ほとんどの場合、システムは **Balanced Security and Connectivity** のポリシーおよび設定をデフォルトとして使用します。

### **Connectivity Over Security ネットワーク分析ポリシーおよび侵入ポリシー**

これらのポリシーは、（すべてのリソースに到達可能な）接続がネットワーク インフラストラクチャのセキュリティよりも優先される組織向けに作成されています。この侵入ポリシーは、**Security over Connectivity** ポリシー内で有効になっているルールよりもはるかに少ないルールを有効にします。トラフィックをブロックする最も重要なルールだけが有効にされます。

### **Security over Connectivity ネットワーク分析ポリシーおよび侵入ポリシー**

これらのポリシーは、ネットワーク インフラストラクチャのセキュリティがユーザの利便性よりも優先される組織向けに作られています。この侵入ポリシーは、正式なトラフィックに対して警告またはドロップする可能性のある膨大な数のネットワーク 異常侵入ルールを有効にします。

### **Maximum Detection ネットワーク分析ポリシーおよび侵入ポリシー**

このポリシーは、**Security over Connectivity** ポリシー以上にネットワーク インフラストラクチャのセキュリティを重視する組織のために作成されています。動作への影響がさらに高くなる可能性があります。たとえば、この侵入ポリシーでは、マルウェア、エクスプロイトキット、古い脆弱性や一般的な脆弱性、および既知の流行中のエクスプロイトを含め、多数の脅威カテゴリのルールを有効にします。

### **No Rules Active 侵入ポリシー**

**No Rules Active** 侵入ポリシーでは、すべての侵入ルールと詳細設定が無効化されます。このポリシーは、他のシステムによって提供されるポリシーのいずれかで有効になっているルールをベースにするのではなく、独自の侵入ポリシーを作成する場合の出発点を提供します。

## カスタム ネットワーク分析とカスタム侵入ポリシーの利点

システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーに設定されたプリプロセッサ オプション、侵入ルール、およびその他の詳細設定は、組織のセキュリティ ニーズに十分に対応しない場合があります。

カスタム侵入ポリシーを作成すると、環境内のシステムのパフォーマンスを向上させ、ネットワークで発生する悪意のあるトラフィックやポリシー違反を重点的に観察できるようになります。設定できるカスタムポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

すべてのカスタムポリシーには基本ポリシー（別名「基本レイヤ」）があり、それによって、ポリシー内のすべてのコンフィギュレーションのデフォルト設定が定義されます。レイヤは、複数のネットワーク分析ポリシーまたは侵入ポリシーを効率的に管理するために使用できる構成要素です。

ほとんどの場合、カスタムポリシーはシステム付属のポリシーに基づきますが、別のカスタムポリシーを使用することもできます。ただし、すべてのカスタムポリシーには、ポリシーチェーンの根本的な基礎としてシステム付属ポリシーが含まれています。システム付属のポリシーはルールの更新によって変更される可能性があるため、カスタムポリシーを基本として使用している場合でも、ルールの更新をインポートするとポリシーに影響が及びます。ルール更新によって展開が影響を受けると、Web インターフェイスは影響を受けたポリシーを失効として扱います。

ユーザが作成するカスタムポリシーに加えて、システムには、初期インラインポリシーと初期パッシブポリシーという2つのカスタム侵入ポリシーと2つのネットワーク分析ポリシーが用意されています。これらのポリシーは、該当する [バランスの取れたセキュリティと接続 (Balanced Security and Connectivity)] ポリシーを基本ポリシーとして使用します。両者の唯一の相違点はドロップ動作です。インラインポリシーではトラフィックのブロックと変更が有効化され、パッシブポリシーでは無効化されます。これらのシステム提供のカスタムポリシーは編集して使用できます。

### カスタム ネットワーク分析ポリシーの利点

デフォルトでは、1つのネットワーク分析ポリシーによって、アクセスコントロールポリシーで処理されるすべての暗号化されていないトラフィックが前処理されます。これは、後でパケットを検査する侵入ポリシー（および侵入ルールセット）に関係なく、すべてのパケットが同じ設定に基づいて復号化および前処理されることを意味します。

初期段階では、システムによって提供される **Balanced Security and Connectivity** ネットワーク分析ポリシーがデフォルトです。前処理を調整する簡単な方法は、カスタムネットワーク分析ポリシーを作成し、それをデフォルトとして使用することです。

使用可能な調整オプションはプリプロセッサによって異なりますが、プリプロセッサおよびデコードを調整できる方法には次のものがあります。

- モニタしているトラフィックに適用されないプリプロセッサを無効にできます。たとえば、HTTP Inspect プリプロセッサは HTTP トラフィックを正規化します。ネットワークに

Microsoft インターネット インフォメーション サービス (IIS) を使用する Web サーバが含まれていないことが確実な場合は、IIS 特有のトラフィックを検出するプリプロセッサオプションを無効にすることで、システム処理のオーバーヘッドを軽減できます。



(注) カスタムネットワーク分析ポリシーでプリプロセッサが無効化されているときに、パケットを有効な侵入ルールまたはプリプロセッサルールと照合して評価するために、プリプロセッサを使用する必要がある場合、システムはプリプロセッサを有効化して使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効なままになります。

- 必要に応じて、特定のプリプロセッサのアクティビティを集中させるポートを指定します。たとえば、DNS サーバの応答や暗号化 SSL セッションをモニタするための追加ポートや、Telnet、HTTP、RPC トラフィックを復号化するポートを特定できます。

複雑な環境での高度なユーザの場合は、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを別々に前処理するように調整することができます。さらに、トラフィックのセキュリティゾーン、ネットワーク、または VLAN に応じて前処理が制御されるようにこれらのポリシーを設定できます (ASA FirePOWER モジュールでは、VLAN に応じて前処理を制限することはできません)。



(注) カスタムネットワーク分析ポリシー (特に複数のネットワーク分析ポリシー) を使用して前処理を調整することは、高度なタスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一のパケットを検査するネットワーク分析ポリシーと侵入ポリシーが相互補完することを許可する場合は、注意する必要があります。

## カスタム侵入ポリシーの利点

侵入防御を実行するように初期設定して、新規にアクセス コントロール ポリシーを作成した場合、そのポリシーでは、デフォルトアクションはすべてのトラフィックを許可しますが、最初にシステム付属の **Balanced Security and Connectivity** 侵入ポリシーでトラフィックをチェックします。アクセス コントロール ルールを追加するか、またはデフォルトアクションを変更しない限り、すべてのトラフィックがその侵入ポリシーによって検査されます。

侵入防御展開をカスタマイズするために、複数の侵入ポリシーを作成し、それぞれがトラフィックを異なる方法で検査するように調整できます。次に、どのポリシーがどのトラフィックを検査するかを指定するルールを、アクセス コントロール ポリシーに設定します。アクセス コントロール ルールは単純でも複雑でもかまいません。セキュリティゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、またはユーザなど、複数の基準を使用してトラフィックを照合および検査します。

侵入ポリシーの主な機能は、次のように、どの侵入ルールおよびプリプロセッサルールを有効にしてどのように設定するかを管理することです。

- 各侵入ポリシーで、環境に適用されるすべてのルールが有効になっていることを確認し、環境に適用されないルールを無効化することによって、パフォーマンスを向上させます。インライン展開では、どのルールによって悪質なパケットをドロップまたは変更するかを指定できます。
- Firepower 推奨機能を使用すると、ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます。
- 必要に応じて、既存のルールの変更や、新しい標準テキストルールの作成により、新たなエクスプロイトの検出やセキュリティ ポリシーの適用が可能です。

侵入ポリシーに対して行えるその他のカスタマイズは次のとおりです。

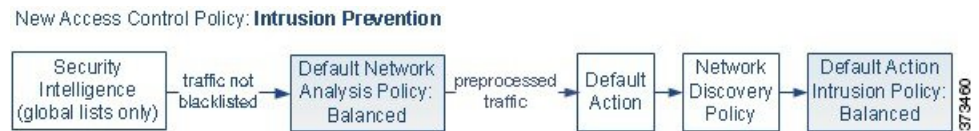
- 機密データ プリプロセッサは、ASCII テキストのクレジットカード番号や社会保障番号などの機密データを検出します。特定の脅威（Back Orifice 攻撃、数種類のポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃）を検出するプリプロセッサは、ネットワーク分析ポリシーで設定します。
- グローバルしきい値を設定すると、侵入ルールに一致するトラフィックが、指定期間内に特定のアドレスまたはアドレス範囲で送受信される回数に基づいて、イベントが生成されます。これにより、大量のイベントによってシステムに過剰な負荷がかかることを回避できます。
- また、個々のルールまたは侵入ポリシー全体に対して、侵入イベント通知を抑制し、しきい値を設定することで、大量のイベントによってシステムに過剰な負荷がかかることを回避することもできます。
- Web インターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、syslog ファシリティへのロギングを有効にしたり、イベントデータを SNMP トラップサーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギングファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。これらのポリシー単位のアラート設定に加えて、各ルールまたはルール グループの侵入イベントを通知する電子メールアラートをグローバルに有効化/無効化できます。どの侵入ポリシーがパケットを処理するかに関わらず、ユーザの電子メールアラート設定が使用されます。

## カスタム ポリシーの制限

前処理および侵入インスペクションは密接に関連しているため、単一パケットを処理して検査するネットワーク分析ポリシーと侵入ポリシーが互いに補完することを許可する設定を行う場合は慎重になる**必要があります**。

デフォルトでは、システムは、管理対象デバイスでアクセス コントロール ポリシーにより処理されるすべてのトラフィックを、1つのネットワーク分析ポリシーを使用して前処理します。次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシー

が最初にトラフィックを処理するしくみを示しています。前処理および侵入防御のフェーズが強調表示されています。



アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が、デフォルトのネットワーク分析ポリシーによってどのように制御されるのか注意してください。初期段階では、システムによって提供される **Balanced Security and Connectivity** ネットワーク分析ポリシーがデフォルトです。

前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。ただし、カスタム ネットワーク分析ポリシーでプリプロセッサが無効化されているときに、前処理されたパケットを有効な侵入ルールまたはプリプロセッサルールと照合して評価する必要がある場合、システムはプリプロセッサを有効化して使用します。ただし、ネットワーク分析ポリシーの Web ユーザ インターフェイスではプリプロセッサは無効なままになります。



- (注) プリプロセッサを無効にするパフォーマンス上の利点を得るには、侵入ポリシーでそのプリプロセッサを必要とするルールが有効になっていないことを確認する**必要があります**。

複数のカスタム ネットワーク分析ポリシーを使用する場合は、さらに課題があります。複雑な展開内の上級ユーザの場合は、一致したトラフィックの前処理にカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティゾーン、ネットワーク、VLAN に合わせて前処理を調整できます。(ただし、ASA FirePOWER VLAN による前処理を制限できません)。これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。各ルールにはネットワーク分析ポリシーが関連付けられており、ルールに一致するトラフィックの前処理を制御します。

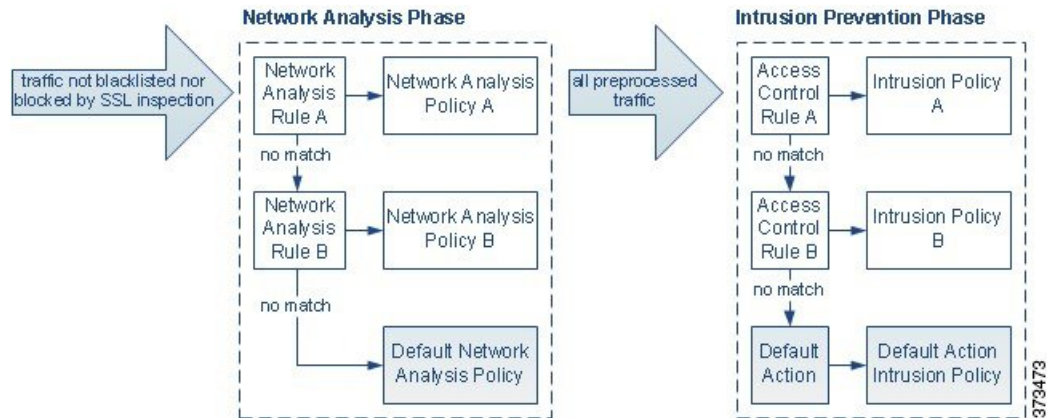


- ヒント** アクセス コントロール ポリシーの詳細設定としてネットワーク分析ルールを設定します。Firepower システムの他のタイプのルールとは異なり、ネットワーク分析ルールは、ネットワーク分析ポリシーに含まれるのではなく、ネットワーク分析ポリシーを呼び出します。

システムは、ルール番号の昇順で、設定済みネットワーク分析ルールとパケットを照合します。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。これにより非常に柔軟にトラフィックを前処理できます。ただし、留意すべき点として、パケットがどのネットワーク分析ポリシーによって前処理されるかに**関係なく**、すべてのパケットは、それら独自のプロセスにおいて引き続きアクセス コントロールルールと照合されます(つまり、侵入ポリシーにより検査される可能性があります)。つまり、特定のネットワーク分析ポリシーでパケットを前処理しても、そのパケットが確実に特定の侵入ポリシーで検査されるわけでは**ありません**。アクセスコントロール

ポリシーを設定するときは、そのポリシーが正しいネットワーク分析ポリシーおよび侵入ポリシーを呼び出して特定の packets を評価するように、慎重に行う **必要があります**。

次の図は、侵入防御（ルール）フェーズよりも前に、別にネットワーク分析ポリシー（前処理）の選択フェーズが発生するしくみを詳細に示しています。簡略化するために、図では検出フェーズとファイル/マルウェア インспекション フェーズが省かれています。また、デフォルトのネットワーク分析ポリシーおよびデフォルトアクションの侵入ポリシーを強調表示しています。



このシナリオでは、アクセス コントロール ポリシーは、2つのネットワーク分析ルールとデフォルトのネットワーク分析ポリシーで設定されています。

- Network Analysis Rule A は、一致するトラフィックを Network Analysis Policy A で前処理します。その後、このトラフィックを Intrusion Policy A で検査されるようにすることができます。
- Network Analysis Rule B は、一致するトラフィックを Network Analysis Policy B で前処理します。その後、このトラフィックを Intrusion Policy B で検査されるようにすることができます。
- 残りのトラフィックはすべて、デフォルトのネットワーク分析ポリシーにより前処理されます。その後、このトラフィックをアクセスコントロールポリシーのデフォルトアクションに関連付けられた侵入ポリシーによって検査されるようにすることができます。

システムはトラフィックを前処理した後、侵入についてトラフィックを検査できます。図では、2つのアクセス コントロールルールとデフォルト アクションが含まれるアクセス コントロールポリシーを示しています。

- アクセス コントロールルール A は、一致したトラフィックを許可します。トラフィックはその後、Intrusion Policy A によって検査されます。
- アクセス コントロールルール B は、一致したトラフィックを許可します。トラフィックはその後、Intrusion Policy B によって検査されます。
- アクセス コントロール ポリシーのデフォルト アクションは一致したトラフィックを許可します。トラフィックはその後、デフォルトアクションの侵入ポリシーによって検査されます。

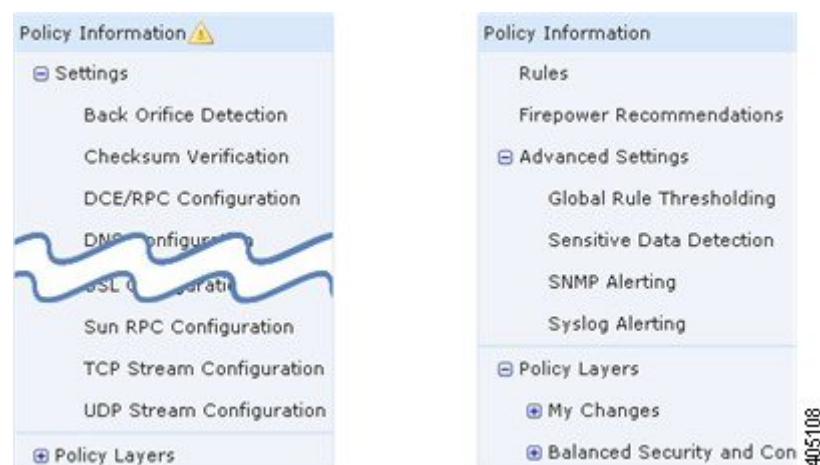
各パケットの処理は、ネットワーク分析ポリシーと侵入ポリシーのペアにより制御されますが、このペアはユーザに合わせて調整されません。アクセス コントロール ポリシーが誤って設定されているため、ネットワーク分析ルール A とアクセス コントロールルール A が同じトラフィックを処理しない場合を想定してください。たとえば、特定のセキュリティゾーンのトラフィックの処理をポリシーペアによって制御することを意図している場合に、誤まって、異なるゾーンを使用するように2つのルールの条件を設定したとします。この誤設定により、トラフィックが誤って前処理される可能性があります。したがって、ネットワーク分析ルールおよびカスタム ポリシーを使用した前処理の調整は、高度なタスクです。

単一の接続の場合は、アクセス コントロールルールよりも前にネットワーク分析ポリシーが選択されますが、一部の前処理（特にアプリケーション層の前処理）はアクセスコントロールルールの選択後に実行されます。これは、カスタムネットワーク分析ポリシーでの前処理の設定には影響しません。

## ナビゲーション ウィンドウ: ネットワーク分析と侵入ポリシー

ネットワーク分析ポリシーと侵入ポリシーは同様の Web インターフェイスを使用して、設定への変更を編集して保存します。

いずれかのタイプのポリシーを編集するときに、Web インターフェイスの左側にナビゲーションパネルが表示されます。次の図は、ネットワーク分析ポリシー（左）および侵入ポリシー（右）のナビゲーションパネルを示しています。



ナビゲーションパネルは境界線によって複数のポリシー設定項目リンクに分割されており、ポリシー層との直接対話により（下側）または直接対話なしで（上側）ポリシー設定項目を設定できます。いずれかの設定ページに移動するには、ナビゲーションパネル内の名前をクリックします。ナビゲーションパネルで影付きで強調表示されている項目は、現在の設定ページを示しています。たとえば、上の図では、[ポリシー情報（Policy Information）] ページがナビゲーションパネルの右側に表示されます。



### [ポリシー情報 (Policy Information)]

[ポリシー情報 (Policy Information)] ページには、一般的に使用される設定の設定オプションが示されます。上記のネットワーク分析ポリシーパネルの図に示すように、ポリシーに未保存の変更がある場合は、ナビゲーションパネルの[ポリシー情報 (Policy Information)]の横にポリシー変更アイコン (⚠) が表示されます。アイコンは、変更を保存すると消えます。

### [ルール (Rules)] (侵入ポリシーのみ)

侵入ポリシーの[ルール (Rules)] ページでは、共有オブジェクトルール、標準テキストルール、およびプリプロセッサルールのルールステータスとその他の設定項目を設定できます。

### [Firepower の推奨事項 (Firepower Recommendations)] (侵入ポリシーのみ)

侵入ポリシーの[Firepower の推奨事項 (Firepower Recommendations)] ページでは、ネットワーク上で検出されたオペレーティングシステム、サーバ、およびクライアントアプリケーションプロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。

### [Settings] (ネットワーク分析ポリシー) および [Advanced Settings] (侵入ポリシー)

ネットワーク分析ポリシーの[設定 (Settings)] ページでは、プリプロセッサを有効または無効にしたり、プリプロセッサの設定ページにアクセスしたりできます。[設定 (Settings)] リンクを展開すると、ポリシー内で有効になっているすべてのプリプロセッサの個々の設定ページへのサブリンクが表示されます。

侵入ポリシーの[詳細設定 (Advanced Settings)] ページでは、詳細設定を有効または無効にしたり、詳細設定の設定ページにアクセスしたりできます。[詳細設定 (Advanced Settings)] リンクを展開すると、ポリシー内で有効になっているすべての詳細設定を個々に設定する設定ページへのサブリンクが表示されます。

### [Policy Layers]

[ポリシー層 (Policy Layers)] ページには、ネットワーク分析ポリシーまたは侵入ポリシーを構成する階層の要約が表示されます。[ポリシー層 (Policy Layers)] リンクを展開すると、ポリシー内の階層に関する概要ページへのサブリンクが表示されます。各階層のサブリンクを展開すると、その階層で有効になっているすべてのルール、プリプロセッサ、または詳細設定の設定ページへのサブリンクがさらに表示されます。

## 競合と変更：ネットワーク分析ポリシーと侵入ポリシー

ネットワーク分析ポリシーや侵入ポリシーを編集するときに、ポリシーに未保存の変更がある場合は、そのことを示すために、ナビゲーションパネルの[ポリシー情報 (Policy Information)]の横にポリシー変更アイコン (⚠) が表示されます。変更をシステムに認識させるには、変更を保存 (確定) する必要があります。



- (注) 保存後は、変更を反映させるためにネットワーク分析ポリシーまたは侵入ポリシーを展開する必要があります。保存しないでポリシーを展開すると、最後に保存された設定が使用されません。

### 編集競合の解決

[ネットワーク分析ポリシー (Network Analysis Policy)] ページ ([ポリシー (Policies)] > [アクセスコントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。) および [侵入ポリシー (Intrusion Policy)] ページ ([ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)]) には、各ポリシーの未保存の変更の有無、および現在ポリシーを編集中のユーザ情報が表示されます。シスコでは、同時に1人だけがポリシーを編集することを推奨します。同時編集を実行すると、次のようになります。

- ネットワーク分析ポリシーまたは侵入ポリシーを編集しているときに、同時に他のユーザが同じポリシーを編集し、ポリシーへの変更を保存した場合、ポリシーを確定すると、他のユーザの変更が上書きされることを警告するメッセージが表示されます。
- 同じユーザとして複数の Web インターフェイス インスタンス経由で同じネットワーク分析ポリシーまたは侵入ポリシーを編集集中に、1つのインスタンスの変更を保存すると、他のインスタンスの変更は保存できません。

### 設定の依存関係の解決

特定の分析を実行する場合、多くのプリプロセッサルールとセキュリティルールでは、最初に特定の手法でトラフィックをデコードまたは前処理するか、他の依存関係を割り当てる必要があります。ネットワーク分析ポリシーまたは侵入ポリシーを保存すると、システムが必要な設定を自動的に有効にするか、または次のように無効な設定はトラフィックに影響しないことが警告されます。

- SNMP ルールアラートを追加しても、SNMP アラートを設定しなかった場合は、侵入ポリシーを保存できません。SNMP アラートを設定するか、またはルールアラートを無効にしてから、再度保存します。
- 侵入ポリシーに有効なセンシティブ データ ルールが含まれているときに、センシティブ データプリプロセッサが有効になっていない場合は、侵入ポリシーを保存できません。システムがプリプロセッサを有効にしてポリシーを保存するように許可するか、またはルールを無効にしてから、再度保存します。
- ネットワーク分析ポリシーで必要なプリプロセッサを無効にしても、ポリシーを引き続き保存できます。ただし、ネットワーク分析ポリシーの Web インターフェイスでプリプロセッサは無効になっていても、システムは無効になっているプリプロセッサを自動的に現在の設定で使用します。

- ネットワーク分析ポリシーでインラインモードを無効にしても、インライン正規化プリプロセッサが有効になっている場合は、ポリシーを引き続き保存できます。ただし、正規化設定が無視されることが警告されます。インラインモードを無効化すると他の設定が無視されるので、プリプロセッサは、チェックサム検証やレートベース攻撃の防御を含めて、トラフィックを変更またはブロックできます。

### ポリシー変更のコミット、破棄、およびキャッシュ

ネットワーク分析ポリシーまたは侵入ポリシーの編集時に、変更を保存しないでポリシーエディタを終了した場合、それらの変更はシステムによってキャッシュされます。システムからログアウトした場合や、システムクラッシュが発生した場合でも、変更はキャッシュされません。システムキャッシュには、ユーザごとに1つのネットワーク分析ポリシーと1つの侵入ポリシーの未保存の変更しか格納されないため、同じタイプの別のポリシーを編集する場合は、その前に、行った変更を確定または破棄する必要があります。システムは、ユーザが最初のポリシーへの変更を保存せずに別のポリシーを編集したり、侵入ルールの更新をインポートした場合に、キャッシュされた変更内容を破棄します。

ネットワーク分析ポリシーエディタまたは侵入ポリシーエディタの [ポリシー情報 (Policy Information)] ページでポリシーの変更内容をコミットまたは破棄できます。

Firepower Management Center 設定では、以下を制御できます。

- ネットワーク分析ポリシーまたは侵入ポリシーへの変更を確定するときに、それに関するコメントの入力を求めるか (または、コメントの入力を必須とするか)
- 変更内容とコメントを監査ログに記録するか

### 関連トピック

- [ネットワーク解析ポリシーの設定の構成](#)
- [侵入ポリシー設定の構成](#)

## ネットワーク分析または侵入ポリシーの終了

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

### 手順

ネットワーク分析、または侵入ポリシーの拡張エディタを終了するには、以下の方法があります。

- キャッシュ：ポリシーを終了し、変更をキャッシュするには、いずれかのメニューを選択するか、別のページへのほかのパスを選択します。終了時に表示される [ページを移動

(Leave page) ]をクリックするか、[ページを移動しない (Stay on page) ]をクリックして拡張エディタに残ります。

- 破棄：保存されていない変更を破棄するには、[ポリシー情報 (Policy Information) ]ページの [変更の破棄 (Discard Changes) ]をクリックし、[OK] をクリックします。
  - 保存：ポリシーの変更を保存するには、[ポリシー情報 (Policy Information) ]ページの [変更の確定 (ommit Changes) ]をクリックします。プロンプトが表示される場合、コメントを入力し、[OK] をクリックします。
-



## 第 69 章

# 侵入ポリシーおよびネットワーク分析ポリシーのレイヤ

以下のトピックでは、侵入ポリシーおよびネットワーク分析ポリシーでレイヤ（層）を使用する方法について説明します。

- [レイヤの基本](#)（1591 ページ）
- [レイヤスタック](#)（1591 ページ）
- [レイヤ管理](#)（1597 ページ）

## レイヤの基本

多数の管理対象デバイスが存在する大規模な組織では、さまざまな部署や事業部門、場合によってはさまざまな企業の固有のニーズをサポートするために、多数の侵入ポリシーやネットワーク分析ポリシーが存在することがあります。両方のポリシータイプでの設定はレイヤと呼ばれる構成要素に含まれており、それを使用することで効率的に複数のポリシーを管理することができます。

侵入ポリシーおよびネットワーク分析ポリシーのレイヤは、原則的に同じ方法で動作します。ポリシータイプの作成および編集は、レイヤを意識せずに行えます。ポリシー設定を変更でき、ポリシーにユーザレイヤを追加していない場合は、システムによって自動的に変更内容が単一の設定可能なレイヤ（最初は *My Changes* という名前が付けられています）に含められます。また、最大 200 までレイヤを追加して、それらのレイヤで設定を任意に組み合わせて構成することもできます。ユーザレイヤのコピー、マージ、移動、削除を実行できます。最も重要なこととして、個々のユーザレイヤを同じタイプの他のポリシーと共有できます。

## レイヤスタック

レイヤスタックは、次の各レイヤから構成されています。

## ユーザ レイヤ

ユーザ設定可能なレイヤです。ユーザ設定可能なレイヤは、コピー、マージ、移動、または削除を行うことができます。また、任意のユーザ設定可能なレイヤが同じタイプの他のポリシーと共有されるように設定することもできます。このレイヤには、最初に My Changes という名前が付けられた自動生成されたレイヤが含まれています。

## 組み込み型レイヤ

読み取り専用の基本ポリシーレイヤです。このレイヤ内のポリシーは、システムによって提供されるポリシー、または自分で作成したカスタム ポリシーにできます。

ネットワーク分析ポリシーまたは侵入ポリシーには、デフォルトでは基本ポリシー レイヤと My Changes レイヤが含まれています。ユーザ レイヤは必要に応じて追加できます。

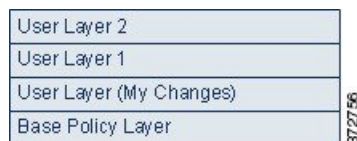
各ポリシーレイヤには、ネットワーク分析ポリシー内のすべてのプリプロセッサまたは侵入ポリシー内のすべての侵入ルールと詳細設定の完全な設定が含まれます。最下部の基本ポリシーレイヤには、ポリシーの作成時に選択した基本ポリシーのすべての設定が含まれます。上位レイヤの設定は、下位レイヤの同じ設定よりも優先されます。レイヤで明示的に設定されていない機能は、明示的に設定されている次の高いレイヤから設定を継承します。システムはレイヤをフラット化します。つまり、ネットワークトラフィックの処理時にすべての設定の蓄積効果のみを適用します。



### ヒント

侵入またはネットワークの分析ポリシーは、基本ポリシーのデフォルト設定のみに基づいて作成できます。侵入ポリシーの場合に、モニタ対象ネットワークの特定のニーズに合わせて侵入ポリシーを調整したいときは、Firepower のルール状態の推奨を使用することもできます。

次の図は、基本ポリシー レイヤと初期設定の My Changes レイヤの他に、2つの追加のユーザ設定可能なレイヤ *User Layer 1* と *User Layer 2* も含まれているレイヤスタックの例を示しています。この図では、ユーザが追加したユーザ設定可能なレイヤそれぞれがスタックの最上位レイヤとして最初に配置されるため、図内の *User Layer 2* が最後に追加されたもので、このスタックの最上位になっていることに注目してください。



ルール更新にポリシーの変更を許可しているかどうかに関わらず、ルール更新での変更は、レイヤで行った変更を上書きしません。これは、ルール更新での変更が、基本ポリシーレイヤのデフォルト設定を決定する基本ポリシーで行われるためです。変更は常により上位のレイヤに加えられ、その変更によって、ルール更新が基本ポリシーに加えた変更が上書きされます。

## 基本レイヤ

侵入ポリシーまたはネットワーク分析ポリシーの基本レイヤ（基本ポリシーとも呼ばれる）は、ポリシーのすべての設定のデフォルト設定を定義し、ポリシーの最下位に位置します。新

しいポリシーを作成し、新しいレイヤを追加しないで設定を変更すると、その変更はMy Changes レイヤに保存され、基本ポリシーの設定を上書きしますが変更はしません。

## システム提供の基本ポリシー

Firepower システムには、ネットワーク分析ポリシーと侵入ポリシーのペアがいくつか提供されています。システム提供のネットワーク分析ポリシーおよび侵入ポリシーを使用して、Cisco Talos Security Intelligence and Research Group (Talos) のエクスペリエンスを活用することができます。これらのポリシーでは、Talos は侵入ルールおよびプリプロセッサ ルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。これらのシステムによって提供されるポリシーをそのまま使用したり、カスタムポリシーのベースとして使用することができます。

システムによって提供されるポリシーをベースとして使用する場合、ルール更新をインポートすると、基本ポリシー内の設定が変更される場合があります。ただし、カスタムポリシーを設定して、これらの変更内容がシステム提供の基本ポリシーに自動的に反映されないようにすることもできます。これにより、ルール更新とは関係ないスケジュールで、システム提供の基本ポリシーを手動で更新できます。いずれの場合も、ルール更新が基本ポリシーに加えた変更によって My Changes または他のレイヤの設定が変更または上書きされることはありません。

システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。

## カスタム基本ポリシー

カスタム ポリシーを基本（ベース）として使用することができます。カスタム ポリシーの設定を調整することで、最も役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

別のポリシーのベースとして使用するカスタムポリシー変更すると、変更内容はこのベースを使用するポリシーのデフォルト設定として自動的に使用されます。

また、ポリシーはすべて、システムが提供するポリシーをポリシーチェーンにおける最終的なベースとしているため、たとえカスタム基本ポリシーを使っても、ルールが更新されればポリシーに影響する可能性があります。チェーン内の最初のカスタム ポリシー（システムによって提供されるポリシーをベースとして使用するポリシー）によってルール更新がその基本ポリシーを変更することが許可されている場合は、ポリシーに影響を受ける可能性があります。

基本ポリシーがどのように変更されたかに関わらず（ルール更新による変更でも、基本ポリシーとして使用するカスタム ポリシーを変更でも）、ユーザの基本ポリシーに対する変更によって My Changes やその他のレイヤの設定が変更または上書きされることはありません。

## 基本ポリシーに対するルール更新の影響

ルール更新をインポートすると、システム提供の侵入ポリシー、アクセスコントロールポリシー、ネットワーク分析ポリシーが変更されます。ルール更新には次の要素が含まれる場合があります。

- 変更されたネットワーク分析プリプロセッサの設定
- 変更された侵入ポリシーおよびアクセスコントロールポリシーの詳細設定
- 新規または更新された侵入ルール
- 既存のルールの変更された状態
- 新しいルールカテゴリとデフォルト変数

ルール更新により、既存のルールがシステム提供のポリシーから削除される場合もあります。デフォルト変数とルールカテゴリに対する変更はシステムレベルで処理されます。

システム提供のポリシーを侵入またはネットワーク分析の基本ポリシーとして使用するときは、ルール更新が基本ポリシー（この場合はシステムによって提供されるポリシーのコピー）を変更することを許可することができます。ルール更新で基本ポリシーの更新を許可する場合は、新しいルール更新によって、基本ポリシーとして使用するシステム提供のポリシーに対する変更と同じ変更が基本ポリシーにも加えられます。対応する設定を変更しなかった場合は、基本ポリシー内の設定によって、ポリシー内の設定が決定されます。ただし、ルール更新では、ポリシー内で行った変更は上書きされません。

ルール更新による基本ポリシーの変更を許可しない場合は、1つ以上のルール更新のインポート後に、基本ポリシーを手動で更新できます。

ルール更新では、侵入ポリシー内のルール状態またはルール更新による基本の侵入ポリシーの変更が許可されているかどうかに関係なく、Talosが削除する侵入ルールが常に削除されます。

ネットワークトラフィックに変更を再展開するまで、現在展開されている侵入ポリシールールは次のように動作します。

- 無効になっている侵入ルールは無効のままになります。
- [イベントを生成する (Generate Events)] に設定されたルールでは、トリガーされたときのイベントの生成が継続されます。
- [ドロップしてイベントを生成する (Drop and Generate Events)] に設定されたルールでは、トリガーされたときのイベントの生成と違反パケットのドロップが継続されます。

次の両方の条件が満たされていない限り、ルール更新でカスタム基本ポリシーは変更されません。

- ルール更新が親ポリシーのシステムによって提供される基本ポリシー（つまり、カスタム基本ポリシーの起源となるポリシー）を変更することを許可している。
- 親の基本ポリシー内の対応する設定が上書きされる親ポリシー内の変更を実施していない。



両方の条件が満たされている場合は、親ポリシーを保存したときに、ルール更新内の変更が子ポリシー（つまり、カスタム基本ポリシーを使用したポリシー）に渡されます。

たとえば、ルール更新で以前に無効になっていた侵入ルールを有効にして、親の侵入ポリシー内のルール状態を変更していない場合は、親ポリシーを保存したときに、変更されたルール状態が基本ポリシーに渡されます。

同様に、ルール更新でデフォルトのプリプロセッサ設定を変更し、親のネットワーク分析ポリシーの設定を変更していない場合は、変更された設定は親ポリシーを保存したときに基本ポリシーに渡されます。

## ベースポリシーの変更

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

別のシステム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

最大5つのカスタム ポリシーをチェーンすることができます。5つのうちの4つのポリシーで事前に作成されたポリシーが基本ポリシーとして使用され、5つ目のポリシーでシステムによって提供されたポリシーをベースとして使用する必要があります。

### 手順

**ステップ 1** ポリシーの編集集中に、ナビゲーション パネルで[ポリシー情報 (Policy Information)]をクリックします。

**ステップ 2** 次の選択肢を設定できます。

- 基本ポリシーを選択する：[基本ポリシー (Base Policy)] ドロップダウンリストから選択します。
- ベースポリシーを変更するルール更新を許可する：[ベースポリシーの管理 (Manage Base Policy)] をクリックし、[新しいルール更新のインストールでポリシーを更新する (Update when a new Rule Update is installed)] チェックボックスをオンにします。

**ヒント** このチェックボックスをオフにしてポリシーを保存してから、ルール更新をインポートすると、[基本ポリシー (Base Policy)] 概要ページに[今すぐ更新 (Update Now)] ボタンが表示され、そのページ上のステータス メッセージが更新されて、ポリシーが期限切れであることが示されます。最近インポートしたルール更新内の変更で基本ポリシーを更新するには、[今すぐ更新 (Update Now)] をクリックします。

**ステップ 3** 最後のコミットからポリシーに加えられた変更を保存するには、[ポリシー情報 (Policy information)] をクリックし、次に[変更をコミット (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## Firepower 推奨レイヤ

侵入ポリシーでルール状態の推奨を生成する場合は、その推奨に基づいてルール状態を自動的に変更するかどうかを選択できます。

下記の図に示すように、推奨されたルール状態を使用すると、侵入ポリシーの基本レイヤのすぐ上に読み取り専用の組み込み Firepower 推奨レイヤが挿入されます。

User Layer 2	405109
User Layer 1	
User Layer (My Changes)	
Firepower Recommendations Layer	
Base Policy Layer	

このレイヤは侵入ポリシー固有のもので、

それ以後、推奨されたルール状態を使用しないことを選択すると、Firepower 推奨レイヤは削除されます。このレイヤは手動で削除できませんが、推奨されるルール状態を使用するかどうかを選択することで、サービスを追加したり削除することができます。

Firepower 推奨レイヤを追加すると、ナビゲーションパネルの [ポリシー階層 (Policy Layers)] の下に Firepower 推奨リンクが追加されます。このリンクから Firepower 推奨レイヤ ページの読み取り専用ビューにアクセスして、[ルール (Rules)] ページの推奨でフィルタリングされたビューを読み取り専用モードで表示できます。

推奨されたルール状態を使用すると、ナビゲーションパネルの Firepower 推奨リンクの下に [ルール (Rules)] サブリンクも追加されます。[ルール (Rules)] サブリンクから、Firepower 推奨レイヤの [ルール (Rules)] ページの読み取り専用画面にアクセスできます。このビューでは次の点に注意してください。

- 状態列にルール状態のアイコンがない場合、状態は基本ポリシーから継承されます。
- このビューまたは他の [ルール (Rules)] ページ ビューの Firepower 推奨列にルール状態のアイコンがない場合、このルールに対する推奨は存在しません。

### 関連トピック

[ネットワーク資産に応じた侵入防御の調整 \(1655 ページ\)](#)

# レイヤ管理

[ポリシー層 (Policy Layers) ] ページには、ネットワーク分析ポリシーまたは侵入ポリシーの完全なレイヤスタックの単一ページの概要が示されます。このページでは、共有レイヤおよび非共有レイヤの追加、レイヤのコピー、マージ、移動、および削除、各レイヤの概要ページへのアクセス、各レイヤ内の有効、無効、および上書きされている設定の設定ページへのアクセスを行うことができます。

各レイヤについて、次の情報が表示されます。

- レイヤが組み込み型レイヤ、共有ユーザレイヤ、または非共有ユーザレイヤであるかどうか
- どのレイヤに最上位の（つまり効果的な）プリプロセッサまたは詳細設定が含まれているか（機能名別に）
- 侵入ポリシーで、状態がレイヤで設定されている侵入ルールの数、および各ルール状態に設定されているルールの数

[ポリシー層 (Policy Layers) ] ページには、有効なすべてのプリプロセッサ（ネットワーク分析）または詳細設定（侵入）、また侵入ポリシーの場合は侵入ルールの最終的な効果の概要も示されます。

各レイヤのサマリーにある機能名は、以下のように、設定がレイヤで有効、無効、上書き、または継承されているかを示します。

機能の状態	機能名
レイヤで有効	プレーンテキストで表示
レイヤで無効	取り消し線が引かれる
上位レイヤの設定によって上書きされる	イタリックテキストで表示
下位レイヤから継承される	表示されない

最大200のレイヤをネットワーク分析ポリシーまたは侵入ポリシーに追加できます。レイヤを追加すると、ポリシーで最上位レイヤとして表示されます。初期状態はすべての機能に対して[継承 (Inherit) ]で、侵入ポリシーでは、イベントのフィルタリング、動的状態、またはルールアクションのアラートは設定されません。

レイヤをポリシーに追加する際は、ユーザが設定可能なレイヤに一意の名前を指定します。その名前は後で変更できます。また、必要に応じて、レイヤを編集する際に表示される説明を追加あるいは変更することもできます。

レイヤはコピーすることも、[ユーザレイヤ (User Layers) ] ページ内での表示位置を上下に移動することもできます。また、初期の My Changes レイヤを含め、ユーザレイヤを削除することも可能です。次の考慮事項に注意してください。

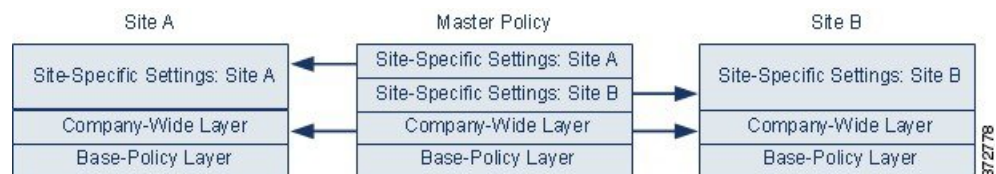
- レイヤをコピーすると、そのコピーが最上位レイヤとして表示されます。
- 共有レイヤをコピーすると、初期状態ではそのレイヤは共有されませんが、必要に応じて、後から共有できます。
- 共有レイヤは削除できません。共有が有効になっているレイヤで別のポリシーと共有していないものは、共有レイヤではありません。

ユーザ設定可能なレイヤの直下に、別のユーザ設定可能なレイヤをマージできます。マージされたレイヤは、どちらかのレイヤに固有だったすべての設定を保持します。また、両方のレイヤに同じプリプロセッサ、侵入ルール、または詳細設定が含まれていた場合、上位のレイヤの設定を受け入れます。マージされたレイヤでは、下位レイヤの名前が保持されます。他のポリシーに追加できる共有可能なレイヤを作成するポリシーでは、共有可能なレイヤのすぐ上に非共有レイヤのある共有可能なレイヤをマージできますが、共有可能なレイヤの直下には非共有レイヤのある共有可能なレイヤをマージすることはできません。別のポリシーに作成した共有レイヤを追加するポリシーでは、共有レイヤをそのすぐ下の非共有レイヤとマージできますが、作成されたレイヤは共有されなくなります。非共有レイヤをその下の共有レイヤとマージすることはできません。

## 共有レイヤ

共有レイヤとは、あるポリシー内で作成して共有を許可し、別のポリシーに追加されたレイヤのことです。共有可能なレイヤとは、共有が許可されているレイヤのことです。

以下の図に示すマスターポリシーの例では、全社的レイヤと、サイト A およびサイト B に固有のレイヤを作成し、これらのサイト固有のレイヤの共有を許可しています。その上で、これらのサイト固有のレイヤを共有レイヤとしてサイト A とサイト B のポリシーに追加しています。



マスターポリシーの全社的なレイヤには、サイト A とサイト B に適用される設定が含まれる一方、サイト固有のレイヤには各サイトに固有の設定が含まれています。たとえば、ネットワーク分析ポリシーの場合、サイト A にはモニタ対象ネットワークに Web サーバがないため、保護したり、HTTP インスペクションプリプロセッサのオーバーヘッドを処理したりする必要はありませんが、両方のサイトで TCP ストリームの前処理が必要になる場合があります。両方のサイトで共有する全社的レイヤで TCP ストリーム処理を有効にし、サイト A で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを無効にして、サイト B で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを有効にできます。サイト固有のポリシーで上位レイヤの設定を編集することで、必要に応じて、設定の調整によって各サイトのポリシーをさらに調整することもできます。

この例のマスターポリシーでフラット化された設定値そのものがトラフィックをモニタするのに役立つわけではありませんが、サイト固有のポリシーを設定および更新する際に時間が節約されるため、ポリシー階層で活用することができます。

その他にも多くのレイヤ設定が可能です。たとえば、企業、部門、ネットワーク、さらにはユーザごとにポリシー階層を定義できます。侵入ポリシーの場合は、一方のレイヤに詳細設定を含め、もう一方にルール設定を含めることもできます。

ユーザ設定可能なレイヤを同じタイプの他のポリシー（侵入またはネットワーク分析）と共有できるように設定できます。共有可能レイヤ内の設定を変更し、変更をコミットすると、そのレイヤを共有するすべてのポリシーが更新され、影響を受けたすべてのポリシーのリストが提供されます。レイヤを作成したポリシーの機能設定のみを変更できます。

別のポリシーに追加しているレイヤの共有を無効にすることはできません。まずレイヤを他のポリシーから削除するか、他のポリシーを削除する必要があります。

基本ポリシーが共有するレイヤが作成されたカスタムポリシーである場合、ポリシーに共有レイヤを追加することはできません。追加した場合、ポリシーで依存関係が循環することになります。

マルチドメイン展開では、先祖ポリシーの共有レイヤを子孫ドメインのポリシーに追加できません。

## レイヤの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

### 手順

**ステップ 1** ポリシーの編集集中に、ナビゲーションパネルで[ポリシー層 (Policy Layers)]をクリックします。

**ステップ 2** [ポリシー層 (Policy Layers)] ページでは、次に示す管理アクションを実行できます。

- 別のポリシーからの共有レイヤの追加：[ユーザレイヤ (User Layers)] の横にある共有レイヤの追加アイコン (⊕) をクリックし、[共有レイヤの追加 (Add Shared Layer)] ドロップダウンリストからレイヤを選択して、[OK] をクリックします。
- 非共有レイヤの追加：[ユーザレイヤ (User Layers)] の横にあるレイヤの追加アイコン (⊕) をクリックし、[名前 (Name)] を入力して、[OK] をクリックします。
- レイヤの説明の追加または変更：レイヤの横にある編集アイコン (✎) をクリックして、[説明 (Description)] を追加または変更します。
- 別のポリシーとのレイヤの共有の許可：レイヤの横にある編集アイコン (✎) をクリックして、[共有 (Sharing)] チェックボックスをオフにします。

- レイヤの名前の変更：レイヤの横にある編集アイコン (✎) をクリックして、[名前 (Name)] を変更します。
- レイヤのコピー：レイヤのコピーアイコン (📄) をクリックします。
- レイヤの削除：レイヤの削除アイコン (🗑️) をクリックして、[OK] をクリックします。
- 2つのレイヤのマージ：2つのレイヤの上部のマージアイコン (📄) をクリックして、[OK] をクリックします。
- レイヤの移動：レイヤサマリ内の任意の空いている場所をクリックし、位置矢印 (👉) が移動するレイヤの上または下の行を指すまでドラッグします。

**ステップ3** 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## レイヤ間のナビゲーション

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

#### 手順

**ステップ1** ポリシーの編集中に、ナビゲーションパネルで[ポリシー層 (Policy Layers)] をクリックします。

**ステップ2** レイヤの移動は、次のいずれかのアクションで実行できます。

- プリプロセッサ ページまたは詳細設定ページにアクセスする：レイヤ レベルのプリプロセッサまたは詳細設定の設定ページにアクセスするには、そのレイヤに対応する行の機能名をクリックします。基本ポリシーおよび共有レイヤでは、設定ページは読み取り専用です。
- ルール ページにアクセスする：ルールの状態タイプでフィルタ処理されたレイヤ レベルのルール設定ページにアクセスする場合は、レイヤの概要でイベントのドロップおよび生

成アイコン (✖)、イベントの生成アイコン (➡)、または無効化アイコン (➡) をクリックします。選択したルール状態に設定されているルールがレイヤに含まれていない場合、ルールは表示されません。

- [ポリシー情報ページ (Policy Information)] ページを表示する : [ポリシー情報ページ (Policy Information)] ページを表示するには、ナビゲーション ウィンドウで [ポリシーの概要 (Policy Summary)] をクリックします。
- レイヤの概要ページを表示する : レイヤの概要ページを表示するには、レイヤに対応する行のレイヤ名をクリックするか、ユーザ レイヤの横にある編集アイコン (✎) をクリックします。表示アイコン (🔍) をクリックして、共有レイヤの読み取り専用のサマリ ページにアクセスすることもできます。

**ステップ 3** 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

---

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[競合と変更 : ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## レイヤでの侵入ルール

レイヤの [ルール (Rules)] ページで個々のレイヤ設定を表示することも、[ルール (Rules)] ページのポリシー ビューですべての設定の最終的な効果を表示することもできます。[ルール (Rules)] ページのポリシー ビューのルール設定を変更する場合、ポリシーの最上位のユーザ設定可能なレイヤを変更します。[ルール (Rules)] ページにあるレイヤ ドロップダウンリストを使用して、別のレイヤに切り替えることができます。

次の表では、複数のレイヤで同じ種類の設定を構成した場合の結果について説明しています。

表 99: レイヤルールの設定

設定可能なレイヤ数	設定の種類	目的
1	ルール状態	<p>下位レイヤのルールに対して設定されたルール状態を上書きします。また、下位レイヤで設定されたそのルールのすべてのしきい値、抑制、レートベースのルール状態、およびアラートを無視します。</p> <p>基本ポリシーまたは下位レイヤからルールのルール状態を継承したい場合は、ルール状態を [継承 (Inherit)] に設定します。侵入ポリシーの [ルール (Rules)] ページは、すべてのルール設定の最終的な効果を示す複合ビューであるため、このページでの作業中にルールの状態を [継承 (Inherit)] に設定することはできないことに注意してください。</p>
1	しきい値 SNMP アラート	<p>下位レイヤのルールの同じ種類の設定を上書きします。しきい値を設定すると、レイヤのルールの既存のしきい値が上書きされることに注意してください。</p>
1 つ以上	抑制 レートベースのルール状態	<p>選択した各ルールの同じ種類の設定を、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせます。ルール状態が設定されているレイヤより下の設定は無視されます。</p>
1 つ以上	コメント	<p>ルールにコメントを追加します。コメントは、ポリシー固有またはレイヤ固有ではなく、ルール固有です。任意のレイヤの 1 つのルールに 1 つ以上のコメントを追加できます。</p>

たとえば、あるレイヤでルール状態を [ドロップしてイベントを生成する (Drop and Generate Events)] に設定し、それよりも上位のレイヤで [無効 (Disabled)] に設定した場合、侵入ポリシーの [ルール (Rules)] ページには、ルールが無効であることが示されます。

別の例として、あるレイヤでルールの送信元ベースの抑制を 192.168.1.1 に設定し、別のレイヤでそのルールの宛先ベースの抑制を 192.168.1.2 に設定した場合、[ルール (Rules)] ページに



は、送信元アドレス 192.168.1.1 と宛先アドレス 192.168.1.2 に関するイベントを抑制する累積的な結果が示されます。抑制およびレートベースのルール状態の設定では、選択した各ルールの同じ種類の設定が、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせられることに注意してください。ルール状態が設定されているレイヤより下の設定は無視されます。

特定のレイヤの各 [ルール (Rules)] ページの色分けでは、有効状態が上位レイヤ、下位レイヤ、現在のレイヤのどれに該当するのかが次の色で示されます。

- 赤：上位レイヤでの有効状態
- 黄色：下位レイヤでの有効状態
- 陰影なし：現在のレイヤでの有効状態

侵入ポリシーの [ルール (Rules)] ページはすべてのルール設定の最終的な効果の複合ビューであるため、ルール状態はこのページでは色分けされません。

## レイヤでの侵入ルールの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入ポリシーでは、すべてのユーザ設定可能なレイヤのルールに対して、ルール状態、イベントフィルタリング、動的状態、アラート、およびルールコメントを設定できます。変更を加えるレイヤにアクセスした後、そのレイヤの [ルール (Rules)] ページの設定を、侵入ポリシーの [ルール (Rules)] ページの設定と同じように追加します。

### 手順

**ステップ 1** 侵入ポリシーの編集に、ナビゲーションパネルで [ポリシー層 (Policy Layers)] を展開します。

**ステップ 2** 変更するポリシー階層を展開します。

**ステップ 3** 変更するポリシーレイヤのすぐ下にある [ルール (Rules)] をクリックします。

**ステップ 4** [ルールを使用した侵入ポリシーの調整 \(1619 ページ\)](#) に示されている任意の設定を変更します。

**ヒント** 編集可能なレイヤから個々の設定を削除するには、そのレイヤの [ルール (Rules)] ページでルールメッセージをダブルクリックして、ルールの詳細を表示します。削除する設定の横にある [削除 (Delete)] をクリックして [OK] を 2 回クリックします。

**ステップ 5** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## 複数のレイヤからのルール設定の削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入ポリシーの複数のレイヤから、特定のタイプのイベントフィルタ、動的状態、またはアラートを同時に削除できます。システムは選択された設定を削除し、ルールの残りの設定をポリシーの最上位の編集可能なレイヤにコピーします。

システムは、すべての設定を削除するか、ルール状態がルールに対して設定されているレイヤに遭遇するまで、下位方向にある各レイヤの同じ種類の設定を削除します。後者の場合、そのレイヤから設定が削除され、設定タイプの削除が停止されます。

共有レイヤまたは基本ポリシーで同じタイプの設定に遭遇したときに、ポリシーの最上位のレイヤが編集可能である場合、システムはそのルールの残りの設定およびルール状態をその編集可能なレイヤにコピーします。そうではない場合、ポリシーの最上位のレイヤが共有レイヤであれば、システムは新しい編集可能なレイヤをその共有レイヤの上に作成し、そのルールの残りの設定およびルール状態をその編集可能なレイヤにコピーします。



- (注) 共有レイヤまたは基本ポリシーから派生したルール設定を削除すると、下位レイヤまたは基本ポリシーからこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーからの変更を無視しないようにするには、最上位のレイヤのサマリーページでルール状態を[継承 (Inherit)] に設定します。

### 手順

- ステップ 1** 侵入ポリシーの編集に、ナビゲーション ウィンドウで [ポリシー情報 (Policy Information)] のすぐ下にある [ルール (Rules)] をクリックします。

ヒント また、任意のレイヤの [ルール (Rules) ] ページでレイヤのドロップダウンリストから [ポリシー (Policy) ] を選択するか、[ポリシー情報 (Policy Information) ] ページの [ルールの管理 (Manage Rules) ] をクリックすることもできます。

**ステップ 2** 複数の設定を削除するルールを選択します。

- 特定の選択 (Choose specific) : 特定のルールを選択するには、各ルールの横にあるチェックボックスをオンにします。
- すべて選択 (Choose all) : 現在のリストのルールをすべて選択するには、列の上部にあるチェックボックスをオンにします。

**ステップ 3** 次のいずれかのオプションを選択します。

- [イベントのフィルタリング (Event Filtering) ] > [しきい値の削除 (Remove Thresholds) ]
- [イベントのフィルタリング (Event Filtering) ] > [抑制の削除 (RemoveSuppressions) ]
- [動的状態 (Dynamic State) ] > [レート ベースのルール状態の削除 (Remove Rate-Based Rule States) ]
- [アラート (Alerting) ] > [SNMP アラートの削除 (Remove SNMP Alerts) ]

(注) 共有レイヤまたは基本ポリシーから派生したルール設定を削除すると、下位レイヤまたは基本ポリシーからこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーからの変更を無視しないようにするには、最上位のレイヤのサマリー ページでルール状態を [継承 (Inherit) ] に設定します。

**ステップ 4** [OK] をクリックします。

**ステップ 5** 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報 (Policy Information) ] をクリックし、[変更の確定 (Commit Changes) ] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

### 次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

### 関連トピック

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## カスタム基本ポリシーからのルール変更の受け入れ

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

レイヤを追加していないカスタムネットワーク分析ポリシーまたは侵入ポリシーが別のカスタムポリシーを基本ポリシーとして使用するとき、以下を行う場合は、そのルール状態を継承するようにルールを設定する必要があります。

- 基本ポリシーのルールに設定されたイベント フィルタ、動的状態、または SNMP アラートを削除する場合
- 基本ポリシーとして使用する他のカスタムポリシー内のルールに行った後続の変更をルールが受け入れるようにする場合

## 手順

**ステップ 1** 侵入ポリシーの編集集中に、ナビゲーションパネルで [ポリシー層 (Policy Layers)] を展開します。

**ステップ 2** [個人用の変更 (My Changes)] を展開します。

**ステップ 3** [個人用の変更 (My Changes)] のすぐ下にある [ルール (Rules)] リンクをクリックします。

**ステップ 4** 設定を受け入れるルールを選択します。次の選択肢があります。

- [特定ルールの選択 (Choose specific rules)] : 特定のルールを選択するには、各ルールの横にあるチェックボックスをチェックします。
- [すべてのルールを選択 (Choose all rules)] : 現在のリストのすべてのルールを選択する場合は、列の最上部にあるチェックボックスをチェックします。

**ステップ 5** [ルール状態 (Rule State)] ドロップダウンリストから、[継承 (Inherit)] を選択します。

**ステップ 6** 最後のコミットからポリシーに加えられた変更を保存するには、[ポリシー情報 (Policy information)] をクリックし、次に [変更をコミット (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

## 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## 関連トピック

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

# レイヤでのプリプロセッサと詳細設定

ネットワーク分析ポリシーでプリプロセッサを設定するときと、侵入ポリシーで詳細詳細を設定するときのメカニズムは同様です。プリプロセッサの有効化および無効化はネットワーク分析の [設定 (Settings)] ページで行うことができ、侵入ポリシーの詳細設定の有効化および無効化は侵入ポリシーの [詳細設定 (Advanced Settings)] ページで行うことができます。これらのページでは、すべての関連機能の有効な状態の概要も示されます。たとえば、ネットワーク

分析SSLプリプロセッサが、あるレイヤでは無効になっていて上位レイヤでは有効になっている場合、[設定 (Settings)] ページにはプリプロセッサが有効であるとして表示されます。これらのページで行った変更は、ポリシーの最上位レイヤに表示されます。Back Orifice プリプロセッサにはユーザ設定可能なオプションがないことに注意してください。

また、プリプロセッサまたは詳細設定を有効化または無効化したり、ユーザ設定可能なレイヤのサマリー ページの設定 ページにアクセスしたりできます。このページで、レイヤの名前および説明を変更し、レイヤを同じタイプの他のポリシーと共有するかどうかを設定できます。ナビゲーションパネルの [ポリシー層 (Policy Layers)] の下のレイヤの名前を選択することによって、別のレイヤのサマリー ページに切り替えることができます。

プリプロセッサまたは詳細設定を有効にすると、その機能の設定 ページへのサブリンクがナビゲーションパネルのレイヤの名前の下に表示され、編集アイコン (✎) がそのレイヤのサマリー ページの機能の横に表示されます。レイヤで機能を無効にしたり、[継承 (Inherit)] に設定した場合はこれらは表示されません。

プリプロセッサまたは詳細設定の状態 (有効または無効) を設定すると、下位レイヤでのその機能の状態と構成設定が上書きされます。プリプロセッサまたは詳細設定についてその状態と設定を基本ポリシーまたは下位レイヤから継承する場合、状態を [継承 (Inherit)] に設定します。[設定 (Settings)] または [詳細設定 (Advanced Settings)] ページで操作するときには、[継承 (Inherit)] の選択項目は使用できないことに注意してください。また、現在有効にされている機能を継承すると、ナビゲーションパネルではその機能のサブリンクが表示されなくなり、設定 ページではその機能の編集アイコンが表示されなくなることに注意してください。

システムは、機能が有効にされている最上位レイヤの設定を使用します。設定を明示的に変更しなかった場合は、デフォルト設定が使用されます。たとえば、あるレイヤでネットワーク分析 DCE/RPC プリプロセッサを有効にして変更し、それより上位のレイヤでプリプロセッサを有効にするが変更はしない場合、システムは上位レイヤのデフォルト設定を使用します。

各レイヤのサマリー ページは次のようにカラーコード化されており、有効な設定が上位レイヤ、下位レイヤ、または現在のレイヤのいずれにあるかが示されます。

- 赤色：有効な設定は上位レイヤにあります
- 黄色：有効な設定は下位レイヤにあります
- 陰影なし：有効な設定は現在のレイヤにあります

[設定 (Settings)] および [詳細設定 (Advanced Settings)] ページは、関連するすべての設定の複合ビューであるため、これらのページは有効な設定の位置を示すためにカラーコーディングを使用しません。

## 層のプリプロセッサと詳細の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

## 手順

---

**ステップ1** ポリシーの編集集中に、ナビゲーションパネルで[ポリシー層 (Policy Layers)]を展開し、変更するレイヤの名前をクリックします。

**ステップ2** 次の選択肢があります。

- 層の名前を変更します。
- 説明を追加または変更します。
- [共有 (Sharing)] チェックボックスをオンまたはオフにして、層を別のポリシーと共有できるようにするかどうかを指定します。
- 有効にしたプリプロセッサ/詳細設定の設定ページにアクセスするには、編集アイコン (✎) または機能のサブリンクをクリックします。
- 現在の層のプリプロセッサ/詳細設定を無効にするには、機能の横にある[無効化 (Disabled)] をクリックします。
- 現在の層のプリプロセッサ/詳細設定を有効にするには、機能の横にある[有効化 (Enabled)] をクリックします。
- 現在の層の下にある最上位レイヤの設定からプリプロセッサ/詳細設定の状態および構成を継承するには、[継承 (Inherit)] をクリックします。

**ステップ3** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

---

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 関連トピック

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)



## 第 70 章

# 侵入ポリシーの使用を開始するには

ここでは、侵入ポリシーの使用を開始する方法について説明します。

- [侵入ポリシーの基本 \(1609 ページ\)](#)
- [侵入ポリシーの管理 \(1611 ページ\)](#)
- [カスタム侵入ポリシーの作成 \(1612 ページ\)](#)
- [侵入ポリシーの編集 \(1613 ページ\)](#)
- [インライン展開でのドロップ動作 \(1615 ページ\)](#)
- [侵入ポリシーの詳細設定 \(1616 ページ\)](#)
- [侵入検知および防御のパフォーマンスの最適化 \(1618 ページ\)](#)

## 侵入ポリシーの基本

侵入ポリシーは定義済みの侵入検知のセットであり、セキュリティ違反についてトラフィックを検査し、インライン展開の場合は、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーは、アクセスコントロールポリシーによって呼び出され、システムの最終防御ラインとして、トラフィックが宛先に到達することを許可するかどうかを判定します。

各侵入ポリシーの中核となるのは、侵入ルールです。ルールを有効にすると、ルールに一致するトラフィックに対して侵入イベントが生成されます（さらに、必要に応じてトラフィックがブロックされます）。ルールを無効にすると、ルールの処理が停止されます。

Firepower システムが提供するいくつかの基本的な侵入ポリシーにより、Cisco Talos Security Intelligence and Research Group (Talos) の経験を活用できます。これらのポリシーに対して、Talos は侵入およびプリプロセッサ ルールの状態（有効または無効）を設定し、他の詳細設定の初期設定も行います。



**ヒント** システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。

カスタム侵入ポリシーを作成すると、以下を実行できます。

- ルールを有効化/無効化することに加え、独自のルールを作成して追加し、検出を調整する。
- ネットワーク上で検出されたオペレーティングシステム、サーバ、およびクライアントアプリケーションプロトコルをそれらの資産を保護するために明確に書き込まれたルールに関連付けるには、Firepower の推奨事項を使用します。
- 外部アラート、センシティブデータの前処理、グローバルルールのしきい値設定など、さまざまな詳細設定を設定する。
- レイヤを構成要素として使用し、複数の侵入ポリシーを効率的に管理する。

インライン展開では、侵入ポリシーによってトラフィックを変更したりブロックすることができます。

- 廃棄ルールを使用すると、一致したパケットをドロップして、侵入イベントを生成できます。侵入またはプリプロセッサの廃棄ルールを設定するには、そのステータスを [ドロップしてイベントを生成する (Drop and Generate Events) ] に設定します。
- 侵入ルールでは、replace キーワードを使用して悪意のあるコンテンツを置き換えることができます。

侵入ルールがトラフィックに影響を与えるようにするには、廃棄ルールおよびコンテンツを置き換えるルールを適切に設定し、さらに管理対象デバイスを適切にインライン展開する（つまり、インラインインターフェイスセットを設定する）必要があります。最後に、侵入ポリシーのドロップ動作（[インライン時にドロップ (Drop when Inline) ] 設定）を有効にします。

留意事項として、侵入ポリシーを調整する場合（特にルールを有効化して追加する場合）、一部の侵入ルールでは、最初に特定の手法でトラフィックをデコードまたは前処理する必要があります。侵入ポリシーによって検査される前に、パケットはネットワーク分析ポリシーの設定に従って前処理されます。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。



**注意** 前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度なタスク**です。



カスタム侵入ポリシーを設定した後、それを1つ以上のアクセスコントロールルールまたはアクセスコントロールポリシーのデフォルトアクションに関連付けることによって、カスタム侵入ポリシーをアクセスコントロール設定の一部として使用できます。これによって、システムは、最終宛先に渡す前に、特定の許可されたトラフィックを侵入ポリシーによって検査します。変数セットを侵入ポリシーと組み合わせて使用することにより、ホームネットワークと外部ネットワークに加えて、必要に応じてネットワーク上のサーバを正確に反映させることができます。

デフォルトでは、暗号化ペイロードの侵入インスペクションは無効化されます。これにより、侵入インスペクションが設定されているアクセスコントロールルールと暗号化された接続を照合する際の誤検出が減少し、パフォーマンスが向上します。

## 侵入ポリシーの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

[侵入ポリシー (Intrusion Policy)] ページ ([ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)]) では、次に示す情報とともに、現在のカスタム侵入ポリシーを表示できます。

- ポリシーが最後に変更された日時 (ローカル時間) とそれを変更したユーザ
- [インライン時にドロップ (Drop when Inline)] 設定が有効になっているかどうか。この設定が有効な場合、インライン展開でトラフィックをドロップしたり変更することができます。
- トラフィックの検査に侵入ポリシーを使用しているアクセスコントロールポリシーとデバイス
- ポリシーに保存されていない変更があるかどうか、およびポリシーを現在編集している人 (いれば) に関する情報
- マルチドメイン展開では、ポリシーが作成されたドメイン

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

### 手順

- ステップ 1 [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。

ステップ2 侵入ポリシーを管理します。

- [比較 (Compare) ]: [ポリシーの比較 (Compare Policies) ]をクリックします ([ポリシーの比較 \(361 ページ\)](#) を参照)。
- 作成: [ポリシーの作成 (Create Policy) ]をクリックします。 [カスタム侵入ポリシーの作成 \(1613 ページ\)](#) を参照してください。
- 削除: 削除するポリシーの横にある削除アイコン (🗑️) をクリックします。別のユーザが保存していないポリシーの変更がある場合は、システムによって確認と通知のプロンプトが表示されます。[OK] をクリックして確認します。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- 編集: 編集するポリシーの横にある編集アイコン (✎) をクリックします。 [侵入ポリシーの編集 \(1613 ページ\)](#) を参照してください。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- エクスポート: 別の Firepower Management Center にインポートするために、侵入ポリシーをエクスポートするには、エクスポートアイコン (📄) をクリックします。 [設定のエクスポート \(214 ページ\)](#) を参照してください。
- 展開: [展開 (Deploy) ]をクリックします ([設定変更の導入 \(350 ページ\)](#) を参照)。
- [レポート (Report) ]: レポートアイコン (📄) をクリックします ([現在のポリシー レポートの生成 \(363 ページ\)](#) を参照)。

## カスタム侵入ポリシーの作成

新しい侵入ポリシーを作成する場合は、一意の名前を付けて基本ポリシーを指定し、ドロップ動作を指定する必要があります。

基本ポリシーは侵入ポリシーのデフォルト設定を定義します。新しいポリシーの設定の変更は、基本ポリシーの設定を変更するのではなく、オーバーライドします。システム提供のポリシーまたはカスタムポリシーを基本ポリシーとして使用できます。

侵入ポリシーのドロップ動作、または[インライン時にドロップ (Drop when Inline) ]の設定によって、廃棄ルール (ルール状態が [ドロップしてイベントを生成する (Drop and Generate Events) ] に設定されている侵入ルールまたはプリプロセッサルール)、およびトラフィックに影響を与えるその他の侵入ポリシー設定のシステムにおける処理方法が決まります。悪意のあるパケットをドロップまたは置き換える場合は、インライン展開でドロップ動作を有効にする必要があります。パッシブ展開では、ドロップ動作に関わらず、システムはトラフィックフローに影響を与えることはできません。

## カスタム侵入ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)] を選択します。

**ステップ 2** [ポリシーの作成 (Create Policy)] をクリックします。別のポリシー内に未保存の変更が存在する場合は、[侵入ポリシー (Intrusion Policy)] ページに戻るかどうか尋ねられたときに [キャンセル (Cancel)] をクリックします。

**ステップ 3** [名前 (Name)] に一意の名前を入力し、オプションで [説明 (Description)] を入力します。

**ステップ 4** [基本ポリシー (Base Policy)] で最初の基本ポリシーを指定します。

システム提供のポリシーまたは別のカスタム ポリシーを基本ポリシーとして使用できます。

**ステップ 5** [インライン展開でのドロップ動作の設定 \(1616 ページ\)](#) の説明に従って、インライン導入でのシステムのドロップ動作を設定します。

**ステップ 6** ポリシーを作成します。

- 新しいポリシーを作成して、[侵入ポリシー (Intrusion Policy)] ページに戻るには、[ポリシーの作成 (Create Policy)] をクリックします。新しいポリシーには基本ポリシーと同じ設定項目が含まれています。
- ポリシーを作成し、高度な侵入ポリシーエディタでそれを開いて編集するには、[ポリシーの作成と編集 (Create and Edit Policy)] をクリックします ([侵入ポリシーの変更 \(1615 ページ\)](#) を参照)。

### 関連トピック

[レイヤでの侵入ルール \(1601 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## 侵入ポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

## 手順

**ステップ1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。

**ステップ2** 設定する侵入ポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ3** ポリシーを編集します。

- 基本ポリシーの変更：[基本ポリシー (Base Policy)] ドロップダウンリストから基本ポリシーを選択します。[ベースポリシーの変更 \(1595 ページ\)](#) を参照してください。
- 詳細設定の構成：ナビゲーションパネルで [詳細設定 (Advanced Settings)] をクリックします。[侵入ポリシーの詳細設定 \(1616 ページ\)](#) を参照してください。
- Firepower 推奨ルールの設定：ナビゲーションパネルで [Firepower 推奨ルール (Firepower Recommended Rules)] をクリックします。[Firepower の推奨事項の生成と適用 \(1658 ページ\)](#) を参照してください。
- インライン展開でのドロップ動作：[インライン時にドロップ (Drop when Inline)] をオンまたはオフにします。[インライン展開でのドロップ動作の設定 \(1616 ページ\)](#) を参照してください。
- 推奨ルール状態によるルールのフィルタ：推奨を生成した後、各推奨タイプの横にある [表示 (View)] をクリックします。すべての推奨を表示するには、[推奨される変更の表示 (View Recommended Changes)] をクリックします。
- 現在のルール状態によるルールのフィルタ：ルール状態タイプ (イベントを生成する、ドロップしてイベントを生成する) の横にある [表示 (View)] をクリックします。[侵入ポリシー内の侵入ルールフィルタ \(1628 ページ\)](#) を参照してください。
- ポリシー階層の管理：ナビゲーションパネルで、[ポリシー層 (Policy Layers)] をクリックします。[レイヤ管理 \(1597 ページ\)](#) を参照してください。
- 侵入ルールの管理：[ポリシー情報 (Policy Information)] をクリックします。[侵入ポリシー内の侵入ルールの表示 \(1621 ページ\)](#) を参照してください。
- 基本ポリシーの設定の表示：[基本ポリシーの管理 (Manage Base Policy)] をクリックします。[基本レイヤ \(1592 ページ\)](#) を参照してください。

**ステップ4** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] を選択して、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[Firepower の推奨事項の生成と適用](#) (1658 ページ)

[レイヤでの侵入ルールの設定](#) (1603 ページ)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー](#) (1587 ページ)

## 侵入ポリシーの変更

新しい侵入ポリシーを作成すると、そのポリシーには基本ポリシーと同じ侵入ルールと詳細設定が付与されます。

システムは、ユーザごとに1つのセキュリティポリシーをキャッシュします。侵入ポリシーの編集に、メニューまたは別のページへのパスを選択すると、そのページから移動しても、変更内容はシステム キャッシュに残ります。

## インライン展開でのドロップ動作

実際にトラフィックを変更せず、使用している設定がインライン展開（つまり、ルーテッド、スイッチド、またはトランスペアレントインターフェイス、あるいはインラインインターフェイスペアを使用して、関連する設定がデバイスに展開されている）でどのように機能するかを評価する場合は、ドロップ動作を無効にすることができます。その場合、システムは侵入イベントを生成しますが、廃棄ルールをトリガーしたパケットをドロップしません。結果を確認したら、ドロップ動作を有効化できます。

パッシブ展開またはタップモードでのインライン展開では、ドロップ動作に関わらず、システムはトラフィックに影響を与えることはできません。つまり、パッシブ展開では、[ドロップしてイベントを生成する (Drop and Generate Events)] に設定されたルールは [イベントを生成する (Generate Events)] に設定されたルールと同様に動作します。システムは侵入イベントを生成しますが、パケットをドロップできません。



(注) FTP を介してマルウェアの転送をブロックするには、Firepower の AMP を正しく設定するだけでなく、アクセス コントロール ポリシーのデフォルトの侵入ポリシーで [インライン時にドロップ (Drop when Inline)] を有効にする必要があります。

侵入イベントを表示する際に、ワークフローにインライン結果を含めることができます。インライン結果は、トラフィックが実際にドロップされたのか、あるいはドロップが想定に過ぎなかったのかを示します。

## インライン展開でのドロップ動作の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ポリシーのドロップ動作を設定します。

- [インライン時にドロップ (Drop when Inline)] チェックボックスをオンにして、侵入ルールのトラフィックへの適用とイベントの生成を許可します。
- [インライン時にドロップ (Drop when Inline)] チェックボックスをオフにすると、侵入ルールのトラフィックへの適用が禁止されますが、イベントは生成されます。

**ステップ 4** [変更を確定 (Commit Changes)] をクリックして、最後のポリシーの確定以降に、このポリシーに加えた変更を保存します。

ポリシーの変更を確定しない場合、最後の確定以降の変更は、別のポリシーを編集するときに破棄されます。

### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## 侵入ポリシーの詳細設定

侵入ポリシーの詳細設定を設定するには、特定の専門知識が必要です。デフォルトで有効になる詳細設定や、詳細設定ごとのデフォルトは、侵入ポリシーの基本ポリシーに応じて決まります。

侵入ポリシーのナビゲーションパネルで [詳細設定 (Advanced Settings)] を選択すると、ポリシーの詳細設定がタイプ別に一覧表示されます。[詳細設定 (Advanced Settings)] ページでは、

侵入ポリシーの詳細設定を有効または無効にしたり、詳細設定の設定ページにアクセスすることができます。詳細設定を行うには、それを有効にする必要があります。

詳細設定を無効にすると、サブリンクと [編集 (Edit)] リンクは表示されなくなりますが、設定は保持されます。侵入ポリシーの一部の設定 (センシティブ データ ルール、侵入ルールの SNMP アラート) では、詳細設定を有効化して適切に設定する必要があります。このように誤って設定された侵入ポリシーは保存できません。

詳細設定を変更する場合、変更する設定と、その変更がネットワークに及ぼす可能性のある影響について理解していることが必要です。

### 特定の脅威の検出 (Specific Threat Detection)

機密データ プリプロセッサは、ASCII テキストのクレジットカード番号や社会保障番号などの機密データを検出します。

特定の脅威 (Back Orifice 攻撃、何種類かのポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃) を検出するプリプロセッサは、ネットワーク分析ポリシーで設定します。

### 侵入ルールしきい値 (Intrusion Rule Thresholds)

グローバルルールのしきい値を設定すると、しきい値を使用して、システムが侵入イベントを記録したり表示したりする回数を制限できるので、多数のイベントでシステムが圧迫されないようにすることができます。

### 外部レスポンス (External Responses)

Web インターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、システムログ (syslog) ファシリティへのロギングを有効にしたり、イベントデータを SNMP トラップサーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギングファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。

これらのポリシー単位のアラート設定に加えて、各ルールまたはルールグループの侵入イベントを通知する電子メールアラートをグローバルに有効化/無効化できます。どの侵入ポリシーがパケットを処理するかに関わらず、ユーザの電子メールアラート設定が使用されます。

### 関連トピック

[機密データ検出の基本](#) (1661 ページ)

[グローバルルールのしきい値の基本](#) (1677 ページ)

## 侵入検知および防御のパフォーマンスの最適化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin (access control); Admin/Discovery Admin (network discovery)

Firepower システムを使用して侵入検知および防御を実行するものの検出データを利用する必要がない場合は、以下の説明に従って新しい検出を無効にしてパフォーマンスを最適化できます。

### 手順

- 
- ステップ 1** ターゲット デバイスに導入したアクセス コントロール ポリシーと関連付けられたルールを変更または削除します。そのデバイスに関連付けられたアクセス制御ルールはいずれも、ユーザ、アプリケーション、または URL の条件を指定できません ([アクセス コントロールルールの作成および編集 \(1350 ページ\)](#) を参照)。
- ステップ 2** ターゲット デバイスのネットワーク検出ポリシーからすべてのルールを削除します ([ネットワーク検出ルールの設定 \(2151 ページ\)](#) を参照)。
- ステップ 3** 変更された設定をターゲットデバイスに導入します ([設定変更の導入 \(350 ページ\)](#) を参照)。
-





## 第 71 章

# ルールを使用した侵入ポリシーの調整

ここでは、ルールを使用して侵入ポリシーを調整する方法について説明します。

- [侵入ルールの調整の基本 \(1619 ページ\)](#)
- [侵入ルールのタイプ \(1620 ページ\)](#)
- [侵入ポリシー内の侵入ルールの表示 \(1621 ページ\)](#)
- [侵入ポリシー内の侵入ルールフィルタ \(1628 ページ\)](#)
- [侵入ルールの状態 \(1639 ページ\)](#)
- [侵入ポリシーの侵入イベント通知のフィルタ \(1641 ページ\)](#)
- [動的侵入ルール状態 \(1649 ページ\)](#)
- [侵入ルールのコメントの追加 \(1653 ページ\)](#)

## 侵入ルールの調整の基本

侵入ポリシーの [ルール (Rules)] ページを使用して、共有オブジェクトルール、標準テキストルール、プリプロセッサルールに関するルール状態とその他の設定を構成できます。

ルールは、ルール状態を [イベントを生成する (Generate Events)] または [ドロップしてイベントを生成する (Drop and Generate Events)] に設定することによって有効にします。ルールを有効にすると、システムがそのルールと一致するトラフィックに対するイベントを生成します。ルールを無効にすると、ルールの処理が停止されます。また、インライン展開で [ドロップしてイベントを生成する (Drop and Generate Events)] に設定されたルールによって、一致するトラフィックに対するイベントが生成され、そのトラフィックが破棄されるように、侵入ポリシーを設定できます。パッシブ展開では、[ドロップしてイベントを生成する (Drop and Generate Events)] に設定されたルールによって、一致するトラフィックに対するイベントが生成されるだけです。

ルールのサブセットを表示するようにルールをフィルタ処理することによって、ルール状態やルール設定を変更するルールのセットを正確に選択できます。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。

## 侵入ルールのタイプ

侵入ルールとは、ネットワーク内の脆弱性を不正利用する試みを検出するためにシステムが使用する、指定されたキーワードと引数のセットのことです。システムはネットワークトラフィックを分析する際に、パケットを各ルールに指定された条件に照らし合わせ、データパケットがルールに指定されたすべての条件を満たす場合、そのルールをトリガーします。

侵入ポリシーには以下の構成要素があります。

- 侵入ルール。共有オブジェクトルールと標準テキストルールに分割されます。
- プリプロセッサルール。パケットデコーダの検出オプション、またはFirepowerシステムに付属のプリプロセッサの1つに関連付けられます。

次の表に、以上のルールタイプの属性を要約します。

表 100: 侵入ルールのタイプ

タイプ (Type)	ジェネレータ ID (GID)	Snort ID (SID)	ソース (Source)	コピーの可否	編集の可否
共有オブジェクトルール	3	1000000 未満	Cisco Talos Security Intelligence and Research Group (Talos)	Yes	制限付き
標準テキストルール	1	1000000 未満	Talos	Yes	制限付き
		1000000 以上	ユーザが作成またはインポート	Yes	Yes
プリプロセッサルール	デコーダまたはプリプロセッサに固有	1000000 未満	Talos	No	No
		1000000 以上	オプション設定時にシステムにより生成	No	No

Talos によって作成されたルールを変更して保存することはできませんが、変更されたルールのコピーをカスタムルールとして保存することはできます。ルールで使用される変数またはルールヘッダー情報情報 (送信元と宛先のポートや IP アドレスなど) を変更できます。マルチドメイン展開では、Talos によって作成されるルールはグローバルドメインに属します。子孫ドメインの管理者は、ルールのローカルコピーを保存してから、ルールを編集できます。

Talos によって作成されるルールには、各デフォルト侵入ポリシー内でデフォルトのルール状態が割り当てられます。ほとんどのプリプロセッサルールがデフォルトで無効になっているため、システムにプリプロセッサルールに対するイベントの生成とインライン展開での違反パケットの破棄を行わせる場合は、これらのルールを有効にする必要があります。

マルチドメイン展開では、子孫ドメインで作成されたか、または子孫ドメインにインポートされたカスタムルールの SID の先頭にドメイン番号が追加されます。たとえば、グローバルドメインに追加されたルールに 1000000 以上の SID があり、子孫ドメインに追加されたルールには [ドメイン番号]1000000 以上の SID があります。

## 侵入ポリシー内の侵入ルールの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入ポリシーでのルールの表示方法を調整でき、複数の条件によってルールをソートできます。特定のルールの詳細を表示して、ルール設定、ルールドキュメント、およびその他のルール仕様を確認することもできます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーションパネルの [ポリシー情報 (Policy Information)] の下にある [ルール (Rules)] をクリックします。







**ステップ 4** ルールを表示している間、以下を実行できます。

- [侵入ポリシー内のルールフィルタの設定 \(1638ページ\)](#) の説明に従ってルールをフィルタリングします。
- ソートの基準とするカラムの一番上のタイトルまたはアイコンをクリックすることによって、ルールをソートします。
- [侵入ルール詳細の表示 \(1623ページ\)](#) の説明に従って、侵入ルールの詳細を表示します。
- [ポリシー (Policy)] ドロップダウンリストから階層を選択することによって、異なるポリシー階層のルールを表示します。

## [侵入ルール (Intrusion Rules)] ページの列

[侵入ルール (Intrusion Rules)] ページでは、メニューバーおよび列ヘッダーに同じアイコンが使用されます。たとえば、[ルール状態 (Rule State)] メニューでは、ルールリストの [ルール状態 (Rule State)] 列と同じアイコン (➡) が使用されます。

表 101: [ルール (Rules) ] ページの列

見出し	説明
GID	ルールのジェネレータ ID (GID) を表す整数。
SID	ルールの固有識別子として機能する Snort ID (SID) を表す整数。 カスタム ルールの場合、SID は 1000000 以上です。 マルチドメイン展開では、子孫ドメインで作成されたか、または子孫ドメインにインポートされたカスタム ルールの SID の先頭にドメイン番号が追加されます。たとえば、グローバルドメインに追加されたルールに 1000000 以上の SID があり、子孫ドメインに追加されたルールには [ドメイン番号]000000 以上の SID があります。
メッセージ	このルールによって生成されるイベントに含まれるメッセージ。ルールの名前としても機能します。
	ルールのルール状態。 <ul style="list-style-type: none"> <li>ドロップしてイベントを生成する (✖)</li> <li>イベントを生成する (➡)</li> <li>無効 (➡)</li> </ul> <p>無効なルールのアイコンは、トラフィックをドロップせずにイベントを生成するように設定されたルールのアイコンのグレー表示されたバージョンです。また、ルールのルール状態アイコンをクリックすると、ルール状態を変更できます。</p>
	ルールの Firepower 推奨ルール状態。
	ルールに適用されるイベントしきい値やイベント抑制などのイベント フィルタ。
	ルールの動的ルール状態。指定されたレート異常が発生した場合に有効になります。
	ルールに対して設定されたアラート (現在は SNMP アラートのみ)。
	ルールに追加されたコメント。

レイヤのドロップダウンリストを使用して、ポリシー内の他のレイヤの [ルール (Rules) ] ページに切り替えることもできます。ポリシーにレイヤを追加しなかった場合にドロップダウンリストに表示される編集可能なビューはポリシーの [ルール (Rules) ] ページと、元は My Changes という名前だったポリシー階層の [ルール (Rules) ] ページだけであることに注意してください。これらのビューの一方を変更すると、もう一方も同じように変更されることにも注意してください。ドロップダウンリストには、読み取り専用の基本ポリシーの [ルール (Rules) ] ページも表示されます。

## 侵入ルールの詳細

[ルールの詳細 (Rule Detail)] ビューで、ルールドキュメント、Firepower の推奨事項、およびルールオーバーヘッドを表示できます。また、ルール固有の機能を表示および追加できます。

表 102: ルールの詳細

項目	説明
要約	ルールの概要。ルールベースのイベントでは、ルールドキュメントに概要情報が含まれている場合にこの行が表示されます。
ルール状態 (Rule State)	ルールの現在のルール状態。ルール状態が設定された階層も示します。
Firepower の推奨事項 (Firepower Recommendation)	Firepower の推奨事項が生成されている場合は、推奨されるルール状態を表すアイコン。[侵入ルール (Intrusion Rules)] ページの列 (1621 ページ) を参照してください。ルールを有効にすることが推奨されている場合、システムは推奨事項をトリガーしたネットワーク アセットまたは設定も示します。
ルールのオーバーヘッド (Rule Overhead)	システム パフォーマンスに対するルールの潜在的影響とルールが誤検出を引き起こす確率。脆弱性にマップされていないローカルルールにはオーバーヘッドが割り当てられていません。
しきい値	このルールに現在設定されているしきい値と、ルールのしきい値を追加するための機能。
抑制 (Suppressions)	このルールに現在設定されている抑制設定と、ルールの抑制を追加するための機能。
動的状態 (Dynamic State)	このルールに現在設定されているレートベースのルール状態と、ルールの動的ルール状態を追加するための機能。
アラート (Alerts)	このルールに設定されている SNMP アラートと、ルールのアラートを追加するための機能。
説明	このルールに追加されたコメントと、ルールのコメントを追加するための機能。
資料	Cisco Talos Security Intelligence and Research Group (Talos) によって提供される現在のルールのルールドキュメント。

## 侵入ルール詳細の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

## 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション ペインで [ルール (Rules)] をクリックします。

**ステップ 4** ルールの詳細を表示したいルールをクリックし、ページの下部にある [詳細の表示 (Show Details)] をクリックします。

[侵入ルールの詳細 \(1623 ページ\)](#) で説明されているように、ルールの詳細が表示されます。

**ステップ 5** ルールの詳細から、以下を設定できます。

- アラート: [侵入ルールの SNMP アラートの設定 \(1627 ページ\)](#) を参照してください。
- コメント: [侵入ルールへのコメントの追加 \(1628 ページ\)](#) を参照してください。
- ダイナミックルールの状態: [\[ルール詳細 \(Rule Details\)\] ページからの動的ルール状態の設定 \(1626 ページ\)](#) を参照してください。
- しきい値: [侵入ルールのしきい値の設定 \(1624 ページ\)](#) を参照してください。
- 抑制: [侵入ルールの抑制の設定 \(1625 ページ\)](#) を参照してください。

## 侵入ルールのしきい値の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

[ルールの詳細 (Rule Detail)] ページで、ルールの単一のしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

無効な値を入力するとフィールドに復元アイコン (↺) が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

## 手順

**ステップ 1** 侵入ルールの詳細で、[しきい値 (Thresholds)] の横にある [追加 (Add)] をクリックします。

**ステップ 2** [タイプ (Type)] ドロップダウンリストから、設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベントインスタンス数に通知を制限する場合は、[制限 (Limit)] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[しきい値 (Threshold)] を選択します。
- 指定されたイベントインスタンス数に達した後で、期間あたり1回ずつ通知を提供する場合は、[両方 (Both)] を選択します。

**ステップ 3** [追跡対象 (Track By)] ドロップダウンリストから、[送信元 (Source)] または [宛先 (Destination)] を選択し、イベントインスタンスが送信元 IP アドレスまたは宛先 IP アドレスのどちらによって追跡されるかを指定します。

**ステップ 4** [カウント (Count)] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

**ステップ 5** [秒数 (Seconds)] フィールドに、イベント インスタンスを追跡する期間 (秒数) を指定する数値を入力します。

**ステップ 6** [OK] をクリックします。

ヒント [イベントフィルタリング (Event Filtering)] 列のルールの横にイベント フィルタ アイコン (🔍) が表示されます。ルールに複数のイベント フィルタを追加すると、アイコン上にイベント フィルタの数が表示されます。

## 侵入ルールの抑制の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入ポリシーのルールに対して1つ以上の抑制を設定できます。

無効な値を入力するとフィールドに復元アイコン (↺) が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

### 手順

**ステップ 1** 侵入ルールの詳細で、[抑制 (Suppressions)] の横にある [追加 (Add)] をクリックします。

**ステップ 2** [抑制タイプ (Suppression Type)] ドロップダウンリストから、次のいずれかのオプションを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[ルール (Rule)] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元 (Source)] を選択します。

[ルール詳細 (Rule Details)] ページからの動的ルール状態の設定

- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先 (Destination)] を選択します。

**ステップ 3** 抑制タイプとして [送信元 (Source)] または [宛先 (Destination)] を選択した場合は、[ネットワーク (Network)] フィールドに IP アドレス、アドレス ブロック、またはそれらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。

侵入ポリシーがアクセス コントロール ポリシーのデフォルト アクションに関連付けられている場合は、デフォルトアクション変数セットでネットワーク変数を指定または列挙することもできます。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

**ステップ 4** [OK] をクリックします。

**ヒント** 抑制するルールの横にある [イベント フィルタリング (Event Filtering)] 列のルールの横にあるイベントフィルタアイコン (🔍) が表示されます。ルールに複数のイベントフィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

[ルール詳細 (Rule Details)] ページからの動的ルール状態の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

1 つのルールに対して 1 つ以上の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2 つの動的ルール状態が競合している場合は、最初のアクションが実行されます。

動的ルール状態はポリシー固有です。

無効な値を入力するとフィールドに復元アイコン (↺) が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

手順

**ステップ 1** 侵入ルールの詳細で、[動的状態 (Dynamic State)] の横にある [追加 (Add)] をクリックします。

**ステップ 2** [追跡対象 (Track By)] ドロップダウンリストから、ルール一致の追跡方法を指定するオプションを選択します。



- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[送信元 (Source)] を選択します。
- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[宛先 (Destination)] を選択します。
- そのルールのすべての一致を追跡する場合は、[ルール (Rule)] を選択します。

**ステップ 3** [追跡対象 (Track By)] を [送信元 (Source)] または [宛先 (Destination)] に設定した場合は、[ネットワーク (Network)] フィールドに追跡する各ホストのアドレスを入力します。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン 展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

**ステップ 4** [レート (Rate)] の横で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [カウント (Count)] フィールドで、しきい値として使用するルール一致の数を指定します。
- [秒 (Seconds)] フィールドで、攻撃を追跡する期間を表す秒数を指定します。

**ステップ 5** [新しい状態 (New State)] ドロップダウンリストから、条件が満たされたときに実行する新しいアクションを選択します。

**ステップ 6** [タイムアウト (Timeout)] フィールドに値を入力します。

タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションがタイムアウトしないようにする場合は、0 を入力します。

**ステップ 7** [OK] をクリックします。

**ヒント** [動的状態 (Dynamic State)] 列のルールの横に動的状態アイコン (🔄) が表示されます。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

## 侵入ルールの SNMP アラートの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

[ルールの詳細 (Rule Detail)] ページで、ルールの SNMP アラートを設定できます。

### 手順

侵入ルールの詳細で、[アラート (Alerts)] の横にある [SNMP アラートの追加 (Add SNMP Alert)] をクリックします。

**ヒント** [アラート (Alerting)] 列のルールの横にアラートアイコン (🚨) が表示されます。ルールに複数のアラートを追加した場合は、アイコン上にアラートの数が表示されません。

## 侵入ルールへのコメントの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

### 手順

**ステップ 1** 侵入ルールの詳細で、[コメント (Comments)] の横の [追加 (Add)] をクリックします。

**ステップ 2** [コメント (Comments)] フィールドに、ルールコメントを入力します。

**ステップ 3** [OK] をクリックします。

**ヒント** システムは [コメント (Comments)] カラムのルールの横にコメントアイコン (💬) を表示します。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

**ステップ 4** ルールコメントを削除するには、ルールコメントセクションで [削除 (Delete)] をクリックします。侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけコメントを削除できます。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 侵入ポリシー内の侵入ルール フィルタ


[ルール (Rules)] ページに表示するルールは、1つの基準または1つ以上の基準の組み合わせに基づいてフィルタ処理できます。


ルールフィルタ キーワードは、ルール状態やイベントフィルタなどのルール設定を適用するルールを見つけやすくします。[ルール (Rules)] ページのフィルタ パネルで必要な引数を選択することによって、キーワードでフィルタ処理すると同時に、キーワードの引数を選択することができます。

## 侵入ルール フィルタの注意事項

作成したフィルタが [フィルタ (Filter)] テキストボックスに表示されます。フィルタ パネルでキーワードとキーワード引数をクリックしてフィルタを作成できます。複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[カテゴリ (Category)] で [プリプロセッサ (preprocessor)] を選択してから、[ルール コンテンツ (Rule Content)] > [GID] の順に選択して、「116」と入力すると、プリプロセッサルールで、かつ、GID が 116 のすべてのルールを取得する「Category: "preprocessor" GID: "116"」というフィルタが返されます。

[カテゴリ (Category)]、[Microsoft 脆弱性 (Microsoft Vulnerabilities)]、[Microsoft ワーム (Microsoft Worms)]、[プラットフォーム特有 (Platform Specific)]、[プリプロセッサ (Preprocessor)]、および [優先度 (Priority)] の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、[カテゴリ (Category)] から [os-linux] と [os-windows] を選択すると、os-linux カテゴリまたは os-windows カテゴリ内のルールを取得する「Category: "os-windows,os-linux"」というフィルタを作成できます。

フィルタ パネルを表示するには、表示アイコン (  ) をクリックします。

フィルタ パネルを非表示にするには、非表示アイコン (  ) をクリックします。

## 侵入ポリシー ルール フィルタ構築のガイドライン

ほとんどの場合、フィルタを作成するときに、侵入ポリシー内の [ルール (Rules)] ページの左側にあるフィルタ パネルを使用して必要なキーワード/引数を選択できます。

フィルタ パネルでは、ルール フィルタがルール フィルタ グループに分類されます。多くのルール フィルタ グループにサブ基準が含まれているため、探している特定のルールを簡単に見つけることができます。一部のルールフィルタには、展開して個別のルールにドリルダウンするための複数のレベルが設定されています。

フィルタ パネル内の項目は、場合によって、フィルタ タイプ グループを表したり、キーワードを表したり、キーワードの引数を表したりします。次の点に注意してください。

- キーワード ([ルール設定 (Rule Configuration)]、[ルール コンテンツ (Rule Content)]、[プラットフォーム特有 (Platform Specific)]、および [優先度 (Priority)]) 以外のフィルタ タイプ グループ見出しを選択すると、そのグループが展開されて使用可能なキーワードが一覧表示されます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定するためのポップアップ ウィンドウが表示されます。

そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [ルール設定 (Rule Configuration)] > [推奨 (Recommendation)] で [ドロップしてイベントを生成する (Drop and Generate Events)] をクリックすると、「Recommendation: "Drop and Generate Events"」がフィルタ テキスト

ボックスに追加されます。その後で、[ルール設定 (Rule Configuration)] > [推奨 (Recommendation)] で [イベントを生成する (Generate Events)] をクリックすると、フィルタが「Recommendation:"Generate Events"」に変更されます。

- キーワード ([カテゴリ (Category)], [分類 (Classifications)], [Microsoft 脆弱性 (Microsoft Vulnerabilities)], [Microsoft ワーム (Microsoft Worms)], [優先度 (Priority)], および [ルールアップデート (Rule Update)]) になっているフィルタ タイプ グループ見出しを選択すると、使用可能な引数が一覧表示されます。

このタイプのグループから項目を選択すると、適用される引数とキーワードがすぐにフィルタに追加されます。キーワードがすでにフィルタ内に存在していた場合は、そのグループに対応するキーワードの既存の引数が置き換えられます。

たとえば、フィルタ パネルの [カテゴリ (Category)] で [os-linux] をクリックすると、「Category:"os-linux"」がフィルタ テキストボックスに追加されます。その後で、[カテゴリ (Category)] で [os-windows] をクリックすると、フィルタが「Category:"os-windows"」に変更されます。

- [ルール コンテンツ (Rule Content)] の下の [参照 (Reference)] はキーワードであり、その下に特定の参照 ID タイプが列挙されます。参照キーワードのいずれかを選択すると、引数を指定するためのポップアップウィンドウが表示され、キーワードが既存のフィルタに追加されます。キーワードがすでにフィルタ内で使用されていた場合は、既存の引数が指定した新しい引数に置き換えられます。

たとえば、フィルタ パネルで [ルール コンテンツ (Rule Content)] > [参照 (Reference)] > [CVE ID] の順にクリックすると、ポップアップウィンドウが開いて CVE ID を指定するよう求められます。「2007」と入力すると、「cve:"2007"」がフィルタ テキストボックスに追加されます。別の例では、フィルタ パネルで [ルール コンテンツ (Rule Content)] > [参照 (Reference)] の順にクリックすると、ポップアップウィンドウが開いて、参照を指定するよう求められます。「2007」と入力すると、「Reference:"2007"」がフィルタ テキストボックスに追加されます。

- 複数のグループからルール フィルタ キーワードを選択した場合は、各フィルタ キーワードがフィルタに追加され、既存のキーワードが維持されます (同じキーワードの新しい値で上書きされなかった場合)。

たとえば、フィルタ パネルの [カテゴリ (Category)] で [os-linux] をクリックすると、「Category:"os-linux"」がフィルタ テキストボックスに追加されます。その後で、[Microsoft 脆弱性 (Microsoft Vulnerabilities)] で [MS00-006] をクリックすると、フィルタが「Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"」に変更されます。

- 複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[カテゴリ (Category)] で [プリプロセッサ (preprocessor)] を選択してから、[ルール コンテンツ (Rule Content)] > [GID] の順に選択して、「116」と入力すると、プリプロセッサルールで、かつ、GID が 116 のすべてのルールを取得する「Category:"preprocessor" GID:"116"」というフィルタが返されます。
- [カテゴリ (Category)], [Microsoft 脆弱性 (Microsoft Vulnerabilities)], [Microsoft ワーム (Microsoft Worms)], [プラットフォーム特有 (Platform Specific)], および [優先度

(Priority) ]の各フィルタグループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、[カテゴリ (Category) ]から [os-linux] と [os-windows] を選択すると、os-linux カテゴリまたは os-windows カテゴリ内のルールを取得する 「Category:"os-windows,app-detect"」 というフィルタを作成できます。

複数のフィルタキーワード/引数のペアで同じルールが取得される場合があります。たとえば、ルールが dos カテゴリでフィルタ処理された場合と High 優先度でフィルタ処理された場合はともに、DOS Cisco attempt rule (SID 1545) が表示されます。



(注) Cisco Talos Security Intelligence and Research Group (Talos) がルール更新メカニズムを使用してルールフィルタを追加または削除する場合があります。

[ルール (Rules) ] ページのルールは、共有オブジェクトルール (ジェネレータ ID 3) または標準テキストルール (ジェネレータ ID 1) のいずれかになります。次の表に、さまざまなルールフィルタの説明を示します。

表 103: ルール フィルタ グループ

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
ルール設定 (Rule Configuration)	ルールの設定に基づいてルールを検索します。	なし	グループ	キーワード
ルール コンテンツ (Rule Content)	ルールの内容に基づいてルールを検索します。	なし	グループ	キーワード
カテゴリ (Category)	ルールエディタで 사용되는ルールカテゴリに基づいてルールを検索します。ローカルルールはローカルサブグループに表示されることに注意してください。	○	キーワード	引数
分類 (Classifications)	ルールによって生成されるイベントのパケット画面内に表示される攻撃分類に基づいてルールを検索します。	なし	キーワード	引数

フィルタグループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
Microsoft 脆弱性 (Microsoft Vulnerabilities)	Microsoft セキュリティ情報番号に従ってルールを検索します。	○	キーワード	引数
Microsoft ワーム (Microsoft Worms)	Microsoft Windows ホストに影響する特定のワームに基づいてルールを検索します。	○	キーワード	引数
プラットフォーム特有 (Platform Specific)	オペレーティングシステムの特定のバージョンとの関連性に基づいてルールを検索します。  ルールが複数のオペレーティングシステムまたは1つのオペレーティングシステムの複数のバージョンに影響する可能性があることに注意してください。たとえば、SID 2260 を有効にすると、Mac OS X、IBM AIX、およびその他のオペレーティングシステムの複数のバージョンに影響します。	○	キーワード	引数  サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。

フィルタグループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
プリプロセッサ (Preprocessors)	個別のプリプロセッサのルールを検索します。  プリプロセッサが有効になっている場合にプリプロセッサオプションに対するイベントを生成し、インライン展開では、違反パケットをドロップします。するためには、そのオプションに関連付けられたプリプロセッサルールを有効にする必要があることに注意してください。	○	グループ	サブグループ
[プライオリティ (Priority) ]	高、中、および低い優先度に基づいてルールを検索します。  ルールに割り当てられた分類によってその優先度が決定されます。これらのグループは、さらにルールカテゴリに分類されます。ローカルルール（つまり、ユーザがインポートまたは作成したルール）は優先度グループに表示されないことに注意してください。	○	キーワード	引数  サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
ルール アップデート (Rule Update)	特定のルール更新を通して追加または変更されたルールを検索します。ルール更新ごとに、更新内のすべてのルール、更新でインポートされた唯一の新しいルール、または更新によって変更された唯一の既存のルールを表示します。	なし	キーワード	引数

## 侵入ルール構成フィルタ

[ルール (Rules) ] ページに表示されたルールをいくつかのルール構成設定でフィルタ処理できます。たとえば、ルール状態が推奨ルール状態と一致しない一連のルールを表示する場合は、[推奨と一致しない (Does not match recommendation) ] を選択することによってルール状態をフィルタ処理できます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定できます。そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタパネルの [ルール設定 (Rule Configuration) ] > [推奨 (Recommendation) ] で [ドロップしてイベントを生成する (Drop and Generate Events) ] をクリックすると、「Recommendation:"Drop and Generate Events"」がフィルタ テキスト ボックスに追加されます。その後で、[ルール設定 (Rule Configuration) ] > [推奨 (Recommendation) ] で [イベントを生成する (Generate Events) ] をクリックすると、フィルタが「Recommendation:"Generate Events"」に変更されます。

## 侵入ルール コンテンツ フィルタ

[ルール (Rules) ] ページに表示されたルールをいくつかのルール コンテンツ項目でフィルタ処理できます。たとえば、ルールの SID を検索することによって、ルールをすばやく取得できます。特定の宛先ポートに送信されるトラフィックを検査するすべてのルールを検索することもできます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定できます。そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタパネルの [ルールコンテンツ (Rule Content) ] で [SID] をクリックすると、ポップアップ ウィンドウが開いて SID の入力促されます。「1045」と入力すると、



「SID:"1045"」がフィルタ テキストボックスに追加されます。その後で、再度 [SID] をクリックして、SID フィルタを「1044」に変更すると、フィルタが「SID:"1044"」に変更されます。

表 104: ルール コンテンツ フィルタ

フィルタ	検索するルールの内容
メッセージ	メッセージフィールドで指定された文字列を含む。
SID	指定された SID がある。
GID	指定された GID がある。
参照	参照フィールドで指定された文字列を含む。また、特定のタイプの参照および指定された文字列でフィルタリングすることもできます。
操作	alert または pass から開始する。
プロトコル	選択されたプロトコルを含む。
方向 (Direction)	ルールに、指定された方向設定が含まれているかどうかに基づく。
ソース IP	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用する。有効な IP アドレス、CIDR ブロック/プレフィックス長、または \$HOME_NET や \$EXTERNAL_NET などの変数を使用してフィルタ処理できます。
宛先 IP (Destination IP)	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用する。有効な IP アドレス、CIDR ブロック/プレフィックス長、または \$HOME_NET や \$EXTERNAL_NET などの変数を使用してフィルタ処理できます。
ソース ポート	指定された送信元ポートを含む。ポート値は、1 ~ 65535 の整数またはポート変数にする必要があります。
接続先ポート (Destination port)	指定された宛先ポートを含む。ポート値は、1 ~ 65535 の整数またはポート変数にする必要があります。
ルールのオーバーヘッド	選択されたルールのオーバーヘッドがある。
メタデータ	一致するキーと値のペアを含むメタデータがある。たとえば、HTTP アプリケーションプロトコルに関連するメタデータを使用したルールを検索するには、「metadata:"service http"」と入力します。

## 侵入ルール カテゴリ

Firepower システムは、ルールが検出するトラフィックのタイプに基づいてカテゴリにルールを配置します。[ルール (Rules)] ページで、ルール カテゴリでフィルタ処理することによって、カテゴリ内のすべてのルールにルール属性を設定できます。たとえば、ネットワーク上に Linux ホストが存在しない場合は、**os-linux** カテゴリでフィルタ処理してから、表示されたすべてのルールを無効にすることによって、**os-linux** カテゴリ全体を無効にすることができます。カテゴリ名の上にポインタを移動すると、そのカテゴリ内のルールを表示できます。



(注) Cisco Talos Security Intelligence and Research Group (Talos) がルール更新メカニズムを使用してルール カテゴリを追加または削除する場合があります。

## 侵入ルールのフィルタ コンポーネント

フィルタパネルでフィルタをクリックしたときに入力される特殊なキーワードとその引数を変更するようにフィルタを編集できます。[ルール (Rules)] ページのカスタム フィルタはルール エディタで使用されるものと同様に機能しますが、フィルタ パネルを通してフィルタを選択したときに表示される構文を使用して、[ルール (Rules)] ページのフィルタに入力されたキーワードのいずれかを使用することもできます。今後使用するキーワードを決定するには、右側のフィルタ パネルで該当する引数をクリックします。フィルタ キーワードと引数構文がフィルタ テキストボックスに表示されます。キーワードのカンマ区切りの複数の引数は [カテゴリ (Category)] と [優先度 (Priority)] のフィルタ タイプでしかサポートされないことに注意してください。

引用符内のキーワードと引数、文字列、およびリテラル文字列と一緒に、複数のフィルタ条件を区切るスペースを使用できます。ただし、正規表現、ワイルドカード文字、および除外文字 (!)、「大なり」記号 (>)、「小なり」記号 (<) などの特殊な演算子をフィルタに含めることはできません。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[カテゴリ (Category)]、[メッセージ (Message)]、および [SID] の各フィールドで指定された単語が検索されます。

gid キーワードと sid キーワードを除くすべての引数と文字列が部分文字列として扱われます。gid と sid の引数は、完全一致のみを返します。

各ルール フィルタに、次の形式で 1 つ以上のキーワードを含めることができます。

```
keyword:"argument"
```

ここで、**Keyword** は侵入ルール フィルタ グループ内のキーワードのいずれかで、**argument** は二重引用符で囲まれ、キーワードに関連した特定のフィールド内で検索される単一の大文字と小文字が区別されない英数字文字列です。キーワードは先頭文字を大文字にして入力する必要があります。ことに注意してください。

gid と sid を除くすべてのキーワードの引数が部分文字列として扱われます。たとえば、引数 123 によって "12345"、"41235"、"45123" などが返されます。gid と sid の引数は完全一致のみを返します。たとえば、sid:3080 は SID 3080 のみを返します。

各ルールフィルタに、1 つ以上の英数字文字列を含めることもできます。文字列はルールの [メッセージ (Message) ] フィールド、Snort ID (SID) 、およびジェネレータ ID (GID) を検索します。たとえば、文字列 123 は、ルールメッセージ内の文字列 "Lotus123" や "123mania" などを返し、SID 6123 や SID 12375 などでも返します。部分的な SID を検索するには、1 つ以上の文字列を使ってフィルタ処理できます。

すべての文字列では大文字と小文字が区別されず、部分的な文字列として扱われます。たとえば、文字列 ADMIN、admin、または Admin はすべて、"admin"、"CFADMIN"、"Administrator" などを返します。

文字列を引用符で囲むと、完全一致を返すことができます。たとえば、引用符付きのリテラル文字列 "overflow attempt" は完全一致のみを返しますが、引用符なしの 2 つの文字列 overflow と attempt で構成されるフィルタは "overflow attempt"、"overflow multipacket attempt"、"overflow with evasion attempt" などを返します。

複数のキーワード、文字列、またはその両方をスペースで区切って任意に組み合わせて入力することで、フィルタリングの結果を絞り込むことができます。結果には、すべてのフィルタ条件に一致するルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のフィルタはそれぞれ同じルールを返します。

- url:at login attempt cve:200
- login attempt cve:200 url:at
- login cve:200 attempt url:at

## 侵入ルールフィルタの使用

侵入ポリシー内の [ルール (Rules) ] ページの左側にあるフィルタ パネルから事前定義のフィルタキーワードを選択できます。フィルタを選択すると、ページに、すべての一致するルールが表示されるか、どのルールも一致しなかったことが表示されます。

フィルタにキーワードを追加してさらに絞り込むことができます。入力されたフィルタは、ルールデータベース全体を検索して、一致するすべてのルールを返します。前回のフィルタ結果がページに表示されている状態でフィルタを入力すると、そのページの内容が消去され、代わりに新しいフィルタの結果が返されます。

また、フィルタを選択したとき、または、フィルタを選択後にその中の引数値を変更したときに指定したものと同一キーワードと引数の構文を使用してフィルタを入力することもできます。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[カテゴリ (Category) ]、[メッセージ (Message) ]、および [SID] の各フィールドで指定された単語が検索されます。

## 侵入ポリシー内のルール フィルタの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

[ルール (Rules)] ページで、ルールのサブセットを表示するようにルールをフィルタ処理できます。その後で、いずれかのページ機能を使用できます。これには、コンテキストメニューで使用可能な機能の選択も含まれます。これは、特定のカテゴリのすべてのルールのしきい値を設定する場合などに便利です。フィルタ処理されている場合もされていない場合も、リスト内のルールで同じ機能を使用できます。たとえば、新しいルール状態を、フィルタ処理されたリスト内のルールまたはフィルタ処理されていないリスト内のルールに適用できます。

すべてのフィルタのキーワード、キーワード引数、および文字列では大文字と小文字が区別されません。フィルタ内に存在するキーワードの引数をクリックすると、既存の引数が置き換えられます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** [ルール (Rules)] をクリックします。

**ステップ 4** 次に示す方法を個別に使用したり、組み合わせて使用することでフィルタを作成します。

- [フィルタ (Filter)] テキストボックスに値を入力して、Enter キーを押します。
- 事前定義されたキーワードのいずれかを展開します。たとえば、[ルール設定 (Rule Configuration)] をクリックします。
- キーワードをクリックして、プロンプトが表示されたら引数の値を指定します。次に例を示します。
  - [ルール設定 (Rule Configuration)] の下で、[ルール状態 (Rule State)] をクリックし、ドロップダウンリストから [イベントの生成 (Generate Events)] を選択して、[OK] をクリックします。
  - [ルール設定 (Rule Configuration)] の下で、[コメント (Comment)] をクリックし、フィルタ条件として使用するコメントテキストの文字列を入力して、[OK] をクリックします。
  - [カテゴリ (Category)] の下で、[アプリ検出 (app-detect)] をクリックします。システムは、これを引数の値として使用します。

- キーワードを展開して、引数の値をクリックします。たとえば、[ルール状態 (Rule State)] を展開して、[イベントの生成 (Generate Events)] をクリックします。

## 侵入ルールの状態

侵入ルールの状態により、個々の侵入ポリシー内のルールを有効または無効にできるだけだけでなく、モニタ対象の条件によってルールがトリガーされたときにシステムが実行するアクションを指定できます。

各デフォルトポリシーの侵入ルールとプリプロセッサルールのデフォルト状態は、Cisco Talos Security Intelligence and Research Group (Talos) が設定します。たとえば、ルールを Security over Connectivity デフォルトポリシーでは有効にして、Connectivity over Security デフォルトポリシーでは無効にすることができます。Talos がルール更新を使用してデフォルトポリシー内の1つ以上のルールのデフォルト状態を変更する場合があります。ルール更新での基本ポリシーの更新を許可すると、ポリシーの作成時に使用されたデフォルトポリシー（または基礎となるデフォルトポリシー）のデフォルト状態が変更されたときの、そのポリシー内のルールのデフォルト状態の変更も許可することになります。ただし、ルール状態を変更している場合は、ルール更新でその変更が上書きされないことに注意してください。

侵入ルールを作成すると、そのルールは、ポリシーの作成時に使用されたデフォルトポリシー内のルールのデフォルト状態を継承します。

## 侵入ルールの状態オプション

侵入ポリシーでは、ルールの状態を次の値に設定できます。

### イベントを生成する (Generate Events)

システムで特定の侵入試行を検出して、一致したトラフィックが見つかった時点で侵入イベントを生成する場合。悪意のあるパケットがネットワークを通過してルールをトリガーすると、そのパケットが宛先に送信され、システムが侵入イベントを生成します。悪意のあるパケットはその対象に到達しますが、イベントロギングによって通知されます。

### ドロップおよびイベントの生成 (Drop and Generate Events)

システムで特定の侵入試行を検出して、その攻撃を含むパケットをドロップし、一致したトラフィックが見つかった時点で侵入イベントを生成する場合。悪意のあるパケットはその対象に到達せず、イベントロギングによって通知されます。

このルール状態に設定されたルールはイベントを生成しますが、7000 または 8000 シリーズデバイスのインラインインターフェイスセットがタップモードの場合の展開を含むパッシブ展開ではパケットをドロップしないことに注意してください。システムがパケットをドロップするには、侵入ポリシーで[インライン時にドロップ (Drop when Inline)] を有効にして、デバイスインラインを展開する必要があります。

**Disable**

システムで一貫するトラフィックを評価しない場合。



- (注) [イベントを生成する (Generate Events)] または [ドロップおよびイベントの生成 (Drop and Generate Events)] オプションのいずれかを選択すると、ルールが有効になります。[無効 (Disable)] を選択すると、ルールが無効になります。

シスコでは、侵入ポリシー内のすべての侵入ルールを有効にしないことを強く推奨しています。すべてのルールが有効になっている場合は、管理対象デバイスのパフォーマンスが低下する可能性があります。代わりに、できるだけネットワーク環境に合わせてルールセットを調整してください。

## 侵入ルール状態の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入ルール状態は、ポリシー固有です。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)] を選択します。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ヒント** このページには、有効なルールの総数、[イベントを生成する (Generate Events)] に設定された有効なルールの総数、および [ドロップしてイベントを生成する (Drop and Generate Events)] に設定された有効なルールの総数が表示されます。また、パッシブ展開では、[ドロップしてイベントを生成する (Drop and Generate Events)] に設定されたルールで行われるのはイベントの生成のみであることにも注意してください。

**ステップ 3** ナビゲーション ウィンドウで、[ポリシー情報 (Policy Information)] のすぐ下にある [ルール (Rules)] をクリックします。

**ステップ 4** ルール状態を設定する 1 つ以上のルールを選択します。

**ステップ 5** 次のいずれかを実行します。

- [ルール状態 (Rule State)] > [イベントの生成 (Generate Events)]

- [ルール状態 (Rule State) ] > [ドロップしてイベントを生成する (Drop and Generate Events) ]
- [ルール状態 (Rule State) ] > [無効化 (Disable) ]

**ステップ 6** 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、ナビゲーションウィンドウで [ポリシー情報 (Policy Information) ] をクリックして、[変更を確定 (Commit Changes) ] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 侵入ポリシーの侵入イベント通知のフィルタ

侵入イベントの重要度は、発生頻度、送信元 IP アドレス、または宛先 IP アドレスに基づいて設定できます。イベントが特定の回数発生するまで注意が必要ない場合もあります。たとえば、何かがサーバにログインしようとしても、特定の回数失敗するまで、気にする必要はありません。一方、ほんの少数の発生を見れば、広範な問題があることを理解できる場合もあります。たとえば、Web サーバに対して DoS 攻撃が行われた場合は、少数の侵入イベントの発生を確認しただけで、その状況に対処しなければならないことが分かります。同じイベントが何百回も確認されれば、システムの機能が麻痺します。

## 侵入イベントのしきい値

指定された期間内にイベントが生成された回数に基づいて、システムが侵入イベントを記録して表示する回数を制限するための個別のルールのしきい値を侵入ポリシー単位で設定できます。これにより、大量の同じイベントが原因で機能が麻痺するのを避けることができます。共有オブジェクトのルール、標準テキストルール、またはプリプロセッサルールごとにしきい値を設定できます。

## 侵入イベントしきい値の設定

しきい値を設定するには、最初にしきい値のタイプを指定します。

表 105: しきい値設定オプション

オプション	説明
制限 (Limit)	<p>指定された数のパケット (count引数によって指定される) が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [制限 (Limit)] に、[カウント (Count)] を 10 に、[秒 (Seconds)] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分間に発生した最初の 10 個を表示した後、イベントの記録を停止します。</p>
しきい値 (Threshold)	<p>指定された数のパケット (count引数によって指定される) が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [しきい値 (Threshold)] に、[カウント (Count)] を 10 に、[秒 (Seconds)] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[秒 (Seconds)] と [カウント (Count)] のカウンタを 0 にリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。</p>
両方	<p>指定された数 (カウント) のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [両方 (Both)] に、[カウント (Count)] を 2 に、[秒 (Seconds)] を 10 に設定した場合、イベント数は以下ようになります。</p> <ul style="list-style-type: none"> <li>• ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません (しきい値が満たされていない)。</li> <li>• ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します (ルールが 2 回目にトリガーとして使用されたときにしきい値が満たされるため)。</li> <li>• ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します (ルールが 2 回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される)。</li> </ul>



次に、トラッキングを指定します。これにより、イベントしきい値が送信元 IP アドレス単位と宛先 IP アドレス単位のどちらで計算されるかが決まります。

表 106: IP しきい値設定オプション

オプション	説明
ソース (Source)	送信元 IP アドレス単位でイベントインスタンスカウントを計算します。
[接続先 (Destination) ]	宛先 IP アドレス単位でイベントインスタンスカウントを計算します。

最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 107: インスタンス/時間のしきい値設定オプション

オプション	説明
メンバー数 (Count)	しきい値を満たすために必要な、追跡する IP アドレス単位で指定された期間単位のイベントインスタンスの数。
秒 (Seconds)	カウントがリセットされるまでの秒数。しきい値タイプを [制限 (limit) ] に、トラッキングを [送信元 IP (Source IP) ] に、[カウント (count) ] を 10 に、[秒 (seconds) ] を 10 に設定した場合は、システムが指定された送信元ポートから 10 秒間に発生した最初の 10 のイベントを記録して表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。

侵入イベントのしきい値設定は、単独で使用することも、レートベースの攻撃防御、`detection_filter` キーワード、および侵入イベント抑制のいずれかと組み合わせて使用することもできます。



ヒント 侵入イベントのパケットビューでしきい値を追加することもできます。

関連トピック

[detection\\_filter キーワード \(1800 ページ\)](#)

[パケットビュー内でのしきい値オプションの設定 \(2589 ページ\)](#)

## 侵入イベントのしきい値の変更と追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入ポリシーの1つ以上の特定のルールにしきい値を設定できます。既存のしきい値設定を個別にまたは同時に変更することもできます。それぞれに1つずつのしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

また、侵入ポリシーに関係したすべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。

無効な値を入力するとフィールドに復元アイコン (🔄) が表示されます。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。



### ヒント

複数の CPU を搭載した管理対象デバイスでグローバルしきい値または個別のしきい値を設定すると、予想より多くのイベントが生成される場合があります。

### 手順

- ステップ 1 [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。
- ステップ 2 編集するポリシーの横にある編集アイコン (✎) をクリックします。  
代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3 [ナビゲーション (navigation)] ペインの [ポリシー情報 (Policy Information)] のすぐ下にある [ルール (Rules)] をクリックします。
- ステップ 4 しきい値を設定するルールを選択します。
- ステップ 5 [イベントのフィルタリング (Event Filtering)] > [しきい値 (Threshold)] を選択します。 >
- ステップ 6 [タイプ (Type)] ドロップダウンリストからしきい値のタイプを選択します。
- ステップ 7 [追跡対象 (Track By)] ドロップダウンリストから、イベントインスタンスが [送信元 (Source)] IP アドレスまたは [宛先 (Destination)] IP アドレスのどちらによって追跡されるかを選択します。
- ステップ 8 [数 (Count)] フィールドに値を入力します。
- ステップ 9 [秒数 (Seconds)] フィールドに値を入力します。
- ステップ 10 [OK] をクリックします。

**ヒント** [イベントフィルタリング (Event Filtering)] カラムのルール横にイベントフィルタアイコン (🔍) が表示されます。ルールに複数のイベントフィルタを追加した場合は、アイコン上の数字がイベントフィルタの数を示します。

**ステップ 11** 最後のコミットからポリシーに加えられた変更を保存するには、[ポリシー情報 (Policy information)] をクリックし、次に [変更をコミット (Commit Changes)] をクリックします。変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

**次のタスク**

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

**関連トピック**

[グローバルルールのしきい値の基本 \(1677 ページ\)](#)

## 侵入イベントしきい値の表示と削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

ルールに関する既存のしきい値設定を表示または削除することができます。[ルールの詳細 (Rules Details)] ビューを使用してしきい値の既存の設定を表示することによって、それらがシステムに適切かどうかを確認できます。そうでない場合は、新しいしきい値を追加して既存の値を上書きすることができます。

侵入ポリシーによって記録されるすべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。

**手順**

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション ウィンドウの [ポリシー情報 (Policy Information)] の直下にある [ルール (Rules)] をクリックします。

- ステップ4** 表示または削除する、しきい値が設定された1つまたは複数のルールを選択します。
- ステップ5** 選択した各ルールのしきい値を削除するには、[イベントフィルタリング (Event Filtering)] > [しきい値の削除 (Remove Thresholds)] の順に選択します。
- ステップ6** [OK] をクリックします。
- ステップ7** 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックし、[変更の確定 (Commit Changes)] をクリックします。
- 変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

---

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[グローバル ルールのしきい値の基本 \(1677 ページ\)](#)

## 侵入ポリシーの抑制の設定

特定の IP アドレスまたは IP アドレスの範囲が特定のルールまたはプリプロセッサをトリガーしたときの侵入イベント通知を抑制できます。これは、誤検出を回避するのに役立ちます。たとえば、特定の 익스プロイトのように見えるパケットを伝送しているメールサーバが存在する場合は、そのメールサーバによってトリガーとして使用されたイベントに関するイベント通知を抑制できます。ルールはすべてのパケットに対してトリガーとして使用されますが、本物の攻撃に対するイベントだけが表示されます。

## 侵入ポリシー抑制タイプ

侵入イベント抑制は、単独で使用することも、レートベースの攻撃防御、`detection_filter` キーワード、および侵入イベントしきい値構成のいずれかと組み合わせて使用することもできることに注意してください。



**ヒント** 侵入イベントのパケットビュー内から抑制を追加できます。また、侵入ルールエディタ ページ ([オブジェクト (Objects)] > [侵入ルール (Intrusion Rules)]) や任意の侵入イベントページ (イベントが侵入ルールによってトリガーされた場合) で右クリックコンテキストメニューを使用して、抑制設定にアクセスすることもできます。

---

#### 関連トピック

[detection\\_filter キーワード \(1800 ページ\)](#)

[パケットビュー内でのしきい値オプションの設定 \(2589 ページ\)](#)

## 特定のルールの侵入イベントの抑制

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入ポリシーのルールに関連する侵入イベント通知を抑制できます。ルールに関する通知が抑制されると、ルールはトリガーとして使用されますが、イベントは生成されません。ルールの1つまたは複数の抑制を設定できます。リスト内の最初の抑制に最も高いプライオリティが割り当てられます。2つの抑制が競合している場合は、最初の抑制のアクションが実行されます。

無効な値を入力するとフィールドに復元アイコン (🔄) が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーションパネルの[ポリシー情報 (Policy Information)]の直下にある[ルール (Rules)] をクリックします。

**ステップ 4** 抑制条件を設定する1つまたは複数のルールを選択します。

**ステップ 5** [イベントフィルタリング (Event Filtering)] > [抑制 (Suppression)] を選択します。

**ステップ 6** [抑制タイプ (Suppression Type)] を選択します。

**ステップ 7** 抑制タイプとして[送信元 (Source)]または[宛先 (Destination)]を選択した場合は、[ネットワーク (Network)]フィールドに、IPアドレス、アドレスブロック、または送信元IPアドレスまたは宛先IPアドレスとして指定する変数、あるいは、これらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。

システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際のIPアドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

**ステップ 8** [OK] をクリックします。

**ヒント** 抑制するルールの横にある[イベントフィルタリング (Event Filtering)]カラムのルールの横にイベントフィルタアイコン (🔍) が表示されます。ルールに複数のイベントフィルタを追加した場合は、アイコン上の数字がイベントフィルタの数を示します。

- ステップ 9** 最後のコミットからポリシーに加えられた変更を保存するには、[ポリシー情報 (Policy information)] をクリックし、次に [変更をコミット (Commit Changes)] をクリックします。変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 抑制条件の表示と削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

既存の抑制条件を表示または削除することもできます。たとえば、メールサーバがエクスプロイトのように見えるパケットを普段から送信しているという理由で、そのメールサーバの IP アドレスから送信されたパケットに関するイベント通知を抑制できます。その後、そのメールサーバが使用停止になり、その IP アドレスが別のホストに再割り当てされたら、その送信元 IP アドレスの抑制条件を削除する必要があります。

### 手順

- ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。
- ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。
- 代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3** ナビゲーションパネルの [ポリシー情報 (Policy Information)] の直下にある [ルール (Rules)] をクリックします。
- ステップ 4** 抑制を表示または削除する 1 つまたは複数のルールを選択します。
- ステップ 5** 次の選択肢があります。
- ルールのすべての抑制を削除するには、[イベントフィルタリング (Event Filtering)] > [抑制の削除 (Remove Suppressions)] を選択します。
  - 特定の抑制設定を削除するには、ルールをクリックして、[詳細の表示 (Show Details)] をクリックします。抑制設定を展開して、削除する抑制設定の横にある [削除 (Delete)] をクリックします。

**ステップ 6** [OK] をクリックします。

**ステップ 7** 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックし、[変更の確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 動的侵入ルール状態

レートベースの攻撃は、ネットワークまたはホストに過剰なトラフィックを送信することによって、低速化または正規の要求の拒否を引き起こし、ネットワークまたはホストを混乱させようとします。レートベースの防御を使用して、特定のルールの過剰なルール一致に対応してルールアクションを変更することができます。

侵入ポリシーにレートベースのフィルタを含めることにより、一定期間においてルールの一一致が過剰に発生した時点を検出できます。インライン展開された管理対象デバイス上でこの機能を使用して、指定された時刻のレートベースの攻撃をブロックしてから、ルール一致がイベントを生成するだけでトラフィックをドロップしないルール状態に戻すことができます。

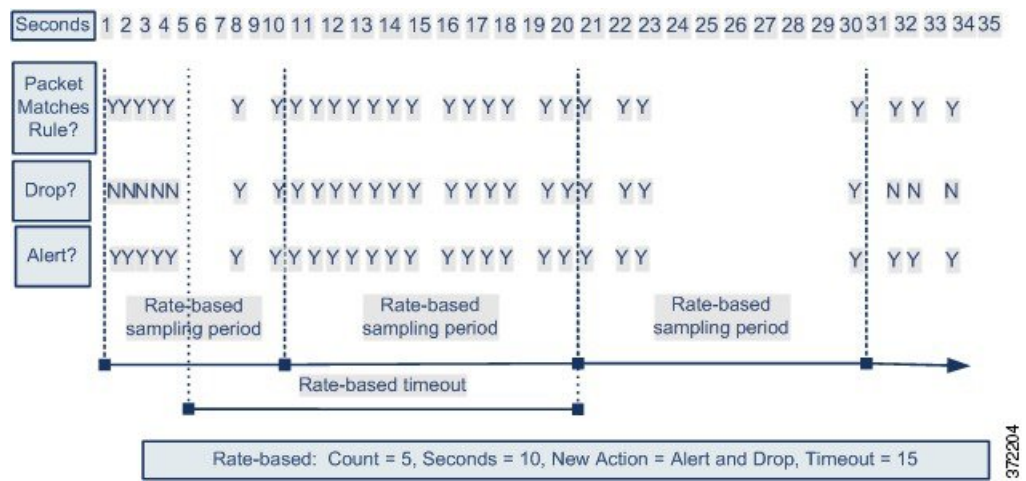
レートベースの攻撃防止は、異常なトラフィックパターンを識別し、正規の要求に対するそのトラフィックの影響を最小限に抑えようとします。特定の宛先 IP アドレスに送信されるトラフィックまたは特定の送信元 IP アドレスから送信されるトラフィックの過剰なルール一致を識別できます。また、検出されたすべてのトラフィックを通して特定のルールの過剰な一致に対処することもできます。

ルールと一致したすべてのパケットをドロップするのではなく、指定された期間に特定の一一致率に達した場合にルールと一致したパケットをドロップするために、ルールを [ドロップしてイベントを生成する (Drop and Generate Events)] 状態に設定しない場合があります。動的ルール状態を使用すれば、ルールのアクションの変更をトリガーするレート、あるレートに達したときに変更すべきアクション、および新しいアクションの継続時間を設定できます。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。繰り返しパスワードを特定しようとする試みが、レートベースの攻撃防止が設定されたルールをトリガーします。レートベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [ドロップしてイベントを生成する (Drop and Generate Events)] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリングレートが現在または過去のサンプリング期間のしきい値を上回っている場合は、新しいアクションが継続されます。新しいアクションは、サンプリ

ングレートがしきい値レートを下回るサンプリング期間の終了後にのみ、[イベントを生成する (Generate Events)] に戻ります。



## ダイナミックな侵入ルール状態の設定

侵入ポリシーでは、侵入ルールまたはプリプロセッサルールのレートベースのフィルタを設定できます。レートベースのフィルタは次の3つの要素で構成されます。

- 特定の秒数以内のルール一致のカウンタとして設定されるルール一致率
- レートを越えた時点で実行される新しいアクション ([イベントを生成する (Generate Events)]、[ドロップしてイベントを生成する (Drop and Generate Events)]、および [無効 (Disable)] の3種類がある)
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウトに達すると、レートがしきい値を下回っていれば、ルールのアクションがルールの初期設定に戻ります。

インライン展開のレートベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レートベースの設定を使用しない場合、[イベントを生成する (Generate Events)] に設定されたルールはイベントを生成しますが、システムはそのようなルールに関するパケットをドロップしません。ただし、攻撃トラフィックが、レートベースの基準が設定されているルールに一致した場合、それらのルールが当初 [イベントのドロップおよび生成 (Drop and Generate Events)] に設定されていないとしても、レートアクションがアクティブである期間は、パケットがドロップされる場合があります。



(注) レートベースアクションでは、無効にされたルールを有効にすることも、無効にされたルールに一致するトラフィックをドロップすることもできません。



同じルールに複数のレート ベース フィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2つのレートベースのフィルタアクションが競合している場合は、最初のレートベースのフィルタのアクションが実行されることに注意してください。

## [ルール (Rule) ] ページからの動的ルール状態の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

1つのルールに対して1つ以上の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2つの動的ルール状態が競合している場合は、最初のアクションが実行されます。

動的ルール状態はポリシー固有です。

無効な値を入力するとフィールドに復元アイコン (↺) が表示されます。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。



(注) 動的ルール状態は、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

### 手順

- ステップ 1 [ポリシー (Policies) ] > [アクセスコントロール (Access Control) ] > [侵入 (Intrusion) ] を選択します。
- ステップ 2 編集するポリシーの横にある編集アイコン (✎) をクリックします。  
代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3 ナビゲーション ウィンドウで、[ポリシー情報 (Policy Information) ] のすぐ下にある [ルール (Rules) ] をクリックします。
- ステップ 4 動的ルール状態を追加する 1 つまたは複数のルールを選択します。
- ステップ 5 [動的状態 (Dynamic State) ] > [レート ベースのルール状態の追加 (Add Rate-Based Rule State) ] を選択します。
- ステップ 6 [追跡対象 (Track By) ] ドロップダウンリストから値を選択します。
- ステップ 7 [追跡対象 (Track By) ] を [送信元 (Source) ] または [宛先 (Destination) ] に設定した場合は、[ネットワーク (Network) ] フィールドに追跡する各ホストのアドレスを入力します。単一の

IP アドレス、アドレス ブロック、変数、またはこれらの任意の組み合わせで構成されたカンマ区切りのリストを指定できます。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

**ステップ 8** [レート (Rate) ] の横で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [カウント (Count) ] フィールドに値を入力します。
- [秒数 (Seconds) ] フィールドに値を入力します。

**ステップ 9** [新しい状態 (New State) ] ドロップダウンリストから、条件が満たされたときに実行する新しいアクションを指定します。

**ステップ 10** [タイムアウト (Timeout) ] フィールドに値を入力します。

タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションのタイムアウトを阻止する場合は、[0] を指定するか、[タイムアウト (Timeout) ] フィールドを空白のままにします。

**ステップ 11** [OK] をクリックします。

**ヒント** [動的状態 (Dynamic State) ] 列のルールの横に動的状態アイコン (🔄) が表示されます。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

**ヒント** ルールのセットに対する動的ルール設定を削除するには、[ルール (Rules) ] ページでルールを選択して、[動的状態 (Dynamic State) ] > [レート ベースの状態の削除 (Remove Rate-Based States) ] を選択します。また、ルールのルール詳細から個別のレート ベースのルール状態フィルタを削除するには、ルールを選択して、[詳細の表示 (Show Details) ] をクリックしてから、削除するレートベースのフィルタのそばにある [削除 (Delete) ] をクリックします。

**ステップ 12** 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、[ポリシー情報 (Policy Information) ] をクリックして、[変更を確定 (Commit Changes) ] をクリックします。変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

---

## 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## 侵入ルールコメントの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入ポリシーのルールにコメントを追加できます。このようにして追加されたコメントはポリシー専用のコメントとなります。よって、ある侵入ポリシーのルールに追加したコメントは、他の侵入ポリシーでは表示されません。追加したコメントは、侵入ポリシーの[ルール (Rules)] ページ上の[ルールの詳細 (Rule Details)] ビューで確認できます。

コメントを含む侵入ポリシーの変更をコミットしてから、ルールの[編集 (Edit)] ページで[ルールコメント (Rule Comment)] をクリックしてコメントを表示することもできます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** [ナビゲーション (navigation)] パネルの[ポリシー情報 (Policy Information)] のすぐ下にある[ルール (Rules)] をクリックします。

**ステップ 4** コメントを追加する 1 つまたは複数のルールを選択します。

**ステップ 5** [コメント (Comments)] > [ルールコメントの追加 (Add Rule Comment)] の順に選択します。 >

**ステップ 6** [コメント (Comments)] フィールドに、ルールコメントを入力します。

**ステップ 7** [OK] をクリックします。

**ヒント** システムは[コメント (Comments)] カラムのルールの横にコメントアイコン (💬) を表示します。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

**ステップ 8** 必要に応じて、コメントの横にある[削除 (Delete)] をクリックし、ルールのコメントを削除します。

侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけコメントを削除できます。侵入ポリシーの変更がコミットされた後は、ルールコメントを削除できなくなります。

**ステップ 9** 最後のコミットからポリシーに加えられた変更を保存するには、[ポリシー情報 (Policy information)] をクリックし、次に [変更をコミット (Commit Changes)] をクリックします。変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

---

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。



## 第 72 章

# ネットワーク資産に応じた侵入防御の調整

以下のトピックでは、Firepower 推奨ルールの使用方法について説明します。

- [Firepower 推奨ルールについて \(1655 ページ\)](#)
- [Firepower 推奨のデフォルト設定 \(1656 ページ\)](#)
- [Firepower 推奨の詳細設定 \(1657 ページ\)](#)
- [Firepower の推奨事項の生成と適用 \(1658 ページ\)](#)

## Firepower 推奨ルールについて

Firepower の侵入ルールの推奨事項を使用して、ネットワーク上で検出されたオペレーティングシステム、サーバ、およびクライアント アプリケーションプロトコルを、それらのアセットを保護するために作成されたルールに関連付けることができます。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。

システムは、侵入ポリシーごとに個別の推奨事項のセットを作成します。これにより、通常、標準テキストルールと共有オブジェクトルールのルール状態の変更が推奨されます。ただし、プリプロセッサおよびデコーダのルールの変更も推奨されます。

ルール状態の推奨事項を生成する場合は、デフォルト設定を使用するか、詳細設定を指定できます。詳細設定では次の操作が可能です。

- システムが脆弱性をモニタするネットワーク上のホストを再定義する。
- ルール オーバーヘッドに基づき、システムが推奨するルールに影響を与える。
- ルールを無効にする推奨事項を生成するかどうかを指定する。

推奨事項をすぐに使用するか、推奨事項（および影響を受けるルール）を確認してから受け入れることができます。

推奨ルール状態を使用することを選択すると、読み取り専用の Firepower 推奨レイヤが侵入ポリシーに追加されますが、後で、推奨ルール状態を使用しないことを選択すると、そのレイヤが削除されます。

侵入ポリシーに最近保存された構成設定に基づいて自動的に推奨を生成するためのタスクをスケジュールできます。

システムは、手動で設定されたルール状態を変更しません。

- 推奨を生成する前に指定したルールの状態を手動で設定すると、その後、システムはそのルールの状態を変更できなくなる。
- 推奨の生成後に指定したルールの状態を手動で設定すると、そのルールの推奨状態が上書きされる。



**ヒント** 侵入ポリシーレポートには、推奨状態と異なるルール状態を持つルールのリストを含めることができます。

推奨が絞り込まれた [ルール (Rules)] ページを表示している最中に、あるいは、ナビゲーションパネルまたは [ポリシー情報 (Policy Information)] ページから [ルール (Rules)] ページに直接アクセスした後に、手動で、ルール状態を設定したり、ルールをソートしたり、[ルール (Rules)] ページで可能なその他の操作 (ルールの抑制やルールしきい値の設定など) を実行することができます。



(注) Cisco Talos Security Intelligence and Research Group (Talos) は、システム提供のポリシーでの各ルールの適切な状態を決定します。システム提供のポリシーを基本ポリシーとして使用し、システムがルールを Firepower の推奨ルール状態に設定できるようにする場合、侵入ポリシーのルールは、シスコが推奨するネットワーク アセットの設定と一致します。

#### 推奨ルールおよびマルチテナンシー

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、先祖ドメインの侵入ポリシーでこの機能を有効にすると、システムはすべての子孫のリーフドメインからのデータを使用して、推奨事項を生成します。これにより、侵入ルールをすべてのリーフドメインに存在しない可能性があるアセットに調整することができ、パフォーマンスに影響を与えることができます。

## Firepower 推奨のデフォルト設定

Firepower 推奨を生成すると、システムがネットワーク資産に関連付けられた脆弱性から保護するルールの基本ポリシーを検索して、その基本ポリシー内のルールの現在の状態を特定します。システムによってルールの状態が推奨されますが、自身で設定する場合はルールを推奨される状態に設定します。

システムによって次の基本的な分析が実行され、推奨が生成されます。

表 108: 脆弱性に基づく Firepower ルール状態推奨

基本ポリシー ルール状態	ルールは検出された資産を保護するか	推奨ルール状態
イベントの生成または無効化	Yes	イベントを生成する (Generate Events)
ドロップおよびイベントの生成	Yes	ドロップおよびイベントの生成 (Drop and Generate Events)
任意	No	無効 (Disable)

Firepower 推奨ルールの詳細設定を変更せずに推奨を生成する場合は、システムが検出対象のネットワーク全体のすべてのホストのルール状態の変更を推奨します。

デフォルトで、システムは、オーバーヘッドが低または中のルールに対してのみ推奨を生成し、ルールを無効にする推奨を生成します。

システムは、Impact Qualification 機能を使用して無効にされた脆弱性に基づく侵入ルールのルール状態を推奨しません。

システムは、常に、ホストにマップされたサードパーティの脆弱性に関連付けられたローカルルールを有効にするように推奨します。

マップされていないローカルルールに対する状態推奨は生成されません。

**関連トピック**

[個々の脆弱性の非アクティブ化 \(2686 ページ\)](#)

[サードパーティ製品のマッピング \(2054 ページ\)](#)

## Firepower 推奨の詳細設定

**推奨とルール状態とのすべての差をポリシー レポートに含める (Include all differences between recommendations and rule states in policy reports)**

デフォルトで、侵入ポリシー レポートには、ポリシーで有効になっているルール、つまり、[イベントを生成する (Generate Events)] と [ドロップしてイベントを生成する (Drop and Generate Events)] のいずれかに設定されているルールが表示されます。また、[すべての差を含める (Include all differences)] オプションを有効にすると、推奨されている状態が保存されている状態と異なるルールが一覧表示されます。ポリシー レポートの詳細については、[ポリシー レポート \(362 ページ\)](#) を参照してください。

**検査対象のネットワーク (Networks to Examine)**

モニタ対象のネットワークまたは推奨について検査する個々のホストを指定します。1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。

指定したホスト内のアドレスのリストは、否定以外の OR 演算でリンクされ、すべての OR 演算の実行後に AND 演算でリンクされます。

ホスト情報に基づいて特定のパケットのアクティブ ルール処理を動的に適応させる場合は、アダプティブ プロファイルの更新 を有効にすることもできます。

### 推奨しきい値（ルール オーバーヘッドの指定）（Recommendation Threshold (By Rule Overhead)）

選択したしきい値をオーバーヘッドが超える侵入ルールが推奨または自動的に有効にされないようにします。

オーバーヘッドは、システムパフォーマンスに対するルールの潜在的影響とルールが誤検出を引き起こす確率に基づいています。オーバーヘッドが高いルールを許可すると、通常、より多くの推奨が生成されるようになりますが、システムパフォーマンスに影響を及ぼす可能性があります。[侵入ルール (Intrusion Rules)] ページのルール詳細ビューでルールのオーバーヘッドの評価を確認できます。

ただし、ルールを無効にする推奨ではルール オーバーヘッドが考慮されません。また、ローカルルールは、サードパーティの脆弱性にマップされていない限り、オーバーヘッドがないものと見なされます。

特定の設定のオーバーヘッド評価のルールについて推奨を生成した場合でも、別のオーバーヘッドの推奨を生成してから、再び元のオーバーヘッド設定の推奨を生成することができます。推奨を生成する回数や生成時に使用する異なるオーバーヘッド設定の数に関係なく、同じルールセットについては、推奨を生成するたびに、オーバーヘッド設定ごとに同じルール状態の推奨が生成されます。たとえば、オーバーヘッドを「中」に設定して推奨を生成し、次に「高」にして推奨を生成してから、再び「中」にして推奨を生成することができます。ネットワーク上のホストとアプリケーションが変更されていない限り、オーバーヘッドが「中」の推奨は、どちらも、そのルールセットに対して同じになります。

### ルールを無効にする推奨を受け入れる（Accept Recommendations to Disable Rules）

Firepower の推奨に基づいて侵入ルールを無効にするかどうかを指定します。

ルールを無効にする推奨を受け入れると、ルールの適用範囲が制限されます。ルールを無効にする推奨を無視すると、ルールの適用範囲が拡大されます。

### 関連トピック

[Firepower システムの IP アドレス表記法](#)（14 ページ）

[アダプティブプロファイルの更新および Firepower 推奨ルール](#)（2014 ページ）

## Firepower の推奨事項の生成と適用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin



Firepower の推奨事項の使用を開始または停止する場合、ネットワークのサイズと侵入ルールセットに応じて、数分かかる場合があります。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、先祖ドメインの侵入ポリシーでこの機能を有効にすると、システムはすべての子孫のリーフドメインからのデータを使用して、推奨事項を生成します。これにより、侵入ルールをすべてのリーフドメインに存在しない可能性があるアセットに調整することができ、パフォーマンスに影響を与えることができます。

## 手順

- ステップ 1** 侵入ポリシー エディタのナビゲーション ウィンドウで、[Firepower の推奨事項 (Firepower Recommendations)] をクリックします。
  - ステップ 2** (オプション) 詳細設定を設定します。 [Firepower 推奨の詳細設定 \(1657 ページ\)](#) を参照してください。
  - ステップ 3** 推奨事項を生成して適用します。
    - 推奨事項の生成および使用 (Generate and Use Recommendations) : 推奨事項を生成して、一致するようにルール状態を変更します。これまでに推奨事項を生成したことがない場合にのみ使用できます。
    - 推奨事項の生成 (Generate Recommendations) : 推奨事項を使用しているかどうかに関係なく、新しい推奨事項を生成しますが、一致するようにルールの状態を変更しません。
    - 推奨事項の更新 (Update Recommendations) : 推奨事項を使用している場合は、推奨事項を生成してルールの状態を一致するように変更します。それ以外の場合は、ルールの状態を変更することなく、新しい推奨事項を生成します。
    - 推奨事項の使用 (Use Recommendations) : ルールの状態を未実装の推奨事項に一致するように変更します。
    - 推奨事項を使用しない (Do Not Use Recommendations) : 推奨事項の使用を停止します。推奨事項の適用前にルールの状態を手動で変更した場合、ルールの状態は指定した値に戻ります。それ以外の場合、ルールの状態はデフォルト値に戻ります。
- 推奨事項の生成時に、システムは推奨される変更の概要を表示します。システムによって状態の変更が推奨されるルールのリストを表示するには、新しく提案されたルール状態の横にある [表示 (View)] をクリックします。
- ステップ 4** 実装した推奨事項を評価して調整します。

ほとんどの Firepower の推奨事項を承認する場合でも、ルールの状態を手動で設定することで、個別の推奨事項を上書きできます。 [侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。
  - ステップ 5** 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[Firepower の推奨ルールの自動化 \(229 ページ\)](#)



## 第 73 章

# 機密データの検出

ここでは、機密データ検出とその設定方法について説明します。

- [機密データ検出の基本 \(1661 ページ\)](#)
- [グローバル センシティブ データ検出オプション \(1663 ページ\)](#)
- [個別のセンシティブ データ タイプのオプション \(1664 ページ\)](#)
- [システム提供のセンシティブ データのタイプ \(1665 ページ\)](#)
- [センシティブ データ検出の設定 \(1666 ページ\)](#)
- [監視対象のアプリケーション プロトコルおよび機密データ \(1668 ページ\)](#)
- [モニタ対象のアプリケーション プロトコルの選択 \(1669 ページ\)](#)
- [特別なケース：FTP トラフィックでのセンシティブ データの検出 \(1670 ページ\)](#)
- [カスタム 機密データ タイプ \(1671 ページ\)](#)

## 機密データ検出の基本

社会保障番号、クレジットカード番号、運転免許証番号などのセンシティブ データは、インターネットに意図的に、または誤って漏洩される可能性があります。システムには、ASCII テキストのセンシティブ データに関するイベントを検出し、生成できるセンシティブ データ プロセッサが用意されています。このプロセッサは、特に誤って漏洩されたデータの検出に役立ちます。

グローバルセンシティブ データ プリプロセッサ オプションは、プリプロセッサの動作を制御します。以下のことを指定するグローバル オプションを変更できます。

- プリプロセッサが、ルールをトリガーしたパケットで、クレジットカード番号または社会保障番号の下位 4 桁を除くすべての桁を置換するかどうか
- センシティブ データをモニタする、ネットワーク上の宛先ホスト
- イベントの生成基準となる、単一のセッションでの全データ タイプの合計オカレンス数

個別のデータ タイプによって、指定した宛先ネットワーク トラフィックで検出しイベントを生成できるセンシティブ データを特定します。以下のことを指定するデータ タイプ オプションのデフォルト設定を変更できます。

- 検出されたデータタイプに対して単一のセッションごとのイベントを生成する基準とするしきい値
- 各データタイプをモニタする宛先ポート
- 各データタイプをモニタするアプリケーションプロトコル

指定するデータパターンを検出するためのカスタムデータタイプを作成および変更することができます。たとえば、病院で患者番号を保護するためのデータタイプを作成したり、大学で固有の番号パターンを持つ学生番号を検出するためのデータタイプを作成したりすることが考えられます。

システムはトラフィックに対して個別のデータタイプを照合することによって、TCPセッションごとにセンシティブデータを検出します。侵入ポリシーの、各データタイプのデフォルト設定およびすべてのデータタイプに適用されるグローバルオプションのデフォルト設定は変更できます。Firepower システムには、一般的に使用されているデータタイプがすでに定義されています。カスタムデータタイプを作成することも可能です。

センシティブデータのプリプロセッサルールは、各データタイプに関連付けられます。各データタイプのセンシティブデータ検出とイベント生成を有効にするには、そのデータタイプに対応するプリプロセッサルールを有効にします。設定ページのリンクを使用すると、センシティブデータルールにフィルタリングされたビューが [ルール (Rules)] ページに表示されます。このビューで、ルールを有効または無効にしたり、その他のルール属性を設定したりできます。

変更を侵入ポリシーに保存する際に提示されるオプションによって、データタイプに関連付けられたルールが有効になっていてセンシティブデータ検出が無効になっている場合には、自動的にセンシティブデータプリプロセッサを有効にすることができます。



#### ヒント

機密データプリプロセッサでは、FTPまたはHTTPを使用してアップロードおよびダウンロードされる暗号化されていない Microsoft Word ファイル内の機密データを検出できます。これが可能である理由は、Word ファイルが ASCII テキストとフォーマット設定コマンドを分けてグループ化する方式だからです。

このシステムは、暗号化または難読化された機密データ、あるいは圧縮または符号化された形式の機密データ（たとえば、Base64 でエンコードされた電子メールの添付ファイルなど）の検出は行いません。たとえば、システムは電話番号 (555)123-4567 を検出しますが、(5 5 5) 1 2 3 -4 5 6 7 のようにスペースで難読化されたバージョン、あるいは <b>(555)</b><i>123--4567</i> のように HTML コードが介在するバージョンは検出しません。ただし、<b>(555)-123-4567</b> のように、HTML にコーディングされた番号のパターンの途中でコードが入っていなければ検出されます。

# グローバルセンシティブデータ検出オプション

グローバルセンシティブデータ オプションはポリシーに固有であり、すべてのデータ タイプに適用されます。

## マスク

ルールをトリガーしたパケットで、クレジットカード番号および社会保障番号の下位4桁を除くすべての桁を「X」に置換します。Web インターフェイスの侵入イベント パケット ビュー およびダウンロードされたパケットでは、マスクされた番号が表示されます。

## ネットワーク

センシティブ データをモニタする 1 つ以上の宛先ホストを指定します。単一の IP アドレス、アドレスブロック、あるいはこのいずれかまたは両方のカンマ区切りリストを指定できます。空白のフィールドは、any として解釈されます。これは、任意の宛先 IP アドレスを意味します。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン 展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

## グローバルしきい値 (Global Threshold)

グローバルしきい値イベントの生成基準となる、単一セッションでの全データ タイプの合計オカレンス数を指定します。データタイプの組み合わせを問わず、プリプロセッサは指定された数のデータ タイプを検出すると、グローバルしきい値イベントを生成します。1 ~ 65535 の値を指定できます。

シスコでは、このオプションに、ポリシーで有効にする個々のデータ タイプに対するしきい値のどれよりも大きい値を設定することを推奨しています。

グローバルしきい値については、以下の点に注意してください。

- 複数のデータ タイプを合わせたオカレンス数を検出して イベントを生成し、インライン 展開では、違反パケットをドロップします。するには、プリプロセッサ ルールの 139:1 を有効にする必要があります。
- プリプロセッサが生成するグローバルしきい値イベントは、セッションあたり最大1件です。
- グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立しています。つまり、グローバルしきい値に達すると、個別データ タイプに対するイベントしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も当てはまります。

## 関連トピック

[Firepower システムの IP アドレス表記法](#) (14 ページ)

## 個別のセンシティブデータタイプのオプション

最低でも、カスタムデータタイプごとにイベントしきい値を指定し、モニタする少なくとも1つのポートまたはアプリケーションプロトコルを指定する必要があります。

各システム定義済みデータタイプでは、デフォルト値が変更されない限り、アクセス不能な `sd_pattern` キーワードを使用して、トラフィックで検出する組み込みデータパターンを定義します。カスタムデータタイプを作成して、そのデータタイプに対し、単純な正規表現を使用して独自のデータパターンを指定することもできます。

センシティブデータタイプは、センシティブデータ検出が有効になっているすべての侵入ポリシーに表示されます。システム提供のデータタイプは読み取り専用として表示されます。カスタムデータタイプの場合、名前とパターンフィールドは読み取り専用として表示されますが、他のオプションはポリシー固有の値に設定できます。

マルチドメイン展開では、現在のドメインで作成されたセンシティブデータタイプが表示されます。これは編集できます。また、先祖ドメインで作成されたデータタイプも表示されますが、これらは限定的に編集できます。先祖データタイプの場合、名前とパターンフィールドは読み取り専用として表示されますが、他のオプションはポリシー固有の値に設定できます。

表 109: 個別のデータタイプのオプション

オプション	説明
データタイプ	データタイプの一意の名前を指定します。
しきい値 (Threshold)	<p>イベント生成の基準とする、データタイプのオカレンス数を指定します。1 ~ 255 の値を指定できます。</p> <p>プリプロセッサが検出したデータタイプに対して生成するイベント数は、セッションごとに1つであることに注意してください。グローバルしきい値イベントと個別データタイプイベントは、互いに独立していることにも注意してください。つまり、データタイプイベントしきい値に達すると、グローバルイベントしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も同様です。</p>
宛先ポート (Destination Ports)	データタイプでモニタする宛先ポートを指定します。単一のポート、複数のポートをカンマで区切ったリスト、または任意の宛先ポートを意味する <code>any</code> を指定できます。

オプション	説明
アプリケーション プロトコル (Application Protocols)	データ タイプでモニタする最大 8 つのアプリケーション プロトコルを指定します。モニタするアプリケーション プロトコルを識別するには、アプリケーション デテクタをアクティブにする必要があります。  従来のデバイスの場合、この機能には制御ライセンスが必要であることに注意してください。
パターン	検出するパターンを指定します。このフィールドは、カスタム データ タイプの場合にのみ存在します。

関連トピック

[ディテクタのアクティブおよび非アクティブの設定 \(2118 ページ\)](#)

## システム提供のセンシティブ データのタイプ

それぞれの侵入ポリシーには、よく使用されるデータパターンを検出するためのシステム提供のデータ タイプが含まれています。これらのデータ パターンには、クレジットカード番号、電子メールアドレス、米国の電話番号、および米国の社会保障番号などがあります (番号にはハイフン付きのパターン、ハイフン抜きのパターンがあります)。

それぞれのシステム提供のデータ タイプは、ジェネレータ ID (GID) が 138 に設定された単一のセンシティブ データのプリプロセッサ ルールに関連付けられます。侵入ポリシーで関連する機密データ ルールを有効にして、ポリシーで使用する各データ タイプに対してイベントを生成し、インライン展開では、違反パケットをドロップします。する必要があります。

次の表に、各データ タイプの説明と対応するプリプロセッサ ルールの一覧を示します。

表 110: システム提供のセンシティブ データのタイプ

データ タイプ	説明	プリプロセッサ ルール GID:SID
クレジットカード番号	Visa <sup>®</sup> 、MasterCard <sup>®</sup> 、Discover <sup>®</sup> 、および American Express <sup>®</sup> の 15 桁または 16 桁のクレジットカード番号 (通常の区切り文字として使用されるハイフンまたはスペースが含まれるパターンと含まれないパターン) に一致します。また、Luhn アルゴリズムを使用してクレジットカード番号の検査数字を確認します。	138:2

データタイプ	説明	プリプロセッサルールGID:SID
電子メールアドレス	電子メールアドレスに一致します。	138:5
米国の電話番号	米国の電話番号 (\\d\\{3\\}) ?\\d\\{3\\}-\\d\\{4\\} のパターンに準拠) に一致します。	138:6
米国の社会保障番号 (ハイフンなし)	米国の9桁の社会保障番号 (有効な3桁のエリア番号と有効な2桁のグループ番号が含まれ、ハイフンを使用していない番号) に一致します。	138:4
米国の社会保障番号 (ハイフンあり)	米国の9桁の社会保障番号 (有効な3桁のエリア番号と有効な2桁のグループ番号が含まれ、ハイフンを使用している番号) に一致します。	138:3

社会保障番号以外の9桁の番号からの誤検出を軽減するために、プリプロセッサでは、各社会保障番号の4桁のシリアル番号の前にある3桁のエリア番号と2桁のグループ番号を検証するアルゴリズムを使用します。プリプロセッサは2009年11月末までの社会保障グループ番号を検証します。

## センシティブデータ検出の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	保護またはコントロール	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

センシティブデータ検出は、Firepower システムのパフォーマンスに非常に大きな影響を与える可能性があるため、以下のガイドラインに従うことをお勧めします。

- 基本侵入ポリシーとして [アクティブなルールなし (No Rules Active) ] デフォルトポリシーを選択します。
- 次の設定が対応するネットワーク分析ポリシーで有効になっていることを確認します。
  - [アプリケーション層プリプロセッサ (Application Layer Preprocessors) ] の下の [FTP と Telnet の構成 (FTP and Telnet Configuration) ]



- [トランスポートまたはネットワーク レイヤ プロセッサ (Transport/Network Layer Preprocessors) ] の下の [IP 最適化 (IP Defragmentation) ] および [TCP ストリームの構成 (TCP Stream Configuration) ]

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

## 手順

- ステップ 1** [ポリシー (Policies) ] > [アクセスコントロール (Access Control) ] > [侵入 (Intrusion) ] を選択します。
- ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。  
代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3** ナビゲーション パネルで [詳細設定 (Advanced Settings) ] をクリックします。
- ステップ 4** [特定の脅威検出 (Specific Threat Detection) ] の下の [センシティブデータ検出 (Sensitive Data Detection) ] が無効になっている場合は、[有効化 (Enabled) ] をクリックします。
- ステップ 5** [センシティブデータ検出 (Sensitive Data Detection) ] の横にある編集アイコン (✎) をクリックします。
- ステップ 6** 次の選択肢があります。
  - [グローバルセンシティブデータ検出オプション \(1663 ページ\)](#) の説明に従って、グローバル設定を変更します。
  - [ターゲット (Targets) ] セクションでデータ タイプを選択し、[個別のセンシティブデータタイプのオプション \(1664 ページ\)](#) の説明に従って、データタイプ構成を変更します。
  - カスタムセンシティブデータを検査するには、[カスタム機密データタイプ \(1671 ページ\)](#) を参照してください。
- ステップ 7** データ タイプでモニタするアプリケーションプロトコルを追加または削除します。[監視対象のアプリケーションプロトコルおよび機密データ \(1668 ページ\)](#) を参照してください。  
(注) FTP トラフィックでセンシティブデータを検出するには、Ftp data アプリケーションプロトコルを追加します。
- ステップ 8** オプションで、センシティブデータプリプロセッサルールを表示するには、[センシティブデータ検出のルールの設定 (Configure Rules for Sensitive Data Detection) ] をクリックします。  
リストされているルールを有効または無効にすることができます。[ルール (Rules) ] ページで使用可能なその他の操作 (ルールの抑制、レートベース攻撃防止など) のセンシティブデータルールも設定できます。詳細については、[侵入ルールのタイプ \(1620 ページ\)](#) を参照してください。

**ステップ 9** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーションパネルで [ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

ポリシーでセンシティブデータプリプロセッサルールを有効にして、センシティブデータ検出を有効にしていなければ、変更をポリシーに保存する際に、センシティブデータ検出を有効にするよう求めるプロンプトが出されます。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

### 次のタスク

- 侵入イベントを生成する場合は、センシティブデータ検出ルール (138:2、138:3、138:4、138:5、138:6、138:>999999、または 139:1) を有効にします。詳細については、[侵入ルールの状態 \(1639 ページ\)](#)、[グローバルセンシティブデータ検出オプション \(1663 ページ\)](#)、[システム提供のセンシティブデータのタイプ \(1665 ページ\)](#)、および[カスタム機密データタイプ \(1671 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[特別なケース : FTP トラフィックでのセンシティブデータの検出 \(1670 ページ\)](#)

## 監視対象のアプリケーションプロトコルおよび機密データ

各データタイプでモニタするアプリケーションプロトコルを最大 8 つ指定できます。選択するアプリケーションプロトコルごとに、少なくとも 1 つのディテクタを有効にする必要があります。デフォルトでは、すべてのディテクタがアクティブになっています。有効になっているディテクタがないアプリケーションプロトコルについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザ定義ディテクタが有効になります。

各データタイプをモニタするアプリケーションプロトコルまたはポートを少なくとも 1 つ指定する必要があります。ただし、FTP トラフィックでセンシティブデータを検出する場合を除き、シスコでは最も包括的なカバレッジにするために、アプリケーションプロトコルを指定する際には対応するポートを指定することを推奨しています。たとえば、HTTP を指定するとしたら、既知の HTTP ポート 80 を設定することをお勧めします。このように設定すると、ネットワークの新しいホストが HTTP を実装する場合には、システムは新しい HTTP アプリケーションプロトコルを検出する間、ポート 80 をモニタします。

FTP トラフィックでセンシティブデータを検出する場合は、FTP data アプリケーションプロトコルを指定する必要があります。この場合、ポート番号を指定する利点はありません。

関連トピック

[ディテクタのアクティブおよび非アクティブの設定](#) (2118 ページ)

[特別なケース：FTP トラフィックでのセンシティブデータの検出](#) (1670 ページ)

## モニタ対象のアプリケーションプロトコルの選択

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Control	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

モニタ対象のアプリケーションプロトコルは、システムが提供するセンシティブデータタイプとカスタムのセンシティブデータタイプの両方で指定できます。選択するアプリケーションプロトコルはポリシー固有になります。

手順

- ステップ 1 [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。
- ステップ 2 編集するポリシーの横にある編集アイコン (✎) をクリックします。  
代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3 ナビゲーションパネルで [詳細設定 (Advanced Settings)] をクリックします。
- ステップ 4 [特定の脅威検出 (Specific Threat Detection)] の下の [センシティブデータ検出 (Sensitive Data Detection)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。
- ステップ 5 [センシティブデータの検出 (Sensitive Data Detection)] の横にある編集アイコン (✎) をクリックします。
- ステップ 6 [データタイプ (Data Types)] の下でデータタイプの名前をクリックします。
- ステップ 7 [アプリケーションプロトコル (Application Protocols)] フィールドの横にある編集アイコン (✎) をクリックします。
- ステップ 8 次の選択肢があります。
  - モニタするアプリケーションプロトコルを追加するには、[使用可能 (Available)] リストからアプリケーションプロトコルを 1 つ以上選択して、右矢印 ([>]) ボタンをクリックします。モニタするアプリケーションプロトコルは、8 つまで追加できます。
  - モニタ対象からアプリケーションプロトコルを削除するには、[有効 (Enabled)] リストから削除するプロトコルを選択して、左矢印 ([<]) ボタンをクリックします。
- ステップ 9 [OK] をクリックします。

**ステップ 10** 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、ナビゲーションウィンドウで [ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

ポリシーの変更を確定しない場合、最後の確定以降の変更は、別のポリシーを編集するときに破棄されます。

---

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[特別なケース：FTP トラフィックでのセンシティブデータの検出 \(1670 ページ\)](#)

## 特別なケース：FTP トラフィックでのセンシティブデータの検出

一般に、センシティブデータをモニタするトラフィックを決めるには、導入でのモニタ対象のポートを指定するか、アプリケーションプロトコルを指定します。

ただし、FTP トラフィックでセンシティブデータを検出するには、ポートまたはアプリケーションプロトコルを指定するだけでは不十分です。FTP トラフィックのセンシティブデータは、FTP アプリケーションプロトコルのトラフィックで検出されますが、FTP アプリケーションプロトコルは断続的に発生し、一時的なポート番号を使用するため、センシティブデータを検出するのが困難です。FTP トラフィックでセンシティブデータを検出するには、以下の設定を含めることが**必須**となります。

- FTP data アプリケーションプロトコルを指定すると、FTP トラフィックでのセンシティブデータの検出が可能になります。

FTP トラフィックでセンシティブデータを検出するという特殊な場合では、FTP data アプリケーションプロトコルを指定すると、検出が呼び出される代わりに、FTP トラフィックでセンシティブデータを検出するために FTP/Telnet プロセッサの高速処理が呼び出されます。

- FTP データ ディテクタが有効であることを確認します (デフォルトで有効にされています)。
- 設定に、センシティブデータをモニタするポートが少なくとも1つ含まれていることを確認します。

FTP トラフィックでセンシティブデータを検出することだけが目的の場合を除き (そのような場合はほとんどありません)、FTP ポートを指定する必要はありません。通常のセンシティブデータ設定には、HTTP ポートや電子メールポートなどの他のポートが含まれることになりま

す。モニタ対象の FTP ポートを 1 つだけ指定し、他のポートを指定しない場合、シスコでは FTP コマンドポート 23 を指定することを推奨しています。

#### 関連トピック

[FTP/Telnet デコーダ](#) (1874 ページ)

[ディテクタのアクティブおよび非アクティブの設定](#) (2118 ページ)

[センシティブ データ検出の設定](#) (1666 ページ)

## カスタム 機密データ タイプ

作成するカスタム データタイプごとに、単一の機密データプリプロセッサルールも作成します。このルールのジェネレータ ID (GID) は 138 で、Snort ID (SID) は 1000000 以上 (これは、ローカルルールの SID) です。マルチドメイン展開では、子孫ドメインで作成されたか、または子孫ドメインにインポートされたカスタム ルールの SID の先頭にドメイン番号が追加されます。たとえば、グローバルドメインに追加されたルールに 1000000 以上の SID があり、子孫ドメインに追加されたルールには [ドメイン番号]000000 以上の SID があります。

ポリシーで使用する各カスタム データタイプに対し、関連付けられた機密データルールを有効にして検出を有効にし、イベントを生成し、インライン展開では、違反パケットをドロップします。する必要があります。

機密データルールを有効にするには、設定ページに表示されるリンクを利用できます。このリンクを使用すると、すべてのシステム定義済み機密データルールおよびカスタム機密データルールを表示するフィルタリングされたビューの侵入ポリシーの [ルール (Rules)] ページが表示されます。また、侵入ポリシーの [ルール (Rules)] ページでローカルフィルタリングカテゴリを選択することで、カスタム機密データルールをカスタム ローカルルールとともに表示できます。カスタム機密データルールは、侵入ルールエディタ ページ ([オブジェクト (Objects)] > [侵入ルール (Intrusion Rules)]) には表示されないことに注意してください。

カスタム データタイプを作成すると、システム内の任意の侵入ポリシーで、マルチドメイン展開の場合は現在のドメイン内の侵入ポリシーでそれを有効にすることができます。カスタム データタイプを有効にするには、そのカスタム データタイプの検出に使用するポリシーで、関連する機密データルールを有効にする必要があります。

## カスタム機密データ タイプのデータ パターン

カスタム データタイプのデータパターンを定義するには、以下の要素からなる単純な正規表現のセットを使用します。

- 3 つのメタ文字
- メタ文字をリテラル文字として使用するためのエスケープ文字
- 6 文字クラス

メタ文字は正規表現内で特別な意味を持つリテラル文字です。

表 111: 機密データパターンのメタ文字

メタ文字	説明	例
?	先行する文字またはエスケープシーケンスのゼロまたは1つのオカレンスに一致します。つまり、先行する文字またはエスケープシーケンスはオプションです。	colou?r は、color または colour に一致します。
{n}	先行する文字またはエスケープシーケンスの n 回の繰り返しに一致します。	たとえば、\d{2} は 55、12 などに一致し、\1{3} は abc、www などに、\w{3} は a1B、25C などに、x{5} は xxxxx に一致します。
\	メタ文字を実際の文字として使用できます。また、事前定義された文字クラスを指定するためにも使われます。	その他、\? は疑問符に、\\ はバックスラッシュに、\d は数字に一致します。

特定の文字をリテラル文字として機密データプリプロセッサに正しく解釈させるには、バックスラッシュで文字をエスケープする必要があります。

表 112: 機密データパターンのエスケープ文字

使用するエスケープ文字	表現されるリテラル文字
\?	?
\{	{
\}	}
\\	\

カスタム機密データパターンを定義するときは、文字クラスを使用できます。

表 113: 機密データパターンの文字クラス

文字クラス	説明	文字クラスの定義
\d	ASCII 文字の数字 0 ~ 9 に一致します。	0 ~ 9
\D	ASCII 文字の数字ではないバイトに一致します。	0 ~ 9 以外
\l (小文字の「エル」)	任意の ASCII 文字に一致します。	a ~ z および A ~ Z

文字クラス	説明	文字クラスの定義
\L	ASCII 文字ではないバイトに一致します。	a ~ z および A ~ Z 以外
\w	任意の ASCII 英数字に一致します。 PCRE 正規表現とは異なり、アンダースコア ( _ ) は含まれないことに注意してください。	a ~ z、A ~ Z、および 0 ~ 9
\W	ASCII 英数字でないバイトに一致します。	a-zA-Z0-9 以外

プリプロセッサは、そのまま入力された文字を、正規表現の一部ではなく、リテラル文字として扱います。たとえば、データパターン `1234` は `1234` に一致します。

以下に、システム定義済み機密データルール 138:4 で使用するデータパターンの例を示します。このパターンでは、エスケープされた数値の文字クラス、複数個を示すメタ文字およびオプション指定子のメタ文字、リテラルハイフン ( - ) 文字、および左右の括弧 ( ) 文字を使用して、米国の電話番号を検出します。

```
(\d{3}) ?\d{3}-\d{4}
```

カスタムデータパターンを作成する際には注意が必要です。以下に、電話番号を検出するための別のデータパターンを示します。このパターンでは有効な構文を使用しているものの、多数の誤検出が発生する可能性があります。

```
(?\d{3})? ?\d{3}-?\d{4}
```

上記の 2 番目の例では、オプションの括弧、オプションのスペース、オプションのハイフンを組み合わせているため、目的とする以下のパターンの電話番号が検出されます。

- (555) 123-4567
- 555123-4567
- 5551234567

ただし、2 番目の例のパターンでは、以下の潜在的に無効なパターンも検出されて、結果的に誤検出となります。

- (555 1234567
- 555)123-4567
- 555) 123-4567

最後に、説明目的の極端な例として、小規模な企業ネットワーク上のすべての宛先トラフィックで小さいイベントしきい値を使用して、小文字の `a` を検出するデータパターンを作成するとします。このようなデータパターンは、わずかに数分で文字通り数百万ものイベントを生成することになり、システムを過負荷に陥らせる可能性があります。

## カスタム センシティブ データ タイプの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

マルチドメイン展開では、現在のドメインで作成されたセンシティブ データ タイプが表示されます。これは編集できます。また、先祖ドメインで作成されたデータタイプも表示されますが、これらは限定的に編集できます。先祖のデータタイプについては、名前およびパターンフィールドは読み取り専用として表示されますが、その他のオプションはポリシー固有の値に設定できます。

データタイプのセンシティブ データ ルールがいずれかの侵入ポリシーで有効にされている場合、そのデータタイプを削除することはできません。

### 手順

- ステップ 1 [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。
- ステップ 2 編集するポリシーの横にある編集アイコン (✎) をクリックします。  
代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3 ナビゲーション パネルで [詳細設定 (Advanced Settings)] をクリックします。
- ステップ 4 [特定の脅威検出 (Specific Threat Detection)] の下の [センシティブ データ検出 (Sensitive Data Detection)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。
- ステップ 5 [センシティブ データ検出 (Sensitive Data Detection)] の横にある編集アイコン (✎) をクリックします。
- ステップ 6 [データ タイプ (Data Types)] の横にある追加アイコン (+) をクリックします。
- ステップ 7 データタイプの名前を入力します。
- ステップ 8 このデータタイプで検出するパターンを入力します。[カスタム機密データタイプのデータパターン \(1671 ページ\)](#) を参照してください。
- ステップ 9 [OK] をクリックします。
- ステップ 10 必要に応じて、データタイプ名をクリックし、[個別のセンシティブ データタイプのオプション \(1664 ページ\)](#) で説明されているオプションを変更します。
- ステップ 11 必要に応じて、削除アイコン (🗑️) をクリックしてカスタムデータタイプを削除し、[OK] をクリックして確認します。



(注) いずれかの侵入ポリシーでデータ タイプのセンシティブ データ ルールが有効になっている場合は、そのデータタイプを削除できないことが警告されます。再度削除を試みる前に、影響を受けるポリシーでセンシティブ データ ルールを無効にする必要があります。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

**ステップ 12** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーションパネルで [ポリシー情報 (Policy Information) ] をクリックして、[変更を確定 (Commit Changes) ] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

**次のタスク**

- データ型を使用する各ポリシーで、関連付けられたカスタム センシティブ データの前処理ルールを有効にします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

**関連トピック**

[カスタムセンシティブ データ タイプの編集 \(1675 ページ\)](#)

## カスタムセンシティブ データ タイプの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

カスタム センシティブ データ タイプのすべてのフィールドを編集できます。ただし、名前またはパターンフィールドを変更すると、システム内のすべての侵入ポリシーのこれらの設定が変更されることに注意してください。その他のオプションは、ポリシー固有の値に設定できません。

マルチドメイン展開では、現在のドメインで作成されたセンシティブ データ タイプが表示されます。これは編集できます。また、先祖ドメインで作成されたデータタイプも表示されますが、これらは限定的に編集できます。先祖のデータタイプについては、名前およびパターンフィールドは読み取り専用として表示されますが、その他のオプションはポリシー固有の値に設定できます。

## 手順

- 
- ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。
- ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。
- 代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3** ナビゲーション パネルで [詳細設定 (Advanced Settings)] をクリックします。
- ステップ 4** [特定の脅威検出 (Specific Threat Detection)] の下の [センシティブ データ検出 (Sensitive Data Detection)] が無効になっている場合は、[有効 (Enabled)] をクリックします。
- ステップ 5** [センシティブ データ検出 (Sensitive Data Detection)] の横にある [編集 (Edit)] をクリックします。
- ステップ 6** [ターゲット (Targets)] セクションで、カスタム データ タイプの名前をクリックします。
- ステップ 7** [データ タイプの名前およびパターンの編集 (Edit Data Type Name and Pattern)] をクリックします。
- ステップ 8** データタイプの名前およびパターンを変更します。[カスタム機密データタイプのデータパターン \(1671 ページ\)](#) を参照してください。
- ステップ 9** [OK] をクリックします。
- ステップ 10** 残りのオプションをポリシー固有の値に設定します。[個別のセンシティブ データ タイプのオプション \(1664 ページ\)](#) を参照してください。
- ステップ 11** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーションパネルで [ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。
- 変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。
- 

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。



## 第 74 章

# 侵入イベント ログイングのグローバル制限

次のトピックでは、侵入イベント ログイングをグローバルに制限する方法について説明します。

- [グローバル ルールのしきい値の基本 \(1677 ページ\)](#)
- [グローバル ルールしきい値オプション \(1678 ページ\)](#)
- [グローバルなしきい値の設定 \(1681 ページ\)](#)
- [グローバルしきい値の無効化 \(1682 ページ\)](#)

## グローバル ルールのしきい値の基本

グローバルルールのしきい値は、侵入ポリシーによってイベント ログイングの限界を設定します。すべてのトラフィックに対するグローバルルールのしきい値を設定して、指定された期間に特定の送信元または宛先からのイベントがポリシーで記録および表示される頻度を制限できます。ポリシー内で共有オブジェクトのルール、標準テキストルール、またはプリプロセッサルールごとにしきい値を設定できます。グローバルしきい値を設定すると、上書きする特定のしきい値を指定していないポリシー内の各ルールでそのしきい値が適用されます。しきい値により、多数のイベントでいっぱいになることを回避できます。

すべての侵入ポリシーにはデフォルトのグローバルルールしきい値が含まれていて、デフォルトですべての侵入ルールとプリプロセッサルールに適用されます。このデフォルトのしきい値は、宛先へのトラフィックでのイベントの数を 60 秒あたり 1 個のイベントに制限しています。

次の操作を実行できます。

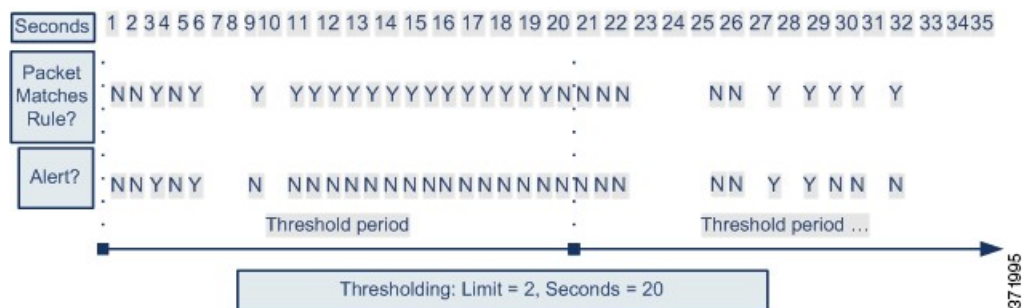
- グローバルしきい値の変更。
- グローバルしきい値の無効化。
- 特定のルールに個別のしきい値を設定して、グローバルしきい値の上書き。

たとえば、グローバル制限しきい値を 60 秒ごとに 5 個のイベントに設定してから、SID 1315 について特定のしきい値として 60 秒ごとに 10 個のイベントに設定できます。他のすべてのルールでは 60 秒ごとに 6 個以上のイベントは生成されませんが、SID 1315 では 60 秒ごとに最大 10 個のイベントが生成されます。



**ヒント** 複数の CPU を搭載した管理対象デバイスでグローバルしきい値または個別のしきい値を設定すると、予想より多くのイベントが生成される場合があります。

次の図で、グローバルルールのしきい値がどのように機能するかを示します。この例では、特定のルールに対して攻撃が進行中です。グローバル制限しきい値は、各ルールのイベント生成が 20 秒あたり 2 つのイベントに制限されるように設定されています。期間は 1 秒で始まり 21 秒で終わることに注意してください。期間が終了すると、サイクルが再び開始され、次の 2 つのルール一致によってイベントが生成されます。その後、その期間にさらにイベントが生成されることはありません。



## グローバルルールしきい値オプション

デフォルトのしきい値では、各ルールのイベント生成が、同じ宛先に送られるトラフィックで 60 秒あたり 1 つのイベントに制限されます。グローバルルールしきい値オプションのデフォルト値は次のとおりです。

- タイプ (Type) : 制限 (Limit)
- 追跡対象 (Track By) : 宛先 (Destination)
- カウント (Count) : 1
- 秒 (Seconds) : 60

これらのデフォルト値は次のように変更することができます。

表 114: しきい値のタイプ

オプション	説明
制限 (Limit)	<p>指定された数のパケット (count 引数によって指定される) が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。</p> <p>たとえば、タイプを [制限 (Limit)] に、[カウント (Count)] を 10 に、[秒 (Seconds)] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分間に発生した最初の 10 個を表示した後、イベントの記録を停止します。</p>
しきい値 (Threshold)	<p>指定された数のパケット (count 引数によって指定される) が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。</p> <p>たとえば、タイプを [しきい値 (Threshold)] に、[カウント (Count)] を 10 に、[秒 (Seconds)] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[秒 (Seconds)] と [カウント (Count)] のカウンタを 0 にリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。</p>

オプション	説明
両方	<p>指定された数（カウント）の packets がルールをトリガーとして使用した後で、指定された期間ごとに1回イベントを記録して表示します。</p> <p>たとえば、タイプを [両方（Both）] に、[カウント（Count）] を 2 に、[秒（Seconds）] を 10 に設定した場合、イベント数は以下ようになります。</p> <ul style="list-style-type: none"> <li>• ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。</li> <li>• ルールが 10 秒間に 2 回トリガーされた場合、システムは1つのイベントを生成します（ルールが2回目にトリガーとして使用されたときにしきい値が満たされるため）。</li> <li>• ルールが 10 秒間に 4 回トリガーされた場合、システムは1つのイベントを生成します（ルールが2回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される）。</li> </ul>

[追跡対象（Track By）] オプションにより、イベントインスタンスの数が送信元 IP アドレスと宛先 IP アドレスのどちらに基づいて計算されるかが決まります。

また、しきい値を定義するインスタンスの数と期間を次のように指定できます。

表 115: インスタンス/時間のしきい値設定オプション

オプション	説明
メンバー数（Count）	<p>[制限（Limit）] しきい値の場合は、しきい値を満たすために必要な、追跡する IP アドレスまたはアドレス範囲単位で指定された期間単位のイベントインスタンスの数。</p> <p>[しきい値（Threshold）] しきい値の場合は、しきい値として使用するルールの一致回数。</p>

オプション	説明
秒 (Seconds)	<p>[制限 (Limit)] しきい値の場合は、攻撃を追跡する期間の秒数。</p> <p>[しきい値 (Threshold)] しきい値の場合は、カウントをリセットするまでの経過時間 (秒数)。しきい値タイプを [制限 (Limit)] に、トラッキングを [送信元 (Source)] に、[カウント (Count)] を 10 に、[秒 (Seconds)] を 10 に設定した場合、特定の送信元ポートで 10 秒間に発生した最初の 10 のイベントを記録し表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。</p>

関連トピック

[グローバルなしきい値の設定 \(1681 ページ\)](#)

[侵入イベントのしきい値 \(1641 ページ\)](#)

## グローバルなしきい値の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

- ステップ 1 [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択します。
- ステップ 2 編集するポリシーの横にある編集アイコン (✎) をクリックします。  
代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3 ナビゲーションパネルで [詳細設定 (Advanced Settings)] をクリックします。
- ステップ 4 [侵入ルールしきい値 (Intrusion Rule Thresholds)] で [グローバルルールしきい値 (Global Rule Thresholding)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

- ステップ 5** [グローバルルールしきい値 (Global Rule Thresholding)] の横にある編集アイコン (✎) をクリックします。
- ステップ 6** [タイプ (Type)] オプション ボタンを使用して、[秒 (Seconds)] フィールドで指定された時間内に適用するしきい値のタイプを指定します。
- ステップ 7** [追跡対象 (Track By)] オプション ボタンを使用して、追跡方法を指定します。
- ステップ 8** [カウント (Count)] フィールドに値を入力します。
- ステップ 9** [秒 (Seconds)] フィールドに値を入力します。
- ステップ 10** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。
- 変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[グローバルルールしきい値オプション \(1678 ページ\)](#)

[レイヤでの侵入ルールの設定 \(1603 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## グローバルしきい値の無効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

デフォルトですべてのルールにしきい値を適用するのではなく、特定のルールに関するイベントにしきい値を適用する場合は、最高位のポリシー階層でグローバルしきい値を無効にできます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

#### 手順

- ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)] を選択します。



**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション ウィンドウで [詳細設定 (Advanced Settings)] をクリックします。

**ステップ 4** [侵入ルールしきい値 (Intrusion Rule Thresholds)] で、[グローバルルールしきい値 (Global Rule Thresholding)] の隣にある [無効 (Disabled)] をクリックします。

**ステップ 5** 最後のポリシーの確定以降にこのポリシーに加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

---

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

- [競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)
- [レイヤでの侵入ルールの設定 \(1603 ページ\)](#)





## 第 75 章

# 侵入ルール エディタ

以下のトピックでは、侵入ルール エディタの使用方法について説明します。

- [侵入ルールの編集について \(1685 ページ\)](#)
- [ルールの詳細 \(1686 ページ\)](#)
- [カスタム ルールの作成 \(1701 ページ\)](#)
- [ルールの検索 \(1706 ページ\)](#)
- [侵入ルール エディタ ページでのルールのフィルタリング \(1708 ページ\)](#)
- [侵入ルールのキーワードと引数 \(1712 ページ\)](#)

## 侵入ルールの編集について

侵入ルールは、ネットワークの脆弱性を不正利用する試みを検出するために使用するキーワードや引数です。ネットワークトラフィックの分析では、パケットを各ルールで指定した条件と比較します。パケットのデータがルールで指定したすべての条件に一致すると、そのルールがトリガーされます。アラートルールであれば、侵入イベントが生成されます。通過ルールであれば、トラフィックを無視します。インライン展開の廃棄ルールでは、システムがパケットを破棄してイベントを生成します。侵入イベントは、Firepower Management Center の Web インターフェイスから表示して評価できます。

Firepower システムの侵入ルールには、共有オブジェクトルールと標準テキスト ルールの 2 種類があります。Cisco Talos Security Intelligence and Research Group (Talos) では、共有オブジェクトルールを使うことにより、従来の標準テキストルールではできなかった方法で脆弱性に対する攻撃を検出できます。共有オブジェクトルールを作成することはできません。独自の侵入ルールを作成する場合は、標準テキストルールを作成します。

発生する可能性のあるイベントのタイプを調整するために、カスタム標準テキストルールを作成することができます。このマニュアルでは特定のエクスプロイトの検出を目的とするルールについて説明することもあります。優秀なルールのほとんどは、特定の既知のエクスプロイトではなく既知の脆弱性を悪用しようとするトラフィックをターゲットとすることに注意してください。ルールを作成してルールのイベントメッセージを指定することにより、攻撃とポリシー回避を示唆するトラフィックをより簡単に識別できます。

カスタム侵入ポリシーでカスタム標準テキストルールを有効にすると、一部のルールキーワードと引数では、トラフィックを特定の方法で最初に復号化または前処理する必要があることに留意してください。この章では、前処理を制御するネットワーク分析ポリシーで設定する必要があるオプションについて説明します。注意点として、必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。



**注意** 作成した侵入ルールを実稼働環境で使用する前に、制御されたネットワーク環境で必ずテストしてください。不適切に作成された侵入ルールは、システムのパフォーマンスに重大な影響を与える可能性があります。

マルチドメイン展開では、現在のドメインで作成されたルールが表示されます。これは編集できます。先祖ドメインで作成されたルールも表示されますが、これは編集できません。下位のドメインで作成されたルールを表示および編集するには、そのドメインに切り替えます。システム提供の侵入ルールはグローバルドメインに属します。子孫ドメインの管理者は、これらのシステムルールをローカルにコピーして編集できます。

## ルールの詳細

すべての標準テキストルールには、ルールヘッダーとルールオプションという2つの論理セクションが含まれています。ルールヘッダーの内容は次のとおりです。

- ルールのアクションまたはタイプ
- プロトコル
- 送信元および宛先の IP アドレスとネットマスク
- 送信元から宛先へのトラフィック フローを示す方向インジケータ
- 送信元ポートと宛先ポート

ルール オプション セクションの内容は次のとおりです。

- イベント メッセージ
- キーワードとそのパラメータおよび引数
- ルールをトリガーとして使用するためにパケットのペイロードが一致しなければならないパターン
- パケットのどの部分をルールエンジンで検査するかの指定

次の図に、ルールの構成要素を示します。

Rule Header

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
```

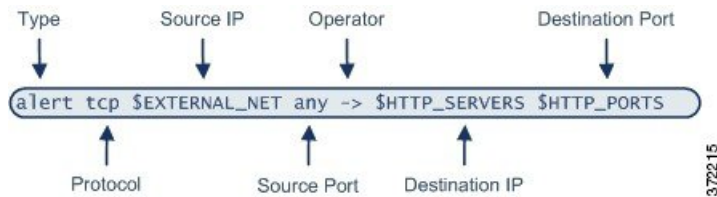
Rule Keywords and Arguments

```
(msg:"WEB-IIS newdsn.exe access";
flow:to_server,established; uricontent:"/scripts/
tools/newdsn.exe"; nocase; metadata:service http;
reference:bugtraq,1818; reference:cve,1999-0191;
reference:nessus,10360; classtype:web-application-
activity; sid:1024; rev:10; )
```

ルールのオプションセクションは、カッコで囲まれたセクションであることに注意してください。侵入ルール エディタは、標準テキスト ルールの作成を支援する使いやすいインターフェイスを備えています。

## 侵入ルール ヘッダー

すべての標準テキストルールおよび共有オブジェクトルールに、パラメータと引数を含むルールヘッダーがあります。ルールヘッダーの構成要素を以下に示します。



次の表では、上記のルールヘッダーの各部分について説明します。

表 116: ルールヘッダーの値

ルールヘッダーのコンポーネント	値の例	機能
操作	alert	トリガー時に侵入イベントを生成します。
プロトコル	tcp	TCP トラフィックのみをテストします。
送信元 IP アドレス	\$EXTERNAL_NET	内部ネットワーク上に存在しないホストから送られてきたトラフィックをテストします。
送信元ポート	任意	発信元ホスト上の任意のポートから送られてきたトラフィックをテストします。
演算子	->	(このネットワーク上の Web サーバに向かう) 外部トラフィックをテストします。
宛先 IP アドレス	\$HTTP_SERVERS	この内部ネットワーク上の Web サーバとして指定された任意のホストに送られるトラフィックをテストします。

ルールヘッダーのコンポーネント	値の例	機能
宛先ポート	\$HTTP_PORTS	この内部ネットワーク上の HTTP ポートに送られるトラフィックをテストします。



(注) 前述の例では、ほとんどの侵入ルールの場合と同様に、デフォルト変数が使用されています。

#### 関連トピック

[変数セット](#) (444 ページ)

## 侵入ルール ヘッダー アクション

各ルールヘッダーには、パケットがルールをトリガーとして使用したときにシステムで行われるアクションを指定するパラメータが1つ含まれています。アクションが[アラート (alert)]に設定されたルールは、それをトリガーとして使用したパケットに関する侵入イベントを生成し、そのパケットの詳細をログに記録します。アクションが *pass* に設定されたルールは、それをトリガーとして使用したパケットに関するイベントを生成せず、そのパケットの詳細も記録しません。



(注) インライン展開において、ルール状態が[ドロップしてイベントを生成する (Drop and Generate Events)]に設定されたルールは、それをトリガーとして使用したパケットに関する侵入イベントを生成します。また、パッシブ展開で廃棄ルールを適用した場合は、ルールがアラートルールとして機能します。

デフォルトでは、パスルールがアラートルールをオーバーライドします。パスルールを作成することで、アラートルールを無効にする代わりに、パスルールで定義された基準を満たすパケットが特定の状況でアラートルールをトリガーとして使用しないことを指定できます。たとえば、ユーザ "anonymous" として FTP サーバにログインする試行を検索するルールをアクティブのままにする必要があるとします。ただし、1つ以上の正式な匿名 FTP サーバがネットワークに存在する場合、そのような特定のサーバで匿名ユーザにより最初のルールがトリガーとして使用されないことを指定するパスルールを作成し、アクティブにすることができます。

侵入ルールエディタで、[アクション (Action)] リストからルールタイプを選択します。

## 侵入ルール ヘッダー プロトコル

各ルールヘッダーで、ルールにより検査されるトラフィックのプロトコルを指定する必要があります。次のネットワーク プロトコルを分析対象として指定できます。

- ICMP (Internet Control Message Protocol)
- インターネットプロトコル (IP)



(注) プロトコルが ip に設定されている場合、システムは侵入ルールヘッダー内のポート定義を無視します。

- 伝送制御プロトコル (TCP)
- ユーザ データグラム プロトコル (UDP)

TCP、UDP、ICMP、IGMP など、IANA によって割り当てられたすべてのプロトコルを検査するには、プロトコルタイプとして **IP** を使用します。



(注) 現在のところ、IP ペイロード内の次のヘッダー (TCP ヘッダーなど) でパターンを照合するルールを作成することはできません。代わりに、最後にデコードされたプロトコルからコンテンツ照合が始まります。次善策として、ルールオプションを使用して TCP ヘッダー内のパターンを照合できます。

侵入ルールエディタで、[プロトコル (Protocol)] リストからプロトコルタイプを選択します。

**関連トピック**

[侵入ルールヘッダープロトコル \(1688 ページ\)](#)

## 侵入ルールヘッダーの方向

ルールによる検査対象となるパケットが進むべき方向を、ルールヘッダー内で指定できます。以下の表は、それらのオプションを示しています。

表 117: ルールヘッダー内の方向オプション

使用するフィルタ	テスト対象
指向性	指定された送信元 IP アドレスから指定された宛先 IP アドレスに向かうトラフィックのみ
双方向	指定された送信元 IP アドレスと宛先 IP アドレスの間を移動するすべてのトラフィック

## 侵入ルールヘッダーの送信元と宛先の IP アドレス

パケット検査の対象を、特定の IP アドレスから発信されたパケットまたは特定の IP アドレスに向かうパケットに制限すると、システムが実行しなければならないパケット検査の量が減ります。さらに、ルールをより具体化し、送信元および宛先 IP アドレスが疑わしい動作を示していないパケットに対してルールがトリガーとして使用される可能性をなくすと、誤検出も減ります。



**ヒント** システムは IP アドレスのみを認識し、送信元/宛先 IP アドレスのホスト名を受け入れません。

侵入ルールエディタの [送信元 IP (Source IPs)] フィールドと [宛先 IP (Destination IPs)] フィールドで、送信元および宛先の IP アドレスを指定します。

標準テキストルールの作成時には、必要に応じて、さまざまな方法で IPv4 アドレスと IPv6 アドレスを指定できます。単一の IP アドレス、any、IP アドレス リスト、CIDR 表記、プレフィクス長、ネットワーク変数、ネットワーク オブジェクトあるいはネットワーク オブジェクトグループを指定できます。加えて、1つの特定の IP アドレスまたは IP アドレスのセットを除外するよう指定できます。IPv6 アドレスを指定するときには、RFC 4291 で定義された任意のアドレス指定規則を使用できます。

マルチドメイン展開では、この設定でリテラル IP アドレスを使用すると、予期しない結果になる可能性があります。たとえば、グローバル ドメイン内にリテラル送信元 IP アドレス (192.0.2.2) の侵入ルールを作成し、子孫ドメインで使用する侵入ポリシーでそのルールを有効にするとします。この場合、発生したイベントは子孫ドメイン A (192.0.2.2 が DeviceA を表すドメイン) と子孫ドメイン B (192.0.2.2 が DeviceB を表すドメイン) の両方で確認されることとなりますが、侵入に対する脆弱性を確実に示すのは、いずれか一方のイベントのセットだけです。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

## 侵入ルールの IP アドレスの構文

次の表では、送信元と宛先の IP アドレスを指定するさまざまな方法を要約します。

表 118: 送信元/宛先 IP アドレスの構文

指定する項目	使用するフィルタ	例
任意の IP アドレス	任意	任意
1つの特定の IP アドレス	IP アドレス 同じルール内に IPv4 と IPv6 の送信元アドレスと宛先アドレスを混在させないでください。	192.168.1.1 2001:db8::abcd
IP アドレスのリスト	複数の IP アドレスをカンマで区切り、それを大カッコ ([]) で囲む	[192.168.1.1,192.168.1.15] [2001:db8::b3ff, 2001:db8::0202]
IP アドレスのブロック	IPv4 CIDR ブロックまたは IPv6 アドレス プレフィクス表記	192.168.1.0/24 2001:db8::/32
特定の 1つの IP アドレスまたはアドレスセットを除くすべて	拒否する IP アドレスの前に付ける「!」記号	!192.168.1.15 !2001:db8::0202:b3ff:fe1e



指定する項目	使用するフィルタ	例
特定の 1 つ以上の IP アドレスを除く、IP アドレスブロック内のすべて	アドレス ブロックの後に、除外アドレスのリストまたはブロック	[10.0.0/8, !10.2.3.4, !10.1.0.0/16]  [2001:db8::/32, !2001:db8::8329, !2001:db8::0202]
ネットワーク変数で定義された IP アドレス	§ で始まる大文字の変数名  プリプロセッサルールは、侵入ルールで使われているネットワーク変数で定義されたホストとは無関係に、イベントをトリガーできることに注意してください。	\$HOME_NET
IP アドレス変数で定義されたアドレスを除く、すべての IP アドレス	大文字の変数名の前に !\$ を付ける	!\$HOME_NET
ネットワークオブジェクトまたはネットワークオブジェクトグループで定義された IP アドレス	!{object_name} という形式でオブジェクト名またはグループ名。	\${192.168sub16}
ネットワークオブジェクトまたはネットワークオブジェクトグループで定義されたアドレスを除く、すべての IP アドレス	オブジェクト名またはグループ名を中カッコ ({} ) で囲み、その前に !\$ を付ける。	!\${192.168sub16}

以下の説明では、いくつかの IP アドレス入力方法に関する追加情報を提供します。

### 任意の IP アドレス

任意の IPv4 または IPv6 アドレスを示す「any」という単語を、ルールの送信元 IP アドレスまたは宛先 IP アドレスとして指定できます。

たとえば、次のルールでは [Source IPs] フィールドと [Destination IPs] フィールドで引数 **any** を使用して、任意の IPv4 または IPv6 の送信元または宛先アドレスを持つパケットを評価します。

```
alert tcp any any -> any any
```

また、任意の IPv6 アドレスを示すために :: を指定することもできます。

## 複数の IP アドレス

次の例に示すように、カンマを使って複数の IP アドレスを区切り、オプションで、非拒否リストを大カッコで囲むことにより、個別の IP アドレスを列挙できます。

```
[192.168.1.100,192.168.1.103,192.168.1.105]
```

IPv4 アドレスと IPv6 アドレスのいずれかだけを列挙することも、任意に組み合わせて列挙することもできます（次の例を参照）。

```
[192.168.1.100,2001:db8::1234,192.168.1.105]
```

以前のソフトウェアリリースでは IP アドレス リストを大カッコで囲む必要がありましたが、現在ではこれが必須でないことに注意してください。また、オプションで、リストを入力するときに各カンマの前または後にスペースを含めることができます。



(注) 否定リストは、大カッコで囲む必要があります。

また、IPv4 クラスレスドメイン間ルーティング (CIDR) 表記または IPv6 プレフィクス長を使用してアドレスブロックを指定することもできます。次に例を示します。

- 192.168.1.0/24 は、サブネット マスク 255.255.255.0 の 192.168.1.0 ネットワーク内の IPv4 アドレス、つまり 192.168.1.0 ~ 192.168.1.255 を指定します。
- 2001:db8::/32 は、プレフィクス長 32 ビットの 2001:db8:: ネットワーク内の IPv6 アドレス、つまり 2001:db8:: ~ 2001:db8:fff:fff:fff:fff:fff:fff を指定します。



ヒント IP アドレスのブロックを指定する必要があるが、CIDR またはプレフィクス長表記を単独で使ってそれを表現できない場合は、1つの IP アドレス リスト内でいくつかの CIDR ブロックとプレフィクス長を使用できます。

## ネットワーク オブジェクト

次の構文を使用して、ネットワーク オブジェクトまたはネットワーク オブジェクト グループを指定できます。

```
${object_name | group_name}
```

引数の説明

- `object_name` はネットワーク オブジェクトの名前です
- `group_name` はネットワーク オブジェクト グループの名前です

192.168sub16 という名前のネットワーク オブジェクトと all\_subnets という名前のネットワーク オブジェクト グループをすでに作成済みであるとし、ネットワーク オブジェクトを使用して IP アドレスを特定するには、たとえば次のように指定できます。

```
#{192.168sub16}
```

ネットワーク オブジェクト グループを使用するには、次のように指定できます。

```
#{all_subnets}
```

さらに、ネットワーク オブジェクトとネットワーク オブジェクト グループで否定を使用することもできます。次に例を示します。

```
!#{192.168sub16}
```

### IP アドレスの否定

特定の IP アドレスを否定するために感嘆符 (!) を使用できます。つまり、1 つ以上の特定の IP アドレスを除く、すべての IP アドレスに一致させることができます。たとえば、`!192.168.1.1` は 192.168.1.1 以外の任意の IP アドレスを、`!2001:db8:ca2e::fa4c` は 2001:db8:ca2e::fa4c 以外の任意の IP アドレスを指定します。

一連の IP アドレスを拒否するには、大かっこで囲んだ IP アドレスのリストの前に「!」記号を付けます。たとえば、`![192.168.1.1,192.168.1.5]` は 192.168.1.1 と 192.168.1.5 を除くすべての IP アドレスを定義します。



(注) IP アドレスのリストを否定するには、大カッコを使用する必要があります。

否定文字と一緒に IP アドレス リストを使用する場合は注意が必要です。たとえば、192.168.1.1 と 192.168.1.5 を除くすべてのアドレスと一致させるために `![192.168.1.1,192.168.1.5]` を使用した場合、システムはこの構文を「192.168.1.1 以外のすべて、または 192.168.1.5 以外のすべて」と解釈します。

192.168.1.5 は 192.168.1.1 ではなく、192.168.1.1 は 192.168.1.5 ではないため、この両方の IP アドレスが `![192.168.1.1,192.168.1.5]` という IP アドレス値に一致します。つまり、実質的に「any」を使用するのと同じです。

代わりに `![192.168.1.1,192.168.1.5]` を使用してください。システムはこの構文を「**192.168.1.1** でなく、しかも 192.168.1.5 でない」と解釈し、大カッコ内に列挙されたものを除くすべての IP アドレスに一致します。

論理的に言って、any を除外 (negation) と同時に使用できないことに注意してください。any を除外すると「アドレスなし」を意味することになります。

### 関連トピック

[変数セット](#) (444 ページ)

## 侵入ルールヘッダーの送信元および宛先ポート

侵入ルールエディタの [送信元ポート (Source Port)] フィールドと [宛先ポート (Destination Port)] フィールドで、送信元および宛先ポートを指定します。

## 侵入ルールのポート構文

Firepower System では、特定のタイプの構文を使用して、ルールヘッダーで使用されるポート番号を定義できます。



(注) プロトコルが ip に設定されている場合、システムは侵入ルールヘッダー内のポート定義を無視します。

次の例に示すように、カンマでポートを区切ることによって、ポートのリストを指定できます。

```
80, 8080, 8138, 8600-9000, !8650-8675
```

任意により、次の例は、ポートリストを括弧で囲む方法を示します。この方法は旧バージョンのソフトウェアでは必要でしたが、今後は括弧で囲む必要ありません。

```
[80, 8080, 8138, 8600-9000, !8650-8675]
```

次の例に示すように、否定されたポートリストは括弧で示す必要がある点にご注意ください：

```
![20, 22, 23]
```

次の表に、使用可能な構文を要約します。

表 119: 送信元宛先ポート構文

指定する項目	用途	例
任意のポート	任意	任意
1つの特定のポート	ポート番号	80
ポートの範囲	範囲内の最初のポート番号と最後のポート番号をダッシュでつなぐ	80-443
1つの特定のポートに等しい、またはより小さいすべてのポート	ポート番号の前にダッシュを付ける	-21
1つの特定のポートに等しい、またはより大きいすべてのポート	ポート番号の後ろにダッシュを付ける	80-
1つの特定のポートまたはポート範囲を除く、すべてのポート	否定する場合には、ポート、ポートリスト、ポート範囲の前に文字 ! を付けます。  否定が「ポートなし」を示す場合を除いて、すべてのポート宛先に論理上、否定を使用できる点にご注意ください。	!20
ポート変数で定義されるすべてのポート	§ の後ろに英大文字の変数名	\$HTTP_PORTS

指定する項目	用途	例
ポート変数で定義されるポートを除く、すべてのポート	!\$ の後ろに英大文字の変数名	!\$HTTP_PORTS

## 侵入イベント詳細

標準のテキストルールを作成するときには、ルールでエクスプロイト試行を検出する対象となる脆弱性についてのコンテキスト情報を含めることができます。また、脆弱性データベースへの外部参照を含めたり、組織内でイベントに設定するプライオリティを定義したりすることもできます。アナリストがイベントを認識すると、そのプライオリティ、エクスプロイト、および既知の対策についての情報をすぐに入手できます。

### メッセージ

ルールのトリガー時にメッセージとして表示される、意味のあるテキストを指定できます。メッセージを読むと、ルールで攻撃試行を検出する対象となった脆弱性の特性をすぐに理解できます。中カッコ ({} ) を除く、印字可能な任意の標準 ASCII 文字を使用できます。システムは、メッセージ全体を囲んでいる引用符を取り除きます。



#### ヒント

ルールメッセージの指定は必須です。また、空白文字のみ、1 つ以上の引用符のみ、1 つ以上のアポストロフィのみ、あるいは空白文字/引用符/アポストロフィだけの組み合わせでメッセージを構成することはできません。

侵入ルールエディタでイベントメッセージを定義するには、[メッセージ (Message) ] フィールドにイベントメッセージを入力します。

### 分類 (Classification)

ルールごとに、イベントの packets 表示に含める攻撃分類を指定できます。次の表に、それぞれの分類の名前と番号を示します。

表 120: ルールの分類

番号 (Number)	分類名	説明
1	not-suspicious	不審ではないトラフィック
2	unknown	不明なトラフィック
3	bad-unknown	有害な可能性のあるトラフィック
4	attempted-recon	情報漏えいが試行された
5	successful-recon-limited	情報漏えいが発生

番号 (Number)	分類名	説明
[6]	successful-recon-largescale	大規模な情報漏えい
7	attempted-dos	サービス妨害が試行された
8	successful-dos	サービス妨害 (DoS)
9	attempted-user	ユーザ特権の獲得が試行された
10	unsuccessful-user	ユーザ特権の獲得が失敗した
11	successful-user	ユーザ特権の獲得に成功
12	attempted-admin	管理者特権の獲得が試行された
13	successful-admin	管理者特権の獲得に成功
18	rpc-portmap-decode	RPC クエリのデコード
15	shellcode-detect	実行可能コードが検出された
16	string-detect	疑わしい文字列が検出された
17	suspicious-filename-detect	疑わしいファイル名が検出された
18	suspicious-login	疑わしいユーザ名を使用したログイン試行が検出された
19	system-call-detect	システム コールが検出された
20	tcp-connection	TCP 接続が検出された
21	trojan-activity	ネットワーク トロイの木馬が検出された
22	unusual-client-port-connection	通常とは異なるポートをクライアントが使用していた
23	network-scan	ネットワーク スキャンの検出
24	denial-of-service	サービス妨害攻撃の検出
25	non-standard-protocol	非標準プロトコルまたはイベントの検出
26	protocol-command-decode	一般的なプロトコル コマンド デコード
27	web-application-activity	脆弱な可能性のある Web アプリケーションへのアクセス
36	web-application-attack	Web アプリケーション攻撃
29	misc-activity	その他のアクティビティ

番号 (Number)	分類名	説明
30	misc-attack	その他の攻撃
31	icmp-event	一般的な ICMP イベント
32	inappropriate-content	不適切な内容が検出された
33	policy-violation	企業プライバシー侵害の可能性
34	default-login-attempt	デフォルトのユーザ名とパスワードによるログイン試行
35	sdf	機密データ
36	malware-cnc	既知のマルウェア コマンドと制御トラフィック
37	client-side-exploit	既知のクライアント側エクスプロイト試行
38	file-format	既知の悪意のあるファイルまたはファイルベースのエクスプロイト

### カスタム分類

定義したルールによって生成されるイベントの packets 表示記述の内容をもっとカスタマイズする必要がある場合には、カスタム分類を作成できます。

引数	説明
分類名	分類の名前。40 文字を超える文字を使用すると、ページが読みにくくなります。<>()\'" & \$ ; 文字および空白文字はサポートされていません。
分類の説明	分類の説明。英数字とスペースを使用できます。<>()\'" & \$ ; 文字はサポートされていません。
[プライオリティ (Priority) ]	[高 (High) ]、[中 (medium) ]、または [低 (low) ]。

### カスタム プライオリティ

デフォルトでは、ルールのイベント分類からルールのプライオリティが派生します。ただし、priority キーワードをルールに追加し、高、中、または低のプライオリティを選択することで、ルールの分類優先度を上書きすることができます。たとえば、Web アプリケーション攻撃を検出するルールに高プライオリティを割り当てるには、priority キーワードをルールに追加して、プライオリティとして [高 (high) ] を選択します。

## カスタム参照

reference キーワードを使用すると、イベントに関する外部 Web サイトや追加情報への参照を追加できます。参照を追加すると、アナリストは参照情報をすぐに利用できるため、パケットがルールをトリガーとして使用した理由を特定するのに役立ちます。次の表に、既知の 익스プロイトや攻撃についてのデータを提供する外部システムをいくつか示します。

表 121: 外部攻撃識別システム

システム ID (System ID)	説明	ID の例
bugtraq	[Bugtraq] ページ	8550
cve	[Common Vulnerabilities and Exposure] ページ	CAN-2003-0702
mcafee	[McAfee] ページ	98574
url	Web サイト参照	www.example.com?exploit=14
msb	Microsoft セキュリティ情報	MS11-082
nessus	[Nessus] ページ	10039
secure-url	セキュア Web サイト参照 (https://...)	intranet/exploits/exploit=14 任意のセキュア Web サイトで secure-url を使用できることに注意してください。

次のように、参照値を入力して参照を指定します。

```
id_system,id
```

ここで、id\_system はプレフィックスとして使用されるシステム、id は Bugtraq ID、CVE 番号、Arachnids ID、または URL (http://なし) です。

たとえば、Bugtraq ID 17134 に記載されている Microsoft Commerce Server 2002 サーバ上の認証バイパス脆弱性を指定するには、次の値を入力します。

```
bugtraq,17134
```

参照をルールに追加するときには、次の点に注意してください。

- カンマの後ろにスペースを入力しないでください。
- システム ID に大文字を使用しないでください。

## 関連トピック

[カスタム分類の追加](#) (1699 ページ)



[イベント優先順位の定義](#) (1699 ページ)

[イベント参照の定義](#) (1700 ページ)

## カスタム分類の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

マルチドメイン展開では、現在のドメインで作成されたカスタム分類がシステムで表示されません。これらの分類には、優先度を設定できます。先祖ドメインで作成されたカスタム分類も表示されますが、これらの分類には優先度は設定できません。下位のドメインで作成されたカスタム分類を表示および編集するには、そのドメインに切り替えます。

### 手順

**ステップ 1** ルールの作成または編集時に、[分類 (Classification)] ドロップダウンリストから [分類の編集 (Edit Classifications)] を選択します。

代わりに [分類の表示 (View Classifications)] が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 2** [侵入イベント詳細 \(1695 ページ\)](#) の説明に従い、[分類名 (Classification Name)] と [分類の説明 (Classification Description)] を入力します。

**ステップ 3** [優先度 (Priority)] ドロップダウン リストから分類の優先度を選択します。

**ステップ 4** [追加 (Add)] をクリックします。

**ステップ 5** [完了 (Done)] をクリックします。

### 次のタスク

- ルールの作成または編集を続けます。詳細については、[新規規則の作成 \(1702 ページ\)](#) または [既存の規則の変更 \(1703 ページ\)](#) を参照してください。

### 関連トピック

[カスタム ルールの作成](#) (1701 ページ)

## イベント優先順位の定義

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

## 手順

- 
- ステップ 1** ルールの作成または編集時に、[検出オプション (Detection Options)] ドロップダウン リストから [優先順位 (priority)] を選択します。
- ステップ 2** [Add Option] をクリックします。
- ステップ 3** [優先順位 (priority)] ドロップダウン リストから値を選択します。
- ステップ 4** [保存 (Save)] をクリックします。
- 

## 次のタスク

- ルールの作成または編集を続けます。詳細については、[新規ルールの作成 \(1702 ページ\)](#) または [既存のルールの変更 \(1703 ページ\)](#) を参照してください。

## 関連トピック

[カスタム ルールの作成 \(1701 ページ\)](#)

## イベント参照の定義

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

## 手順

- 
- ステップ 1** ルールの作成または編集時に、[検出オプション (Detection Options)] ドロップダウン リストから [参照 (reference)] を選択します。
- ステップ 2** [Add Option] をクリックします。
- ステップ 3** [侵入イベント詳細 \(1695 ページ\)](#) の説明に従って、[参照 (reference)] フィールドに値を入力します。
- ステップ 4** [保存 (Save)] をクリックします。
- 

## 次のタスク

- ルールの作成または編集を続けます。詳細については、[新規ルールの作成 \(1702 ページ\)](#) または [既存のルールの変更 \(1703 ページ\)](#) を参照してください。

## 関連トピック

[カスタム ルールの作成 \(1701 ページ\)](#)

# カスタム ルールの作成

カスタム侵入ルールは以下の方法で作成できます。

- 独自の標準テキスト ルールを作成する
- 既存の標準テキスト ルールを新規ルールとして保存する
- システムが提供する共有オブジェクト ルールを新規ルールとして保存する
- 先祖ルールを子孫ドメインにおける新規ルールとして保存する（マルチドメイン展開の場合）
- ローカルルール ファイルをインポートする

作成方法に関わらず、システムはカスタム ルールをローカル ルールに分類して保存します。

カスタム侵入ルールを作成すると、システムは一意的ルール番号（番号の形式はGID:SID:Rev）を割り当てます。この番号には次の要素が含まれます。

## GID

ジェネレータ ID。標準テキスト ルールでは、値は 1 です。すべての共有オブジェクト ルールを新規ルールとして保存する場合、値は 3 です。

## SID

Snort ID。ルールがシステム ルールのローカルルールであるかどうかを示します。新しいルールを作成すると、システムは次に使用可能なローカル ルール SID 番号を割り当てます。

ローカル ルールの SID 番号は 1000000 から始まり、新しいローカル ルールにつき番号が 1 ずつ増えます。マルチドメイン展開では、子孫ドメインで作成されたか、または子孫ドメインにインポートされたカスタムルールの SID の先頭にドメイン番号が追加されます。たとえば、グローバル ドメインに追加されたルールに 1000000 以上の SID があり、子孫ドメインに追加されたルールには [ドメイン番号]000000 以上の SID があります。

## Rev

改訂番号。新しいルールのリビジョン番号は 1 です。カスタムルールを変更するたびに、リビジョン番号が 1 ずつ増えます。

カスタム標準テキストルールでは、ルールヘッダー設定、ルールキーワード、およびルール引数を設定できます。特定のプロトコルを使用する、特定の IP アドレスまたはポートを行き来するトラフィックだけをルールで照合するよう、ルールヘッダーを設定できます。

システムが提供する標準テキスト ルールまたは共有オブジェクト ルールのカスタム ルールで変更できるルールヘッダー情報は、送信元と宛先ポートと IP アドレスなどの情報に限られません。ルールキーワードやルール引数は変更できません。

共有オブジェクトルールのヘッダー情報を変更して変更内容を保存すると、ルールの新しいインスタンスが作成され、ジェネレータ ID (GID) 3、およびカスタムルールとして次に使用可能な SID が割り当てられます。システムは、共有オブジェクトルールの新しいインスタンス

を予約済み `soid` キーワードにリンクします。これにより、新しく作成したルールが Cisco Talos Security Intelligence and Research Group (Talos) 作成のルールにマップされます。ユーザが作成した共有オブジェクトルールのインスタンスは削除できますが、Talos が作成した共有オブジェクトルールは削除できません。

## 新規ルールの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

### 手順

- ステップ 1** 次のいずれかの方法を使用して侵入ルールにアクセスします。
- [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)] を選択し、[侵入ルール (Intrusion Rules)] をクリックします。
  - [オブジェクト (Objects)] > [侵入ルール (Intrusion Rules)] を選択します。
- ステップ 2** [Create Rule] をクリックします。
- ステップ 3** [メッセージ (Message)] フィールドに値を入力します。
- ステップ 4** 次の各ドロップダウン リストから値を選択します。
- [分類 (Classification)]
  - 操作
  - プロトコル
  - 方向 (Direction)
- ステップ 5** 次のフィールドに値を入力します。
- [送信元 IP (Source IPs)]
  - [宛先 IP (Destination IPs)]
  - 送信元ポート (Source Port)
  - 宛先ポート (Destination Port)
- これらのフィールドに値を指定しない場合、システムは値 [すべて (any)] を使用します。
- (注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。
- ステップ 6** [検出オプション (Detection Options)] ドロップダウン リストから値を選択します。
- ステップ 7** [Add Option] をクリックします。
- ステップ 8** 追加したキーワードの引数を入力します。

**ステップ 9** 必要に応じて、手順 6～8 を繰り返します。

**ステップ 10** 複数のキーワードを追加した場合、以下を実行できます。

- キーワードの並べ替え：移動するキーワードの横にある上矢印または下矢印をクリックします。
- キーワードの削除：そのキーワードの横にある [X] をクリックします。

**ステップ 11** [新規として保存 (Save As New) ] をクリックします。

**次のタスク**

- 該当する侵入ポリシー内の新規または変更されたルールを有効にします ([侵入ポリシー内の侵入ルールの表示 \(1621 ページ\)](#) を参照)。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 既存のルールの変更

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

カスタム侵入ルールは変更できます。マルチドメイン展開では、現在のドメインに属しているカスタム侵入ルールのみを変更できます。

システム提供のルールと先祖ドメインに属しているルールは、新しいカスタムルールとしてローカルルール カテゴリに保存してから変更できます。

**手順**

**ステップ 1** 次のいずれかの方法を使用して侵入ルールにアクセスします。

- [ポリシー (Policies) ] > [アクセス コントロール (Access Control) ] > [侵入 (Intrusion) ] を選択し、[侵入ルール (Intrusion Rules) ] をクリックします。
- [オブジェクト (Objects) ] > [侵入ルール (Intrusion Rules) ] を選択します。

**ステップ 2** 変更するルールを見つけます。次の選択肢があります。

- フォルダからルールに移動します。
- ルールを検索します。[ルールの検索 \(1706 ページ\)](#) を参照してください。
- ルールが属しているグループにフィルタを適用します。[フィルタリングルール \(1711 ページ\)](#) を参照してください。

**ステップ 3** ルールの横にある編集アイコン (  ) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 4** ルールタイプに応じて、ルールを変更します。

(注) 共有オブジェクトルールのプロトコルは変更しないでください。これを変更すると、ルールの効果がなくなる可能性があります。

**ステップ 5** 次の選択肢があります。

- カスタムルールを編集していて、そのルールの現在のバージョンを上書きする場合は、[保存 (Save)] をクリックします。
- システム提供のルールまたは先祖ドメインに属しているルールを編集している場合や、カスタムルールを編集しているときに変更を新しいルールとして保存する場合は、[新規に保存 (Save As New)] をクリックします。

#### 次のタスク

- システム提供のルールの代わりにローカルで変更したルールを使用するには、[侵入ルールの状態 \(1639 ページ\)](#) の手順に従ってシステム提供のルールを非アクティブ化してから、ローカルルールをアクティブ化します。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[ルールの検索 \(1706 ページ\)](#)

[侵入ルールエディタ ページでのルールのフィルタリング \(1708 ページ\)](#)

## 侵入ルールへのコメントの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

任意の侵入ルールにコメントを追加できます。コメントにより、環境や条件の説明と、ルールやルールが検出する悪意あるプログラム、スクリプト (エクスプロイト) やポリシー違反の詳細を示すことができます。

マルチドメイン展開では、現在のドメインで作成されたコメントが表示されます。これは削除できます。先祖ドメインで作成されたコメントも表示されますが、これは削除できません。下位のドメインで作成されたコメントを表示するには、そのドメインに切り替えます。

## 手順

**ステップ 1** 次のいずれかの方法を使用して侵入ルールにアクセスします。

- [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)] を選択し、[侵入ルール (Intrusion Rules)] をクリックします。
- [オブジェクト (Objects)] > [侵入ルール (Intrusion Rules)] を選択します。

**ステップ 2** 注釈を付けるルールを探します。次の選択肢があります。

- フォルダからルールに移動します。
- ルールを探します。 [ルールの検索 \(1706 ページ\)](#) を参照してください。
- ルールが属するグループをフィルタします。 [フィルタリングルール \(1711 ページ\)](#) を参照してください。

**ステップ 3** ルールの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

**ステップ 4** [Rule Comment] をクリックします。

**ステップ 5** テキスト ボックスにコメントを入力します。

**ステップ 6** [コメントを追加 (Add a Comment)] をクリックします。

**ヒント** また、侵入イベントのパケット ビューで、ルール コメントを追加して表示することもできます。

## 次のタスク

- ルールの作成または編集を続けます。詳細については、 [新規ルールの作成 \(1702 ページ\)](#) または [既存のルールの変更 \(1703 ページ\)](#) を参照してください。

## 関連トピック

[ルールの検索 \(1706 ページ\)](#)

[イベント情報のフィールド \(2583 ページ\)](#)

# カスタム ルールの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入ポリシーで現在有効になっていないカスタムルールを削除することができます。システムにより提供されている標準テキストルールおよび共有オブジェクトルールは削除できません。マルチドメイン導入では、現在のドメインで作成されたローカルルールのみを削除できます。

削除されたルールは削除済みカテゴリに保存されます。削除済みのルールを、新しいルールの基準として使用することができます。侵入ポリシーの [Rules] ページには削除済みカテゴリが表示されないため、削除したカスタムルールを有効にすることはできません。



#### ヒント

カスタムルールには、変更されたヘッダー情報で保存する共有オブジェクトルールが含まれます。また、これらはローカルルールカテゴリに保存され、3のGIDを使用してリストされます。変更した共有オブジェクトルールは削除できますが、元の共有オブジェクトルールは削除できません。

#### 手順

**ステップ 1** 次のいずれかの方法を使用して侵入ルールにアクセスします。

- [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択し、[侵入ルール (Intrusion Rules)] をクリックします。
- [オブジェクト (Objects)] > [侵入ルール (Intrusion Rules)] を選択します。

**ステップ 2** 次の2つの選択肢があります。

- すべてのローカルルールを削除します：[ローカルルールの削除 (Delete Local Rules)] をクリックし、[OK] をクリックします。
- 1つのルールを削除します：[ルールのグループ化基準 (Group Rules By)] ドロップダウンから [ローカルルール (Local Rules)] を選択し、削除するルールの隣にある削除アイコン (🗑️) をクリックし、[OK] をクリックして削除を確認します。

#### 関連トピック

[侵入ルールの状態](#) (1639 ページ)

## ルールの検索

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

Firepower システムには、数千もの標準テキストルールが用意されています。また、Cisco Talos Security Intelligence and Research Group (Talos) は新しい脆弱性およびエクスプロイトが見つ



かったときのルールを追加を継続します。特定のルールを簡単に検索して、そのルールをアクティブ化、非アクティブ化、または編集することができます。

手順

**ステップ 1** 次のいずれかの方法を使用して侵入ルールにアクセスします。

- [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)] を選択し、[侵入ルール (Intrusion Rules)] をクリックします。
- [オブジェクト (Objects)] > [侵入ルール (Intrusion Rules)] を選択します。

**ステップ 2** ツールバーで [検索 (Search)] をクリックします。

**ステップ 3** 検索条件を追加します。

**ステップ 4** [検索 (Search)] をクリックします。

次のタスク

- 見つかったルール (システムルールの場合はルールのコピー) を表示または編集する場合は、ハイパーリンクが付いたルールメッセージをクリックします。詳細については、[新規ルールの作成 \(1702 ページ\)](#) または [既存のルールの変更 \(1703 ページ\)](#) を参照してください。

## 侵入ルールの検索条件

次の表には、利用可能な検索オプションについて説明しています。

表 122: ルール検索規則

オプション	説明
署名 ID	SnortID (SID) に基づいて1つのルールを検索するには、SID 番号を入力します。複数のルールを検索するには、SID 番号リストをコンマで区切って入力します。このフィールドは、80 文字以内です。
ジェネレータ ID	標準テキストルールを検索するには、[1] を選択します。共有オブジェクトのルールを検索するには、[3] を選択します。
メッセージ	特定のメッセージのあるルールを検索するには、[メッセージ (Message)] フィールドのルールメッセージから単語を1つ入力します。たとえば、DNS エクスプロイトを検索するには、DNS を入力します。バッファ オーバーフロー エクスプロイトを検索するには、overflow と入力します。
プロトコル	特定のプロトコルのトラフィックを評価するルールを検索するには、そのプロトコルを選択します。プロトコルを選択しない場合、検索結果に、すべてのプロトコルのルールが表示されます。

オプション	説明
送信元ポート	指定ポートから発信されるパケットを調べるルールを検索するには、送信元ポート番号またはポート関連変数を入力します。
接続先ポート	特定ポートを宛先にしたパケットを調べるルールを検索するには、宛先ポート番号かポート関連変数を入力します。
ソース IP	特定の IP アドレスから発信されるパケットを調べるルールを検索するには、送信元 IP アドレスまたは IP アドレス関連変数を入力します。
宛先 IP (Destination IP)	特定の IP アドレスに送信するパケットを調べるルールを検索するには、宛先 IP アドレスまたは IP アドレス関連変数を入力します。
キーワード	特定のキーワードを検索するには、キーワード検索オプションを使用できます。キーワードを選択して、検索するキーワード値を入力します。特定値以外の任意の値に一致させるには、キーワードの前に疑問符 (!) を入力します。
カテゴリ (Category)	特定カテゴリのルールを検索するには、カテゴリ リストからカテゴリを選択します。
分類	特定の分類のあるルールを検索するには、分類リストから分類名を選択します。
ルール状態 (Rule State)	特定のポリシー内のルールや特定のルール状態を検索するには、最初のルール状態リストからポリシーを選択し、第2のリストから状態を選択して、イベントの作成、イベントのドロップ、作成、無効に設定されたルールを検索します。

## 侵入ルールエディタ ページでのルールのフィルタリング

侵入ルールエディタ ページ上でルールをフィルタリングして、ルールのサブセットを表示することができます。たとえば、あるルールまたはその状態を変更したいが、数千ものルールの中からそれを見つけるのが困難な場合に、この機能が役立つことがあります。

フィルタを入力すると、1つ以上の一致するルールを含むフォルダがページに表示され、一致するルールがない場合はメッセージが表示されます。

### フィルタリング ガイドライン

フィルタには、特殊なキーワードとその引数、文字列、引用符で囲んだリテラル文字列、さらに複数のフィルタ条件を区切るスペースを含めることができます。ただし、正規表現、ワイルドカード文字、および否定文字 (!)、「大なり」記号 (>)、「小なり」記号 (<)などの特殊な演算子をフィルタに含めることはできません。

すべてのキーワード、キーワード引数、および文字列では大文字と小文字が区別されません。gid キーワードと sid キーワードを除くすべての引数と文字列が部分文字列として扱われます。gid と sid の引数は、完全一致のみを返します。

フィルタ処理前の元のページで1つのフォルダを展開すると、その後のフィルタ処理でそのフォルダ内の一致が返されるときにフォルダが展開したままになります。探しているルールが多数のルールを含むフォルダ内に存在する場合には、これが役立つことがあります。

1つのフィルタを後続の別のフィルタで制約することはできません。入力されたフィルタは、ルールデータベース全体を検索して、一致するすべてのルールを返します。前回のフィルタ結果がページに表示されている状態でフィルタを入力すると、そのページの内容が消去され、代わりに新しいフィルタの結果が返されます。

フィルタ処理されている場合もされていない場合も、リスト内のルールで同じ機能を使用できます。たとえば、侵入ルールエディタ ページでは、リストがフィルタ処理されているかどうかに関わらず、リスト内のルールを編集できます。また、ページのコンテキストメニューの任意のオプションを使用することもできます。



**ヒント** すべてのサブグループ内のルールの合計数が多い場合は、フィルタリングに長い時間がかかることがあります。これは、個別のルールの数がかなり少なくても、1つのルールが複数のカテゴリに出現することがあるためです。

## キーワードフィルタリング

各ルールフィルタに、次の形式で1つ以上のキーワードを含めることができます。

`keyword:argument`

ここで、**keyword** は次の表のいずれかのキーワード、**argument** はキーワードに関連する特定のフィールドで検索される単一の、大文字/小文字を区別しない英数字文字列です。

`gid` と `sid` を除くすべてのキーワードの引数が部分文字列として扱われます。たとえば、引数 `123` によって `"12345"`、`"41235"`、`"45123"` などが返されます。`gid` と `sid` の引数は完全一致のみを返します。たとえば、`sid:3080` は `SID 3080` のみを返します。



**ヒント** 部分的な `SID` を検索するには、1つ以上の文字列を使ってフィルタ処理できます。

次の表に、ルールのフィルタ処理に使用できる特定のフィルタリングキーワードと引数を示します。

表 123: ルールフィルタ キーワード

キーワード	説明	例
<code>arachnids</code>	ルール参照内の Arachnids ID 全体またはその一部分に基づいて1つ以上のルールを返します。	<code>arachnids:181</code>
<code>bugtraq</code>	ルール参照内の Bugtraq ID 全体またはその一部分に基づいて1つ以上のルールを返します。	<code>bugtraq:2120</code>

キーワード	説明	例
cve	ルール参照内の CVE 番号全体またはその一部分に基づいて 1 つ以上のルールを返します。	cve:2003-0109
gid	引数 1 は標準のテキストルールを返します。引数 3 は共有オブジェクトルールを返します。	gid:3
mcafee	ルール参照内の McAfee ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。	mcafee:10566
msg	ルールの [メッセージ (Message)] フィールド (イベントメッセージとも呼ばれる) の全体またはその一部分に基づいて 1 つ以上のルールを返します。	msg:chat
nessus	ルール参照内の Nessus ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。	nessus:10737
ref	ルール参照内またはルールの [メッセージ (Message)] フィールド内の単一の英数字文字列の全体または一部分に基づいて、1 つ以上のルールを返します。	ref:MS03-039
sid	正確な Snort ID を持つルールを返します。	sid:235
url	ルール参照内の URL 全体またはその一部分に基づいて 1 つ以上のルールを返します。	url:faqs.org

#### 関連トピック

[イベント参照の定義](#) (1700 ページ)

[侵入イベント詳細](#) (1695 ページ)

[プリプロセッサのジェネレータ ID](#) (2573 ページ)

## 文字列フィルタリング

各ルールフィルタに 1 つ以上の英数字文字列を含めることができます。文字列により、ルールの [メッセージ (Message)] フィールド、Snort ID ID (SID)、およびジェネレータ ID が検索されます。たとえば、文字列 123 を指定すると、ルールメッセージ内の文字列「Lotus123」や「123mania」などが返され、さらに、SID 6123、SID 12375 などにも返されます。

すべての文字列では大文字と小文字が区別されず、部分的な文字列として扱われます。たとえば、文字列 ADMIN、admin、または Admin はすべて、「admin」、「CFADMIN」、「Administrator」などを返します。

文字列を引用符で囲むと、完全一致を返すことができます。たとえば、引用符付きのリテラル文字列 "overflow attempt" は完全一致のみを返しますが、引用符なしの 2 つの文字列 overflow と attempt で構成されるフィルタは "overflow attempt"、"overflow multipacket attempt"、"overflow with evasion attempt"などを返します。

関連トピック

[侵入イベント詳細](#) (1695 ページ)

[プリプロセッサのジェネレータ ID](#) (2573 ページ)

## キーワードと文字列の組み合わせによるフィルタリング

複数のキーワード、文字列、またはその両方をスペースで区切って任意に組み合わせて入力することで、フィルタリングの結果を絞り込むことができます。結果には、すべてのフィルタ条件に一致するルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のフィルタはそれぞれ同じルールを返します。

- url:at login attempt cve:200
- login attempt cve:200 url:at
- login cve:200 attempt url:at

## フィルタリングルール

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

[侵入ルール (Intrusion Rules) ] ページで、ルールをサブセットにフィルタ処理すると、より簡単に特定のルールを見つけることができます。その後で、いずれかのページ機能を使用できます。これには、コンテキストメニューで使用可能な機能の選択も含まれます。

編集する特定のルールを見つけるのに、規則のフィルタリングはとても役立ちます。

### 手順

**ステップ 1** 次のいずれかの方法を使用して侵入ルールにアクセスします。

- [ポリシー (Policies) ] > [アクセスコントロール (Access Control) ] > [侵入 (Intrusion) ] を選択し、[侵入ルール (Intrusion Rules) ] をクリックします。
- [オブジェクト (Objects) ] > [侵入ルール (Intrusion Rules) ] を選択します。

**ステップ 2** フィルタリングする前に、次の選択を行います。

- 該当のルールグループを展開します。複数のルールグループにも、展開できるサブグループがあります。

また、ルールがどのグループに含まれているか予想できる場合は、フィルタ処理前の元のページでそのグループを展開しておくとな便利な場合があります。その後のフィルタ処理で

そのフォルダ内の一致した結果が返されると、およびフィルタ消去アイコン (✕) をクリックしてフィルタ処理前のページに戻ったときに、グループが展開されたままになりません。

- [グループルール (Group Rules By)] ドロップダウンリストから別のグループメソッドを選択します。

**ステップ3** [グループルール (Group Rules By)] リストでフィルタアイコン (🔍) の横にあるテキストボックスにフィルタ制約を入力します。

**ステップ4** Enter を押します。

- (注) フィルタクリアアイコン (✕) をクリックして、現在のフィルタ処理されたリストをクリアします。

## 侵入ルールのキーワードと引数

ルール言語では、キーワードを組み合わせることによってルールの動作を指定できます。キーワードとそれに関連する値 (引数と呼ばれる) は、ルールエンジンによって検査されるパケットおよびパケット関連値をシステムがどのように評価するかを決定します。Firepower システムでは現在、コンテンツマッチング、プロトコル固有のパターンマッチング、状態固有のマッチングなどのインスペクション機能を実行するためのキーワードがサポートされています。キーワードあたり最大100個の引数を定義し、互換性のある任意の数のキーワードを組み合わせることで非常に具体的なルールを作成できます。これにより、誤検出や検出漏れの可能性が減少し、受け取った侵入情報に集中的に取り組むことができます。

また、パッシブ展開でアダプティブプロファイルの更新を使用すると、ルールメタデータとホスト情報に基づいて特定の packets に対するアクティブルール処理を動的に調整できます。

ここに記載されているキーワードは、ルールエディタの検出オプションとして表示されます。

### 関連トピック

[アダプティブプロファイルについて](#) (2013 ページ)

## content キーワードと protected\_content キーワード

content キーワードまたは protected\_content キーワードを使用すると、パケット内から検出するコンテンツを指定できます。

ほとんどの場合、content または protected\_content キーワードの後ろに修飾子を付けて、コンテンツを検索すべき場所、検索で大文字/小文字を区別するかどうか、およびその他のオプションを指定する必要があります。

ルールでイベントがトリガーとして使用されるためには、すべてのコンテンツマッチングが真でなければならないことに注意してください。つまり、各コンテンツマッチングは相互にAND関係にあります。

また、インライン展開では、有害なコンテンツを照会した後でそれを同じ長さの独自のテキスト文字列に置き換えるルールをセットアップできることに注意してください。

### content

content キーワードを使用すると、ルールエンジンはパケットペイロードまたはストリームでその文字列を検索します。たとえば、いずれかの content キーワードの値として /bin/sh と入力した場合、ルールエンジンはパケットペイロード内で文字列 /bin/sh を検索します。

ASCII 文字列、16 進コンテンツ（バイナリ バイト コード）、またはその両方の組み合わせを使用してコンテンツを照会できます。キーワード値の中で 16 進コンテンツをパイプ文字 (|) で囲みます。たとえば、|90C8 C0FF FFFF|/bin/sh のように 16 進コンテンツと ASCII コンテンツを混在させることができます。

1つのルール内で複数のコンテンツマッチングを指定できます。これを行うには、content キーワードの追加のインスタンスを使用します。コンテンツマッチングごとに、ルールをトリガーとして使用させるにはパケットペイロードまたはストリームでコンテンツ一致が見つからなければならないことを指定できます。



**注意** Not オプションが選択された 1 つの content キーワードだけを含むルールを作成した場合、侵入ポリシーの効果なくなる可能性があります。

### protected\_content

protected\_content キーワードを使用すると、ルール引数を設定する前に、検索コンテンツ文字列をエンコードすることができます。キーワードを設定する前に、ルール作成者がハッシュ関数（SHA-512、SHA-256、または MD5）を使用して文字列をエンコードします。

content キーワードの代わりに protected\_content キーワードを使用した場合でも、ルールエンジンがパケットペイロードまたはストリームの中で文字列を検索する方法に違いはなく、ほとんどのキーワードオプションが想定どおりに機能します。次の表は、protected\_content キーワードオプションと content キーワードオプションの間の例外的な相違点を要約しています。

表 124: protected\_content オプションの例外

オプション	説明
ハッシュ タイプ (Hash Type)	protected_content ルール キーワードの新しいオプション。
[大文字小文字の区別なし (Case Insensitive) ]	未サポート
次の範囲内 (Within)	未サポート

オプション	説明
奥行き (Depth)	未サポート
長さ (Length)	<code>protected_content</code> ルール キーワードの新しいオプション。
高速パターンマッチ機能を使用 (Use Fast Pattern Matcher)	未サポート
高速パターン マッチ機能のみ (Fast Pattern Matcher Only)	未サポート
高速パターンマッチ機能オフセットおよび長さ (Fast Pattern Matcher Offset and Length)	未サポート

Cisco では、`protected_content` キーワードを含むルールに 1 つ以上の `content` キーワードを含めることを推奨しています。こうすると、ルール エンジンが常に高速パターン マッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルール内の `protected_content` キーワードの前に `content` キーワードを配置します。ルールに 1 つ以上の `content` キーワードが含まれている場合は、`content` キーワードの **Use Fast Pattern Matcher** 引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。



**注意** **Not** オプションが選択された 1 つの `protected_content` キーワードだけを含むルールを作成した場合、侵入ポリシーの効果なくなる可能性があります。

#### 関連トピック

[カスタム ルールの作成](#) (1701 ページ)

[基本コンテンツおよび `protected\_content` キーワードの引数](#) (1714 ページ)

[`replace` キーワード](#) (1727 ページ)

## 基本コンテンツおよび `protected_content` キーワードの引数

`content` または `protected_content` キーワードを変更するパラメータを使用すると、コンテンツ検索の位置や大文字/小文字の区別を制約できます。`content` または `protected_content` キーワードを変更するオプションを設定して、検索対象となるコンテンツを指定します。

### [大文字小文字の区別なし (Case Insensitive) ]



(注) このオプションは `protected_content` キーワードの設定ではサポートされません。



ASCII 文字列でコンテンツ一致を検索するときに大文字/小文字の区別を無視するようルールエンジンに指示できます。検索で大文字と小文字を区別しないようにするには、コンテンツ検索の指定時に [大文字小文字の区別なし (Case Insensitive)] をオンにします。

### Hash Type



(注) このオプションは `protected_content` キーワードで**のみ**設定できます。

[ハッシュタイプ (Hash Type)] ドロップダウンを使用して、検索文字列のエンコードに使用されたハッシュ関数を特定します。 `protected_content` 検索文字列のハッシュ方式として、SHA-512、SHA-256、および MD5 がサポートされています。選択したハッシュタイプとハッシュされたコンテンツの長さが一致しない場合、システムはルールを保存しません。

自動的に Cisco 設定のデフォルト値が選択されます。 [デフォルト (Default)] が選択される場合、ルールに特定のハッシュ関数は含まれず、SHA-512 がハッシュ関数であると見なされます。

### Raw Data

[raw データ (Raw Data)] オプションを使用すると、ルールエンジンは、正規化されたペイロードデータ (ネットワーク分析ポリシーによってデコードされたデータ) を分析する前にオリジナルの packets ペイロードを分析します。引数値は使用されません。正規化の前に、ペイロード内の Telnet ネゴシエーションオプションを検査するために Telnet トラフィックを分析する場合に、このキーワードを使用できます。

同じ content または `protected_content` キーワードで、**Raw Data** オプションを HTTP コンテンツオプションと一緒に使用することはできません。



ヒント HTTP トラフィックで raw データを検査するかどうか、また、どの程度の量の raw データを検査するかを決定するため、HTTP 検査プリプロセッサの [クライアントフローの深さ (Client Flow Depth)] オプションと [サーバフローの深さ (Server Flow Depth)] オプションを設定することができます。

### 注

指定したコンテンツと一致しないコンテンツを検索するには、[一致しない (Not)] オプションを選択します。 [一致しない (Not)] オプションが選択された content または `protected_content` キーワードを含むルールを作成する場合には、そのルール内に、[一致しない (Not)] オプションが選択されていない別の content または `protected_content` キーワードを 1 つ以上含める必要があります。

**注意**

content または protected\_content キーワードに対して **Not** オプションをオンにした場合は、そのキーワードだけを含むルールを作成しないでください。侵入ポリシーの効果がなくなる可能性があります。

たとえば、SMTP ルール 1:2541:9 に 3 つの content キーワードが含まれており、そのうちの 1 つで [一致しない (Not) ] オプションが選択されているとします。[一致しない (Not) ] オプションが選択されているキーワード以外のすべての content キーワードを削除すると、このルールに基づくカスタムルールが無効になります。このようなルールを侵入ポリシーに追加すると、そのポリシーの効果がなくなる可能性があります。

**ヒント**

同じ content キーワードで、[Not] チェック ボックスと [Use Fast Pattern Matcher] チェック ボックスを同時に選択することはできません。

## コンテンツ (content) および保護コンテンツ (protected\_content) キーワード検索位置

検索位置オプションを使用すると、指定したコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

### 許可された組み合わせ：content 検索位置の引数

次のように、2 つの content 位置ペアのいずれかを使用すると、指定したコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

- パケットペイロードの先頭を基準にして検索する場合は、[オフセット (Offset) ] と [奥行き (Depth) ] を一緒に使用します。
- 現在の検索位置を基準にして検索する場合は、[距離 (Distance) ] と [次の範囲内 (Within) ] を一緒に使用します。

ペアに含まれるオプションのどちらか 1 つだけを指定した場合は、そのペアのもう 1 つのオプションのデフォルトが想定されます。

**Offset** および **Depth** オプションと、**Distance** および **Within** オプションを混合することはできません。たとえば、**Offset** と **Within** をペアにすることはできません。1 つのルール内で任意の数の位置オプションを使用できます。

位置が指定されない場合は、[オフセット (Offset) ] と [奥行き (Depth) ] のデフォルトが想定されます。つまり、コンテンツ検索はパケットペイロードの先頭から始まってパケットの末尾まで続きます。

また、既存の byte\_extract 変数を使用して位置オプションの値を指定することもできます。

**ヒント**

1 つのルール内で任意の数の位置オプションを使用できます。

## 関連トピック

[byte\\_extract キーワード](#) (1733 ページ)

### 許可された組み合わせ：protected\_content 検索位置の引数

次のように、必須の[長さ (Length)]protected\_content 位置オプションを[オフセット (Offset)] または [距離 (Distance)] 位置オプションと組み合わせて使用すると、指定されたコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

- パケット ペイロードの先頭を基準にして、保護された文字列を検索するには、[長さ (Length)] と [オフセット (Offset)] を一緒に使用します。
- 現在の検索位置を基準にして、保護された文字列を検索するには、[長さ (Length)] と [距離 (Distance)] を一緒に使用します。



#### ヒント

1つのキーワード設定内で[オフセット (Offset)] オプションと [距離 (Distance)] オプションを併用することはできませんが、1つのルール内では任意の数の位置オプションを使用できます。

位置が指定されない場合は、デフォルトが想定されます。つまり、コンテンツ検索はパケットペイロードの先頭から始まってパケットの末尾まで続きます。

また、既存の byte\_extract 変数を使用して位置オプションの値を指定することもできます。

## 関連トピック

[byte\\_extract キーワード](#) (1733 ページ)

### content および protected\_content の検索位置の引数

#### 奥行



(注) このオプションは、content キーワードを設定する場合に**のみ**サポートされます。

オフセット値の先頭からの（またはオフセットが設定されていない場合はパケットペイロード先頭からの）コンテンツ検索の最大の深さをバイト単位で指定します。

たとえば、ルールのコンテンツ値が cgi-bin/phf、offset 値が 3、depth 値が 22 である場合、ルールヘッダーで指定されたパラメータを満たすパケット内で、cgi-bin/phf 文字列との一致の検索がバイト位置 3 から始まり、22 バイト処理した後（バイト位置 25 で）停止します。

指定したコンテンツの長さ以上の、最大 65535 バイトまでの値を指定する必要があります。値 0 は指定できません。

デフォルトの深さは、「パケットの末尾まで検索」です。

### 距離 (Distance)

以前に見つかったコンテンツ一致から数えて、指定されたバイト数の後に出現する後続のコンテンツ一致を見つけるようルールエンジンに指示します。

Distance (距離) カウンタはバイト 0 から始まるため、最後に見つかったコンテンツ一致から順方向に移動すべきバイト数よりも 1 つ少ない数値を指定してください。たとえば 4 を指定した場合、5 番目のバイトから検索が始まります。

-65535 ~ 65535 バイトを値として指定できます。負の Distance 値を指定した場合は、検索を開始するバイト位置がパケットの先頭から外れる可能性があります。実際にはパケットの第 1 バイトから検索が開始されますが、計算ではパケットの外側のバイトも考慮されます。たとえば、パケット内の現在の位置が第 5 バイトで、次のコンテンツ ルール オプションで Distance 値 -10 および within 値 20 が指定された場合、検索はペイロードの先頭から開始され、[Within] オプションが 15 に調整されます。

デフォルトの距離は 0 で、これは最後のコンテンツ一致の後のパケット内の現在位置という意味です。

### 長さ (Length)



(注) このオプションは protected\_content キーワードを設定する場合に**のみ**サポートされます。

**Length** protected\_content キーワード オプションは、ハッシュされていない検索文字列の長さをバイト単位で示します。

たとえば、コンテンツ sample1 を使ってセキュア ハッシュを生成した場合には、**Length** 値として 7 を使用します。このフィールドに値を入力することは**必須**です。

### Offset

パケット ペイロードの先頭を基準とする、コンテンツの検索を開始するパケット ペイロード内の位置をバイト単位で指定します。65535 ~ 65535 バイトを値として指定できます。

オフセット カウンタはバイト 0 から始まるため、パケット ペイロードの先頭から順方向に移動すべきバイト数よりも 1 つ少ない数値を指定してください。たとえば 7 を指定した場合は、8 番目のバイトから検索が始まります。

デフォルトのオフセットは 0 で、これはパケットの先頭を意味します。

### Within



(注) このオプションは、content キーワードを設定する場合に**のみ**サポートされます。

[次の範囲内 (Within) ] オプションを使用すると、ルールをトリガーとして使用させるには、最後に見つかったコンテンツ一致の末尾以降、指定のバイト数以内に次のコンテンツ一致が発生する必要があることを指示できます。たとえば **Within** 値として 8 を指定した場合、次のコ

コンテンツ一致がパケットペイロードの次の8バイト以内に発生する必要があります。発生しない場合は、ルールをトリガーとして使用する基準が満たされません。

指定したコンテンツの長さ以上の、最大 65535 バイトまでの値を指定できます。

[Within] のデフォルトは「パケットの末尾まで検索」です。

## 概要：HTTP content および protected\_content キーワードの引数

HTTP content または protected\_content キーワード オプションを使用すると、HTTP Inspect プリプロセッサによってデコードされた HTTP メッセージ内でコンテンツ一致を検索する位置を指定できます。

次の2つのオプションは、HTTP 応答内のステータス フィールドを検索します。

- HTTP ステータス コード (HTTP Status Code)
- HTTP ステータス メッセージ (HTTP Status Message)

ルールエンジンは未加工の正規化されていないステータス フィールドを検索しますが、ここでは、他の Raw HTTP フィールドと正規化された HTTP フィールドを併用する際に考慮すべき制限についての説明を簡略化するために、これらのオプションが別個に列挙されていることに注意してください。

次の5つのオプションは、必要に応じて HTTP 要求、応答、またはその両方の中で正規化フィールドを検索します。

- HTTP URI
- HTTP メソッド (HTTP Method)
- HTTP ヘッダー (HTTP Header)
- HTTP Cookie
- HTTP クライアント ボディ (HTTP Client Body)

次の3つのオプションは、必要に応じて HTTP 要求、応答、またはその両方の中で未加工の (正規化されていない) 非ステータス フィールドを検索します。

- HTTP Raw URI
- HTTP Raw ヘッダー (HTTP Raw Header)
- HTTP Raw Cookie

HTTP content オプションを選択する場合は、次のガイドラインに従ってください。

- HTTP content オプションは TCP トラフィックにのみ適用されます。
- パフォーマンスへの悪影響を避けるために、指定したコンテンツが出現する可能性のあるメッセージ部分だけを選択してください。

たとえば、ショッピングカートメッセージの場合のように大きな cookie がトラフィックに含まれている可能性がある場合は、HTTP cookie ではなく HTTP ヘッダーの中で指定のコンテンツを検索することができます。

- HTTP Inspect プリプロセッサの正規化機能を活用し、パフォーマンスを向上させるには、作成するすべての HTTP 関連ルールの中に少なくとも 1 つの content または protected\_content キーワードを含め、それに対して **HTTP URI**、**HTTP Method**、**HTTP Header**、または **HTTP Client Body** オプションを選択します。
- HTTP content または protected\_content キーワード オプションと組み合わせて replace キーワードを使用することはできません。

単一の正規化された HTTP オプションまたはステータスフィールドを指定できます。または、複数の正規化 HTTP オプションとステータスフィールドを任意に組み合わせて、コンテンツ領域をマッチング対象にすることもできます。ただし、HTTP フィールドオプションを使用する場合には次の制限事項に注意してください。

- 同じ content または protected\_content キーワードの中で、[生データ (Raw Data) ] オプションを HTTP オプションと一緒に使用することはできません。
- Raw HTTP フィールドオプション ([HTTP Raw URI]、[ HTTP Raw ヘッダー (HTTP Raw Header) ]、または [HTTP Raw Cookie] ) と、それぞれに対応する正規化されたオプション ([HTTP URI]、[HTTP ヘッダー (HTTP Header) ]、または [HTTP Cookie]) を同じ content または protected\_content キーワード内で一緒に使用することはできません。
- [高速パターン マッチ機能を使用 (Use Fast Pattern Matcher) ] を、次の 1 つ以上の HTTP フィールドオプションと組み合わせて選択することはできません。

[HTTP Raw URI]、[HTTP raw ヘッダー (HTTP Raw Header) ]、[HTTP Raw Cookie]、[HTTP Cookie]、[HTTP メソッド (HTTP Method) ]、[HTTP ステータス メッセージ (HTTP Status Message) ]、[HTTP ステータス コード (HTTP Status Code) ]

ただし、次のいずれかの正規化フィールドを検索するために高速パターンマッチ機能を使用する content または protected\_content キーワードでは、上記のオプションを含めることができます。

[HTTP URI]、[HTTP ヘッダー (HTTP Header) ]、[HTTP クライアント ボディ (HTTP Client Body) ]

たとえば、[HTTP Cookie]、[HTTP ヘッダー (HTTP Header) ]、[高速パターンマッチ機能を使用 (Use Fast Pattern Matcher) ] を選択した場合、ルール エンジン は HTTP cookie と HTTP ヘッダーの両方でコンテンツを検索しますが、高速パターン マッチ機能は HTTP cookie ではなく、HTTP ヘッダーにのみ適用されます。

- 制限付きオプションと制限なしオプションを併用した場合、高速パターンマッチ機能は、指定された制限なしフィールドのみを検索することで、侵入ルールエディタにルールを渡して (制限付きフィールドの評価を含む) 完全な評価を行うべきかどうかを検査します。

## 関連トピック

[content キーワードの高速パターン マッチ機能の引数](#) (1724 ページ)

## HTTP コンテンツと `protected_content` キーワードの引数

### HTTP URI

正規化された要求 URI フィールド内でコンテンツ一致を検索するには、このオプションを選択します。

このオプションと `pcre` キーワードの HTTP URI (U) オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。



- 
- (注) パイプライン処理された HTTP 要求パケットには複数の URI が含まれています。[HTTP URI] が選択されている場合、パイプライン処理された HTTP 要求パケットをルールエンジンが検出すると、そのパケット内のすべての URI でコンテンツ一致が検索されます。
- 

### HTTP Raw URI

正規化された要求 URI フィールド内でコンテンツ一致を検索するには、このオプションを選択します。

このオプションと `pcre` キーワードの HTTP URI (U) オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。



- 
- (注) パイプライン処理された HTTP 要求パケットには複数の URI が含まれています。[HTTP URI] が選択されている場合、パイプライン処理された HTTP 要求パケットをルールエンジンが検出すると、そのパケット内のすべての URI でコンテンツ一致が検索されます。
- 

### HTTP メソッド

(URI で識別されるリソースに対して行う GET や POST などのアクションを特定する) 要求メソッドフィールド内のコンテンツ一致を検索するには、このオプションを選択します。

### HTTP Header

HTTP 要求内の (cookie を除く) 正規化されたヘッダー フィールドでコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は応答内でも検索されます。

このオプションと `pcre` キーワードの HTTP 見出し (H) オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。

### HTTP Raw Header

HTTP 要求内の (cookie を除く) raw ヘッダー フィールドでコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は応答内でも検索されます。

このオプションと `pcre` キーワードの HTTP 未加工見出し (D) オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。

### HTTP Cookie

正規化された HTTP クライアント要求見出し内で識別される cookie でコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [HTTP 応答の検査 (Inspect HTTP Responses)] オプションが有効になっている場合は応答 `set-cookie` データ内でも検索されます。システムは、メッセージ本文に含まれる cookie を本文の内容として扱うことに注意してください。

cookie 内だけで一致を検索するには、HTTP Inspect プリプロセッサの [HTTP Cookie の検査 (Inspect HTTP Cookies)] オプションを有効にする必要があります。これを有効にしない場合、ルール エンジン は cookie を含む見出し全体を検索します。

次の点に注意してください。

- このオプションと `pcre` キーワードの HTTP cookie (C) オプションを一緒に使用して、同じコンテンツを検索することはできません。
- `Cookie:` ヘッダー名と `Set-Cookie:` ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す `CRLF` は cookie の一部としてではなく、ヘッダーの一部として検査されます。

### HTTP Raw Cookie

未加工 HTTP クライアント要求見出し内で識別される cookie でコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [HTTP 応答の検査 (Inspect HTTP Responses)] オプションが有効になっている場合は応答 `set-cookie` データ内でも検索されます。システムは、メッセージ本文に含まれる cookie を本文の内容として扱うことに注意してください。

cookie 内だけで一致を検索するには、HTTP Inspect プリプロセッサの [HTTP Cookie の検査 (Inspect HTTP Cookies)] オプションを有効にする必要があります。これを有効にしない場合、ルール エンジン は cookie を含む見出し全体を検索します。

次の点に注意してください。

- このオプションと `pcre` キーワードの HTTP 未加工 cookie (K) オプションを一緒に使用して同じコンテンツを検索することはできません。
- `Cookie:` ヘッダー名と `Set-Cookie:` ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す `CRLF` は cookie の一部としてではなく、ヘッダーの一部として検査されます。



### HTTP Client Body

HTTP クライアント要求内のメッセージ本文でコンテンツ一致を検索するには、このオプションを選択します。

このオプションが機能するためには、HTTP Inspect プリプロセッサの [HTTP クライアント ボディの抽出の深さ (HTTP Client Body Extraction Depth) ] オプションで 0 ~ 65535 の値を指定する必要があります。ご注意ください。

### HTTP ステータス コード (HTTP Status Code)

HTTP 応答内の 3 桁のステータス コードでコンテンツ一致を検索するには、このオプションを選択します。

このオプションで一致が返されるようにするには、HTTP Inspect プリプロセッサの [HTTP 応答の検査 (Inspect HTTP Responses) ] オプションを有効にする必要があります。

### HTTP Status Message

HTTP 応答のステータス コードに付加されるテキスト記述の中でコンテンツ一致を検索するには、このオプションを選択します。

このオプションで一致が返されるようにするには、HTTP Inspect プリプロセッサの [HTTP 応答の検査 (Inspect HTTP Responses) ] オプションを有効にする必要があります。

### 関連トピック

[PCRE 修飾子のオプション \(1742 ページ\)](#)

[サーバレベルの HTTP 正規化オプション \(1885 ページ\)](#)

## 概要 : content キーワードによる高速パターン マッチ機能



(注) これらのオプションは、protected\_content キーワードの設定ではサポートされません。

高速パターン マッチ機能は、パケットをルール エンジンに渡す前に、評価するルールをすばやく決定します。この初期決定により、パケット評価で使用されるルール数が大幅に減るため、パフォーマンスが向上します。

デフォルトで、高速パターンマッチ機能は、ルールで指定された最長のコンテンツをパケットで検索します。これは、不必要なルール評価をできるだけ減らすためです。次の例のようなルールフラグメントがあるとします。

```
alert tcp any any -> any 80 (msg:"Exploit"; content:"GET";  
http_method; nocase; content:"/exploit.cgi"; http_uri;  
nocase;)
```

ほとんどすべての HTTP クライアント要求にはコンテンツ GET が含まれていますが、コンテンツ /exploit.cgi を含む要求は稀です。GET を高速パターン コンテンツとして使用した場合、ルール エンジンではほとんどのケースでこのルールを評価し、一致はほとんど検出されません。

しょう。しかし、/exploit.cgi を使用するとほとんどのクライアントの GET 要求は評価されないため、パフォーマンスが向上します。

指定されたコンテンツが高速パターン マッチ機能で検出された場合にのみ、ルールエンジンはパケットをルールに照らして評価します。たとえば、ルール内の 1 つの content キーワードでコンテンツ short を指定し、別のキーワードで longer、さらに 3 番目のキーワードで longest を指定した場合、高速パターン マッチ機能はコンテンツ longest を使用し、ルールエンジンがペイロード内で longest を検出した場合にのみ、ルールが評価されます。

## content キーワードの高速パターン マッチ機能の引数

### Use Fast Pattern Matcher

使用する高速パターンマッチ機能の短い検索パターンを指定するには、このオプションを使用します。理論的には、指定したパターンの方が最長パターンよりもパケット内で見つかる可能性が低いいため、よりの絞って対象のエクスプロイトを識別できます。

[高速パターン マッチ機能を使用 (Use Fast Pattern Matcher)] と他のオプションを同じ content キーワード内で選択する場合は、次の制限事項に注意してください。

- ルールごとに 1 回だけ、[高速パターン マッチ機能を使用 (Use Fast Pattern Matcher)] を指定できます。
- [高速パターン マッチ機能を使用 (Use Fast Pattern Matcher)] と [一致しない (Not)] を組み合わせて選択した場合は、[距離 (Distance)]、[次の範囲内 (Within)]、[オフセット (Offset)]、または [奥行き (Depth)] を使用できません。
- [高速パターン マッチ機能を使用 (Use Fast Pattern Matcher)] を、次のいずれかの HTTP フィールド オプションと組み合わせて選択することはできません。

[HTTP Raw URI]、[HTTP raw ヘッダー (HTTP Raw Header)]、[HTTP raw クッキー (HTTP Raw Cookie)]、[HTTP クッキー (HTTP Cookie)]、[HTTP メソッド (HTTP Method)]、[HTTP ステータス メッセージ (HTTP Status Message)]、または [HTTP ステータス コード (HTTP Status Code)]

ただし、次のいずれかの正規化フィールドを検索するために高速パターンマッチ機能を使用する content キーワードでは、上記のオプションを含めることができます。

[HTTP URI]、[HTTP ヘッダー (HTTP Header)]、または [HTTP クライアント ボディ (HTTP Client Body)]

たとえば、[HTTP Cookie]、[HTTP Header]、および [Use Fast Pattern Matcher] を選択した場合、ルールエンジンは HTTP cookie と HTTP ヘッダーの両方でコンテンツを検索しますが、高速パターン マッチ機能は HTTP cookie ではなく、HTTP ヘッダーにのみ適用されます。

未加工 HTTP フィールド オプション ([HTTP Raw URI]、[HTTP raw ヘッダー (HTTP Raw Header)]、または [HTTP raw クッキー (HTTP Raw Cookie)]) と、それぞれに対応する正規化されたオプション ([HTTP URI]、[HTTP ヘッダー (HTTP Header)]、または [HTTP クッキー (HTTP Cookie)]) を同じ content キーワード内で一緒に使用できないことに注意してください。

制限付きオプションと制限なしオプションを併用した場合、高速パターンマッチ機能は、指定された制限なしフィールドのみを検索することで、ルールエンジンにパケットを渡して（制限付きフィールドの評価を含む）完全な評価を行うべきかどうかを検査します。

- オプションで、[高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] を選択した場合には [高速パターン マッチ機能のみ（Fast Pattern Matcher Only）] または [高速パターン マッチ機能オフセットおよび長さ（Fast Pattern Matcher Offset and Length）] を選択することもできますが、この両方は選択できません。
- Base64 データの検査時には高速パターン マッチ機能を使用できません。

### Fast Pattern Matcher Only

このオプションを使用すると、content キーワードをルールオプションとしてではなく、高速パターン マッチ機能オプションとしてのみ使用できます。指定したコンテンツをルールエンジンで評価する必要がない場合、このオプションを使ってリソースを節約できます。たとえば、ペイロード内のいずれかの場所にコンテンツ 12345 が存在することだけを必要とするルールがあるとします。高速パターンマッチ機能でパターンが検出された場合に、ルール内の追加のキーワードに照らしてパケットを評価できます。パターン 12345 が含まれているかどうかを判断するために、ルールエンジンがパケットを再評価する必要はありません。

指定されたコンテンツに関連する他の条件がルールに含まれている場合は、このオプションを使用しないでください。たとえば、別のルール条件で abcd が 1234 の前に出現するかどうかを判断する場合には、このオプションを使ってコンテンツ 1234 を検索しないでください。[高速パターン マッチ機能のみ（Fast Pattern Matcher Only）] を指定すると、指定されたコンテンツがルールエンジンによって検索されないため、このケースではルールエンジンが相対的な位置を判断できません。

このオプションを使用するときには、次の条件に注意してください。

- 指定されたコンテンツは位置に依存しない、つまり、ペイロードのどこにでも出現する可能性があるため、位置オプション（[距離（Distance）]、[次の範囲内（Within）]、[オフセット（Offset）]、[奥行き（Depth）]、[高速パターン マッチ機能オフセットおよび長さ（Fast Pattern Matcher Offset and Length）]）を使用することはできません。
- このオプションを [一致しない（Not）] と組み合わせて使用することはできません。
- このオプションを [高速パターン マッチ機能オフセットおよび長さ（Fast Pattern Matcher Offset and Length）] と組み合わせて使用することはできません。
- 大文字/小文字を区別しない方法ですべてのパターンが高速パターン マッチ機能に挿入されるため、指定したコンテンツは「大文字/小文字の区別なし」として扱われます。これは自動的に処理されるため、このオプションの選択時に [大文字小文字の区別なし（Case Insensitive）] を選択する必要はありません。
- [高速パターン マッチ機能のみ（Fast Pattern Matcher Only）] オプションを使用する content キーワードの直後に、現在の検索位置を基準にして検索位置を設定する次のキーワードを続けないようにしてください。

• isdataat

- pcre
- content ([距離 (Distance) ] または [次の範囲内 (Within) ] が選択されている場合)
- content ([HTTP URI] が選択されている場合)
- asnl
- byte\_jump
- byte\_test
- byte\_math
- byte\_extract
- base64\_decode

### Fast Pattern Matcher Offset and Length

[高速パターン マッチ機能オフセットおよび長さ (Fast Pattern Matcher Offset and Length) ] オプションを使用すると、検索するコンテンツの一部分を指定できます。これにより、パターンが非常に長く、ルール的一致の可能性を判断するのにパターンの一部分だけで十分な場合に、メモリ消費を抑えることができます。高速パターンマッチ機能によってルールが選択されたときに、パターン全体がルールに照らして評価されます。

次の構文に従い、検索を開始する位置 (オフセット) およびコンテンツ内をどれほど検索するか (長さ) をバイト単位で指定することにより、高速パターンマッチ機能で使用する部分を決定します。

```
offset,length
```

たとえば、次のコンテンツに対して

```
1234567
```

次のようにオフセットと長さのバイト数を指定した場合、

```
1,5
```

高速パターン マッチ機能はコンテンツ 23456 のみを検索します。

このオプションを [Fast Pattern Matcher Only] と一緒に使用できないことに注意してください。

### 関連トピック

[概要 : HTTP content および protected\\_content キーワードの引数 \(1719 ページ\)](#)

[base64\\_decode キーワードと base64\\_data キーワード \(1815 ページ\)](#)

## replace キーワード

インライン導入で `replace` キーワードを使用すると、指定したコンテンツ、または Cisco SSL アプライアンスによって検出された SSL トラフィック内のコンテンツを置き換えることができます。

`replace` キーワードを使用するには、`content` キーワードを使って特定の文字列を検索するカスタムの標準テキストルールを作成します。その後、`replace` キーワードを使用して、コンテンツを置き換える文字列を指定します。置換値とコンテンツ値は同じ長さである必要があります。



(注) `protected_content` キーワード内でハッシュされたコンテンツを置き換えるために `replace` キーワードを使用することはできません。

オプションで、以前の Firepower システム ソフトウェア バージョンとの下位互換性を維持するために、置換文字列を引用符で囲むことができます。引用符を含めない場合は、それらが自動的にルールに追加されるため、構文的に正しいルールになります。置換テキストの一部として先行引用符または後続引用符を含めるには、次の例に示すように、バックスラッシュを使ってエスケープする必要があります。

```
"replacement text plus \"quotation\" marks"
```

1つのルール内に複数の `replace` キーワードを含めることができますが、`content` キーワードごとに1つずつしか含めることができません。ルールによって検出されたコンテンツの最初のインスタンスだけが置き換えられます。

次に、`replace` キーワードの使用例を示します。

- エクスプロイトを含んでいる着信パケットをシステムが検出した場合、有害な文字列を無害な文字列に置き換えることができます。このテクニックは、有害なパケットを単に破棄するよりも効果的である場合があります。破棄されたパケットを攻撃者が単に再送信し続け、やがてネットワーク防御を通り抜けるか、ネットワークを氾濫させるという攻撃シナリオがあります。パケットを破棄する代わりに別の文字列に置換することで、脆弱ではないターゲットに対して攻撃が実行されたと攻撃者に思い込ませることができます。
- (たとえば Web サーバの) 脆弱なバージョンが稼働しているかどうかを調べる偵察攻撃が懸念される場合は、発信パケットを検出して、バナーを独自のテキストに置換できます。



(注) 置換ルールを使用するインライン侵入ポリシー内でルール状態が[イベントを生成する (Generate Events)]に設定されていることを確認してください。ルールを[ドロップしてイベントを生成する (Drop and Generate Events)]に設定した場合はパケットが破棄され、コンテンツが置き換えられません。

文字列置換プロセスでは、宛先ホストがエラーなしでパケットを受信できるように、パケットチェックサムがシステムによって自動的に更新されます。

replace キーワードは、HTTP 要求メッセージの content キーワード オプションと組み合わせて使用できないことに注意してください。

#### 関連トピック

[content キーワードと protected\\_content キーワード \(1712 ページ\)](#)

[概要：HTTP content および protected\\_content キーワードの引数 \(1719 ページ\)](#)

## byte\_jump キーワード

byte\_jump キーワードは、指定されたバイトセグメントで定義されるバイト数を計算し、指定したオプションに応じて、指定されたバイトセグメントの末尾から、パケットペイロードの先頭または末尾から、あるいは最後のコンテンツ一致に対して相対的なポイントから順方向に、パケット内でそのバイト数だけスキップします。パケットの特定のバイトセグメントが、パケット内の可変データに含まれるバイト数を示す場合には、これが役立ちます。

次の表では、byte\_jump キーワードで必要な引数を説明します。

表 125: byte\_jump の必須引数

引数	説明
Bytes	<p>パケットから抽出するバイト数。</p> <p>DCE/RPC を指定せずに使用する場合、許可される値は 0 ~ 10 ですが、次の制限があります。</p> <ul style="list-style-type: none"> <li>From End 引数とともに使用すると、バイト数は 0 になることがあります。Bytes が 0 の場合、抽出された値は 0 です。</li> <li>1、2、または 4 以外のバイト数を指定する場合は、番号タイプ (16 進数、8 進数、または 10 進数) を指定する必要があります。</li> </ul> <p>DCE/RPC とともに使用する場合、許可される値は 1、2、および 4 です。</p>
Offset	<p>ペイロード内で処理を開始するバイト数。offset カウンタはバイト 0 から始まるため、パケットペイロードの先頭、または最後に見つかったコンテンツ一致から順方向にジャンプさせるバイト数から 1 を差し引いて offset 値を計算してください。</p> <p>-65535 ~ 65535 バイトを指定できます。</p> <p>また、既存の byte_extract 変数または byte_math 結果を使用してこの引数の値を指定することもできます。</p>

次の表で説明するオプションを使用すると、必須の引数に指定された値をシステムがどのように解釈するかを定義できます。

表 126: byte\_jump の追加のオプション引数

引数	説明
Relative	最後に見つかったコンテンツ一致で検出された最後のパターンを基準にしてオフセットを計算します。
Align	変換されたバイト数を、次の 32 ビット境界に切り上げます。
Multiplier	ルールエンジンで最終的な byte_jump 値を算出するために、パケットから得られた byte_jump 値に掛ける値を示します。 つまり、ルールエンジンは、指定されたバイトセグメントで定義されるバイト数だけスキップする代わりに、Multiplier 引数で指定される整数を乗算したバイト数だけスキップします。
Post Jump Offset	他の byte_jump 引数を適用した後に、順方向または逆方向にスキップするバイト数 (-65535 ~ 65535)。正の値は順方向にスキップし、負の値は逆方向にスキップします。無効にするには、フィールドを空白のままにするか、0 を入力します。 <b>DCE/RPC</b> 引数を選択すると、一部の byte_jump 引数が適用されないことに注意してください。
From Beginning	ルールエンジンが、パケット内の現在の位置からではなく、パケットペイロードの先頭からペイロード内の指定されたバイト数をスキップする必要があることを示します。
From End	ジャンプは、バッファの最後のバイトのすぐ後のバイトから実行されます。
Bitmask	AND 演算子を使用して、指定した 16 進数のビットマスクを、Bytes 引数から抽出したバイトに適用します。 ビットマスクは 1 ~ 4 バイトです。 結果は、マスク内の末尾のゼロの数と等しい数のビット分だけ右にシフトされます。

**DCE/RPC**、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

バイト数を byte\_extract キーワードでどのように計算するか定義するには、次の表の中から引数を選択します。バイト順引数を選択しなかった場合、ルールエンジンはビッグエンディアンのバイト順を使用します。

表 127: byte\_jump のバイト順引数

引数	説明
Big Endian	デフォルトのネットワークバイト順であるビッグエンディアンバイト順でデータを処理します。

引数	説明
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に <code>byte_jump</code> キーワードを指定します。  DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアンバイト順を決定します。 <b>Number Type</b> 引数と <b>Endian</b> 引数は適用されません。  この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて <code>byte_jump</code> を使用することもできます。

次の表に示すいずれか1つの引数を使用して、パケット内のストリングデータをシステムがどのように表示するかを定義します。

表 128: 番号タイプ引数

引数	説明
Hexadecimal String	変換後のストリング データを 16 進形式で表現します。
Decimal String	変換後のストリング データを 10 進形式で表現します。
Octal String	変換後のストリング データを 8 進形式で表現します。

たとえば、次のような値を `byte_jump` に設定した場合、

- Bytes = 4
- Offset = 12
- Relative enabled
- Align enabled

ルール エンジン は、最後に見つかったコンテンツ一致から 13 バイト後に出現する 4 つのバイトで記述される数値を計算して、そのバイト数だけパケット内を順方向にスキップします。たとえば、ある特定のパケット内で計算される 4 つのバイトが 00 00 00 1F である場合、ルール エンジン はこれを 31 に変換します。align が指定されている（次の 32 ビット境界まで移動するようエンジンに指示する）ため、ルール エンジン はパケット内を 32 バイト先までスキップします。

あるいは、次のような値を `byte_jump` に設定した場合、

- Bytes = 4
- Offset = 12
- From Beginning enabled
- Multiplier = 2



ルールエンジンは、パケットの先頭から 13 バイト後に出現する 4 つのバイトで記述される数値を計算します。その後、その数値に 2 を掛けてスキップする総バイト数を計算します。たとえば、ある特定のパケット内で計算される 4 つのバイトが 00 00 00 1F である場合、ルールエンジンはこれを 31 に変換し、それに 2 を掛けて 62 にします。[From Beginning] が有効になっているため、ルールエンジンはパケット内の最初の 63 バイトをスキップします。

関連トピック

[byte\\_extract キーワード \(1733 ページ\)](#)

[DCE/RPC キーワード \(1771 ページ\)](#)

## byte\_test キーワード

byte\_test キーワードは、指定されたバイトセグメントを Value 引数およびその演算子に対してテストします。

次の表に、byte\_test キーワードに必要な引数を説明します。

表 129: byte\_test の必須引数

引数	説明
Bytes	<p>パケットから計算するバイト数。</p> <p>DCE/RPC を指定せずに使用する場合、許可される値は 1 ~ 10 です。ただし、1、2、または 4 以外のバイト数を指定する場合は、番号タイプ (16 進数、8 進数、または 10 進数) を指定する必要があります。</p> <p>DCE/RPC とともに使用する場合、許可される値は 1、2、および 4 です。</p>
値	<p>テストする値 (演算子を含む)。</p> <p>サポートされている演算子: &lt;, &gt;, =, !, &amp;, ^, !&gt;, !&lt;, !=, !&amp;, または !^。</p> <p>たとえば !1024 と指定した場合、byte_test は指定された数値を変換し、それが 1024 と等しくなければイベントが生成されます (他のすべてのキーワードパラメータが一致する場合)。</p> <p>「!」と「!=」は等価であることに注意してください。</p> <p>また、既存の byte_extract 変数または byte_math 結果を使用してこの引数の値を指定することもできます。</p>
Offset	<p>ペイロード内で処理を開始するバイト数。offset カウンタはバイト 0 から始まるため、パケットペイロードの先頭、または最後に見つかったコンテンツ一致から順方向にカウントするバイト数から 1 を差し引いて offset 値を計算してください。</p> <p>既存の byte_extract 変数または byte_math result 変数を使用して、この引数の値を指定することができます。</p>

次の表に示す引数を使用すると、システムで byte\_test 引数がどのように使用されるかをさらに定義できます。

表 130: byte\_test の追加のオプション引数

引数	説明
Bitmask	AND 演算子を使用して、指定した 16 進数のビットマスクを、Bytes 引数から抽出したバイトに適用します。 ビットマスクは 1〜4 バイトです。 結果は、マスク内の末尾のゼロの数と等しい数のビット分だけ右にシフトされます。
Relative	最後に見つかったパターン一致を基準にしてオフセットを計算します。

DCE/RPC、Endian、または Number Type のうち 1 つだけを指定できます。

検査対象となるバイトを byte\_test キーワードでどのように計算するか定義するには、次の表の中から引数を選択します。バイト順引数を選択しなかった場合、ルールエンジンはビッグエンディアンのバイト順を使用します。

表 131: byte\_test のバイト順引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に byte_test キーワードを指定します。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。Number Type 引数と Endian 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて byte_test を使用することもできます。

次の表に示すいずれか 1 つの引数を使用して、パケット内のストリングデータをシステムがどのように表示するかを定義できます。

表 132: byte-test の番号タイプ引数

引数	説明
Hexadecimal String	変換後のストリング データを 16 進形式で表現します。
Decimal String	変換後のストリング データを 10 進形式で表現します。

引数	説明
Octal String	変換後のストリング データを 8 進形式で表現します。

たとえば、次のような値を `byte_test` に指定した場合、

- Bytes = 4
- Operator and Value > 128
- Offset = 8
- Relative enabled

ルールエンジンは、最後に見つかったコンテンツ一致から（それを基準にして）9 バイト後に出現する 4 つのバイトで記述される数値を計算し、その計算値が 128 バイトを超えた場合に、ルールがトリガーとして使用されます。

#### 関連トピック

[byte\\_extract キーワード \(1733 ページ\)](#)

[DCE/RPC キーワード \(1771 ページ\)](#)

## byte\_extract キーワード

`byte_extract` キーワードを使用すると、指定したバイト数をパケットから変数の中に読み込むことができます。後で、その変数を、同じルール内で他の検出キーワードの特定の引数の値として使用できます。

たとえば、パケットデータに含まれるバイト数が特定のバイトセグメントで記述されている場合、パケットからデータサイズを抽出するには、これが役立ちます。たとえば、特定のバイトセグメントにおいて、後続データが 4 バイト構成であると記述されている場合、データサイズ 4 バイトを抽出して変数値として使用できます。

`byte_extract` を使用するとき、1 つのルール内で最大 2 つの異なる変数を同時に作成できます。`byte_extract` 変数を何回でも再定義できます。同じ変数名と別の変数定義を使って新しい `byte_extract` キーワードを入力した場合、その前の変数定義がオーバーライドされます。

次の表で、`byte_extract` キーワードに必要な引数について説明します。

表 133: `byte_extract` の必須引数

引数	説明
Bytes to Extract	パケットから抽出するバイト数。 1、2、または 4 以外のバイト数を指定する場合は、番号タイプ（16 進数、8 進数、または 10 進数）を指定する必要があります。

引数	説明
Offset	<p>ペイロード内でデータの抽出を開始するバイト数。-65535～65535 バイトを指定できます。オフセットカウンタはバイト0から始まるため、順方向に数えるバイト数から1を差し引いてオフセット値を計算してください。たとえば、順方向に8バイト数えるには7を指定します。ルールエンジンは、パケットペイロードの先頭から (<b>Relative</b> も一緒に指定した場合は最後に見つかったコンテンツ一致の後から) 順方向に数えます。負の数は、<b>Relative</b> も指定した場合にのみ指定できます。</p> <p>既存の <code>byte_math</code> の結果を使用して、この引数の値を指定することもできます。</p>
Variable Name	他の検出キーワードの引数で使用する変数名。英数字の文字列を指定できます (ただし文字で始まる必要があります)。

抽出対象のデータを見つける方法をさらに詳しく定義するには、次の表に示す引数を使用できます。

表 134: `byte_extract` の追加のオプション引数

引数	説明
Multiplier	パケットから抽出された値の乗数。0～65535を指定できます。乗数を指定しない場合のデフォルト値は1です。
Align	抽出された値を最も近い2バイトまたは4バイト境界に切り上げます。 <b>Multiplier</b> も一緒に選択した場合、システムはこの調整の前に乗数を適用します。
Relative	ペイロードの先頭ではなく、最後に見つかったコンテンツ一致の末尾を基準にして <b>Offset</b> を計算します。
Bitmask	<p>AND 演算子を使用して、指定した16進数のビットマスクを、Bytes to Extract 引数から抽出したバイトに適用します。</p> <p>ビットマスクは1～4バイトです。</p> <p>結果は、マスク内の末尾のゼロの数と等しい数のビット分だけ右にシフトされます。</p>

**DCE/RPC**、**Endian**、または **Number Type** のうち1つだけを指定できます。

検査対象となるバイトを `byte_extract` キーワードでどのように計算するか定義するには、次の表の中から引数を選択できます。バイト順引数を選択しなかった場合、ルールエンジンはビッグエンディアンのバイト順を使用します。

表 135: byte\_extract のバイト順引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に byte_extract キーワードを指定します。  DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。Number Type 引数と Endian 引数は適用されません。  この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて byte_extract を使用することもできます。

データを読み取るときの数値タイプを ASCII 文字列として指定できます。パケット内のストリングデータをシステムがどのように認識するかを定義するには、次の表のいずれかの引数を選択できます。

表 136: byte\_extract の番号タイプ引数

引数	説明
Hexadecimal String	抽出されたストリング データを 16 進形式で読み取ります。
Decimal String	抽出されたストリング データを 10 進形式で読み取ります。
Octal String	抽出されたストリング データを 8 進形式で読み取ります。

たとえば、byte\_extract の値を次のように指定した場合、

- Bytes to Extract = 4
- Variable Name = var
- Offset = 8
- Relative = enabled

ルールエンジンは、最後に見つかったコンテンツ一致から（それを基準にして）9 バイト後に出現する、4 バイトで表現される数値を var という名前の変数の中に読み込みます。後でこの変数を、特定のキーワード引数の値としてルール内で指定できます。

byte\_extract キーワードで定義した変数を指定できるキーワード引数を、次の表に列挙します。

表 137: byte\_extract 変数を使用できる引数

キーワード	引数
content	Depth、Offset、Distance、Within
byte_jump	Offset
byte_test	Offset、Value
byte_math	RValue、Offset
isdataat	Offset

関連トピック

- [DCE/RPC プリプロセッサ \(1856 ページ\)](#)
- [DCE/RPC キーワード \(1771 ページ\)](#)
- [基本コンテンツおよび protected\\_content キーワードの引数 \(1714 ページ\)](#)
- [byte\\_jump キーワード \(1728 ページ\)](#)
- [byte\\_test キーワード \(1731 ページ\)](#)
- [パケット特性 \(1794 ページ\)](#)

## byte\_math キーワード

byte\_math キーワードは、抽出された値と指定された値または既存の変数の算術演算を実行し、その結果を新しい結果変数に格納します。結果の変数は、他のキーワードの引数として使用することができます。

ルール内で複数の byte\_math キーワードを使用して、複数の byte\_math 操作を実行できます。

次の表で、byte\_math キーワードに必要な引数について説明します。

表 138: byte\_math の必須引数

引数	説明
Bytes	<p>パケットから計算するバイト数。</p> <p>DCE/RPC を指定せずに使用する場合、許可される値は 1 ~ 10 です。</p> <ul style="list-style-type: none"> <li>• 演算子が +、-、*、または / の場合、バイト数は 1 ~ 10 になります。</li> <li>• 演算子が &lt;&lt; または &gt;&gt; の場合、バイト数は 1 ~ 4 になります。</li> <li>• 1、2、または 4 以外のバイト数を指定する場合は、番号タイプ (16 進数、8 進数、または 10 進数) を指定する必要があります。</li> </ul> <p>DCE/RPC とともに使用する場合、許可される値は 1、2、および 4 です。</p>

引数	説明
Offset	<p>ペイロード内で処理を開始するバイト数。offsetカウンタはバイト0から始まるため、パケットペイロードの先頭、または最後に見つかったコンテンツ一致 (Relative を指定した場合) から順方向にジャンプさせるバイト数から 1 を差し引いて offset 値を計算してください。</p> <p>-65535 ~ 65535 バイトを指定できます。</p> <p>ここでは、byte_extract 変数を指定することもできます。</p>
演算子	+、-、*、/、<<、または >>
RValue	演算子に続く値。これは、符号なし整数またはbyte_extract から渡される変数です。
Result Variable	<p>byte_math の計算結果が格納される変数の名前。この変数は、他のキーワードの引数として使用することができます。</p> <p>この値は符号なし整数として格納されます。</p> <p>この変数名には次の条件があります。</p> <ul style="list-style-type: none"> <li>• 英数字を使用する必要がある</li> <li>• 先頭を数字にすることはできない</li> <li>• Microsoft のファイル名/変数名の規則でサポートされている特殊文字を含めることができる</li> <li>• 特殊文字のみの名前にはできない</li> </ul>

次の表で説明するオプションを使用すると、必須の引数に指定された値をシステムがどのように解釈するかを定義できます。

表 139: byte\_math の追加のオプション引数

引数	説明
Relative	<p>ペイロードの先頭ではなく、最後に見つかったコンテンツ一致で検出された最後のパターンを基準にしてオフセットを計算します。</p>
Bitmask	<p>AND 演算子を使用して、指定した 16 進数のビットマスクを、Bytes 引数から抽出したバイトに適用します。</p> <p>ビットマスクは 1 ~ 4 バイトです。</p> <p>結果は、マスク内の末尾のゼロの数と等しい数のビット分だけ右にシフトされます。</p>

DCE/RPC、Endian、または Number Type のうち 1 つだけを指定できます。

バイト数を `byte_math` キーワードでどのように計算するか定義するには、次の表の中から引数を選択します。バイト順引数を選択しなかった場合、ルールエンジンはビッグエンディアンのバイト順を使用します。

表 140: `byte_math` のバイト順引数

引数	説明
Big Endian	デフォルトのネットワークバイト順であるビッグエンディアンバイト順でデータを処理します。
Little Endian	リトルエンディアンバイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に <code>byte_math</code> キーワードを指定します。  DCE/RPC プリプロセッサがビッグエンディアンまたはリトルエンディアンバイト順を決定します。 <b>Number Type</b> 引数と <b>Endian</b> 引数は適用されません。  この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて <code>byte_math</code> を使用することもできます。

次の表に示すいずれか1つの引数を使用して、パケット内のstringデータをシステムがどのように表示するかを定義します。

表 141: 番号タイプ引数

引数	説明
Hexadecimal String	stringデータを16進形式で表現します。
Decimal String	stringデータを10進形式で表現します。
Octal String	stringデータを8進形式で表現します。

たとえば、次のような値を `byte_math` に設定した場合、

- Bytes = 2
- Offset = 0
- Operator = \*
- RValue = height
- Result Variable = area

ルールエンジンは、パケット内の最初の2バイトに記述された番号を抽出し、RValue（既存の変数 `height` を使用）を乗じて新しい変数 `area` を作成します。



表 142: *byte\_math* 変数を使用できる引数

キーワード	引数
byte_jump	Offset
byte_test	Offset、 Value
byte_extract	Offset
isdataat	Offset

## 概要 : pcre キーワード

pcre キーワードを使用すると、指定されたコンテンツをパケットペイロード内で検査するために Perl 互換正規表現 (PCRE) を使用できます。PCRE を使用すると、同じ内容のわずかなバリエーションにそれぞれ一致する複数のルールを作成する手間が省けます。

正規表現は、さまざまな方法で表現されることのあるコンテンツを検索する場合に役立ちます。パケットのペイロード内でコンテンツを検索するときには、コンテンツがさまざまな属性を持つ可能性があることを考慮すべき場合があります。

侵入ルールで使われる正規表現構文は完全な正規表現ライブラリのサブセットであり、完全なライブラリ内のコマンドで使用される構文とはいくつかの点で異なることに注意してください。侵入ルールエディタを使用して pcre キーワードを追加するときには、次の形式で完全な値を入力します。

```
!/pcre/ ismxAEGRBUIPHDMCKSY
```

### 引数の説明

- 「!」は否定オプションです (正規表現に一致しないパターンを照合する場合に使用します)。
- /pcre/ は Perl 互換正規表現です。
- ismxAEGRBUIPHDMCKSY は修飾子オプションの任意の組み合わせです。

また、次の表に示す文字をエスケープする必要があることに注意してください。これにより、パケットペイロード内で特定のコンテンツを検索するために PCRE でこれらの文字を使用した場合、ルールエンジンがそれを正しく解釈ようになります。

表 143: エスケープする PCRE 文字

エスケープする必要のある文字	バックスラッシュを使用した場合	16進コードを使用した場合
# (ナンバー記号)	\#	\x23
; (セミコロン)	\;	\x3B

エスケープする必要のある文字	バックスラッシュを使用した場合	16進コードを使用した場合
(縦棒)	\	\x7C
: (コロン)	\:	\x3A

`m?regex?`を使用することもできます。ここで、`?`は「/」以外のデリミタです。正規表現内でスラッシュと一致させる必要があり、バックスラッシュを使ってそれをエスケープしたくない場合には、これを使用できます。たとえば、「`m?regex? ismxAEGRBUIPHDMCKSY`」のように使用できます。`regex`はPerl互換正規表現、`ismxAEGRBUIPHDMCKSY`は修飾子オプションの任意の組み合わせです。



**ヒント** オプションで、Perl互換正規表現を引用符で囲むこともできます（例：`pcre_expression`または`"pcre_expression"`）。引用符が任意ではなく必須であった旧バージョンに慣れている経験豊富なユーザのために、引用符を使用するオプションが提供されています。保存後のルールを侵入ルールエディタで表示すると、引用符が表示されません。

## PCRE の構文

`pcre` キーワードでは、標準のPerl互換正規表現（PCRE）構文を使用できます。以下の項では、この構文について説明します。



**ヒント** ここではPCREで使用可能な基本的な構文について説明しますが、PerlおよびPCRE専用のオンラインリファレンスやブックで、さらに詳しい情報を参照することもできます。

### メタ文字

メタ文字は正規表現内で特別な意味を持つリテラル文字です。メタ文字を正規表現内で使用するときには、その前にバックスラッシュを付けて「エスケープする」必要があります。

次の表に、PCREで使用可能なメタ文字について説明し、それぞれの例を示します。

表 144: PCRE メタ文字

メタ文字	説明	例
.	改行以外の任意の文字と一致します。修飾オプションとして <code>s</code> が使用されている場合は、改行文字も含まれます。	<code>abc.</code> は、 <code>abcd</code> 、 <code>abc1</code> 、 <code>abc#</code> などと一致します。
*	ある文字または式の 0 回以上の出現と一致します。	<code>abc*</code> は、 <code>abc</code> 、 <code>abcc</code> 、 <code>abccc</code> 、 <code>abccccc</code> などと一致します。

メタ文字	説明	例
?	ある文字または式の 0 回または 1 回の出現と一致します。	abc? は abc に一致します。
+	ある文字または式の 1 回以上の出現と一致します。	abc+ は、abc、abcc、abccc、abccccc などと一致します。
()	式をグループ化します。	(abc)+ は、abc、abcabc、abcabcabc などと一致します。
{}	ある文字または式の一致回数の限度を指定します。下限と上限を設定する場合には、下限と上限をカンマで区切ります。	a{4,6} は、aaaa、aaaaa、または aaaaaa と一致します。 (ab){2} は abab と一致します。
[]	文字クラスを定義できます。セットの中で記述される任意の文字または文字の組み合わせに一致します。	[abc123] は、a または b または c などと一致します。
^	文字列の先頭でコンテンツを照合します。また、文字クラスの中で否定としても使用されます。	^in は、info 内の「in」と一致しますが、bin では一致しません。[^a] は、a を含まない任意の文字列と一致します。
\$	文字列の末尾でコンテンツを照合します。	ce\$ は、announce 内の「ce」と一致しますが、cent では一致しません。
	OR 式を示します。	(MAILTO HELP) は、MAILTO または HELP と一致します。
\	メタ文字を実際の文字として使用できます。また、事前定義された文字クラスを指定するためにも使われます。	\. はピリオドと一致し、\* はアスタリスクと一致し、\\ はバックスラッシュと一致します。\\d は数字と一致し、\\w は英数字と一致します。

### 文字クラス

文字クラスには、英字、数字、英数字、および空白文字があります。大カッコで囲んで独自の文字クラスを作成できます。また、事前定義のクラスをさまざまな文字タイプのショートカットとして使用することもできます。追加の修飾子なしで文字クラスを使用すると、1 つの文字クラスは 1 桁または 1 文字に一致します。

次の表に、PCRE で使用できる事前定義の文字クラスの説明と例を示します。

表 145: PCRE 文字クラス

文字クラス	説明	文字クラスの定義
\d	数字 (桁) と一致します。	[0-9]
\D	数字以外の任意の文字と一致します。	[^0-9]

文字クラス	説明	文字クラスの定義
\w	英数字（語）と一致します。	[a-zA-Z0-9_]
\W	英数字以外の任意の文字と一致します。	[^a-zA-Z0-9_]
\s	スペース、復帰、タブ、改行、および改ページを含む空白文字と一致します。	[\r\t\n\f]
\S	空白文字以外の任意の文字と一致します。	[^\r\t\n\f]

## PCRE 修飾子のオプション

`pcre` キーワードの値の中で正規表現構文を指定した後、修飾オプションを使用できます。これらの修飾子は、Perl、PCRE、および Snort 固有の処理機能を実行します。修飾子は、常に PCRE 値の末尾に、次の形式で出現します。

```
/pcre/ismxAEGRBUIPHDMCKSY
```

ここで、`ismxAEGRBUPHMC` には、次の表に示す任意の修飾オプションを含めることができます。



**ヒント** オプションで、正規表現と修飾オプションを引用符で囲むことができます（たとえば `"/pcre/ismxAEGRBUIPHDMCKSY"`）。引用符が任意ではなく必須であった旧バージョンに慣れている経験豊富なユーザのために、引用符を使用するオプションが提供されています。保存後のルールを侵入ルール エディタで表示すると、引用符が表示されません。

次の表に、Perl 処理機能を実行するために使用できるオプションを説明します。

表 146: Perl 関連の正規表現後オプション

オプション	説明
i	正規表現で大文字と小文字を区別しないようにします。
s	ドット文字 (.) は、改行または \n 文字を除くすべての文字を表します。オプションとして "s" を使用すると、これをオーバーライドして、改行文字を含むすべての文字をドット文字に一致させることができます。
m	デフォルトで、1つの文字列は複数文字からなる単一行として扱われ、^と\$は特定の文字列の先頭および末尾に一致します。オプションとして "m" を使用すると、^および\$はバッファの先頭または末尾だけでなく、バッファ内の改行文字の直前または直後のコンテンツとも一致します。
x	エスケープされた（バックスラッシュが先行する）場合、および文字クラスに含まれる場合を除き、空白データ文字がパターン内に出現してもそれを無視します。

次の表に、正規表現の後ろに使用できる PCRE 修飾子の説明を示します。

表 147: PCRE 関連の正規表現後オプション

オプション	説明
A	文字列の先頭でパターンが一致する必要があります（正規表現で ^ を使用した場合と同じ）。
E	対象の文字列の末尾でのみ一致するように \$ を設定します。（E を伴わない \$ は、それが改行である場合には最後の文字の直前とも一致しますが、他の改行文字の直前とは一致しません）。
G	デフォルトでは、* + と ? は「最長マッチ」を実行します。つまり、複数の一致が見つかった場合は最も長い一致が選択されます。G 文字を使用するとこの動作が変更され、常に最初の一致がこれらの文字で選択されます。ただし後ろに疑問符 (?) が続く場合を除きます。たとえば、*?+? と ?? は G 修飾子を使った構造内で最長マッチを実行し、疑問符が付いていない *、+、または ? は最長マッチではありません。

次の表に、正規表現の後ろに使用できる Snort 固有の修飾子の説明を示します。

表 148: Snort 固有の正規表現後の修飾子

オプション	説明
R	ルールエンジンで見つかった最後の一致の末尾を基準にして、一致するコンテンツを検索します。
B	プリプロセッサによってデコードされる前のデータ内のコンテンツを検索します（このオプションは、content または protected_content キーワードとともに生データ (Raw Data) 引数を使用する場合に似ています）。
U	<p>HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージの URI 内のコンテンツを検索します。このオプションと content または protected_content キーワードの HTTP URI オプションを一緒に使用して、同じコンテンツを検索することはできません。</p> <p>パイプライン処理された HTTP 要求パケットには複数の URI が含まれていることに注意してください。U オプションを含む PCRE 式を使用すると、ルールエンジンは、パイプライン処理された HTTP 要求パケット内の最初の URI でのみコンテンツ一致を検索します。パケット内のすべての URI を検索するには、U オプションを使った PCRE 式を一緒に使用するかどうかに関係なく、[HTTP URI] を選択した content または protected_content キーワードを使用してください。</p>

オプション	説明
I	<p>HTTP Inspect プリプロセッサによってデコードされた raw HTTP 要求メッセージの URI 内のコンテンツを検索します。このオプションと content または protected_content キーワードの <b>HTTP Raw URI</b> オプションと一緒に使用して、同じコンテンツを検索することはできません。</p>
P	<p>HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージ本文の中でコンテンツを検索します。</p>
H	<p>HTTP Inspect プリプロセッサによってデコードされた HTTP 要求または応答メッセージの (cookie を除く) ヘッダー内のコンテンツを検索します。このオプションと content または protected_content キーワードの <b>HTTP Header</b> オプションと一緒に使用して、同じコンテンツを検索することはできません。</p>
D	<p>HTTP Inspect プリプロセッサによってデコードされた未加工の HTTP 要求または応答メッセージの (cookie を除く) ヘッダー内のコンテンツを検索します。このオプションと content または protected_content キーワードの <b>HTTP Raw Header</b> オプションと一緒に使用して、同じコンテンツを検索することはできません。</p>
M	<p>HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージのメソッドフィールド内のコンテンツを検索します。メソッドフィールドは、URI で識別されるリソースに対して実行すべきアクション (GET、PUT、CONNECT など) を特定します。</p>
C	<p>HTTP Inspect プリプロセッサの [HTTP Cookie の検査 (Inspect HTTP Cookies)] オプションが有効になっている場合は、HTTP 要求見出しの cookie 内の正規化済みコンテンツを検索します。さらに、プリプロセッサの [HTTP 応答の検査 (Inspect HTTP Responses)] オプションが有効になっている場合は、HTTP 応答見出しの set-cookie 内も検索します。[HTTP Cookie の検査 (Inspect HTTP Cookies)] が有効になっていない場合は、cookie または set-cookie データを含む見出し全体を検索します。</p> <p>次の点に注意してください。</p> <ul style="list-style-type: none"> <li>• メッセージ本文に含まれる cookie は、本文のコンテンツとして扱われます。</li> <li>• このオプションと content または protected_content キーワードの <b>HTTP Cookie</b> オプションと一緒に使用して、同じコンテンツを検索することはできません。</li> <li>• Cookie: ヘッダー名と Set-Cookie: ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す CRLF は cookie の一部としてではなく、ヘッダーの一部として検査されます。</li> </ul>

オプション	説明
K	<p>HTTP Inspect プリプロセッサの [HTTP Cookie の検査 (Inspect HTTP Cookies) ] オプションが有効になっている場合は、HTTP 要求見出しの cookie 内の未加工コンテンツを検索します。さらに、プリプロセッサの [HTTP 応答の検査 (Inspect HTTP Responses) ] オプションが有効になっている場合は、HTTP 応答見出しの set-cookie 内も検索します。[HTTP Cookie の検査 (Inspect HTTP Cookies) ] が有効になっていない場合は、cookie または set-cookie データを含む見出し全体を検索します。</p> <p>次の点に注意してください。</p> <ul style="list-style-type: none"> <li>• メッセージ本文に含まれる cookie は、本文のコンテンツとして扱われます。</li> <li>• このオプションと content または protected_content キーワードの <b>HTTP Raw Cookie</b> オプションを一緒に使用して、同じコンテンツを検索することはできません。</li> <li>• Cookie: ヘッダー名と Set-Cookie: ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す CRLF は cookie の一部としてではなく、ヘッダーの一部として検査されます。</li> </ul>
S	HTTP 応答内の 3 桁のステータス コードを検索します。
Y	HTTP 応答内のステータス コードに付加されるテキスト記述を検索します。



(注) U オプションと R オプションを組み合わせ使用しないでください。パフォーマンスの問題が発生する可能性があります。また、他の HTTP コンテンツオプション (I、P、H、D、M、C、K、S または Y) と組み合わせ使用しないでください。

関連トピック

概要 : [HTTP content および protected\\_content キーワードの引数](#) (1719 ページ)

## PCRE のキーワード値の例

次に、pcre で入力できる値の例を示し、それぞれの例で何が一致するかを説明します。

- `/feedback[ (\d{0,1}) ]?\.cgi/U`

この例では、URI データにのみ配置された、feedback の後に 0 個または 1 個の数字、さらに .cgi が続くインスタンスをパケットペイロード内で検索します。

この例は以下のものと一致します。

- `feedback.cgi`

- feedback1.cgi
- feedback2.cgi
- feedback3.cgi

この例は、以下のものとは一致しません。

- feedbacka.cgi
  - feedback11.cgi
  - feedback21.cgi
  - feedbackzb.cgi
- **`/^ez(\w{3,5})\.cgi/iU`**

この例では、先頭の `ez` の後に 3～5 文字の単語、さらに `.cgi` が続く文字列をパケットペイロード内で検索します。この検索では大文字と小文字を区別せず、URI データだけを検索します。

この例は以下のものと一致します。

- EZBoard.cgi
- ezman.cgi
- ezadmin.cgi
- EZAdmin.cgi

この例は、以下のものとは一致しません。

- ezez.cgi
  - fez.cgi
  - abcezboard.cgi
  - ezboardman.cgi
- **`/mail(file|seek)\.cgi/U`**

この例では、URI データ内の `mail` の後に `file` と `seek` のどちらかが続く文字列をパケットペイロードで検索します。

この例は以下のものと一致します。

- mailfile.cgi
- mailseek.cgi

この例は、以下のものとは一致しません。

- MailFile.cgi
- mailfilefile.cgi



• `m?http\\x3a\\x2f\\x2f.*(\\n|\\t)+?U`

この例では、任意の数の文字の後ろにある、HTTP 要求内のタブまたは改行文字を示す URI コンテンツをパケット ペイロード内で検索します。この例では、式で `m?regex?` を使用して、`http:\\\\` を使用しないようにしています。コロンの前にバックスラッシュがあることに注意してください。

この例は以下のものと一致します。

- `http://www.example.com?scriptvar=x&othervar=\\n\\.\\.\\.`
- `http://www.example.com?scriptvar=\\t`

この例は、以下のものとは一致しません。

- `ftp://ftp.example.com?scriptvar=&othervar=\\n\\.\\.\\.`
- `http://www.example.com?scriptvar=|/bin/sh -i|`

• `m?http\\x3a\\x2f\\x2f.*=|.*\\|+?sU`

この例では、(改行を含む) 任意の数の文字の後に1つの等号、さらに任意の数の文字または空白を含むパイプ文字が続くという構成の URL をパケット ペイロード内で検索します。この例では、式で `m?regex?` を使用して、`http:\\\\` を使用しないようにしています。

この例は以下のものと一致します。

- `http://www.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?input=|cat /etc/passwd|`

この例は、以下のものとは一致しません。

- `ftp://ftp.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?value=x&input?|cat /etc/passwd|`
- `/[0-9a-f]{2}\\:[0-9a-f]{2}\\:[0-9a-f]{2}\\:[0-9a-f]{2}\\:[0-9a-f]{2}\\:[0-9a-f]{2}/i`

この例では、MAC アドレスをパケット ペイロード内で検索します。コロン文字がバックスラッシュでエスケープされていることに注意してください。

## metadata キーワード

metadata キーワードを使用すると、記述情報をルールに追加できます。また、metadata キーワードを `service` 引数とともに使用すると、ネットワーク トラフィック内のアプリケーションとポートを特定することができます。追加する情報を使用して、要件に適合するルールを編成または識別することができ、追加する情報や `service` 引数についてルールを検索することができます。

システムは次の形式の引数に基づいてメタデータを検証します。

*key value*

ここで、*key* と *value* は、スペースで区切られた記述の組み合わせです。これは、Cisco 提供のルールにメタデータを追加するために Cisco Talos Security Intelligence and Research Group (Talos) VRT で使用されている形式です。

または、次の形式を使用することもできます。

*key = value*

たとえば、*key value* 形式で次のようにカテゴリとサブカテゴリを使用し、作成者と日付によってルールを識別できます。

```
author SnortGuru_20050406
```

1つのルール内で複数の *metadata* キーワードを使用できます。また、以下の例に示すように、単一の *metadata* キーワード内で複数の *key value* 引数をカンマで区切ることもできます。

```
author SnortGuru_20050406, revised_by SnortUser1_20050707,
revised_by SnortUser2_20061003,
revised_by SnortUser1_20070123
```

使用できる形式は *key value* と *key=value* だけに限定されません。ただし、これらの形式に基づく検証に起因する制限事項を把握しておく必要があります。

### 注意すべき制限のある文字

次の文字制限に注意してください。

- セミコロン (;) またはコロン (:) を使用しないでください。
- システムはコンマを、複数の *key value* 引数または *key=value* 引数の区切り文字であると解釈します。次に例を示します。

*key value, key value, key value*

- システムは等号 (=) または余白文字を、*key* と *value* の間の区切り文字であると解釈します。次に例を示します。

*key value*

*key=value*

その他のすべての文字が使用可能です。

### 注意すべき予約済みメタデータ

*metadata* キーワードでは、次の単語を単一の引数として、または *key value* 引数内の *key* として使用しないでください。これらは Talos 用に予約されています。

```
application
engine
impact_flag
os
policy
rule-type
rule-flushing
soid
```



- (注) ローカルルールを適切に機能させるために制限付きメタデータをどうしても追加する必要がある場合は、サポート担当にお問い合わせください。

### 影響レベル1

metadata キーワードでは、次に示す予約済み *key value* 引数を使用できます。

```
impact_flag red
```

この *key value* 引数は、インポートしたローカルルールまたは侵入ルールエディタを使って作成したカスタムルールに関する影響フラグを赤（レベル1）に設定します。

「送信元または宛先のホストがウイルス、トロイの木馬、その他の有害ソフトウェアによって侵害されている可能性があることを、ルールをトリガーしているパケットが示している」と Talos が判断した場合、Talos は Cisco 提供のルールに `impact_flag red` 引数を含めます。

### 関連トピック

[ローカル侵入ルールファイルインポート](#) (184 ページ)

[侵入イベントのクリップボード](#) (2599 ページ)

## サービスメタデータ

システムは、ネットワークのホストで動作しているアプリケーションを検出し、ネットワークトラフィックにアプリケーションプロトコル情報を挿入します。これは、検出ポリシーの設定に関係なく実行されます。TCP または UDP ルールで `metadata` キーワード `service` 引数を使用して、ネットワークトラフィックのアプリケーションプロトコルとポートを照合することができます。ルールで1つ以上の `service` アプリケーション引数を単一のポート引数と組み合わせることができます。

### サービスアプリケーション

`metadata` キーワードとともに `service` を *key* として、アプリケーションを *value* として使用し、パケットを識別されたアプリケーションプロトコルと一致させることができます。たとえば、次に示す `metadata` キーワード内の *key value* 引数は、ルールを HTTP トラフィックに関連付けます。

```
service http
```

複数のアプリケーションをカンマで区切って指定することもできます。次に例を示します。

```
service http, service smtp, service ftp
```



- 注意** 侵入ルールでサービスメタデータを使用するためには、[適応型プロファイルの設定 \(2016ページ\)](#) で説明されているように、アダプティブプロファイルを有効（デフォルト状態）にする必要があります。

次の表に、`service` キーワードとともに使用される最も一般的なアプリケーション値を示します。



(注) 表にないアプリケーションを特定することが難しい場合は、サポートにお問い合わせください。

表 149: `service` 値

値	説明
<code>cvs</code>	Concurrent Versions System (バージョン管理システム)
<code>dcerpc</code>	分散コンピューティング環境/リモートプロシージャコールシステム
<code>dns</code>	ドメインネームシステム
<code>finger</code>	Finger User Information Protocol
<code>FTP</code>	File Transfer Protocol
<code>ftp-data</code>	File Transfer Protocol (データチャネル)
<code>http</code>	ハイパーテキスト転送プロトコル
<code>imap</code>	Internet Message Access Protocol
<code>isakmp</code>	Internet Security Association and Key Management Protocol
<code>mysql</code>	My Structured Query Language (構造化照会言語)
<code>netbios-dgm</code>	NETBIOS Datagram Service
<code>netbios-ns</code>	NETBIOS Name Service
<code>netbios-ssn</code>	NETBIOS Session Service
<code>nntp</code>	Network News Transfer Protocol
<code>oracle</code>	Oracle Net Services
<code>shell</code>	OS Shell
<code>pop2</code>	Post Office Protocol バージョン 2
<code>pop3</code>	Post Office Protocol バージョン 3
<code>smtpt</code>	Simple Mail Transfer Protocol
<code>snmp</code>	簡易ネットワーク管理プロトコル
<code>ssh</code>	セキュアシェルネットワークプロトコル

値	説明
sunrpc	Sun リモート プロシージャ コール プロトコル
telnet	Telnet ネットワーク プロトコル
tftp	トリビアル ファイル転送プロトコル
x11	X Window システム

### サービス ポート

Metadata キーワードとともに `service` を *key* として、指定したポート引数を *value* として使用し、ルールがアプリケーションと組み合わせてポートを照合する方法を定義できます。

次の表の任意のポート値を、ルールごとに1つ指定できます。

表 150: `service` ポート値

値	説明
<code>else-ports</code> または <code>unknown</code>	<p>次の条件のいずれかが満たされるとルールが適用されます。</p> <ul style="list-style-type: none"> <li>• パケット アプリケーションが既知で、ルール アプリケーションと一致する。</li> <li>• パケット アプリケーションが不明で、パケット ポートがルール ポートと一致する。</li> </ul> <p><code>else-ports</code> および <code>unknown</code> の値では、<code>service</code> がポート修飾子なしでアプリケーションプロトコルを指定する場合にシステムで使用されるデフォルトの動作が生成されます。</p>
<code>and-ports</code>	<p>パケットアプリケーションが既知で、ルールアプリケーションと一致し、パケット ポートがルール ヘッダーのポートと一致する場合、ルールが適用されます。アプリケーションを指定しないルールで <code>and-ports</code> を使用することはできません。</p>
<code>or-ports</code>	<p>次の条件のいずれかが満たされるとルールが適用されます。</p> <ul style="list-style-type: none"> <li>• パケット アプリケーションが既知で、ルール アプリケーションと一致する。</li> <li>• パケット アプリケーションが不明で、パケット ポートがルール ポートと一致する。</li> <li>• パケット アプリケーションはルール アプリケーションと一致せず、パケット ポートはルール ポートと一致する。</li> <li>• ルールはアプリケーションを指定せず、パケット ポートはルール ポートと一致する。</li> </ul>

次の点に注意してください。

- service アプリケーション引数を service and-ports 引数とともに含める必要があります。
- ルールで上記の表の値が複数指定されている場合、ルールが一番最後にある値が適用されます。
- ポートおよびアプリケーション引数は任意の順序にすることができます。

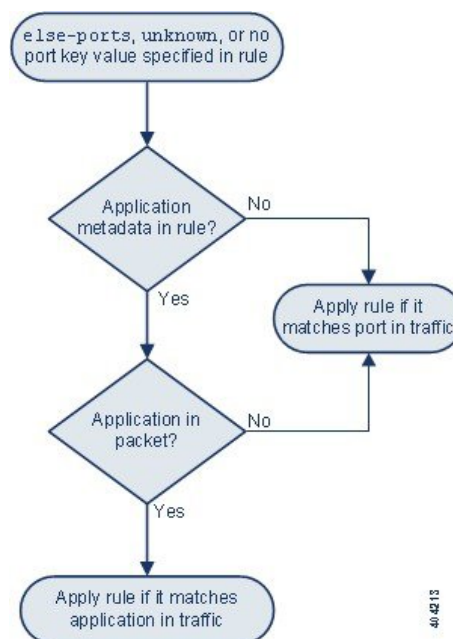
and-ports 値を除き、1 つ以上の service アプリケーション引数の有無にかかわらず、service ポート引数を含めることができます。次に例を示します。

service or-ports, service http, service smtp

### トラフィックのアプリケーションとポート

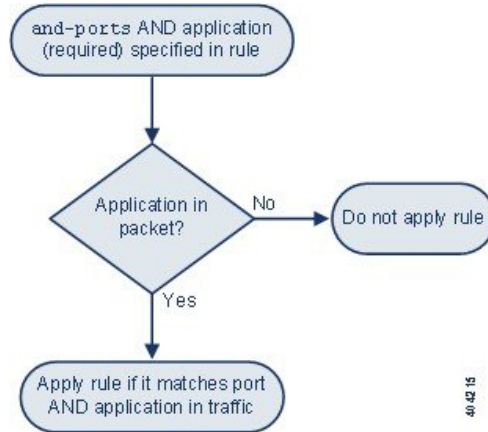
次の図は、侵入ルールでサポートされるアプリケーションとポートの組み合わせ、およびパケットデータにこれらのルール制約を適用した結果を示しています。

ホストアプリケーション プロトコル else 送信元/宛先ポート :

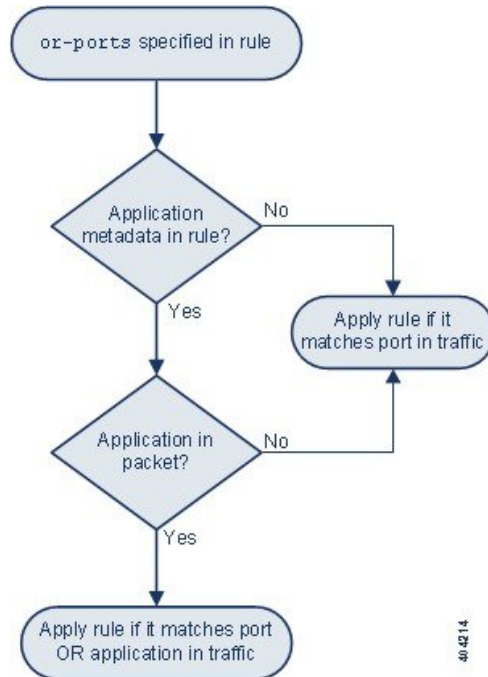


404213

ホストアプリケーションプロトコル and 送信元/宛先ポート :



ホストアプリケーションプロトコル or 送信元/宛先ポート :



一致する例

metadata キーワードを service 引数とともに使用した次のサンプルルールを、一致するデータおよび一致しないデータの例とともに示します。

- alert tcp any any -> any [80,8080] (metadata:service and-ports, service http, service smtp;)

一致する例	一致しない例
<ul style="list-style-type: none"> <li>• TCP ポート 80 経由の HTTP トラフィック</li> <li>• TCP ポート 8080 経由の HTTP トラフィック</li> <li>• TCP ポート 80 経由の SMTP トラフィック</li> <li>• TCP ポート 8080 経由の SMTP トラフィック</li> </ul>	<ul style="list-style-type: none"> <li>• ポート 80 または 8080 の POP3 トラフィック</li> <li>• ポート 80 または 8080 の不明なアプリケーション トラフィック</li> <li>• ポート 9999 の HTTP トラフィック</li> </ul>

• alert tcp any any -> any [80,8080] (metadata:service or-ports, service http;)

一致する例	一致しない例
<ul style="list-style-type: none"> <li>• あらゆるポートの HTTP トラフィック</li> <li>• ポート 80 の SMTP トラフィック</li> <li>• ポート 8080 の SMTP トラフィック</li> <li>• ポート 80 および 8080 の不明なアプリケーションのトラフィック</li> </ul>	<ul style="list-style-type: none"> <li>• 80 または 8080 以外のポートの非 HTTP および非 SMTP トラフィック</li> </ul>

• 次のいずれかの規則 :

- alert tcp any any -> any [80,8080] metadata:service else-ports, service http;)
- alert tcp any any -> any [80,8080] metadata:service unknown, service http;)
- alert tcp any any -> any [80,8080] metadata:service http;)

一致する例	一致しない例
<ul style="list-style-type: none"> <li>• あらゆるポートの HTTP トラフィック</li> <li>• パケットアプリケーションが不明な場合はポート 80</li> <li>• パケットアプリケーションが不明な場合はポート 8080</li> </ul>	<ul style="list-style-type: none"> <li>• ポート 80 または 8080 の SMTP トラフィック</li> <li>• ポート 80 または 8080 の POP3 トラフィック</li> </ul>

## メタデータ検索のガイドライン

metadata キーワードを使用するルールを検索するには、ルールの [検索 (Search) ] ページで metadata キーワードを選択して、オプションで、メタデータの一部を入力します。たとえば次のように入力できます。



- search と入力すると、*key* として search が使用されているすべてのルールが表示されます。
- search http と入力すると、*key* として search、*value* として http がそれぞれ使用されているすべてのルールが表示されます。
- author snortguru と入力すると、*key* として author、*value* として SnortGuru がそれぞれ使用されているすべてのルールが表示されます。
- author s と入力すると、*key* として author、さらに *value* として SnortGuru、SnortUser1、SnortUser2 などの語が使用されているすべてのルールが表示されます。



**ヒント** *key* と *value* の両方を検索するときには、ルール内の *key value* 引数で使用されているのと同じ接続演算子（等号 [=] または空白文字）を検索で使用してください。*key* の後に等号 (=) と空白文字のどちらを入力するかに応じて、異なる結果が検索で返されます。

なお、メタデータ追加のために使用する形式とは無関係に、システムはメタデータ検索語を *key value* または *key=value* 引数の全部または一部として解釈します。たとえば、次に示すメタデータは *key value* または *key=value* 形式に従っていませんが、有効なメタデータです。

```
ab cd ef gh
```

ただし、この例に含まれる各スペースは *key* と *value* の間の区切り文字としてシステムで解釈されます。次に示す並列語や単一語を検索で使用すると、この例のメタデータを含むルールを正しく検出できます。

```
cd ef
ef gh
ef
```

一方、次の検索を使用した場合、単一の *key value* 引数としてシステムによって解釈されるため、ルールを検出できません。

```
ab ef
```

#### 関連トピック

[ルールの検索](#) (1706 ページ)

## IP ヘッダー値

キーワードを使用すると、パケットの IP ヘッダーの中で攻撃やセキュリティ ポリシー違反の可能性を識別できます。

## fragbits

fragbits キーワードは、IP 見出し内のフラグメントビットと予約ビットを検査します。パケットごとに、予約ビット、More Fragments ビット、および Don't Fragment ビットを任意に組み合わせて検査できます。

表 151: Fragbits 引数の値

引数	説明
R	予約済みビット
M	More Fragments ビット
D	Don't Fragment ビット

fragbits キーワードを使ってルールを微調整するために、次の表に示す演算子をルール内の引数値の後ろに指定できます。

表 152: Fragbit 演算子

演算子	説明
プラス記号 (+)	パケットは、指定されたすべてのビットと一致する必要があります。
アスタリスク (*)	パケットは、指定されたどのビットと一致することもできます。
感嘆符 (!)	指定されたどのビットも設定されていない場合、パケットが基準を満たします。

たとえば、(他のビットの有無とは無関係に) 少なくとも予約済みビットが設定されたパケットに対してイベントを生成するには、fragbits 値として R+ を使用します。

## id

id キーワードは、キーワード引数で指定される値に照らして IP 見出しフラグメント識別フィールドを検査します。一部のサービス拒否ツールやスキャナは、このフィールドを、容易に検出できる特定の番号に設定します。たとえば、Synscan ポートスキャンを検出する SID 630 では、id 値が 39426 (スキャナから伝送されるパケットの ID 番号として使われる静的な値) に設定されます。



(注) id 引数値は数値でなければなりません。

## ipopts

IPopts キーワードを使用すると、指定された IP 見出しオプションをパケット内で検索できます。次の表に、使用可能な引数値を示します。

表 153: IPoption 引数

引数	説明
rr	経路を記録
eol	リストの末尾
nop	オペレーションなし
ts	タイムスタンプ
sec	IP セキュリティ オプション
lsrr	厳密でない送信元ルーティング
ssrr	厳密な送信元ルーティング
satid	ストリーム識別子

アナリストが最も頻繁に監視するのは、厳密な送信元ルーティングと厳密でない送信元ルーティングです。これらのオプションは送信元 IP アドレスのスプーフィングを示している可能性があるためです。

### ip\_proto

ip\_proto キーワードを使用すると、キーワードの値として指定された IP プロトコルを含むパケットを識別できます。IP プロトコルは 0 ~ 255 の数値として指定できます。これらの番号を、<、>、または ! 演算子と組み合わせることができます。たとえば、ICMP 以外のプロトコルを使用しているトラフィックを検査するには、ip\_proto キーワードの値として !1 を使用します。1つのルール内で ip\_proto キーワードを複数回にわたって使用できます。ただし、ルールエンジンはキーワードの複数インスタンスをブール和関係 (AND) と解釈することに注意してください。たとえば、ip\_proto:!3; ip\_proto:!6 を含むルールを作成した場合、このルールは GGP プロトコルおよび TCP プロトコルを使用するトラフィックを無視します。

### tos

一部のネットワークでは、ネットワーク上を移動するパケットの優先度を設定するタイプオブサービス (ToS) 値が使用されます。tos キーワードを使用すると、キーワードの引数で指定された値に照らしてパケットの IP 見出し ToS 値を検査できます。tos キーワードを使用するルールは、ToS が指定の値に設定され、しかもルール内の残りの基準を満たすパケットに対してトリガーとして使用されます。



(注) tos の引数値は数値でなければなりません。

[ToS] フィールドは IP ヘッダープロトコルでは非推奨になり、[Differentiated Services Code Point (DSCP)] フィールドに置き換えられています。

## ttl

パケットの存続可能時間 (time-to-live、ttl) 値は、パケットが破棄される前に生成できるホップ数を示します。ttl キーワードを使用すると、キーワードの引数として指定された値または値の範囲に照らしてパケットの IP 見出し ttl 値を検査できます。ttl キーワードパラメータを 0 や 1 などの低い値に設定すると役立つことがあります。これは、低い存続可能時間値がトレースルートや侵入回避の試みを示している場合があるためです。(ただし、このキーワードの適切な値は、管理対象デバイスの配置やネットワークトポロジによって異なります)。次のように構文を使用します。

- TTL 値に特定の 1 つの値を設定するには、0 ~ 255 の整数を使用します。値の前に等号 (=) を付けることもできます (たとえば 5 または =5 を指定できます)。
- TTL 値の範囲を指定するには、ハイフン (-) を使用します (たとえば、0-2 は 0 ~ 2 のすべての値、-5 は 0 ~ 5 のすべての値、5- は 5 ~ 255 のすべての値をそれぞれ指定します)。
- 特定の値より大きい TTL 値を指定するには、「大なり」記号 (>) を使用します (たとえば、>3 は 3 より大きいすべての値を指定します)。
- 特定の値以上の TTL 値を指定するには、「大なりイコール」記号 (>=) を使用します (たとえば、>=3 は 3 以上のすべての値を指定します)。
- 特定の値より小さい TTL 値を指定するには、「小なり」記号 (<) を使用します (たとえば、<3 は 3 より小さいすべての値を指定します)。
- 特定の値以下の TTL 値を指定するには、「小なりイコール」記号 (<=) を使用します (たとえば、<=3 は 3 以下のすべての値を指定します)。

## ICMP ヘッダー値

Firepower システムでサポートされるキーワードを使用すると、ICMP パケットヘッダー内の攻撃やセキュリティポリシー違反を識別できます。なお、ほとんどの ICMP タイプおよびコードを検出する事前定義ルールがあることに注意してください。既存のルールを有効にするか、既存のルールに基づいてローカルルールを作成することを考慮してください。ICMP ルールを最初から作成するよりも、ニーズを満たすルールを見つける方が時間の節約になる可能性があります。

### icmp\_id と icmp\_seq

ICMP の識別番号とシーケンス番号は、ICMP 応答と ICMP 要求を関連付けるうえで役立ちます。通常のトラフィックでは、これらの値はパケットに動的に割り当てられます。一部のコバートチャンネルおよび Distributed Denial of Server (DDoS) プログラムは、静的な ICMP ID およびシーケンス値を使用します。次のキーワードを使用すると、静的な値を含む ICMP パケットを識別できます。

キーワード	定義 (Definition)
icmp_id	ICMP エコー要求または応答パケットの ICMP ID 番号を検査します。ICMP ID 番号に対応する数値を icmp_id キーワードの引数として使用します。
icmp_seq	icmp_seq キーワードは、ICMP エコー要求または応答パケットの ICMP シーケンスを検査します。ICMP シーケンス番号に対応する数値を icmp_seq キーワードの引数として使用します。

### itype

itype キーワードを使用して、特定の ICMP メッセージタイプ値を含むパケットを検索します。有効な ICMP タイプ値と無効な ICMP タイプ値のいずれかを指定して、さまざまなタイプのトラフィックを検査できます。たとえば、サービス拒否攻撃やフラッディング攻撃を発生させるために攻撃者が範囲外の ICMP タイプ値を設定することがあります。

「小なり」 (<) と「大なり」 (>) を使用して itype 引数値の範囲を指定できます。

次に例を示します。

- <35
- >36
- 3<>55

### icode

ICMP メッセージには、宛先が到達不能である場合の詳細を示すコード値が含まれることがあります。

icode キーワードを使用すると、特定の ICMP コード値を含むパケットを識別できます。有効な ICMP コード値と無効な ICMP コード値のいずれかを指定することにより、さまざまなタイプのトラフィックを検査できます。

「小なり」 (<) と「大なり」 (>) を使用して icode 引数値の範囲を指定できます。

次に例を示します。

- 35 より小さい値を検索するには <35 と指定します。
- 36 より大きい値を検索するには >36 と指定します。
- 3 ~ 55 の間にある値を検索するには、3<>55 と指定します。



#### ヒント

icode キーワードと itype キーワードを一緒に使用すると、両方に一致するトラフィックを識別できます。たとえば、ICMP 宛先到達不能コードタイプと ICMP ポート到達不能コードタイプを含む ICMP トラフィックを特定するには、値 3 の itype キーワード（宛先到達不能）と、値 3 の icode キーワード（ポート到達不能）を指定します。

## TCP ヘッダー値とストリーム サイズ

Firepower システムでは、パケットの TCP ヘッダーと TCP ストリーム サイズを使って試行される攻撃を識別するためのキーワードを使用できます。

### ack

ack キーワードを使用すると、パケットの TCP 確認応答番号と特定の値を比較できます。パケットの TCP 確認応答番号が、ack キーワードに指定された値と一致した場合に、ルールがトリガーとして使用されます。

ack の引数値は数値でなければなりません。

### フラグ (Flags)

flags キーワードを使用すると、複数の TCP フラグを任意に組み合わせて指定できます。検査対象のパケットでこれらが設定されている場合、ルールがトリガーとして使用されます。



- (注) 従来、flags の値として A+ を使用していたケースでは、代わりに flow キーワードおよび値 established を使用してください。一般に、フラグのすべての組み合わせが検出されるようにするには、フラグの使用時に flow キーワードおよび値 stateless を使用する必要があります。

次の表に示す flags キーワードの値を確認または無視することができます。

表 154: flags の引数

引数	TCP フラグ
ACK	データを確認応答します。
Psh	このパケットでデータが送信される必要があります。
Syn	新しい接続。
Urg	パケットに緊急データが含まれています。
Fin	接続が閉じられました。
Rst	接続が異常終了しました。
CWR	ECN 輻輳ウィンドウが減少しました。旧 R1 引数（下位互換性を維持するために引き続きサポートされています）。
ECE	ECN エコー。旧 R2 引数（下位互換性を維持するために引き続きサポートされています）。

flags キーワードを使用する場合、複数のフラグに対する照合方法をシステムに指示するための演算子を使用できます。次の表に、これらの演算子の説明を示します。

表 155: flags と一緒に使用する演算子

演算子	説明	例
すべて	パケットは、指定されたすべてのフラグを含んでいる必要があります。	Urg と all を選択すると、パケットが緊急フラグを含んでいる必要があること、および他のフラグが含まれる可能性があることを指定できます。
任意	パケットは、指定された任意のフラグを含むことができます。	Ack、Psh、および any を選択すると、ルールをトリガーとして使用するためには Ack と Psh のどちらか（または両方）のフラグが設定される必要があること、およびパケット内で他のフラグも設定されている可能性があることを指定できます。
ノット	パケットは、指定されたフラグセットを含んではなりません。	Urg と not を選択すると、このルールをトリガーとして使用するパケットに関して緊急フラグが設定されないことを指定できます。

### flow

flow キーワードを使用すると、セッション特性に基づいてルールで検査されるパケットを選択できます。flow キーワードを使用することで、ルールの適用対象となるトラフィック フロー方向を指定して、クライアントフローとサーバフローのどちらかにルールを適用できます。flow キーワードによるパケット検査の方法を指定するには、分析すべきトラフィックの方向、検査するパケットの状態、およびパケットが再構築ストリームの一部かどうかを設定できます。

ルールの処理時に、パケットのステートフルインスペクションが実行されます。ステートレストラフィック（セッションコンテキストが確立されていないトラフィック）を TCP ルールで無視するには、flow キーワードをルールに追加して、そのキーワードで **Established** 引数を選択する必要があります。UDP ルールでステートレストラフィックを無視するには、flow キーワードをルールに追加して、**Established** 引数と方向引数のどちらか（または両方）を選択する必要があります。これにより、TCP または UDP ルールでパケットのステートフルインスペクションが実行されます。

方向引数を追加した場合、ルールエンジンは、指定された方向と一致するフローを伴う確立された状態のパケットだけを検査します。たとえば、TCP または UDP 接続が検出されたときトリガーとして使用されるルールに、flow キーワードおよび established 引数と From Client 引数を追加した場合、ルールエンジンはクライアントから送信されたパケットだけを検査します。



**ヒント** パフォーマンスを最大にするには、必ず TCP ルールまたは UDP セッションルールに flow キーワードを含めてください。

次の表に、flow キーワードで指定できるストリーム関連引数の説明を示します。

表 156: *flow* の状態関連引数

引数	説明
Established	確立された接続でトリガーとして使用されます。
Stateless	ストリーム プロセッサの状態に関係なくトリガーとして使用されます。

次の表に、`flow` キーワードで指定できる方向オプションの説明を示します。

表 157: *flow* の方向引数

引数	説明
To Client	サーバ応答でトリガーとして使用されます。
To Server	クライアント応答でトリガーとして使用されます。
From Client	クライアント応答でトリガーとして使用されます。
From Server	サーバ応答でトリガーとして使用されます。

From Server と To Client の機能が同じであること、および To Server と From Client の機能も同じであることに注意してください。これらのオプションは、ルールに文脈と読みやすさを加味するために提供されています。たとえば、サーバからクライアントへの攻撃を検出するよう設計されたルールを作成する場合は、From Server を使用します。一方、クライアントからサーバへの攻撃を検出するよう設計されたルールを作成する場合は、From Client を使用します。

次の表に、`flow` キーワードで指定できるストリーム関連引数の説明を示します。

表 158: *flow* のストリーム関連引数

引数	説明
Ignore Stream Traffic	再構築されたストリーム パケットでトリガーとして使用されません。
Only Stream Traffic	再構築されたストリーム パケットでのみトリガーとして使用されます。

たとえば、`flow` キーワードの値として To Server, Established, Only Stream Traffic を使用すると、ストリームプリプロセッサで再構築された、確立済みセッションでクライアントからサーバに移動するトラフィックを検出できます。

## seq

`seq` キーワードを使用すると、静的なシーケンス番号値を指定できます。パケットのシーケンス番号が、指定された引数と一致する場合、そのキーワードを含むルールがトリガーとして使



用されます。このキーワードはあまり使用されませんが、静的シーケンス番号付きの生成済みパケットを使用する攻撃やネットワーク スキャンを識別するうえでこれが役立ちます。

**window**

window キーワードを使用すると、特定の TCP ウィンドウ サイズを指定できます。このキーワードを含むルールは、指定された TCP ウィンドウ サイズのパケットが検出されるたびにトリガーされます。このキーワードはあまり使用されませんが、静的 TCP ウィンドウ サイズ付きの生成済みパケットを使用する攻撃やネットワーク スキャンを識別するうえでこれが役立ちます。

**stream\_size**

次に示す形式で、stream\_size キーワードとストリーム プリプロセッサを組み合わせると、TCP ストリームのサイズをバイト単位で特定できます。

direction, operator, bytes

ここで、bytes はバイト数です。引数内の各オプションをカンマ (,) で区切る必要があります。

次の表は、stream\_size キーワードで指定できる大文字/小文字を区別しない方向オプションを示しています。

表 159: stream\_size キーワードの方向引数

引数	説明
client	指定されたストリームサイズに一致するクライアントからのストリームでトリガーとして使用されます。
server	指定されたストリームサイズに一致するサーバからのストリームでトリガーとして使用されます。
both	指定されたストリームサイズに一致するクライアントからのトラフィックとサーバからのトラフィックの両方によってトリガーとして使用されます。  たとえば both, >, 200 という引数は、クライアントからのトラフィックが 200 バイトを超え、しかもサーバからのトラフィックが 200 バイトを超えている場合にトリガーとして使用されます。
either	指定されたストリームサイズに一致するクライアントまたはサーバからのトラフィック (どちらか先に出現した方) によってトリガーとして使用されます。  たとえば both, >, 200 という引数は、クライアントからのトラフィックが 200 バイトを超え、しかもサーバからのトラフィックが 200 バイトを超えている場合にトリガーとして使用されます。

次の表に、stream\_size キーワードで使用できる演算子の説明を示します。

表 160: stream\_size キーワードの引数演算子

演算子	説明
=	次の値と等しい
!=	等しくない
>	より大きい
<	より少ない
>=	右辺と比較して大きいか等しい
<=	右辺と比較して小さいか等しい

たとえば、クライアントからサーバに移動する 5001216 バイト以上の TCP ストリームを検出するには、stream\_size キーワードの引数として client, >=, 5001216 を使用できます。

## stream\_reassemble キーワード

stream\_reassemble キーワードを使用すると、接続での検査対象トラフィックがルール条件と一致した場合に、1つの接続の TCP ストリーム再構築を有効/無効にすることができます。オプションで、このキーワードを1つのルール内で複数回使用することができます。

ストリーム再構築を有効または無効にするには、次の構文を使用します。

```
enable|disable, server|client|both, option, option
```

次の表に、stream\_reassemble キーワードで使用できるオプション引数の説明を示します。

表 161: stream\_reassemble のオプション引数

引数	説明
noalert	ルールで他にどの検出オプションが指定されているかに関係なく、イベントを生成しません。
fastpath	一致の検出時に残りの接続トラフィックを無視します。

たとえば、次のルールは、HTTP 応答で 200 OK ステータスコードが検出される接続に対してイベントを生成せずに、TCP クライアント側ストリーム再構築を無効にします。

```
alert tcp any 80 -> any any (flow:to_client, established; content: "200 OK";
stream_reassemble:disable, client, noalert
```

## SSL キーワード

SSL ルールキーワードを使用すると、Secure Sockets Layer (SSL) プリプロセッサを呼び出し、暗号化セッションのパケットから SSL のバージョンとセッション状態に関する情報を抽出できます。

SSL または Transport Layer Security (TLS) を使用する暗号化セッションを確立するためにクライアントとサーバが通信するとき、ハンドシェイクメッセージが交換されます。セッション中に伝送されるデータは暗号化されますが、ハンドシェイクメッセージは暗号化されません。

SSL プリプロセッサは、特定のハンドシェイクフィールドから状態とバージョンの情報を抽出します。ハンドシェイク内の 2 つのフィールドは、セッション暗号化に使われる SSL または TLS のバージョンとハンドシェイクのステージを示します。

### ssl\_state

ssl\_state キーワードを使用すると、暗号化されたセッションの状態情報と照合することができます。同時に使用される複数の SSL バージョンを検査するには、1 つのルール内で複数の ssl\_version キーワードを使用します。

ルールで ssl\_state キーワードが使用されている場合、ルールエンジンは SSL プリプロセッサを呼び出して、トラフィック内の SSL 状態情報を検査します。

たとえば、チャレンジ長が非常に長く、データが多すぎる ClientHello メッセージを送信することによってサーバ上のバッファオーバーフローを引き起そうとする攻撃者の試みを検出するには、ssl\_state キーワードと引数 client\_hello を使用し、異常に大きなパケットを検査することができます。

SSL 状態に関する複数の引数を指定するには、カンマ区切りのリストを使用します。複数の引数を列挙した場合、システムは OR 演算子を使ってそれら进行评估します。たとえば、引数として client\_hello および server\_hello を指定すると、システムは client\_hello または server\_hello のどちらかを含むトラフィックに照らしてルール进行评估します。

次のように、引数を除外することもできます。

```
!client_hello, !unknown
```

接続が一連の状態のそれぞれに到達したことを確認するには、ssl\_state ルールオプションを使用する複数のルールを使う必要があります。ssl\_state キーワードは、次の識別子を引数として受け入れます。

表 162: ssl\_state の引数

引数	目的
client_hello	クライアントが暗号化セッションを要求する、メッセージタイプ ClientHello のハンドシェイクメッセージを照合します。
server_hello	クライアントからの暗号化セッション要求に対してサーバが応答する、メッセージタイプ ServerHello のハンドシェイクメッセージを照合します。

引数	目的
client_keyx	サーバからのキーの受信を確認するためにクライアントがサーバにキーを送信する、メッセージタイプ ClientKeyExchange のハンドシェイク メッセージを照合します。
server_keyx	サーバからのキーの受信を確認するためにクライアントがサーバにキーを送信する、メッセージタイプ ServerKeyExchange のハンドシェイク メッセージを照合します。
unknown	任意のハンドシェイク メッセージタイプを照合します。

### ssl\_version

ssl\_version キーワードを使用すると、暗号化されたセッションのバージョン情報と照合することができます。ルールで ssl\_version キーワードが使用されている場合、ルールエンジンは SSL プリプロセッサを呼び出して、トラフィック内の SSL バージョン情報を検査します。

たとえば、SSL バージョン 2 にバッファ オーバーフロー脆弱性があることがわかっている場合、ssl\_version キーワードで sslv2 引数を使用して、その SSL バージョンを使用するトラフィックを識別できます。

SSL バージョンに関する複数の引数を指定するには、カンマ区切りのリストを使用します。複数の引数を列挙した場合、システムは OR 演算子を使ってそれら进行评估します。たとえば、SSLv2 を使用していない暗号化トラフィックを識別するには、

ssl\_version:ssl\_v3,tls1.0,tls1.1,tls1.2 をルールに追加できます。このルールは、SSL バージョン 3、TLS バージョン 1.0、TLS バージョン 1.1、または TLS バージョン 1.2 を使用するトラフィックを評価します。

ssl\_version キーワードは、次の SSL/TLS バージョン識別子を引数として受け入れます。

表 163: ssl\_version の引数

引数	目的
sslv2	Secure Sockets Layer (SSL) バージョン 2 を使用してエンコードされたトラフィックを照合します。
sslv3	Secure Sockets Layer (SSL) バージョン 3 を使用してエンコードされたトラフィックを照合します。
tls1.0	Transport Layer Security (TLS) バージョン 1.0 を使用してエンコードされたトラフィックを照合します。
tls1.1	Transport Layer Security (TLS) バージョン 1.1 を使用してエンコードされたトラフィックを照合します。
tls1.2	Transport Layer Security (TLS) バージョン 1.2 を使用してエンコードされたトラフィックを照合します。

## appid キーワード

パケットからアプリケーションプロトコル、クライアントアプリケーション、Webアプリケーションを特定するために appid キーワードを使用できます。たとえば、ある脆弱性をもつことが知られている特定のアプリケーションを検出することを考えます。

侵入ルールの appid キーワードの中で、[AppID の設定 (Configure AppID)] をクリックし、検出するアプリケーションを 1 つまたは複数選択します。

### 使用可能なアプリケーションの参照

条件の作成を初めて開始するときは、[使用可能なアプリケーション (Available Applications)] リストは制約されておらず、システムが検出するすべてのアプリケーションをページごとに 100 個ずつ表示します。

- アプリケーションを確認していくには、リストの下にある矢印をクリックします。
- アプリケーションの特性に関するサマリー情報と参照できるインターネットの検索リンクが示されているポップアップウィンドウを表示するには、アプリケーションの横にある情報アイコン (i) をクリックします。

### アプリケーションフィルタの使用

照合するアプリケーションを見つけやすくするために、[使用可能なアプリケーション (Available Applications)] リストを次のように制約できます。

- アプリケーションを検索するには、リスト上部にある [名前を検索 (Search by name)] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するアプリケーションが表示されます。
- フィルタを適用してアプリケーションを制約するには、[アプリケーションフィルタ (Application Filters)] リストを使用します。フィルタを適用すると、[使用可能なアプリケーション (Available Applications)] リストが更新されます。便宜上、システムはロック解除アイコン (🔓) を使用して、復号化されたトラフィック (暗号化されているトラフィックまたは暗号化されていないトラフィックではなく) でのみ識別できるアプリケーションをマークします。



- (注) [アプリケーションフィルタ (Application Filters)] リストで 1 つ以上のフィルタを選択し、しかも [使用可能なアプリケーション (Available Applications)] リストを検索した場合、選択内容と検索フィルタ適用後の [使用可能なアプリケーション (Available Applications)] リストが AND 演算を使って結合されます。

### アプリケーションの選択

アプリケーションを1つだけ選択するには、そのアプリケーションを選択し、[ルールへの追加 (Add to Rule)] をクリックします。フィルタで限定されている現在の表示のすべてのアプリケーションを選択するには、右クリックして [すべて選択 (Select All)] を選択します。

## アプリケーション層プロトコル値

アプリケーション層プロトコル値の正規化と検査はほとんどがプリプロセッサによって実行されますが、種々のプリプロセッサオプションを使用して、アプリケーション層値をさらに検査できます。

### RPC キーワード

rpc キーワードは、TCP または UDP パケットでオープン ネットワーク コンピューティング リモート プロシージャ コール (ONC RPC) サービスを識別します。これにより、ホスト上の RPC プログラムの識別試行を検出することができます。ネットワークで実行中のいずれかの RPC サービスを悪用できるかどうか判断するために、侵入者は RPC ポートマッパーを使用できます。また、ポートマッパーを使用せずに RPC を実行中の他のポートへのアクセスを試みることもできます。次の表に、rpc キーワードで使用できる引数を列挙します。

表 164: rpc キーワードの引数

引数	説明
アプリケーション	RPC アプリケーション番号
手順	呼び出される RPC プロシージャ
version	RPC バージョン

rpc キーワードの引数を指定するには、次の構文を使用します。

```
application,procedure,version
```

ここで、application は RPC アプリケーション番号、procedure は RPC プロシージャ番号、version は RPC バージョン番号です。rpc キーワードのすべての引数を指定する必要があります。引数のいずれかを指定できない場合は、アスタリスク (\*) で置き換えてください。

たとえば、任意のプロシージャまたはバージョンの RPC ポートマッパー (100000 という番号で示される RPC アプリケーション) を検索するには、引数として 100000,\*,\* を使用します。

### ASN.1 キーワード

asn1 キーワードを使用すると、さまざまな有害エンコードを検索しながら、パケットまたはパケットの一部をデコードできます。

次の表に、asn1 キーワードの引数について説明します。

表 165: asn.1 キーワードの引数

引数	説明
Bitstring Overflow	無効な、リモートで悪用可能なビットストリング エンコードを検出します。
Double Overflow	標準バッファより大きい二重 ASCII エンコードを検出します。これは Microsoft Windows の悪用可能な機能であることが知られていますが、現時点でどのサービスが悪用可能であるかは不明です。
Oversize Length	指定された引数より大きい ASN.1 タイプ長を検出します。たとえば Oversize Length を 500 に設定した場合、500 を上回る ASN.1 タイプによってルールがトリガーとして使用されます。
Absolute Offset	パケットペイロードの先頭からの絶対オフセットを設定します (offset カウンタがバイト 0 から始まることに注意してください)。たとえば SNMP パケットをデコードするには、Absolute Offset を 0 に設定し、Relative Offset を設定しません。Absolute Offset として正または負の値が可能です。
Relative Offset	これは、最後に見つかったコンテンツ一致、pcrcr、または byte_jump からの相対オフセットです。コンテンツ "foo" の直後の ASN.1 シーケンスをデコードするには、Relative Offset を 0 に設定し、Absolute Offset を設定しません。Relative Offset として正または負の値が可能です。(オフセット カウンタが 0 から始まることに注意してください。)

たとえば、Microsoft ASN.1 ライブラリにおける既知の脆弱性ではバッファ オーバーフローが発生し、攻撃者は特別に細工した認証パケットを使ってその状態を悪用できます。システムが asn.1 データをデコードするとき、パケット内の exploit コードは、システム レベル特権付きでホスト上で動作したり、DoS 状態を引き起したりすることができます。次のルールは、asn1 キーワードを使用して、この脆弱性を悪用する試みを検出します。

```

alert tcp $EXTERNAL_NET any -> $HOME_NET 445
(flow:to_server, established; content:"|FF|SMB|73|";
nocase; offset:4; depth:5;
asn1:bitstring_overflow,double_overflow,oversize_length 100,
relative_offset 54;)
    
```

上記のルールの場合、任意のポートおよび \$EXTERNAL\_NET 変数で定義された任意の IP アドレスから発信され、ポート 445 を使用する \$HOME\_NET 変数で定義された任意の IP アドレスに向かう TCP トラフィックに対して、イベントが生成されます。加えて、サーバへの TCP 接続が確立された時点でのみルールを実行します。その後、ルールは特定の位置にある特定のコンテンツを検査します。最後に、ルールは asn1 キーワードを使用して、ビットストリング エンコードと二重 ASCII エンコードを検出し、最後に見つかったコンテンツ一致の末尾から 55 バイト目以降、長さ 100 バイトを超える asn.1 タイプ長を識別します。(offset カウンタがバイト 0 から始まることに注意してください。)

## urilen キーワード

urilen キーワードと HTTP Inspect プリプロセッサを組み合わせて使用すると、特定の長さ、最大長を下回る、最小長を上回る、または指定された範囲内の URI を HTTP トラフィック内で検査できます。

HTTP Inspect プリプロセッサがパケットを正規化して検査した後、ルールエンジンはルールに照らしてそのパケットを評価し、urilen キーワードで指定された長さ条件に URI が一致するかどうか判断します。このキーワードを使用すると、URI 長の脆弱性をエクスプロイトしようとする試みを検出できます。たとえばバッファ オーバーフローを発生させて、攻撃者が DoS 状態を引き起こしたり、システムレベル特権付きでホスト上でコードを実行したりしようと試みる可能性があります。

ルール内で urilen キーワードを使用するときには、次の点に注意してください。

- 必ず flow:established キーワードおよび他の 1 つ以上のキーワードを組み合わせて、urilen キーワードを使用してください。
- ルールプロトコルは常に TCP です。
- ターゲットポートは常に HTTP ポートです。

URI 長を指定するときには、10 進のバイト数、「小なり」 (<)、および「大なり」 (>) を使用します。

次に例を示します。

- 5 バイト長の URI を検出するには、5 を指定します。
- 5 バイト長を下回る URI を検出するには、< 5 (1 つの空白文字で区切る) を指定します。
- 5 バイト長を上回る URI を検出するには、> 5 (1 つの空白文字で区切る) を指定します。
- 3 ~ 5 バイト長の URI を検出するには、3 <> 5 (<> の前後に空白文字を 1 つずつ含む) を指定します。

たとえば、Novell の eDirectory バージョン 8.8 に付属のサーバモニタリングおよび診断ユーティリティ iMonitor バージョン 2.4 には、脆弱性があることが知られています。長すぎる URI を含むパケットはバッファ オーバーフローを発生させるため、攻撃者はシステムレベル特権付きでホスト上で動作したり、DoS 状態を引き起こしたりできる特別に細工したパケットを使ってその状態をエクスプロイトできます。次のルールは、urilen キーワードを使用して、この脆弱性を悪用する試みを検出します。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"EXPLOIT eDirectory 8.8 Long URI iMonitor buffer
overflow attempt"; flow:to_server,established;
urilen:> 8192; uricontent:"/nds/"; nocase;
classtype:attempted-admin; sid:x; rev:1;)
```

上記のルールの場合、任意のポートおよび \$EXTERNAL\_NET 変数で定義された任意の IP アドレスから発信され、\$HTTP\_PORTS 変数で定義されたポートを使用して、\$HOME\_NET 変数で



定義された任意の IP アドレスに向かう TCP トラフィックに対して、イベントが生成されます。加えて、サーバへの TCP 接続が確立された時点でのみ、パケットがルールに照らして評価されます。ルールは、`urilen` キーワードを使用して、長さ 8192 バイトを超える URI を検出します。最後に、ルールは URI を検索して、大文字/小文字を区別しない特定のコンテンツ `/nds/` を探します。

**関連トピック**

- [侵入ルール ヘッダー プロトコル \(1688 ページ\)](#)
- [侵入ルール ヘッダーの送信元および宛先ポート \(1693 ページ\)](#)
- [定義済みデフォルト変数 \(447 ページ\)](#)

## DCE/RPC キーワード

次の表で説明する 3 つの DCE/RPC キーワードを使用して、DCE/RPC セッション トラフィックの 익스プロイトをモニタできます。これらのキーワードを含むルールを処理するとき、システムは DCE/RPC プリプロセッサを呼び出します。

表 166: DCE/RPC キーワード

使用するフィルタ	使用方法	検出対象
<code>dce_iface</code>	単独	特定の DCE/RPC サービスを特定するパケット
<code>dce_opnum</code>	<code>dce_iface</code> の後ろ	特定の DCE/RPC サービス オペレーションを特定するパケット
<code>dce_stub_data</code>	<code>dce_iface + dce_opnum</code> の後ろ	特定の処理要求または応答を定義するスタブデータ

表に示されているように、`dce_opnum` の前に必ず `dce_iface` を配置し、`dce_stub_data` の前に必ず `dce_iface + dce_opnum` を配置する必要があることに注意してください。

また、これらの DCE/RPC キーワードを他のルール キーワードと組み合わせて使用することもできます。DCE/RPC ルールでは、**DCE/RPC** の引数が選択された状態で `byte_jump`、`byte_test`、`byte_extract` の各キーワードを使用することに注意してください。

シスコでは、DCE/RPC キーワードを含むルールに 1 つ以上の `content` キーワードを含めることを推奨しています。こうすると、ルール エンジンが常に高速パターン マッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルールに 1 つ以上の `content` キーワードが含まれている場合は、`content` キーワードの [高速パターン マッチ機能を使用 (Use Fast Pattern Matcher)] 引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。

次のケースでは、DCE/RPC バージョンおよび隣接ヘッダー情報を一致コンテンツとして使用できます。

- ルールに他の `content` キーワードが含まれていない
- ルールにもう 1 つ `content` キーワードが含まれているが、DCE/RPC バージョンおよび隣接情報が、他方の `content` よりも特有のパターンを表している

たとえば、DCE/RPCバージョンおよび隣接情報は通常、1バイトのコンテンツよりも特有です。

次に示すバージョンおよび隣接情報コンテンツ一致のいずれか1つを使用して、ルール限定を終了する必要があります。

- コネクション型DCE/RPCルールでは、コンテンツ |05 00 00| (メジャーバージョン 05、マイナーバージョン 00、および要求 PDU (プロトコルデータユニット) タイプ 00) を使用します。
- コネクションレス型DCE/RPCルールでは、コンテンツ |04 00| (バージョン 04、要求 PDU タイプ 00) を使用します。

いずれの場合も、DCE/RPC プリプロセッサで完了済みの処理を繰り返すことなく高速パターンマッチ機能呼び出すために、ルール内の最後のキーワードとしてバージョンおよび隣接情報の content キーワードを配置してください。ルールの末尾に配置される content キーワードは、高速パターンマッチ機能呼び出す手段として使われるバージョン コンテンツに当てはまりますが、ルール内の他のコンテンツ一致には必ずしも当てはまらないことに注意してください。

#### 関連トピック

[DCE/RPC プリプロセッサ \(1856 ページ\)](#)

[content キーワードと protected\\_content キーワード \(1712 ページ\)](#)

[content キーワードの高速パターンマッチ機能の引数 \(1724 ページ\)](#)

[概要 : byte\\_jump および byte\\_test キーワード](#)

[byte\\_extract キーワード \(1733 ページ\)](#)

## dce\_iface

dce\_iface キーワードを使用すると、特定の DCE/RPC サービスを識別できます。

オプションで、dce\_iface キーワードを dce\_opnum キーワードおよび dce\_stub\_data キーワードと組み合わせて使用すると、検査する DCE/RPC トラフィックをさらに限定することができます。

固定型 16 バイト Universally Unique Identifier (UUID) は、それぞれの DCE/RPC サービスに割り当てられるアプリケーションインターフェイスを識別します。たとえば、UUID 4b324fc8-670-01d3-1278-5a47bf6ee188 は、srsvcs サービスとしても知られる DCE/RPC lanmanserver サービスを識別します。このサービスは、ピアツーピアプリンタ、ファイル、および SMB 名前付きパイプを共有するためのさまざまな管理機能を提供します。DCE/RPC プリプロセッサは UUID および関連するヘッダー値を使用して DCE/RPC セッションを追跡します。

インターフェイス UUID は、次のように、ハイフンで区切られた 5 つの 16 進文字列で構成されます。

```
<4hexbytes>-<2hexbytes>-<2hexbytes>-<2hexbytes>-<6hexbytes>
```

次に示す netlogon インターフェイスの UUID のように、ハイフンを含む UUID 全体を入力することで、インターフェイスを指定します。

12345678-1234-abcd-ef00-01234567cffb

UUID内の最初の3つの文字列はビッグエンディアンバイト順で指定される必要があることに注意してください。通常、公開されたインターフェイスリストやプロトコルアナライザにはUUIDが正しいバイト順で表示されますが、それを入力する前にUUIDバイト順を変更しなければならない場合もあります。次に示すメッセージャーサービスUUIDの場合、リトルエンディアンバイト順の最初の3つの文字列を含む未加工ASCIIテキストで表示されることがあります。

f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc

この同じUUIDをdce\_ifaceキーワードに指定するには、次のようにハイフンを挿入し、最初の3つの文字列をビッグエンディアンバイト順で配置できます。

5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc

1つのDCE/RPCセッションに複数のインターフェイスへの要求を含めることができますが、1つのルールには1つのdce\_ifaceキーワードだけを含めてください。追加のインターフェイスを検出するには、追加のルールを作成します。

DCE/RPCアプリケーションインターフェイスにはインターフェイスバージョン番号も割り当てられます。オプションで、インターフェイスバージョンを指定できます。その際、バージョンが指定値に等しい、等しくない、指定値より小さい、または大きいことを示す演算子を使用します。

TCPセグメンテーションやIPフラグメンテーションに加えて、コネクション型とコネクションレス型の両方のDCE/RPCをフラグメント化することができます。通常、先頭以外のDCE/RPCフラグメントを指定のインターフェイスに関連付けるのはあまり効率的ではありません。このようにすると、多数の誤検出が発生する可能性があります。ただし、柔軟性を維持するために、オプションで、指定されたインターフェイスに照らしてすべてのフラグメントを評価できます。

次の表に、dce\_ifaceキーワードの引数を要約します。

表 167: dce\_iface の引数

引数	説明
Interface UUID	DCE/RPC トラフィック内で検出対象となる特定のサービスのアプリケーションインターフェイスを識別する、ハイフンを含むUUID。指定されたインターフェイスに関連付けられた任意の要求がインターフェイス UUID に一致します。
Version	オプションで、アプリケーション インターフェイス バージョン番号 0 ~ 65535 と、検出対象のバージョンが指定値より大きい (>)、小さい (<)、等しい (=)、または等しくない (!) を示す演算子。

引数	説明
All Fragments	オプションで、関連するすべてのDCE/RPCフラグメント内のインターフェイスの照合、およびインターフェイスバージョン（指定されている場合）での照合を有効にします。この引数はデフォルトで無効になっています。これは、最初のフラグメントまたはフラグメント化されていないパケット全体が指定のインターフェイスに関連付けられている場合にのみ、キーワードが一致することを意味します。この引数を有効にすると、誤検出が発生する可能性があることに注意してください。

## dce\_opnum キーワード

dce\_opnum キーワードを DCE/RPC プリプロセッサと組み合わせて使用すると、DCE/RPC サービスが提供する 1 つ以上の特定のオペレーションを識別するパケットを検出できます。

クライアント関数呼び出しは、DCE/RPC 仕様で「オペレーション」と呼ばれる特定のサービス関数を要求します。オペレーション番号 (opnum) は DCE/RPC ヘッダー内の特定のオペレーションを識別します。エクスプロイトは特定のオペレーションを標的にすることがあります。

たとえば UUID 12345678-1234-abcd-ef00-01234567cffb は、数十種類のオペレーションを提供する netlogon サービスのインターフェイスを識別します。その 1 つがオペレーション 6 (NetrServerPasswordSet オペレーション) です。

オペレーション用のサービスを識別するには、dce\_opnum キーワードの前に dce\_iface キーワードを指定する必要があります。

特定のオペレーションを示す 1 つの 10 進数値 (0 ~ 65535 の範囲)、ハイフンで区切られたオペレーション範囲、またはカンマ区切りのオペレーション/範囲リストを任意の順序で指定できます。

次の例は、すべて有効な netlogon オペレーション番号を表しています。

```
15
15-18
15, 18-20
15, 20-22, 17
15, 18-20, 22, 24-26
```

## dce\_stub\_data キーワード

dce\_stub\_data キーワードを DCE/RPC プリプロセッサと組み合わせて使用すると、他のルールオプションとは無関係に、スタブデータの先頭からインスペクションを開始するようルールエンジンに指示できます。dce\_stub\_data キーワードの後に続くパケットペイロードルールオプションは、スタブデータバッファを基準にして適用されます。

DCE/RPC スタブデータは、クライアントプロシージャコールと DCE/RPC ランタイムシステム (DCE/RPC の中核をなすルーチンとサービスを提供するメカニズム) の間のインターフェイスを提供します。DCE/RPC エクスプロイトは、DCE/RPC パケットのスタブデータ部分で識別されます。スタブデータは特定のオペレーションまたは関数呼び出しに関連付けられているため、必ず dce\_stub\_data の前に dce\_iface と dce\_opnum を指定して、関連するサービスとオペレーションを識別してください。

dce\_stub\_data キーワードには引数がありません。

## SIP キーワード

4 つの SIP キーワードを使用すると、SIP セッショントラフィックでエクスプロイトを監視できます。

SIP プロトコルはサービス拒否 (DoS) 攻撃に対して脆弱であることに注意してください。このような攻撃に対処するルールでは、レートベースの攻撃防御を活用できます。

### sip\_header キーワード

sip\_header キーワードを使用すると、抽出された SIP 要求または応答ヘッダーの先頭から検査を開始し、検査対象をヘッダーフィールドに限定することができます。

sip\_header キーワードには引数がありません。

次の例のルールフラグメントは SIP ヘッダーを指し示し、CSeq ヘッダーフィールドに一致します。

```
alert udp any any -> any 5060 ( sip_header; content:"CSeq"; )
```

#### 関連トピック

[動的侵入ルール状態](#) (1649 ページ)

[レートベースの攻撃防御](#) (2000 ページ)

### sip\_body キーワード

sip\_body キーワードを使用すると、抽出された SIP 要求または応答メッセージ本文の先頭から検査を開始し、検査対象をメッセージ本文に限定することができます。

sip\_body キーワードには引数がありません。

次の例のルールフラグメントは SIP メッセージ本文を指し示し、抽出された SDP データの c (接続情報) フィールド内の特定の IP アドレスに一致します。

```
alert udp any any -> any 5060 ( sip_body; content:"c=IN 192.168.12.14"; )
```

ルールが SDP コンテンツの検索だけに限定されないことに注意してください。SIP プリプロセッサはメッセージ本文全体を抽出し、それをルールエンジンで使用できるようにします。

### sip\_method キーワード

各 SIP 要求内の *method* フィールドは要求の目的を識別します。sip\_method キーワードを使用すると、SIP 要求の中で特定のメソッドを検査することができます。複数のメソッドはカンマで区切ります。

次に示す現在定義されている SIP メソッドを指定できます。

```
ack, benotify, bye, cancel, do, info, invite, join, message, notify, options, prack, publish, quath, refer, register, service, sprack, subscribe, unsubscribe, update
```

メソッドでは大文字と小文字が区別されません。複数のメソッドをカンマで区切ることができます。

今後、新しいSIPメソッドが定義される可能性があるため、カスタムメソッド、つまり現在定義されているSIPメソッド以外のメソッドを指定することもできます。可能なフィールド値はRFC2616で定義されています。=、(、)などの制御文字と区切り文字を除いて、すべての文字を使用できます。除外されている区切り文字の完全なリストについては、RFC 2616を参照してください。指定されたカスタムメソッドがトラフィックで検出されると、システムはパケットヘッダーを検査しますが、メッセージは検査されません。

システムでは最大32個のメソッド（現在定義されている21個のメソッドと追加の11個のメソッド）がサポートされます。システムは、設定される未定義のメソッドをすべて無視します。合計32個のメソッドには、SIPプリプロセッサのオプション[検査するメソッド (Methods to Check)]を使って指定されるメソッドが含まれることに注意してください。

否定を使用する場合は、1つのメソッドだけを指定できます。次に例を示します。

```
!invite
```

ただし、1つのルール内の複数の sip\_method キーワードが **AND** 演算で結合されることに注意してください。たとえば、invite と cancel を除くすべての抽出されたメソッドを検査するには、次のような2つの否定付き sip\_method キーワードを使用します。

```
sip_method: !invite
sip_method: !cancel
```

Cisco では、sip\_method キーワードを含むルールに1つ以上の content キーワードを含めることを推奨しています。こうすると、ルールエンジンが常に高速パターンマッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルールに1つ以上の content キーワードが含まれている場合は、content キーワードの [高速パターンマッチ機能を使用 (Use Fast Pattern Matcher)] 引数が有効になっているかどうかに関係なく、ルールエンジンが高速パターンマッチ機能を使用することに注意してください。

### 関連トピック

[SIP プリプロセッサのオプション](#) (1905 ページ)

[content キーワードと protected\\_content キーワード](#) (1712 ページ)

[content キーワードの高速パターンマッチ機能の引数](#) (1724 ページ)

## sip\_stat\_code キーワード

各 SIP 応答内の3桁のステータスコードは、要求されたアクションの結果を示します。

sip\_stat\_code キーワードを使用すると、SIP 応答の中で特定のステータスコードを検査することができます。

1桁の応答タイプ番号1～9、特定の3桁の番号100～999、またはこれらを任意に組み合わせたカンマ区切りリストを指定できます。リスト内のいずれか1つの番号がSIP 応答内のコードに一致する場合、そのリストが一致します。

次の表に、指定可能なSIPステータスコード値の説明を示します。

表 168: sip\_stat\_code の値

検出対象	指定する内容	例	検出結果
1 つの特定のステータスコード	3 桁のステータスコード	189	189
指定された 1 桁で始まる 3 桁のコード	1 桁	1	1xx、つまり 100、101、102 など
値のリスト	特定のコードおよび 1 桁を任意に組み合わせてカンマで区切る	222, 3	222 および 300、301、302 など

また、ルールに content キーワードが含まれているかどうかに関係なく、sip\_stat\_code キーワードを使って指定された値を検索するためにルールエンジンが高速パターンマッチ機能を使用しないことにも注意してください。

## GTP キーワード

3 つの GSRP トンネリングプロトコル (GTP) キーワードを使用すると、GTP バージョン、メッセージタイプ、および情報要素をコマンドチャンネル内で検査できます。content や byte\_jump などの他の侵入ルールキーワードと組み合わせて GTP キーワードを使用することはできません。gtp\_info または gtp\_type キーワードを使用するそれぞれのルールで、gtp\_version キーワードを使用する**必要があります**。

### gtp\_version キーワード

gtp\_version キーワードを使用すると、GTP 制御メッセージの中で GTP バージョン 0、1、または 2 を検査することができます。

定義されているメッセージタイプと情報要素は GTP バージョンによって異なるため、gtp\_type または gtp\_info キーワードを使用するときには、gtp\_version を使用する**必要があります**。値として 0、1、または 2 を指定できます。

### gtp\_type キーワード

それぞれの GTP メッセージは、数値と文字列で構成されるメッセージタイプによって識別されます。gtp\_type キーワードを使用すると、特定の GTP メッセージタイプのトラフィックを検査できます。定義されているメッセージタイプと情報要素は GTP バージョンによって異なるため、gtp\_type または gtp\_info キーワードを使用するときには、gtp\_version も使用する**必要があります**。

次の例に示すように、メッセージタイプとして定義済みの 10 進数値、定義済み文字列、あるいはどちらか（または両方）を任意に組み合わせたカンマ区切りリストを指定できます。

```
10, 11, echo_request
```

リスト内のそれぞれの値または文字列を照合するとき、システムはOR演算を使用します。値と文字列を列挙する順序は重要ではありません。リスト内のいずれか1つの値または文字列の一致により、キーワードが一致します。認識されない文字列または範囲外の値を含むルールを保存しようとする、エラーが発生します。

表に示されているように、GTPバージョンに応じて、同じメッセージタイプの値が異なる場合があることに注意してください。たとえば `sgsn_context_request` メッセージタイプの値は GTPv0 と GTPv1 では 50 ですが、GTPv2 では 130 です。

パケット内のバージョン番号に応じて、`gtp_type` キーワードは異なる値と一致します。上記の例の場合、GTPv0 または GTPv1 パケットではキーワードがメッセージタイプ値 50 と一致しますが、GTPv2 パケットでは値 130 と一致します。パケット内のメッセージタイプ値が、パケットで指定されたバージョンの既知の値でない場合は、キーワードがパケットと一致しません。

メッセージタイプに整数を指定した場合、パケット内で指定されたバージョンとは無関係に、キーワード内のメッセージタイプが GTP パケット内の値と一致すればキーワードが一致します。

次の表に、GTP メッセージタイプごとにシステムで認識される定義済みの値と文字列を示します。

表 169: GTP メッセージタイプ

値	Version 0	Version 1	Version 2
1	echo_request	echo_request	echo_request
2	echo_response	echo_response	echo_response
3	version_not_supported	version_not_supported	version_not_supported
4	node_alive_request	node_alive_request	該当なし
5	node_alive_response	node_alive_response	該当なし
[6]	redirection_request	redirection_request	該当なし
7	redirection_response	redirection_response	該当なし
16	create_pdp_context_request	create_pdp_context_request	該当なし
17	create_pdp_context_response	create_pdp_context_response	該当なし
18	update_pdp_context_request	update_pdp_context_request	該当なし
19	update_pdp_context_response	update_pdp_context_response	該当なし
20	delete_pdp_context_request	delete_pdp_context_request	該当なし
21	delete_pdp_context_response	delete_pdp_context_response	該当なし



値	Version 0	Version 1	Version 2
22	create_aa_pdp_context_request	init_pdp_context_activation_request	該当なし
23	create_aa_pdp_context_response	init_pdp_context_activation_response	該当なし
24	delete_aa_pdp_context_request	該当なし	該当なし
25	delete_aa_pdp_context_response	該当なし	該当なし
26	error_indication	error_indication	該当なし
27	pdu_notification_request	pdu_notification_request	該当なし
36	pdu_notification_response	pdu_notification_response	該当なし
29	pdu_notification_reject_request	pdu_notification_reject_request	該当なし
30	pdu_notification_reject_response	pdu_notification_reject_response	該当なし
31	該当なし	supported_ext_header_notification	該当なし
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response
36	note_ms_present_request	note_ms_present_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	該当なし	該当なし	change_notification_request
39	該当なし	該当なし	change_notification_response
48	identification_request	identification_request	該当なし
49	identification_response	identification_response	該当なし
50	sgsn_context_request	sgsn_context_request	該当なし
51	sgsn_context_response	sgsn_context_response	該当なし
52	sgsn_context_ack	sgsn_context_ack	該当なし
53	該当なし	forward_relocation_request	該当なし
54	該当なし	forward_relocation_response	該当なし
55	該当なし	forward_relocation_complete	該当なし

値	Version 0	Version 1	Version 2
72	該当なし	relocation_cancel_request	該当なし
57	該当なし	relocation_cancel_response	該当なし
58	該当なし	forward_sms_context	該当なし
59	該当なし	forward_relocation_complete_ack	該当なし
60	該当なし	forward_sms_context_ack	該当なし
64	該当なし	該当なし	modify_bearer_command
65	該当なし	該当なし	modify_bearer_failure_indication
66	該当なし	該当なし	delete_bearer_command
67	該当なし	該当なし	delete_bearer_failure_indication
68	該当なし	該当なし	bearer_resource_command
69	該当なし	該当なし	bearer_resource_failure_indication
70	該当なし	ran_info_relay	downlink_failure_indication
71	該当なし	該当なし	trace_session_activation
72	該当なし	該当なし	trace_session_deactivation
73	該当なし	該当なし	stop_paging_indication
95	該当なし	該当なし	create_bearer_request
96	該当なし	mbms_notification_request	create_bearer_response
97	該当なし	mbms_notification_response	update_bearer_request
98	該当なし	mbms_notification_reject_request	update_bearer_response
99	該当なし	mbms_notification_reject_response	delete_bearer_request
100	該当なし	create_mbms_context_request	delete_bearer_response
101	該当なし	create_mbms_context_response	delete_pdn_request
102	該当なし	update_mbms_context_request	delete_pdn_response
103	該当なし	update_mbms_context_response	該当なし
104	該当なし	delete_mbms_context_request	該当なし
105	該当なし	delete_mbms_context_response	該当なし

値	Version 0	Version 1	Version 2
112	該当なし	mbms_register_request	該当なし
113	該当なし	mbms_register_response	該当なし
114	該当なし	mbms_deregister_request	該当なし
115	該当なし	mbms_deregister_response	該当なし
116	該当なし	mbms_session_start_request	該当なし
117	該当なし	mbms_session_start_response	該当なし
118	該当なし	mbms_session_stop_request	該当なし
119	該当なし	mbms_session_stop_response	該当なし
120	該当なし	mbms_session_update_request	該当なし
121	該当なし	mbms_session_update_response	該当なし
128	該当なし	ms_info_change_request	identification_request
129	該当なし	ms_info_change_response	identification_response
130	該当なし	該当なし	sgsn_context_request
131	該当なし	該当なし	sgsn_context_response
132	該当なし	該当なし	sgsn_context_ack
133	該当なし	該当なし	forward_relocation_request
134	該当なし	該当なし	forward_relocation_response
135	該当なし	該当なし	forward_relocation_complete
136	該当なし	該当なし	forward_relocation_complete_ack
137	該当なし	該当なし	forward_access
138	該当なし	該当なし	forward_access_ack
139	該当なし	該当なし	relocation_cancel_request
140	該当なし	該当なし	relocation_cancel_response
141	該当なし	該当なし	configuration_transfer_tunnel
149	該当なし	該当なし	detach
150	該当なし	該当なし	detach_ack

値	Version 0	Version 1	Version 2
151	該当なし	該当なし	cs_paging
152	該当なし	該当なし	ran_info_relay
153	該当なし	該当なし	alert_mme
154	該当なし	該当なし	alert_mme_ack
155	該当なし	該当なし	ue_activity
156	該当なし	該当なし	ue_activity_ack
160	該当なし	該当なし	create_forward_tunnel_request
161	該当なし	該当なし	create_forward_tunnel_response
162	該当なし	該当なし	suspend
163	該当なし	該当なし	suspend_ack
164	該当なし	該当なし	復帰
165	該当なし	該当なし	resume_ack
166	該当なし	該当なし	create_indirect_forward_tunnel_request
167	該当なし	該当なし	create_indirect_forward_tunnel_response
168	該当なし	該当なし	delete_indirect_forward_tunnel_request
169	該当なし	該当なし	delete_indirect_forward_tunnel_response
170	該当なし	該当なし	release_access_bearer_request
171	該当なし	該当なし	release_access_bearer_response
176	該当なし	該当なし	downlink_data
177	該当なし	該当なし	downlink_data_ack
179	該当なし	該当なし	pgw_restart
180	該当なし	該当なし	pgw_restart_ack
200	該当なし	該当なし	update_pdn_request
201	該当なし	該当なし	update_pdn_response
211	該当なし	該当なし	modify_access_bearer_request
212	該当なし	該当なし	modify_access_bearer_response

値	Version 0	Version 1	Version 2
231	該当なし	該当なし	mbms_session_start_request
232	該当なし	該当なし	mbms_session_start_response
233	該当なし	該当なし	mbms_session_update_request
234	該当なし	該当なし	mbms_session_update_response
235	該当なし	該当なし	mbms_session_stop_request
236	該当なし	該当なし	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	該当なし
241	data_record_transfer_response	data_record_transfer_response	該当なし
254	該当なし	end_marker	該当なし
255	pdu	pdu	該当なし

### gtp\_info キーワード

1つのGTPメッセージには多数の情報要素が含まれることがあり、それぞれの要素は定義済み数値および定義済み文字列によって識別されます。gtp\_info キーワードを使用すると、指定された情報要素の先頭から検査を開始し、検査対象を指定の情報要素に限定することができます。定義されているメッセージタイプと情報要素はGTPバージョンによって異なるため、このキーワードを使用するときには、gtp\_version も使用する必要があります。

情報要素に対して定義された10進数値と定義された文字列のどちらでも指定できます。単一の値または文字列を指定することも、1つのルール内で複数のgtp\_info キーワードを使って複数の情報要素を検査することもできます。

1つのメッセージに同じタイプの複数の情報要素が含まれている場合は、すべてが照合対象として検査されます。情報要素が無効な順序で出現する場合は、最後のインスタンスだけが検査されます。

GTPバージョンに応じて、同じ情報要素の値が異なる場合があることに注意してください。たとえば cause 情報要素の値はGTPv0とGTPv1では1ですが、GTPv2では2です。

パケット内のバージョン番号に応じて、gtp\_info キーワードは異なる値と一致します。上記の例の場合、GTPv0またはGTPv1パケットではキーワードが情報要素値1と一致しますが、GTPv2パケットでは値2と一致します。パケット内の情報要素値が、パケットで指定されたバージョンの既知の値でない場合は、キーワードがパケットと一致しません。

情報要素に整数を指定した場合、パケット内で指定されたバージョンとは無関係に、キーワード内のメッセージタイプがGTPパケット内の値と一致すればキーワードが一致します。

次の表に、GTP情報要素ごとにシステムで認識される値と文字列を示します。

表 170: GTP情報要素

値	Version 0	Version 1	Version 2
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	recovery
4	tlli	tlli	該当なし
5	p_tmsi	p_tmsi	該当なし
[6]	qos	該当なし	該当なし
8	recording_required	recording_required	該当なし
9	認証	認証	該当なし
11	map_cause	map_cause	該当なし
12	p_tmsi_sig	p_tmsi_sig	該当なし
13	ms_validated	ms_validated	該当なし
18	recovery	recovery	該当なし
15	selection_mode	selection_mode	該当なし
16	flow_label_data_1	teid_1	該当なし
17	flow_label_signalling	teid_control	該当なし
18	flow_label_data_2	teid_2	該当なし
19	ms_unreachable	teardown_ind	該当なし
20	該当なし	nsapi	該当なし
21	該当なし	ranap	該当なし
22	該当なし	rab_context	該当なし
23	該当なし	radio_priority_sms	該当なし
24	該当なし	radio_priority	該当なし
25	該当なし	packet_flow_id	該当なし
26	該当なし	charging_char	該当なし
27	該当なし	trace_ref	該当なし

値	Version 0	Version 1	Version 2
36	該当なし	trace_type	該当なし
29	該当なし	ms_unreachable	該当なし
71	該当なし	該当なし	apn
72	該当なし	該当なし	ambr
73	該当なし	該当なし	ebi
74	該当なし	該当なし	ip_addr
75	該当なし	該当なし	mei
76	該当なし	該当なし	msisdn
77	該当なし	該当なし	indication
78	該当なし	該当なし	pco
79	該当なし	該当なし	paa
80	該当なし	該当なし	bearer_qos
80	該当なし	該当なし	flow_qos
82	該当なし	該当なし	rat_type
83	該当なし	該当なし	serving_network
84	該当なし	該当なし	bearer_tft
85	該当なし	該当なし	tad
86	該当なし	該当なし	uli
87	該当なし	該当なし	f_teid
88	該当なし	該当なし	tmsi
89	該当なし	該当なし	cn_id
90	該当なし	該当なし	s103pdf
91	該当なし	該当なし	s1udf
92	該当なし	該当なし	delay_value
93	該当なし	該当なし	bearer_context
94	該当なし	該当なし	charging_id

値	Version 0	Version 1	Version 2
95	該当なし	該当なし	charging_char
96	該当なし	該当なし	trace_info
97	該当なし	該当なし	bearer_flag
99	該当なし	該当なし	pdn_type
100	該当なし	該当なし	pti
101	該当なし	該当なし	drx_parameter
103	該当なし	該当なし	gsm_key_tri
104	該当なし	該当なし	umts_key_cipher_quin
105	該当なし	該当なし	gsm_key_cipher_quin
106	該当なし	該当なし	umts_key_quin
107	該当なし	該当なし	eps_quad
108	該当なし	該当なし	umts_key_quad_quin
109	該当なし	該当なし	pdn_connection
110	該当なし	該当なし	pdn_number
111	該当なし	該当なし	p_tmsi
112	該当なし	該当なし	p_tmsi_sig
113	該当なし	該当なし	hop_counter
114	該当なし	該当なし	ue_time_zone
115	該当なし	該当なし	trace_ref
116	該当なし	該当なし	complete_request_msg
117	該当なし	該当なし	guti
118	該当なし	該当なし	f_container
119	該当なし	該当なし	f_cause
120	該当なし	該当なし	plmn_id
121	該当なし	該当なし	target_id
123	該当なし	該当なし	packet_flow_id



値	Version 0	Version 1	Version 2
124	該当なし	該当なし	rab_context
125	該当なし	該当なし	src_rnc_pdcp
126	該当なし	該当なし	udp_src_port
127	charge_id	charge_id	apn_restriction
128	end_user_address	end_user_address	selection_mode
129	mm_context	mm_context	src_id
130	pdp_context	pdp_context	該当なし
131	apn	apn	change_report_action
132	protocol_config	protocol_config	fq_csid
133	gsn	gsn	channel
134	msisdn	msisdn	emlpp_pri
135	該当なし	qos	node_type
136	該当なし	authentication_qu	fqdn
137	該当なし	tft	ti
138	該当なし	target_id	mbms_session_duration
139	該当なし	utran_trans	mbms_service_area
140	該当なし	rab_setup	mbms_session_id
141	該当なし	ext_header	mbms_flow_id
142	該当なし	trigger_id	mbms_ip_multicast
143	該当なし	omc_id	mbms_distribution_ack
144	該当なし	ran_trans	rfsp_index
145	該当なし	pdp_context_pri	uci
146	該当なし	addi_rab_setup	csg_info
147	該当なし	sgsn_number	csg_id
148	該当なし	common_flag	cmi
149	該当なし	apn_restriction	service_indicator

値	Version 0	Version 1	Version 2
150	該当なし	radio_priority_lcs	detach_type
151	該当なし	rat_type	ldn
152	該当なし	user_loc_info	node_feature
153	該当なし	ms_time_zone	mbms_time_to_transfer
154	該当なし	imei_sv	throttling
155	該当なし	camel	arp
156	該当なし	mbms_ue_context	epc_timer
157	該当なし	tmp_mobile_group_id	signalling_priority_indication
158	該当なし	rim_routing_addr	tmgi
159	該当なし	mbms_config	mm_srvc
160	該当なし	mbms_service_area	flags_srvc
161	該当なし	src_rnc_pdc	nmb
162	該当なし	addi_trace_info	該当なし
163	該当なし	hop_counter	該当なし
164	該当なし	plmn_id	該当なし
165	該当なし	mbms_session_id	該当なし
166	該当なし	mbms_2g3g_indicator	該当なし
167	該当なし	enhanced_nsapi	該当なし
168	該当なし	mbms_session_duration	該当なし
169	該当なし	addi_mbms_trace_info	該当なし
170	該当なし	mbms_session_repetition_num	該当なし
171	該当なし	mbms_time_to_data	該当なし
173	該当なし	bss	該当なし
174	該当なし	cell_id	該当なし
175	該当なし	pdu_num	該当なし
177	該当なし	mbms_bearer_capab	該当なし

値	Version 0	Version 1	Version 2
178	該当なし	rim_routing_disc	該当なし
179	該当なし	list_pfc	該当なし
180	該当なし	ps_xid	該当なし
181	該当なし	ms_info_change_report	該当なし
182	該当なし	direct_tunnel_flags	該当なし
183	該当なし	correlation_id	該当なし
184	該当なし	bearer_control_mode	該当なし
185	該当なし	mbms_flow_id	該当なし
186	該当なし	mbms_ip_multicast	該当なし
187	該当なし	mbms_distribution_ack	該当なし
188	該当なし	reliable_inter_rat_handover	該当なし
189	該当なし	rfsp_index	該当なし
190	該当なし	fqdn	該当なし
191	該当なし	evolved_allocation1	該当なし
192	該当なし	evolved_allocation2	該当なし
193	該当なし	extended_flags	該当なし
194	該当なし	uci	該当なし
195	該当なし	csg_info	該当なし
196	該当なし	csg_id	該当なし
197	該当なし	cmi	該当なし
198	該当なし	apn_ambr	該当なし
199	該当なし	ue_network	該当なし
200	該当なし	ue_ambr	該当なし
201	該当なし	apn_ambr_nsapi	該当なし
202	該当なし	ggsn_backoff_timer	該当なし
203	該当なし	signalling_priority_indication	該当なし

値	Version 0	Version 1	Version 2
204	該当なし	signalling_priority_indication_nsapi	該当なし
205	該当なし	high_bitrate	該当なし
206	該当なし	max_mbr	該当なし
251	charging_gateway_addr	charging_gateway_addr	該当なし
255	private_extension	private_extension	private_extension

## SCADA キーワード

ルール エンジン は Modbus および DNP3 ルールを使用して特定のプロトコル フィールドにアクセスします。

## Modbus キーワード

Modbus キーワードを単独で使用することも、`content` や `byte_jump` など他のキーワードと組み合わせで使用することもできます。

### modbus\_data

`modbus_data` キーワードを使用すると、Modbus 要求または応答内の [Data] フィールドの先頭を指し示すことができます。

### modbus\_func

`modbus_func` キーワードを使用すると、Modbus アプリケーション層要求または応答見出し内の [Function Code (機能コード)] フィールドを照合できます。Modbus 機能コードとして、1つの定義済み 10 進数値または 1つの定義済み文字列を指定できます。

次の表に、Modbus 機能コードとしてシステムで認識される定義済みの値と文字列を示します。

表 171: Modbus 機能コード

値	文字列
1	read_coils
2	read_discrete_inputs
3	read_holding_registers
4	read_input_registers
5	write_single_coil
[6]	write_single_register

値	文字列
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
17	report_slave_id
20	read_file_record
21	write_file_record
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue
43	encapsulated_interface_transport

### modbus\_unit

modbus\_unit キーワードを使用すると、Modbus 要求または応答ヘッダー内の [Unit ID] フィールドで 1 つの 10 進数値を照合できます。

## DNP3 キーワード

DNP3 キーワードを単独で使用することも、content や byte\_jump など他のキーワードと組み合わせ使用することもできます。

### dnp3\_data

dnp3\_data キーワードを使用すると、再構築された DNP3 アプリケーション層フラグメントの先頭を指し示すことができます。

DNP3 プリプロセッサは、リンク層フレームをアプリケーション層フラグメントに再構築します。dnp3\_data キーワードは、各アプリケーション層フラグメントの先頭を指し示します。他のルールオプションは、16 バイトごとにデータを分離してチェックサムを追加せずに、フラグメント内の再構築されたデータを照合することができます。

### dnp3\_func

dnp3\_func キーワードを使用すると、DNP3 アプリケーション層要求または応答ヘッダー内の [機能コード (Function Code)] フィールドを照合できます。DNP3 機能コードとして、1 つの定義済み 10 進数値または 1 つの定義済み文字列を指定できます。

次の表に、DNP3 機能コードとしてシステムで認識される定義済みの値と文字列を示します。

表 172: DNP3 機能コード

値	文字列
[0]	confirm
1	read
2	write
3	選択
4	operate
5	direct_operate
[6]	direct_operate_nr
7	immed_freeze
8	immed_freeze_nr
9	freeze_clear
10	freeze_clear_nr
11	freeze_at_time
12	freeze_at_time_nr
13	cold_restart
18	warm_restart
15	initialize_data
16	initialize_appl
17	start_appl
18	stop_appl
19	save_config
20	enable_unsolicited
21	disable_unsolicited
22	assign_class
23	delay_measure
24	record_current_time

値	文字列
25	open_file
26	close_file
27	delete_file
36	get_file_info
29	authenticate_file
30	abort_file
31	activate_config
32	authenticate_req
33	authenticate_err
129	response
130	unsolicited_response
131	authenticate_resp

### dnp3\_ind

dnp3\_ind キーワードを使用すると、DNP3 アプリケーション層応答ヘッダー内の [Internal Indications] フィールド内のフラグを照合できます。

1つの既知のフラグ、または次の例のようなカンマ区切りのフラグリストを示す文字列を指定できます。

```
class_1_events, class_2_events
```

複数のフラグを指定した場合、キーワードはリスト内の任意のフラグと一致します。いくつかのフラグの組み合わせを検出するには、1つのルール内でdnp3\_ind キーワードを複数回使用します。

定義済みのDNP3 内部通知フラグとしてシステムによって認識される文字列構文を以下に示します。

```
class_1_events
class_2_events
class_3_events
need_time
local_control
device_trouble
device_restart
no_func_code_support
object_unknown
parameter_error
event_buffer_overflow
already_executing
config_corrupt
```

```
reserved_2
reserved_1
```

### dnp3\_obj

dnp3\_obj キーワードを使用すると、要求または応答内の DNP3 オブジェクト ヘッダーを照合できます。

DNP3 データは、アナログ入力やバイナリ入力など、さまざまなタイプの一連の DNP3 オブジェクトで構成されます。各タイプは、それぞれ 10 進数値で識別されるグループを使って区別されます（アナログ入力グループ、バイナリ入力グループなど）。各グループ内のオブジェクトは、それぞれオブジェクトデータ形式を指定するオブジェクトバリエーションによってさらに区別されます（16 ビット整数、32 ビット整数、短精度浮動小数点など）。また、オブジェクトバリエーションの各タイプは 10 進数値でも識別可能です。

オブジェクトヘッダーを識別する際には、オブジェクトヘッダーグループのタイプを示す 10 進数値とオブジェクトバリエーションのタイプを示す 10 進数値を指定します。この 2 つの組み合わせによって DNP3 オブジェクトの特定のタイプが定義されます。

## パケット特性

特定のパケット特性を持つパケットに対してのみイベントを生成するルールを作成できます。

### dsize

dsize キーワードはパケットペイロードサイズを検査します。「大なり」演算子と「小なり」演算子 (<, >) を使って値の範囲を指定することができます。次の構文をに従って範囲を指定できます。

```
>number_of_bytes
<number_of_bytes
number_of_bytes<>number_of_bytes
```

たとえば、400 バイトを超えるパケットサイズを指定するには、dtype 値として >400 を使用します。500 バイト未満のパケットサイズを指定するには、<500 を使用します。400 ~ 500 バイトのパケットに対してルールをトリガーとして使用するよう指定するには、400<>500 を使用します。



#### 注意

dsize キーワードは、プリプロセッサによってデコードされる前のパケットを検査します。

### isdataat

isdataat キーワードは、ペイロード内の特定の位置にデータが存在することを確認するよう、ルールエンジンに指示します。

次の表に、isdataat キーワードで使用可能な引数を列挙します。



表 173: isdataat の引数

引数	タイプ (Type)	説明
Offset	必須 (Required)	ペイロード内の特定の位置。たとえば、パケット ペイロード内のバイト位置 50 にデータが出現することを検査するには、オフセット値として 50 を指定します。! 修飾子は isdataat 検査の結果を否定します。特定量のデータがペイロードに存在しない場合は警告が出されます。  また、既存の byte_extract 変数または byte_math 結果を使用してこの引数の値を指定することもできます。
Relative	オプション	最後に見つかったコンテンツ一致を基準にして相対的な位置を計算します。相対位置を指定する場合は、カウンタがバイト 0 から始まることに注意してください。最後に見つかったコンテンツ一致から順方向に移動するバイト数から 1 を差し引いて位置を計算します。たとえば、最後に見つかったコンテンツ一致から 9 バイト後にデータが出現すべきことを指定するには、相対オフセットとして 8 を指定します。
Raw Data	オプション	Firepower システムプリプロセッサによるデコードやアプリケーション層の正規化が行われる前の、元のパケット ペイロードにデータが配置されていることを指定します。前のコンテンツ一致が未加工パケット データ内に存在していた場合は、この引数を <b>Relative</b> と一緒に使用できます。

たとえば、foo というコンテンツを検索するルールで isdataat の値が次のように指定される場合、

- Offset = !10
- Relative = enabled

ルール エンジンが foo の後ろからペイロード末尾までに 10 バイトを検出しない場合、システムは警告を出します。

### sameip

sameip キーワードは、パケットの送信元 IP アドレスと宛先 IP アドレスが同じであることを検査します。このキーワードは引数を受け入れません。

### fragoffset

fragoffset キーワードは、フラグメント化されたパケットのオフセットを検査します。一部の exploit (WinNuke サービス拒否攻撃など) では、特定のオフセットを持つ手動生成されたパケット フラグメントが使われるため、このキーワードが役立ちます。

たとえば、フラグメント化されたパケットのオフセットが 31337 バイトかどうかを検査するには、fragoffset 値として 31337 を指定します。

fragoffset キーワードの引数を指定するときには、次の演算子を使用できます。

表 174: *fragoffset* キーワードの引数演算子

演算子	説明
!	ノット
>	より大きい
<	より少ない

否定 (!) 演算子を < や > と組み合わせて使用できないことに注意してください。

### CVS

`cvs` キーワードは、**Concurrent Versions System (CVS)** トラフィック内で不正な形式の CVS エントリを検査します。攻撃者は不正な形式のエントリを使用して、ヒープオーバーフローを強制的に発生させ、CVS サーバ上で有害コードを実行することができます。このキーワードを使用すると、2つの既知の CVS 脆弱性 CVE-2004-0396 (CVS 1.11.x ~ 1.11.15 と 1.12.x ~ 1.12.7) および CVE-2004-0414 (CVS 1.12.x ~ 1.12.8 と 1.11.x ~ 1.11.16) に対する攻撃を識別できます。`cvs` キーワードは、正しい形式のエントリであることを検査して、不正な形式のエントリが検出された場合はアラートを生成します。

CVS が動作するポートをルールに含める必要があります。さらに、トラフィックが発生する可能性のあるポートを TCP ポリシー内のストリーム再構築用のポートリストに追加することで、CVS セッションの状態を保持できるようにする必要があります。ストリーム再構築が行われるクライアントポートのリストには、TCP ポート 2401 (`pserver`) と 514 (`rsh`) が含まれています。ただし、サーバが `xinetd` サーバ (つまり `pserver`) として動作する場合は、任意の TCP ポート上で動作することに注意してください。すべての非標準ポートを、ストリーム再構築の [クライアントポート (Client Ports)] リストに追加します。

### 関連トピック

[byte\\_extract キーワード \(1733 ページ\)](#)

[TCP ストリームのプリプロセス オプション \(1974 ページ\)](#)

## アクティブ応答のキーワード

システムは、トリガーとして使用された TCP ルールに反応して TCP 接続を閉じるために、またはトリガーとして使用された UDP ルールに反応して UDP セッションを閉じるために、アクティブ応答を開始できます。2つのキーワードにより、別々の方法でアクティブ応答を開始できます。どちらかのキーワードを含むルールをパケットがトリガーとして使用すると、システムは1つのアクティブ応答を開始します。`config response` コマンドを使用して、アクティブ応答インターフェイスおよびパッシブ展開で試行する TCP リセットの回数を設定することもできます。

リセットは接続やセッションに影響を与えるのに間に合うまでに到着する可能性が高いため、アクティブ応答はインライン展開で最も効果を発揮します。たとえば、インライン展開での `react` キーワードに反応して、システムは接続の両端用のトラフィックに TCP リセット (RST) パケットを直接挿入し、通常はこれによって接続が閉じます。

(パッシブ展開ではシステムがパケットを挿入できない、攻撃者がアクティブ応答を無視または回避するよう選択する可能性があるなど) さまざまな理由で、アクティブ応答はファイアウォールの代わりとして想定されていません。

アクティブ応答は戻って来ることがあるため、システムは TCP リセットによる TCP リセットの開始を許可しません。これにより、アクティブ応答が無限に続くことを防止できます。また、システムは、標準的な慣行に従って ICMP 到達不能パケットによる ICMP 到達不能パケットの開始を許可しません。

侵入ルールがアクティブ応答をトリガーとして使用した後、接続またはセッションで追加のトラフィックを検出するよう、TCP ストリーム プリプロセッサを設定できます。追加のトラフィックが検出されると、プリプロセッサは、指定された最大値まで、追加のアクティブ応答を接続またはセッションの両端に送信します。

**関連トピック**

[侵入廃棄ルールでのアクティブ応答 \(1946 ページ\)](#)

**resp キーワード**

resp キーワードを使用すると、ルールヘッダーで TCP プロトコルと UDP プロトコルのどちらが指定されているかに基づいて、TCP 接続または UDP セッションにアクティブに (能動的に) 応答できます。

キーワード引数を使用すると、パケットの方向、および TCP リセット (RST) パケットと ICMP 到達不能パケットのどちらをアクティブ応答として使用するかを指定できます。

任意の TCP リセット引数または ICMP 到達不能引数を使用して、TCP 接続を閉じることができます。UDP セッションを閉じるには、ICMP 到達不能引数だけを使用する必要があります。

また、さまざまな TCP リセット引数を使用することで、パケットの送信元、宛先、またはその両方にアクティブ応答を送ることができます。すべての ICMP 到達不能引数はパケット送信元に送られます。ICMP ネットワーク、ホスト、またはポートのどの到達不能パケットを使用するか (または 3 つすべてを使用するか) を指定できます。

ルールがトリガーとして使用されたときに Firepower システムで実行されるアクションを正確に指定するために、resp キーワードで使用できる引数を次の表に列挙します。

表 175: resp 引数

引数	説明
reset_source	ルールをトリガーとして使用したパケットを送信元エンドポイントに TCP リセットパケットを送ります。この代わりに、下位互換性のためにサポートされている rst_snd を指定することもできます。
reset_dest	ルールをトリガーとして使用したパケットの宛先であるエンドポイントに TCP リセットパケットを送ります。この代わりに、下位互換性のためにサポートされている rst_rcv を指定することもできます。
reset_both	送信側エンドポイントと受信側エンドポイントの両方に TCP リセットパケットを送ります。この代わりに、下位互換性のためにサポートされている rst_all を指定することもできます。

引数	説明
icmp_net	送信側に ICMP ネットワーク到達不能メッセージを送ります。
icmp_host	送信側に ICMP ホスト到達不能メッセージを送ります。
icmp_port	送信側に ICMP ポート到達不能メッセージを送ります。この引数は、UDP トラフィックを終了するために使われます。
icmp_all	送信側に次の ICMP メッセージを転送します。 <ul style="list-style-type: none"> <li>• ネットワーク到達不能</li> <li>• ホスト到達不能</li> <li>• ポート到達不能</li> </ul>

たとえば、ルールがトリガーとして使用されたときに接続の両側をリセットするようルールを設定するには、`resp` キーワードの値として `reset_both` を使用します。

次のように、カンマ区切りのリストを使用して複数の引数を指定できます。

```
argument,argument,argument
```

`config response` コマンドを使用すると、使用するアクティブ応答インターフェイス、およびパッシブ展開で試行する TCP リセットの回数を設定することができます。

#### 関連トピック

[config response コマンド](#) (1799 ページ)

## react キーワード

`react` キーワードを使用すると、パケットがルールをトリガーとして使用した時点でデフォルト HTML ページを TCP 接続クライアントに送信できます。HTML ページの送信後に、システムは TCP リセットパケットを使って接続の両端へのアクティブ応答を開始します。`react` キーワードは UDP トラフィックのアクティブ応答をトリガーとして使用しません。

オプションで、次の引数を指定できます。

```
msg
```

`msg` 引数を使用する `react` ルールがパケットによってトリガーとして使用されると、HTML ページにルール イベント メッセージが表示されます。

`msg` 引数を指定しない場合、HTML ページには次のメッセージが含まれます。

```
You are attempting to access a forbidden site.
Consult your system administrator for details.
```



- (注) アクティブ応答は戻されることがあるため、HTML 応答ページによって react ルールがトリガーとして使用されないようにしてください（結果としてアクティブ応答が無限に続く可能性があります）。Cisco では、react ルールを十分にテストしてから実稼動環境でアクティブにするよう推奨しています。

config response コマンドを使用すると、使用するアクティブ応答インターフェイス、およびパッシブ展開で試行する TCP リセットの回数を設定することができます。

#### 関連トピック

[ルールの詳細](#) (1686 ページ)

[config response コマンド](#) (1799 ページ)

## config response コマンド

**config response** コマンドを使用すると、resp ルールと react ルールによって開始される TCP リセットの動作を詳細に設定できます。また、このコマンドは、廃棄ルールによって開始されるアクティブ応答の動作にも影響を与えます。

**config response** コマンドを使用するには、高度な USER\_CONF 変数内の別個の 1 行にこれを挿入します。

次のように、USER\_CONF 拡張変数の別の行に config response コマンドの形式を挿入します。

- アクティブ応答の試行回数のみを指定するには、次のコマンドを挿入します。

```
config response: attempts att
```

例 : config response: attempts 10

- アクティブ応答インターフェイスのみを指定するには、次のコマンドを挿入します。

```
config response: device dev
```

例 : config response: device eth0

- アクティブ応答の試行回数とアクティブ応答インターフェイスの両方を指定するには、次のコマンドを挿入します。

```
config response: attempts att, device dev
```

#### 引数の説明

- **att** は、受信側ホストにパケットを受け入れさせるために、現在の接続枠で各 TCP リセットパケットを挿入する試行回数 (1~20) です。この連続試行はパッシブ展開でのみ効果があります。インライン展開の場合、システムはトリガーパケットの代わりにリセットパケットをストリームに直接挿入します。ICMP 到着可能な 1 つのアクティブ応答のみが送信されます。
- **dev** は、パッシブ展開でシステムからアクティブ応答を送信したり、インライン展開でアクティブ応答を挿入したりするための代替インターフェイスです。

例 : config response: attempts 10, device eth0



**注意** 機能の説明またはサポート担当の指示に従う場合を除き、侵入ポリシー機能を設定するために高度な `USER_CONF` 変数を使用しないでください。競合または重複する設定が存在すると、システムが停止します。

### 関連トピック

[侵入廃棄ルールでのアクティブ応答](#) (1946 ページ)

[拡張変数](#) (453 ページ)

## detection\_filter キーワード

`detection_filter` キーワードを使用すると、指定された時間内に指定された数のパケットがルールをトリガーとして使用しない限り、ルールでイベントが生成されないようにすることができます。これにより、早すぎるタイミングでルールがイベントを生成することを回避できます。たとえば、数秒間にログイン試行が2～3回失敗することは想定範囲内ですが、同じ時間内に多数の試行が発生した場合はブルートフォースアタックを示唆している可能性があります。

`detection_filter` キーワードの必須の引数は、送信元/宛先のどちらの IP アドレスをシステムで追跡するか、イベントをトリガーする前に検出基準が満たされるべき回数、およびカウントの継続時間を定義します。

イベントのトリガーを遅らせるには、次の構文を使用します。

```
track by_src/by_dst, count count, seconds number_of_seconds
```

`track` 引数は、ルールの検出基準を満たすパケット数をカウントするときに、パケットの送信元 IP アドレスと宛先 IP アドレスのどちらを使用するかを指定します。システムでイベントインスタンスを追跡する方法を指定するには、次の表の中から引数値を選択します。

表 176: `detection_filter` の追跡引数

引数	説明
<code>by_src</code>	送信元 IP アドレスによる検出基準カウント。
<code>by_dst</code>	宛先 IP アドレスによる検出基準カウント。

`count` 引数は、ルールでイベントを生成する前に、指定された時間内に指定された IP アドレスのルールをトリガーすべきパケットの数を指定します。

`seconds` 引数は、ルールでイベントを生成する前に、指定された数のパケットがルールをトリガーすべき時間枠を秒数で指定します。

パケット内でコンテンツ `foo` を検索するルールが、次の引数を含む `detection_filter` キーワードを使用するとします。

```
track by_src, count 10, seconds 20
```

この例のルールは、特定の送信元 IP アドレスから 20 秒以内に 10 個のパケットで `foo` を検出するまでは、イベントを生成しません。システムが最初の 20 秒以内に `foo` を含むパケットを 7 つしか検出しなかった場合は、イベントが生成されません。しかし、最初の 20 秒間で `foo` が 40 回出現した場合は、ルールで 30 個のイベントが生成され、20 秒が経過するとカウントが再開されます。

### しきい値と `detection_filter` キーワードの比較

`detection_filter` キーワードは、非推奨の `threshold` キーワードに代わるものです。 `threshold` キーワードは、下位互換性を維持するために引き続きサポートされていますが、侵入ポリシー内で設定されるしきい値と同じ機能です。

`detection_filter` キーワードは、パケットがルールをトリガーとして使用する前に適用される検出機能です。ルールは、指定されたパケットカウントの前に検出されたトリガーパケットに関してイベントを生成しません。また、インライン展開では、パケットを破棄するようルールで設定されていても、そのようなパケットを破棄しません。逆に、指定されたパケットカウントの後に出現する、ルールをトリガーとして使用するパケットに関してルールはイベントを生成します。また、インライン展開でパケットを破棄するよう設定されている場合は、そのようなパケットを破棄します。

しきい値は、検出アクションを発生させないイベント通知機能です。これは、パケットがイベントをトリガーとして使用した後に適用されます。インライン展開において、パケットを破棄するよう設定されたルールは、ルールしきい値とは無関係に、ルールをトリガーとして使用するすべてのパケットを破棄します。

侵入ポリシー内で `detection_filter` キーワードを侵入イベントしきい値、侵入イベント抑制、および `Rate-Based` 攻撃防御機能と任意に組み合わせて使用することに注意してください。また、侵入ポリシー内の侵入イベントしきい値機能と組み合わせて非推奨の `threshold` キーワードを使用するインポートされたローカルルールを有効にした場合、ポリシー検証が失敗することに注意してください。

### 関連トピック

[侵入イベントのしきい値](#) (1641 ページ)

[侵入ポリシーの抑制の設定](#) (1646 ページ)

[\[ルール \(Rule\)\] ページからの動的ルール状態の設定](#) (1651 ページ)

[ローカル侵入ルールファイルインポート](#) (184 ページ)

## tag キーワード

ホストまたはセッションに関する追加のトラフィックをログに記録するようシステムに指示するには、`tag` キーワードを使用します。`tag` キーワードを使って検出するトラフィックのタイプと量を指定するときには、次の構文を使用します。

```
tagging_type, count, metric, optional_direction
```

次の 3 つの表に、その他の使用可能な引数について説明します。

2つのタイプのタグ機能から選択できます。次の表に、これらのタグ機能の説明を示します。侵入ルールでルールヘッダーオプションのみを設定した場合、`session` タグ引数タイプによって、同じセッションからのパケットが別のセッションからのパケットのように記録されることに注意してください。同じセッションからのパケットをまとめてグループ化するには、同じ侵入ルール内で1つ以上のルールオプション（`flag` キーワードや `content` キーワードなど）を設定します。

表 177: tag の引数

引数	説明
session	ルールをトリガーとして使用したセッション内のパケットをログに記録します。
ホスト	ルールをトリガーとして使用したパケットを送信したホストからのパケットをログに記録します。ホストからのトラフィックのみ（ <code>src</code> ）、またはホストへのトラフィックのみ（ <code>dst</code> ）を記録する方向修飾子を追加できます。

ログに記録するトラフィック量を指定するには、次の引数を使用します。

表 178: カウント引数

引数	説明
count	ルールがトリガーとして使用された後にログに記録するパケット数または秒数。 この単位を指定するには、 <code>count</code> 引数の後に測定基準引数を使用します。

次の表の中から、トラフィックの時間または量ごとにログで使用する測定基準を選択してください。



**注意** 高帯域ネットワークでは、1秒あたり数千パケットが発生する可能性があり、多数のパケットにタグを付けるとパフォーマンスに重大な影響が及ぶ可能性があるため、必ずネットワーク環境に合わせてこの設定を調整してください。

表 179: ログの測定基準引数

引数	説明
packets	ルールのトリガー後に、カウントで指定されるパケット数をログに記録します。
秒	ルールのトリガー後に、カウントで指定される秒数の間、トラフィックを記録します。



たとえば、次の tag キーワード値を使用するルールがトリガーとして使用された場合、

```
host, 30, seconds, dst
```

次の30秒間にクライアントからホストに送信されるすべてのパケットがログに記録されます。

## flowbits キーワード

状態名をセッションに割り当てるには、flowbits キーワードを使用します。すでに名前が付けられた状態に基づいてセッション内の後続パケットを分析することにより、システムは単一セッション内で複数のパケットに及ぶエクスプロイトを検出して警告を出すことができます。

flowbits 状態名は、セッションの特定部分でパケットに割り当てられるユーザ定義のラベルです。パケットの内容に基づいてパケットに状態名を付けると、警告の必要のないパケットと有害なパケットを区別しやすくなります。管理対象デバイスごとに最大 1024 個の状態名を定義できます。たとえば、ログイン成功後にのみ発生することがわかっている有害パケットについて警告するには、flowbits キーワードを使用して、初期ログイン試行を構成するパケットを除去することにより、有害パケットに焦点を絞ることができます。このような機能を実装するには、まず、セッション内のすべてのログイン確立済みパケットに logged\_in 状態のラベルを付けるルールを作成した後、2 番目のルールを作成し、最初のルールで設定された状態を持つパケットを検査してそのようなパケットだけを処理する flowbits をそのルールに含めます。

オプションの *group name* を使用すると、状態のグループに状態名を含めることができます。1 つの状態名は複数のグループに属することができます。グループに関連付けられていない状態は相互排他的ではないため、トリガーとして使用されたルールがグループに関連付けられていない状態を設定した場合、現在設定されている他の状態には影響がありません。

## flowbits キーワードのオプション

次の表に、flowbits キーワードで使用できる演算子、状態、およびグループのさまざまな組み合わせについて説明します。なお、状態名には、英数字、ピリオド (.)、アンダースコア (\_)、およびダッシュ (-) を含めることができます。

表 180: flowbits のオプション

演算子	状態オプション	グループ	説明
set	state_name	オプション	パケットに関する指定された状態を設定します。グループが定義されている場合は、指定されたグループ内で状態を設定します。
set	state_name&state_name	オプション	パケットに関する指定された状態を設定します。グループが定義されている場合は、指定されたグループ内で状態を設定します。
setx	state_name	入力必須	指定されたグループ内でパケットに関して指定された状態を設定し、グループ内の他のすべての状態を解除します。

## flowbits キーワードのオプション

演算子	状態オプション	グループ	説明
setx	state_name&state_name	入力必須	指定されたグループ内でパケットに関して指定された状態を設定し、グループ内の他のすべての状態を解除します。
unset	state_name	グループなし	パケットに関する指定された状態を解除します。
unset	state_name&state_name	グループなし	パケットに関する指定された状態を解除します。
unset	all	入力必須	指定されたグループ内のすべての状態を解除します。
toggle	state_name	グループなし	指定された状態が設定されている場合はそれを解除し、指定された状態が解除されている場合にはそれを設定します。
toggle	state_name&state_name	グループなし	指定された複数の状態が設定されている場合はそれらを解除し、指定された複数の状態が解除されている場合はそれらを設定します。
toggle	all	入力必須	指定されたグループ内で設定されているすべての状態を解除し、指定されたグループ内で解除されているすべての状態を設定します。
isset	state_name	グループなし	指定された状態がパケット内で設定されているかどうかを判別します。
isset	state_name&state_name	グループなし	指定された複数の状態がパケット内で設定されているかどうかを判別します。
isset	state_name state_name	グループなし	指定されたいずれかの状態がパケット内で設定されているかどうかを判別します。
isset	any	入力必須	指定されたグループ内で、いずれかの状態が設定されているかどうかを判別します。
isset	all	入力必須	指定されたグループ内で、すべての状態が設定されているかどうかを判別します。
isnotset	state_name	グループなし	指定された状態がパケット内で設定されていないかどうかを判別します。
isnotset	state_name&state_name	グループなし	指定された複数の状態がパケット内で設定されていないかどうかを判別します。
isnotset	state_name state_name	グループなし	指定されたいずれかの状態が、パケット内で設定されていないかどうかを判別します。

演算子	状態オプション	グループ	説明
isnotset	any	入力必須	パケット内でいずれかの状態が設定されていないかどうかを判別します。
isnotset	all	入力必須	パケット内ですべての状態が設定されていないかどうかを判別します。
reset	(状態なし)	オプション	すべてのパケットのすべての状態を解除します。グループが指定されている場合、グループ内のすべての状態を解除します。
noalert	(状態なし)	グループなし	イベント生成を抑制するには、これを他の演算子と組み合わせて使用します。

## flowbits キーワードの使用に関するガイドライン

flowbits キーワードを使用するときには、次の点に注意してください。

- setx 演算子を使用する場合、指定した状態は、指定したグループ以外のグループに属することができません。
- setx 演算子を複数回定義して、それぞれのインスタンスで別々の状態と同じグループを指定できます。
- setx 演算子を使用してグループを指定する場合、そのグループに対して set、toggle、unset 演算子を使用することはできません。
- isset 演算子と isnotset 演算子は、指定された状態がグループに含まれるかどうかに関係なく、その状態を評価します。
- 侵入ポリシーの保存時、侵入ポリシーの再適用時、および（アクセス コントロール ポリシーで参照される侵入ポリシー数に関係なく）アクセス コントロール ポリシーの適用時には、グループ指定のない isset または isnotset 演算子を含むルールを有効にした場合、対応する状態名とプロトコルに関する flowbits 割り当て（set、setx、unset、toggle）に影響する 1 つ以上のルールを有効にしないと、対応する状態名の flowbits 割り当てに影響するすべてのルールが有効になります。
- 侵入ポリシーの保存時、侵入ポリシーの再適用時、および（アクセス コントロール ポリシーで参照される侵入ポリシー数に関係なく）アクセス コントロール ポリシーの適用時には、グループを指定した isset 演算子または isnotset 演算子を含むルールを有効にした場合、flowbits 割り当て（set、setx、unset、toggle）に影響し、対応するグループ名を定義するすべてのルールもまた有効になります。

## flowbits キーワードの例

この項では、flowbits キーワードを使用する 3 つの例を示します。

## flowbits キーワードの例 : state\_name を使用した設定

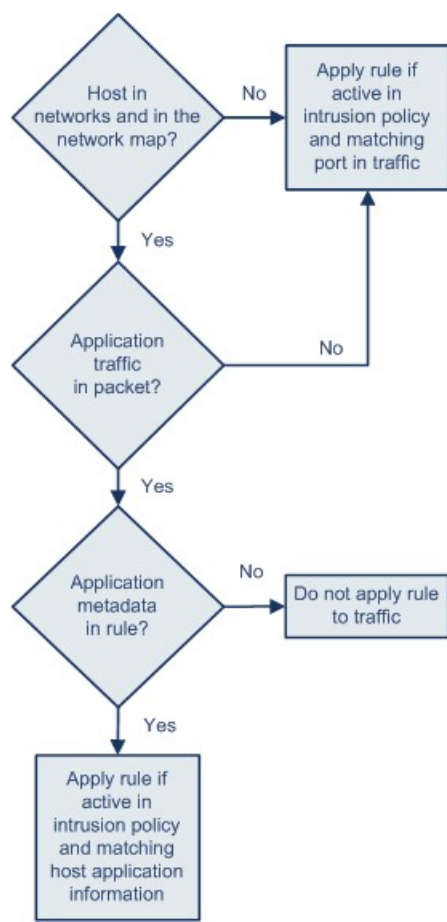
これは、state\_name を使用した flowbits 設定の例です。

Bugtraq ID #1110 に記述されている IMAP 脆弱性について考えてみます。この脆弱性は、IMAP の実装（具体的には LIST、LSUB、RENAME、FIND、および COPY コマンド）で見られます。ただし、攻撃者がこの脆弱性を悪用するには、IMAP サーバにログインする必要があります。IMAP サーバからの LOGIN 確認とそれに続く exploit は必然的に別々のパケットに存在するため、この exploit を検出する非フローベースのルールを作成するのは困難です。flowbits キーワードを使って一連のルールを作成すると、ユーザが IMAP サーバにログイン済みかどうかを追跡し、ログイン済みの場合は、いずれかの攻撃が検出された時点でイベントを生成することができます。ユーザがログイン済みでない場合、攻撃によって脆弱性が悪用されることはないため、イベントが生成されません。

下記の 2 つのルール フラグメントはこの例を示しています。最初のルール フラグメントは IMAP サーバからの IMAP ログイン確認を検索します。

```
alert tcp any 143 -> any any (msg:"IMAP login"; content:"OK
LOGIN"; flowbits:set,logged_in; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。



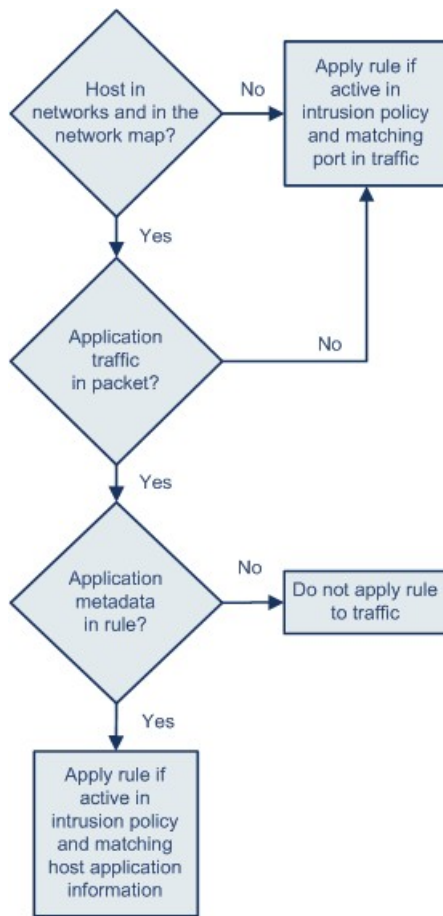
371893

flowbits:set は logged\_in 状態を設定しますが、flowbits:noalert がアラートを抑制することに注意してください。これは、IMAPサーバ上で多数の無害なログインセッションが見つかる可能性があるためです。

次のルールフラグメントは LIST 文字列を検索しますが、セッション内の先行パケットの結果として logged\_in 状態が設定済みでない限り、イベントを生成しません。

```
alert tcp any any -> any 143 (msg:"IMAP LIST";
content:"LIST"; flowbits:isset,logged_in;)
```

次の図は、上記のルールフラグメントにおける flowbits キーワードの効果を示しています。



この場合、最初のフラグメントを含むルールが先行パケットによってトリガーとして使用した場合、2 番目のフラグメントを含むルールがトリガーとして使用し、イベントを生成します。

**flowbits キーワードの例：誤検出イベントを引き起こす設定**

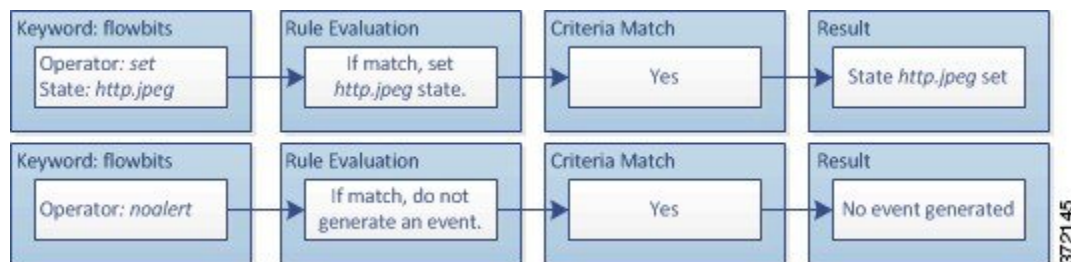
後続パケット内コンテンツが、効力を失った状態を持つルールに一致することによって誤検出イベントが発生する可能性があります。複数のルールで設定された複数の状態名をグループに含めることでこれを回避できます。次の例は、複数の状態名をグループに含めない場合に誤検出が発生する可能性があることを示しています。

flowbits キーワードの例：誤検出イベントを引き起こす設定

1つのセッションで次の3つのルールフラグメントがこの順序でトリガーとして使用される場合を考えてみます。

```
(msg:"JPEG transfer";
content:"image/";pcre:"/^Content-Type\x3a(\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:set,http.jpeg; flowbits:noalert;)
```

次の図は、上記のルールフラグメントにおける flowbits キーワードの効果を示しています。

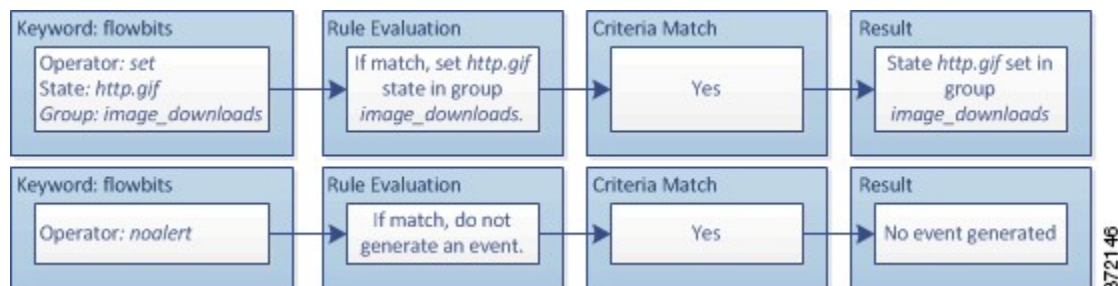


最初のルールフラグメント内の content キーワードと pcre キーワードが JPEG ファイルダウンロードに一致し、flowbits:set,http.jpeg が http.jpeg flowbits ステートを設定し、flowbits:noalert はルールでのイベント生成を抑制します。イベントが生成されない理由は、このルールの目的がファイルダウンロードを検出して flowbits 状態を設定することだからです。これにより、1つ以上のコンパニオンルールで状態名を検査して有害コンテンツを探し、有害コンテンツが検出された時点でイベントを生成できます。

次のルールフラグメントは、上記の JPEG ファイルダウンロードに続く GIF ファイルダウンロードを検出します。

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-Type\x3a(\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:set,http.jpg,image_downloads; flowbits:noalert;)
```

次の図は、上記のルールフラグメントにおける flowbits キーワードの効果を示しています。

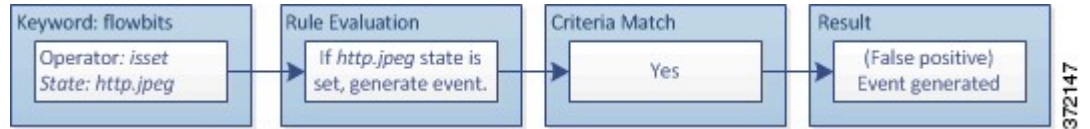


2番目のルール内の content キーワードと pcre キーワードは GIF ファイルダウンロードを照合し、flowbits:set,http.jpg は http.jpg flowbit ステートを設定し、flowbits:noalert はルールでのイベント生成を抑制します。最初のルールフラグメントで設定された http.jpeg 状態が不要になっても引き続き設定されていることに注意してください。これは、後続の GIF ダウンロードが検出されたときに JPEG ダウンロードが既に終了しているはずであるためです。

次に示す 3番目のルールフラグメントは最初のルールフラグメントのコンパニオンです。

```
(msg:"JPEG exploit";?flowbits:isset,http.jpeg;content:"|FF|";
pcr:"?\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/");
```

次の図は、上記のルールフラグメントにおける flowbits キーワードの効果を示しています。



3 番目のルールフラグメントでは、もはや無意味になった http.jpeg ステートが設定されていることを flowbits:isset,http.jpeg が判別し、content と pcre は (GIF ファイルでは無害でも) JPEG ファイル内では有害とみなされるコンテンツを照合します。3 番目のルールフラグメントによって、JPEG ファイル内に存在しないエクスプロイトに関する誤検出イベントが生成されます。

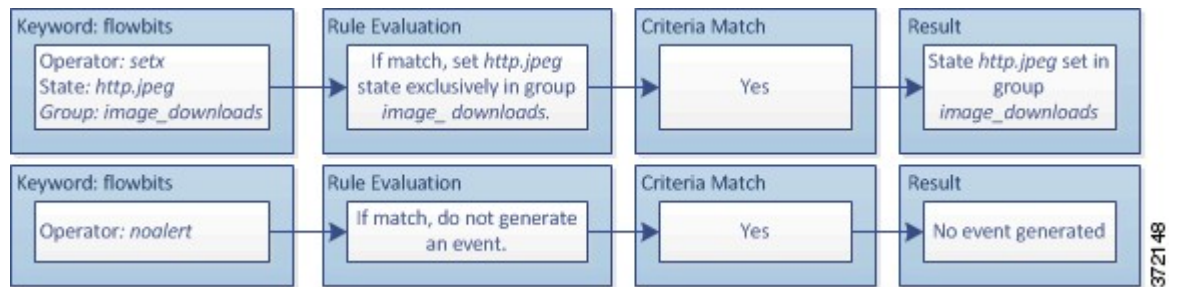
### flowbits キーワードの例：誤検出イベントを防ぐための設定

次の例は、状態名をグループに含めて setx 演算子を使用することで、どのように誤検出を防止できるかを示しています。

前の例とほぼ同じケースを考えます。ただし、最初の 2 つのルールで、同じ状態グループに 2 つの異なる状態名が含まれるようになった点が異なります。

```
(msg:"JPEG transfer";
content:"image/";pcr:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:setx,http.jpeg,image_downloads; flowbits:noalert;)
```

次の図は、上記のルールフラグメントにおける flowbits キーワードの効果を示しています。

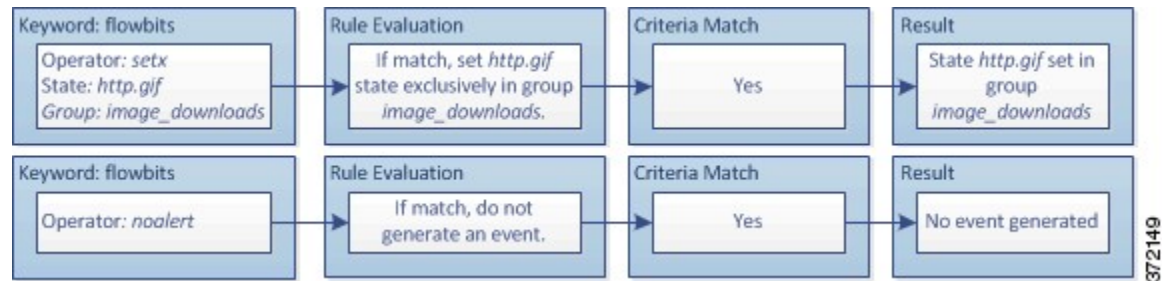


最初のルールフラグメントが JPEG ファイルダウンロードを検出すると、flowbits:setx,http.jpeg,image\_downloads キーワードが flowbits 状態を http.jpeg に設定し、その状態を image\_downloads グループに含めます。

その後、次のルールが後続の GIF ファイルダウンロードを検出します。

```
(msg:"GIF transfer"; content:"image/";
pcr:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:setx,http.jpg,image_downloads; flowbits:noalert;)
```

次の図は、上記のルールフラグメントにおける flowbits キーワードの効果を示しています。

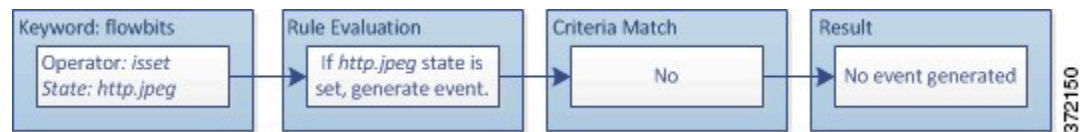


2 番目のルールフラグメントが GIF ダウンロードに一致すると、flowbits:setx,http.jpg,image\_downloads キーワードが http.jpg flowbits ステートを設定し、グループ内の他のステートである http.jpeg を解除します。

次に示す 3 番目のルールフラグメントで誤検出は発生しません。

```
(msg:"JPEG exploit"; ?flowbits:isset,http.jpeg;content:"|FF|";
pcrc: "/?\\xFF[\\xE1\\xE2\\xED\\xFE]\\x00[\\x00\\x01]"/;)
```

次の図は、上記のルールフラグメントにおける flowbits キーワードの効果を示しています。



flowbits:isset,http.jpeg が false であるため、ルールエンジンはルールの処理を停止し、イベントは生成されません。こうして、GIF ファイル内のコンテンツが JPEG ファイルに関するエクスプロイトコンテンツと一致した場合でも誤検出が回避されます。

## http\_encode キーワード

http\_encode キーワードを使用すると、HTTPURI、HTTPヘッダー内の非cookieデータ、HTTP要求ヘッダー内の cookie、HTTP 応答内の set-cookie データのいずれかにおいて、正規化前の HTTP 要求または応答内のエンコードタイプに基づいてイベントを生成できます。

HTTP 応答と HTTP cookie を検査し、http\_encode キーワードを使用しているルールに一致したものを返すように、HTTP Inspect プリプロセッサを設定する必要があります。

また、侵入ルール内の http\_encode キーワードで特定のエンコードタイプによってイベントがトリガーとして使用されるようにするには、HTTP Inspect プリプロセッサ設定で個々の特定のエンコードタイプのデコードオプションとアラートオプションの両方を有効にする必要があります。

次の表は、このオプションでイベントを生成できる、HTTPURI、ヘッダー、cookie、set-cookie のエンコードタイプを説明しています。



表 181: http\_encode エンコードタイプ

エンコードタイプ	説明
utf8	HTTP Inspect プリプロセッサによるデコードで UTF-8 エンコードタイプが有効になっている場合、指定された場所で UTF-8 エンコードを検出します。
double_encode	HTTP Inspect プリプロセッサによるデコードで二重エンコードタイプが有効になっている場合、指定された場所で二重エンコードを検出します。
non_ascii	非 ASCII 文字が検出されても、検出されたエンコードタイプが有効になっていない場合に、指定された場所で非 ASCII 文字を検出します。
uencode	HTTP Inspect プリプロセッサによるデコードで Microsoft %u エンコードタイプが有効になっている場合、指定された場所で Microsoft %u エンコードを検出します。
bare_byte	HTTP Inspect プリプロセッサによるデコードで空白バイトエンコードタイプが有効になっている場合、指定された場所で空白バイトエンコードを検出します。

関連トピック

[HTTP Inspect プリプロセッサ \(1883 ページ\)](#)

[サーバレベルの HTTP 正規化オプション \(1885 ページ\)](#)

## http\_encode キーワードの構文

### エンコーディングの場所

HTTP URI、ヘッダー、または set-cookie などの Cookie で指定されたエンコーディングタイプを検索するかどうかを指定します。

### エンコードタイプ

次のいずれかの形式を使用して、1 つ以上のエンコードタイプを指定します。

```
encode_type
encode_type|encode_type|encode_type...
```

ここで、encode\_type は次のいずれかです。

```
utf8
double_encode
non_ascii
uencode
bare_byte.
```

否定 (!) 演算子と OR (|) 演算子を一緒に使用できないことに注意してください。

## http\_encode キーワードの例：2つの http\_encode キーワードを使用した2つのエンコーディングの検索

次に、同じルールで2つの http\_encode キーワードを使用して、UTF-8 および Microsoft IIS %u エンコーディングの HTTP URI を検索する例を示します。

最初に、http\_encode キーワードを使用します。

- エンコーディングの場所：HTTP URI
- エンコーディングのタイプ：utf8

次に、追加の http\_encode キーワードを使用します。

- エンコーディングの場所：HTTP URI
- エンコーディングのタイプ：uencode

## 概要：file\_type および file\_group キーワード

file\_type と file\_group キーワードを使用すると、タイプとバージョンに基づいて、FTP、HTTP、SMTP、IMAP、POP3、NetBIOS-ssn (SMB) を介して伝送されるファイルを検出できます。1つの侵入ルール内で複数の file\_type キーワードや file\_group キーワードを使用しないでください。



### ヒント

脆弱性データベース (VDB) を更新すると、最新のファイルタイプ、バージョン、グループが侵入ルールエディタに表示されます。



### (注)

システムは、file\_type および file\_group キーワードに値を代入するためにプリプロセッサを自動的に有効にすることはしません。

file\_type または file\_group キーワードに一致するトラフィックに対してイベントを生成し、インライン展開では、違反パケットをドロップします。するには、特定のプリプロセッサを有効にする必要があります。

表 182: file\_type および file\_group の侵入イベントの生成

プロトコル	必要なプリプロセッサまたはプリプロセッサオプション
FTP	FTP/Telnet プリプロセッサおよび [TCP ペイロードの正規化 (Normalize TCP Payload) ] インライン正規化プリプロセッサ オプション
HTTP	HTTP トラフィックでの侵入イベントを生成する HTTP Inspect プリプロセッサ。

プロトコル	必要なプリプロセッサまたはプリプロセッサオプション
SMTP	HTTP トラフィックでの侵入イベントを生成する SMTP プリプロセッサ
IMAP	IMAP プリプロセッサ
POP3	POP プリプロセッサ
NetBIOS-ssn (SMB)	DCE/RPC プリプロセッサおよび [SMB ファイル インспекション (SMB File Inspection) ] DCE/RPC プリプロセッサ オプション

関連トピック

- [脆弱性データベースの更新 \(177 ページ\)](#)
- [FTP/Telnet デコーダ \(1874 ページ\)](#)
- [インライン正規化プリプロセッサ \(1951 ページ\)](#)
- [HTTP Inspect プリプロセッサ \(1883 ページ\)](#)
- [SMTP プリプロセッサ \(1920 ページ\)](#)
- [IMAP プリプロセッサ \(1912 ページ\)](#)
- [POP プリプロセッサ \(1916 ページ\)](#)
- [DCE/RPC プリプロセッサ \(1856 ページ\)](#)

## file\_type キーワードと file\_group キーワード

### file\_type

file\_type キーワードを使用すると、トラフィック内で検出対象となるファイルのタイプとバージョンを指定できます。ファイルタイプ引数 (**JPEG** や **PDF** など) は、トラフィックで検出するファイルの形式を識別します。



(注) 同じ侵入ルール内で file\_type キーワードを別の file\_type キーワードまたは file\_group キーワードと一緒に使用しないでください。

デフォルトでは [任意のバージョン (Any Version) ] が選択されますが、一部のファイルタイプではバージョンオプション (たとえば **PDF** バージョン **1.7**) を選択することにより、トラフィックで検出対象となる特定のファイルタイプバージョンを識別できます。

### file\_group

file\_group キーワードを使用すると、トラフィック内で検出する類似のファイルタイプからなる Cisco 定義のグループを選択できます (**マルチメディア**、**オーディオ** など)。また、ファイルグループには、グループ内の各ファイルタイプに関する Cisco 定義のバージョンも含まれています。



(注) 同じ侵入ルール内で `file_group` キーワードを別の `file_group` キーワードまたは `file_type` キーワードと一緒に使用しないでください。

## file\_data キーワード

`file_data` キーワードは、`content`、`byte_jump`、`byte_test`、`pcre` などの他のキーワードで使用可能な位置引数の参照として機能するポイントです。`file_data` キーワードが指し示すデータのタイプは、検出されるトラフィックによって決まります。`file_data` キーワードを使用すると、次のペイロードタイプの先頭を指し示すことができます。

- HTTP 応答本文

HTTP 応答パケットを検査するには、HTTP Inspect プリプロセッサを有効にして、HTTP 応答を検査するようプリプロセッサを設定する必要があります。HTTP Inspect プリプロセッサが HTTP 応答本文データを検出した場合に、`file_data` キーワードが一致します。

- 非圧縮 gzip ファイル データ

HTTP 応答本文内の非圧縮 gzip ファイルを検査するには、HTTP Inspect プリプロセッサを有効にする必要があります、さらに HTTP 応答を検査して HTTP 応答本文内の gzip 圧縮ファイルを復元するようプリプロセッサを設定する必要があります。詳細については、サーバーレベルの HTTP 正規化オプション [HTTP 応答の検査 (Inspect HTTP Responses) ] および [圧縮データの検査 (Inspect Compressed Data) ] を参照してください。`file_data` キーワードは、HTTP Inspect プリプロセッサが HTTP 応答本文内で非圧縮 gzip データを検出した場合に一致します。

- 正規化された JavaScript

正規化された JavaScript データを検査するには、HTTP Inspect プリプロセッサを有効にして、HTTP 応答を検査するようプリプロセッサを設定する必要があります。`file_data` キーワードは、HTTP Inspect プリプロセッサが応答本文データ内で JavaScript を検出した場合に一致します。

- SMTP ペイロード

SMTP ペイロードを検査するには、SMTP プリプロセッサを有効にする必要があります。`file_data` キーワードは、SMTP プリプロセッサが SMTP データを検出した場合に一致します。

- SMTP、POP、または IMAP トラフィック内のエンコードされた電子メール添付ファイル

SMTP、POP、または IMAP トラフィック内の電子メール添付ファイルを検査するには、それぞれ SMTP、POP、または IMAP プリプロセッサを単独で、または任意に組み合わせで有効にする必要があります。その後、有効にしたプリプロセッサごとに、デコード対象のそれぞれの添付ファイルエンコードタイプをデコードするようプリプロセッサが設定されていることを確認する必要があります。プリプロセッサごとに設定可能な添付ファイ

ルデコード オプションは、[Base64 復号の深さ (Base64 Decoding Depth) ]、[7 ビット/8 ビット/バイナリ復号の深さ (7-Bit/8-Bit/Binary Decoding Depth) ]、[Quoted Printable 復号の深さ (Quoted-Printable Decoding Depth) ]、および [UNIX 間復号の深さ (Unix-to-Unix Decoding Depth) ] です。

1 つのルール内で複数の file\_data キーワードを使用できます。

#### 関連トピック

[HTTP Inspect プリプロセッサ \(1883 ページ\)](#)

[サーバレベルの HTTP 正規化オプション \(1885 ページ\)](#)

[SMTP プリプロセッサ \(1920 ページ\)](#)

[IMAP プリプロセッサ \(1912 ページ\)](#)

## pkt\_data キーワード

pkt\_data キーワードは、content、byte\_jump、byte\_test、pcrcr などの他のキーワードで使用可能な位置引数の参照として機能するポインタです。

正規化された FTP、Telnet、または SMTP トラフィックが検出された場合、pkt\_data キーワードは、正規化されたパケットペイロードの先頭を指します。その他のトラフィックが検出された場合、pkt\_data キーワードは、未加工の TCP または UDP ペイロードの先頭を指します。

侵入ルールで検査するために、該当するトラフィックをシステムで正規化するには、次の正規化オプションを有効にする必要があります。

- 検査のために FTP トラフィックを正規化するには、FTP & Telnet プリプロセッサの [FTP コマンドでの Telnet エスケープ コードの検出 (Detect Telnet Escape codes within FTP commands) ] オプションを有効にします。
- 検査のために Telnet トラフィックを正規化するには、FTP & Telnet プリプロセッサの Telnet の [正規化 (Normalize) ] オプションを有効にします。
- 検査のために SMTP トラフィックを正規化するには、SMTP プリプロセッサの [正規化 (Normalize) ] オプションを有効にします。

1 つのルール内で複数の pkt\_data キーワードを使用できます。

#### 関連トピック

[クライアントレベルの FTP オプション \(1880 ページ\)](#)

[Telnet オプション \(1874 ページ\)](#)

[SMTP プリプロセッサのオプション \(1920 ページ\)](#)

## base64\_decode キーワードと base64\_data キーワード

base64\_decode キーワードと base64\_data キーワードを組み合わせると、指定したデータを Base64 データとしてデコードおよび検査するようルールエンジンに指示できます。たと

例えば HTTP PUT および POST 要求内の Base64 エンコード HTTP 認証要求見出しと Base64 エンコード データを検査する場合に、これが役立つ可能性があります。

これらのキーワードは特に、HTTP 要求内の Base64 データをデコードして検査するうえで役立ちます。また、長いヘッダー行を複数行に拡張するために HTTP で使われるのと同じ方法でスペース文字やタブ文字を使用する SMTP などのプロトコルでも、これらを使用できます。この行拡張（折り返しとも言う）を使用するプロトコル内に行拡張が存在しない場合、後続スペース/タブを伴わない復帰または改行が出現した箇所で検査が終了します。

### base64\_decode

base64\_decode キーワードは、パケットデータを Base64 データとしてデコードするようルールエンジンに指示します。オプションの引数を使用すると、デコードするバイト数と、デコードを開始するデータ内の位置を指定できます。

base64\_decode キーワードは 1 つのルール内で 1 回だけ使用可能です。また、少なくとも 1 つの base64\_data キーワードのインスタンスの前にこれを配置する必要があります。

Base64 データをデコードする前に、ルールエンジンは、複数行にわたって折り返された長いヘッダーを元どおりに広げます。ルールエンジンが次のいずれかに遭遇するとデコードが終了します。

- ヘッダー行の末尾
- デコード対象として指定されたバイト数
- パケットの末尾

次の表に、base64\_decode キーワードで使用可能な引数の説明を示します。

表 183: base64\_decode のオプション引数

引数	説明
Bytes	デコードするバイト数を指定します。これを指定しない場合、ヘッダー行の末尾またはパケットペイロード末尾のどちらかが先に出現するまでデコードが続行されます。ゼロ以外の正の値を指定できます。
Offset	パケットペイロードの先頭を基準にしたオフセットを決定します。さらに <b>Relative</b> も指定した場合は、現在の検査位置を基準にしたオフセットを決定します。ゼロ以外の正の値を指定できます。
Relative	現在の検査位置を基準にして検査することを指定します。

### base64\_data

base64\_data キーワードは、base64\_decode キーワードを使ってデコードされた Base64 データを検査するための参照を提供します。base64\_data キーワードは、デコードされた Base64 データの先頭から検査を開始するよう設定します。オプションで、content や byte\_test などの他のキーワードで使用可能な位置引数を使用して、検査位置をさらに指定することもできます。

base64\_decode キーワードを使用した後に base64\_data キーワードを 1 回以上使用する必要があります。オプションで、base64\_data を複数回使用して、デコードされた Base64 データの先頭に戻ることができます。

Base64 データを検査するときには、次の点に注意してください。

- 高速パターン マッチ機能は使用できません。
- 中間的な HTTP コンテンツ引数を使ってルール内で Base64 検査を中断する場合は、Base64 データをさらに検査する前に、別の base64\_data キーワードをルールに挿入する必要があります。

#### 関連トピック

[概要 : HTTP content および protected\\_content キーワードの引数 \(1719 ページ\)](#)

[content キーワードの高速パターン マッチ機能の引数 \(1724 ページ\)](#)

base64\_decode キーワードと base64\_data キーワード





## 第 76 章

# 侵入防御パフォーマンスの調整

以下のトピックでは、侵入防御のパフォーマンスを調整する方法について説明します。

- [侵入防御のパフォーマンス チューニングについて \(1819 ページ\)](#)
- [侵入に対するパターン一致の制限 \(1820 ページ\)](#)
- [正規表現による侵入ルールのオーバーライドの制限 \(1821 ページ\)](#)
- [侵入ルールの正規表現制限のオーバーライド \(1822 ページ\)](#)
- [パケットごとの侵入イベント生成の制限 \(1823 ページ\)](#)
- [パケットごとに生成される侵入イベントの制限 \(1824 ページ\)](#)
- [パケットおよび侵入ルールの遅延しきい値構成 \(1825 ページ\)](#)
- [侵入パフォーマンス統計情報のロギング設定 \(1832 ページ\)](#)
- [侵入パフォーマンス統計情報のロギングの設定 \(1833 ページ\)](#)

## 侵入防御のパフォーマンス チューニングについて

Cisco では、侵入行為のトラフィックを分析する際のシステムのパフォーマンスを向上するための機能を提供しています。次の操作を実行できます。

- イベントキューで許可するパケット数を指定できます。ストリーム再構成の前後に、より大きなストリームに再構築されるパケットのインスペクションを有効または無効にできます。
- パケットペイロードの内容を検査するための侵入ルールで使用される PCRE のデフォルトの一致および再帰の制限をオーバーライドできます。
- 複数のイベントが生成された場合にパケットまたはパケットストリームごとに複数のイベントをルールエンジンがログに記録するようにして、レポートされるイベント以外の情報も収集できます。
- デバイスの遅延をパケットおよびルール遅延しきい値構成の許容レベルで保持する必要性とセキュリティのバランスを保つことができます。
- デバイスはそのパフォーマンスをモニタおよび報告する動作に関する基本的なパラメータを設定できます。システムがデバイスのパフォーマンス統計情報を更新する間隔を指定できます。

これらのパフォーマンス設定は、各アクセスコントロールポリシーごとに設定し、その設定はその親のアクセスコントロールポリシーによって呼び出されるすべての侵入ポリシーに適用されます。

## 侵入に対するパターン一致の制限

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

- ステップ 1** アクセスコントロールポリシーエディタで、[詳細 (Advanced)] タブをクリックします。
- ステップ 2** [パフォーマンス設定 (Performance Settings)] の横にある編集アイコン (✎) をクリックします。  
  
代わりに表示アイコン (🔍) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベースポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。
- ステップ 3** [パフォーマンス設定 (Performance Settings)] ポップアップウィンドウ内の [パターン一致の制限 (Pattern Matching Limits)] タブをクリックします。
- ステップ 4** [パケットごとに分析するパターン状態の最大値 (Maximum Pattern States to Analyze Per Packet)] フィールドに、キューに含めるイベントの最大数の値を入力します。
- ステップ 5** ストリーム再構成の前後で、データのより大きなストリームに再構築されるパケットのインスペクションを無効にするには、[今後の再構成の対象となるトラフィックでコンテンツチェックを無効にする (Disable Content Checks on Traffic Subject to Future Reassembly)] チェックボックスをオンにします。再構成の前後の検査はより多くの処理オーバーヘッドを必要とするため、パフォーマンスが低下する可能性があります。
- ステップ 6** [OK] をクリックします。
- ステップ 7** [保存 (Save)] をクリックしてポリシーを保存します。

### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

# 正規表現による侵入ルールのオーバーライドの制限

デフォルトの正規表現の制限によってパフォーマンスの最低レベルが確保されます。これらの制限をオーバーライドすると、セキュリティが向上する可能性があります。非効率的な正規表現に対してパケット評価を許可することで、パフォーマンスが著しく影響を受ける可能性があります。



**注意** 非効率的なパターンの影響に関する知識があり、侵入ルールの作成経験が豊富であるユーザ以外は、デフォルトの PCRE の制限をオーバーライドしないでください。

表 184: 正規表現の制約オプション

オプション	説明
検索結果の制限状態 (Match Limit State)	[制限に合わせる (Match Limit)] をオーバーライドするかどうかを指定します。次の選択肢があります。 <ul style="list-style-type: none"> <li>• [デフォルト (Default)] を選択して、[制限に合わせる (Match Limit)] に設定した値を使用する</li> <li>• [無制限 (Unlimited)] を選択して、無制限の数の試行を許可する</li> <li>• [カスタム (Custom)] を選択して、[制限に合わせる (Match Limit)] に対して 1 以上の制限を指定するか、または PCRE の一致の評価を完全に無効化するために 0 を指定する</li> </ul>
制限に合わせる (Match Limit)	PCRE 正規表現で定義されたパターンに一致することを試行する回数を指定します。

オプション	説明
検索結果の再起制限状態 (Match Recursion Limit State)	<p>[再起制限に合わせる (Match Recursion Limit)] をオーバーライドするかどうかを指定します。次の選択肢があります。</p> <ul style="list-style-type: none"> <li>• [デフォルト (Default)] を選択して、[再起制限に合わせる (Match Recursion Limit)] に設定した値を使用する</li> <li>• [無制限 (Unlimited)] を選択して、無制限の数の再帰を許可する</li> <li>• [カスタム (Custom)] を選択して、[再起制限に合わせる (Match Recursion Limit)] に対して 1 以上の制限を指定するか、または PCRE の再帰を完全に無効化するために 0 を指定する</li> </ul> <p>[再起制限に合わせる (Match Recursion Limit)] が意味を持つためには、[制限に合わせる (Match Limit)] よりも小さい必要があることに注意してください。</p>
再起制限に合わせる (Match Recursion Limit)	パケットペイロードに対して PCRE 正規表現を評価する際の再帰数を指定します。

## 関連トピック

[概要 : pcre キーワード \(1739 ページ\)](#)

## 侵入ルールの正規表現制限のオーバーライド

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

## 手順

- ステップ 1** アクセスコントロールポリシーエディタで、[詳細 (Advanced)] タブをクリックします。
- ステップ 2** [パフォーマンス設定 (Performance Settings)] の横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔒) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する (Inherit from base policy) ] をオフにして、編集を有効にします。

- ステップ 3 [パフォーマンス設定 (Performance Settings) ] ポップアップ ウィンドウ内の [正規表現の制限 (Regular Expression Limits) ] タブをクリックします。
- ステップ 4 [正規表現による侵入ルールのオーバーライドの制限 \(1821 ページ\)](#) に示したオプションを変更できます。
- ステップ 5 [OK] をクリックします。
- ステップ 6 [保存 (Save) ] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## パケットごとの侵入イベント生成の制限

侵入ルールエンジンがルールに対してトラフィックを評価する場合、特定のパケットまたはパケット ストリームに生成されたイベントをイベント キューに配置し、キュー内の上位のイベントをユーザインターフェイスに報告します。侵入イベントロギングの制限を設定する場合、キュー内に配置可能なイベントの数および記録されるイベントの数を指定できます。また、キュー内のイベントの順序を決定する条件を選択できます。

表 185: 侵入イベント ロギング制限のオプション

オプション	説明
パケットごとに保存されるイベントの最大数 (Maximum Events Stored Per Packet)	特定のパケットまたはパケット ストリームに対して保存できるイベントの最大数。
パケットごとにログに記録されるイベントの最大数 (Maximum Events Logged Per Packet)	特定のパケットまたはパケット ストリームに対して記録されるイベントの数。これは、[パケットごとに保存されるイベントの最大数 (Maximum Events Stored Per Packet) ] 値を超えてはいけません。

オプション	説明
イベントログギングの順位決定の基準 (Prioritize Event Logging By)	<p>イベント キュー内のイベントの順序を決定するために使用する値。最上位のイベントがユーザ インターフェイスから報告されます。次の中から選択できます。</p> <ul style="list-style-type: none"> <li>• <code>priority</code>。 イベントの優先順位によってキュー内のイベントを並べ替えます。</li> <li>• <code>content_length</code>。 最も長い識別コンテンツの一致によってイベントを並べ替えます。 イベントがコンテンツ長によって並べ替えられる場合、ルール イベントは常にデコード イベントおよびプリプロセッサ イベントよりも優先されます。</li> </ul>

## パケットごとに生成される侵入イベントの制限

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

- ステップ 1** アクセス コントロール ポリシー エディタで、[詳細 (Advanced)] タブをクリックします。
- ステップ 2** [パフォーマンス設定 (Performance Settings)] の横にある編集アイコン (✎) をクリックします。  
  
代わりに表示アイコン (🔍) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。
- ステップ 3** [パフォーマンス設定 (Performance Settings)] ポップアップ ウィンドウ内の [侵入イベントのログ制限 (Intrusion Event Logging Limits)] タブをクリックします。
- ステップ 4** [パケットごとの侵入イベント生成の制限 \(1823 ページ\)](#) に示したオプションを変更できます。
- ステップ 5** [OK] をクリックします。
- ステップ 6** [保存 (Save)] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の導入 (350 ページ) を参照してください。

## パケットおよび侵入ルールの遅延しきい値構成

各アクセスコントロールポリシーには、しきい値を使用してパケットとルールの処理パフォーマンスを管理する、遅延ベースの設定があります。

パケット遅延しきい値構成は、該当するデコーダ、プリプロセッサ、およびルールによるパケット処理の総経過時間を測定し、処理時間が設定可能なしきい値を超えるとパケットのインスペクションを終了します。

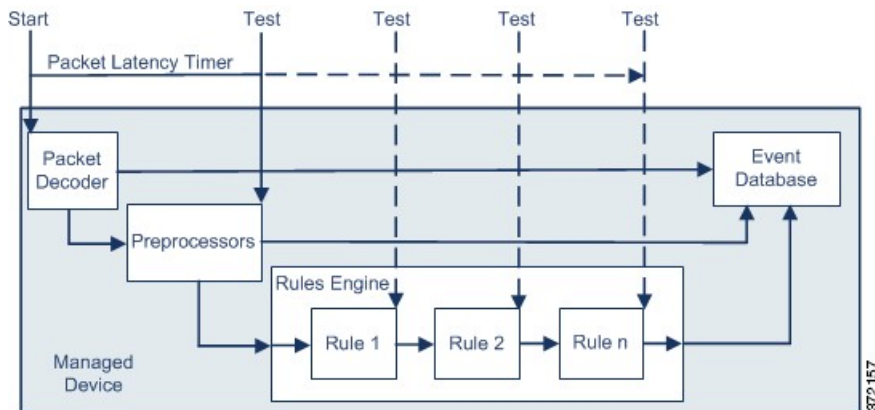
ルール遅延しきい値構成は、各ルールが個別のパケットの処理に費やした時間を測定し、処理時間が遅延しきい値ルールをある回数（設定可能）連続して超えた場合は、そのルールに違反した処理を、関連するルールのグループとともに指定された期間中断し、中断期間終了後にルールを回復します。

### パケット遅延しきい値構成

パケット遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値はソフトウェアベースの遅延の実装であり、厳密なタイミングを適用するわけではありません。

遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。ただし、パケット遅延しきい値構成では、セキュリティと接続性のバランスを取るために使用可能なツールが用意されています。

デコーダの処理の開始時に各パケットのタイマーが起動します。タイミングは、パケットのすべての処理が終了するか、または処理時間がタイミングテストポイントでしきい値を超えるまで続きます。



上の図に示すように、パケット遅延タイミングは次のテストポイントでテストされます。

- すべてのデコーダおよびプリプロセッサの処理の完了後、ルールの処理が開始される前

- 各ルールによる処理の後

処理時間が任意のテスト ポイントでしきい値を超えると、パケットの検査は停止します。



#### ヒント

パケットの合計処理時間にルーチン TCP ストリームまたは IP フラグメント再構成の時間は含まれません。

パケット遅延しきい値構成は、パケットを処理するデコーダ、プリプロセッサ、またはルールによってトリガーされるイベントに影響を与えません。該当するデコーダ、プリプロセッサ、またはルールは、パケットが完全に処理されるか、または遅延しきい値を超えたためにパケット処理が終了されるか、どちらか先に発生した時点まで通常通りトリガーされます。廃棄ルールがインライン展開の侵入を検知すると、その廃棄ルールがイベントをトリガーし、パケットは廃棄されます。



#### (注)

パケット遅延しきい値違反のためにパケットの処理が終了した後は、ルールに対してパケットは評価されません。イベントを引き起こす可能性があったルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

パケット遅延のしきい値は、パッシブおよびインライン展開の両方でシステムのパフォーマンスを向上させ、インライン展開では過度の処理時間を必要とするパケットの検査を停止することにより遅延を低減できます。これらのパフォーマンス上のメリットは、以下のような場合にもたらされます。

- パッシブ展開およびインライン展開の両方で、複数のルールによるパケットの順次検査に長時間かかる場合
- インライン展開で、ユーザが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット処理を遅らせる場合

パッシブ展開では、パケットの処理を停止しても、処理が単に次のパケットに移るだけで、ネットワーク パフォーマンスの回復につながらない可能性があります。

## パケット遅延しきい値構成の注意事項

表 186: パケット遅延しきい値構成オプション

オプション	説明
しきい値 (マイクロ秒) (Threshold (microseconds))	パケットのインスペクションが終了する時間をマイクロ秒単位で指定します。

ルール 134:3 を有効にして、パケット遅延しきい値を超えたためにシステムがパケットのインスペクションを終了する場合に イベントを生成し、インライン展開では、違反パケットをド



ロップします。できます。詳細については、[侵入ルールの状態オプション \(1639ページ\)](#) を参照してください。

システムパフォーマンスおよびパケット遅延の測定に影響する要因は、CPU速度、データレート、パケットサイズ、プロトコルタイプなど多数あります。このためシスコは、ユーザ独自の計算によってご自身のネットワーク環境に合った設定を行うまで、次の表のしきい値設定を使用することを推奨します。

表 187: 最小のパケット遅延しきい値設定

データ レート	最小しきい値設定 (マイクロ秒)
1 Gbps	100
100 Mbps	250
5 Mbps	[1000]

独自の設定を計算する場合は、次の項目を決定します。

- 1秒あたりの平均パケット数
- 1パケットあたりの平均マイクロ秒数

パケットインスペクションを不必要に中断することがないように、ネットワークの1パケットあたりの平均マイクロ秒数に重要な安全係数を乗算します。

たとえば、シスコは1ギガビット環境で100マイクロ秒の最小パケット遅延しきい値を推奨しています。この最小推奨値は、1秒あたり平均250,000パケットを示すテストデータに基づいています。これは、1マイクロ秒あたり0.25パケット、言い換えると1パケットあたり4マイクロ秒に相当します。25倍すると推奨最小しきい値の100マイクロ秒が得られます。

## パケット遅延しきい値の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

- ステップ 1** アクセス コントロール ポリシー エディタで、[詳細 (Advanced)] タブをクリックします。
- ステップ 2** [遅延ベースのパフォーマンス設定 (Latency-Based Performance Settings)] の横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔒) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。

- ステップ 3 [遅延ベースのパフォーマンス設定 (Latency-Based Performance Settings)] ポップアップ ウィンドウで [パケット処理 (Packet Handling)] タブをクリックします。
- ステップ 4 推奨される最小しきい値の設定については、[パケット遅延しきい値構成の注意事項 \(1826 ページ\)](#) を参照してください。
- ステップ 5 [OK] をクリックします。
- ステップ 6 [保存 (Save)] をクリックしてポリシーを保存します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ルール遅延しきい値構成

ルール遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値はソフトウェアベースの遅延の実装であり、厳密なタイミングを適用するわけではありません。

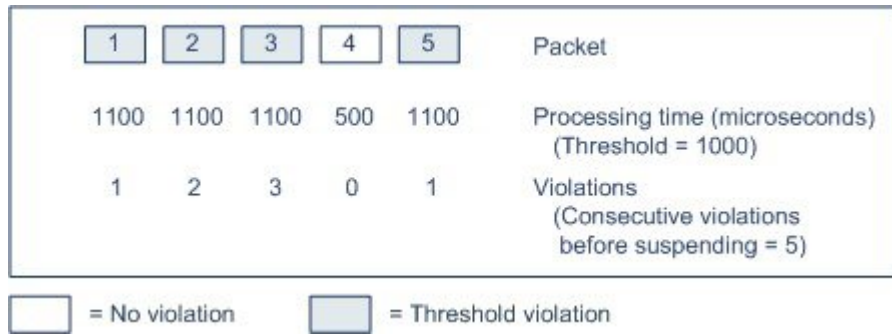
遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。ただし、ルール遅延しきい値構成では、セキュリティと接続性のバランスを取るために使用可能なツールが用意されています。

パケットがルールのグループに対して処理されるたびに、タイマーが処理時間を測定します。ルール処理時間が指定されたルール遅延しきい値を超えると、システムでカウンタが増加します。連続したしきい値違反の数が指定した数に達すると、システムは次のアクションを実行します。

- 指定された時間、ルールを一時停止する
- ルールが一時停止されたことを示すイベントをトリガーとして使用する
- 一時停止期間が過ぎたらルールを再度有効にする
- ルールが再び有効になったことを示すイベントをトリガーとして使用する

ルールのグループが一時停止しているか、またはルール違反が連続していない場合は、カウンタがゼロになります。ルールを一時停止する前に連続する違反の一部を許可することにより、パフォーマンスへの影響がわずかであると考えられる散発的なルール違反を無視し、繰り返しルール遅延しきい値を超えるルールにより重大な影響に焦点を当てることができます。

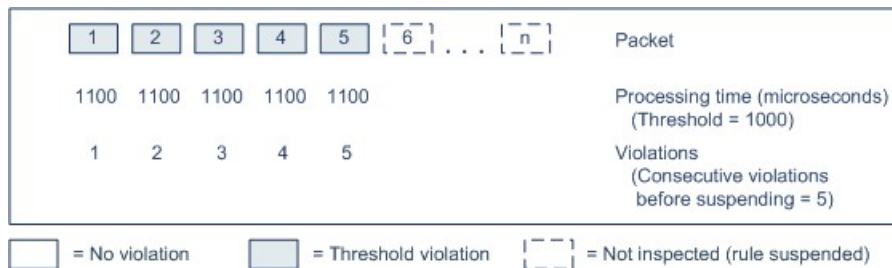
次の例は、ルールが一時停止にならない、5 つの連続したルール処理時間を示します。



372158

上の例で、最初の3個の各パケットの処理に必要な時間は1000マイクロ秒というルール遅延しきい値に違反し、違反カウンタは各違反のたびに増加します。4個目のパケット処理はしきい値に違反しないので、違反カウンタはゼロにリセットされます。5個目のパケットはしきい値に違反し、違反カウンタは1から再開します。

次の例は、ルールが一時停止になる、5つの連続したルール処理時間を示します。



372159

2番目の例で、5個のパケットのそれぞれの処理に必要な時間は1000マイクロ秒というルール遅延しきい値に違反します。各パケットの1100マイクロ秒というルール処理時間が指定された連続する5回の違反に対する1000マイクロ秒というしきい値に違反するため、ルールのグループは一時停止されます。図中のパケット6からnで表される後続のパケットは、一時停止期間が経過するまで、一時停止されたルールに対して検査されません。ルールが再有効化された後にさらにパケットが発生すると、違反カウンタはゼロから再開されます。

ルール遅延しきい値構成は、パケットを処理するルールによってトリガーされる侵入イベントに影響を及ぼしません。ルール処理時間がしきい値を超えるかどうかにかかわらず、パケット内で検出されるすべての侵入に対して、ルールはイベントをトリガーします。侵入を検知するルールがインライン展開の廃棄ルールである場合、パケットは廃棄されます。廃棄ルールがパケット内で侵入を検出し、その結果ルールが一時停止されると、廃棄ルールは侵入イベントをトリガーし、パケットは廃棄され、そのルールと関連するすべてのルールが一時停止されます。



(注) パケットは一時停止されたルールに対して評価されません。イベントを引き起こす可能性があった一時停止ルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

ルール遅延しきい値構成は、パッシブとインラインの両方の展開でシステムのパフォーマンスを向上することができます。また、パケットの処理に最も多くの時間を必要とするルールを一時停止することで、インライン展開の遅延を減らすことができます。設定可能な時間が過ぎるまで、パケットは一時停止されたルールに対して再度評価されず、過負荷のデバイスに回復の時間が与えられます。これらのパフォーマンス上のメリットは、以下のような場合にもたらされます。

- 短期間で作成され、ほとんどテストされていないルールが過剰な処理時間を必要とする場合
- ユーザが非常に大きなファイルをダウンロードするときなど、ネットワークパフォーマンスの低下がパケット インспекションを遅らせる場合

## ルール遅延しきい値構成の注記

ルール遅延しきい値、一時停止されるルールの一時停止時間、ルールを一時停止する前に発生する必要がある連続したしきい値違反の回数の変更を行うことができます。

ルールによるパケット処理時間が、[ルール停止前の連続しきい値違反 (Consecutive Threshold Violations Before Suspending Rule)] で指定された回数連続して [しきい値 (Threshold)] を超えると、ルール遅延しきい値構成は [停止時間 (Suspension Time)] で指定された時間、ルールを一時停止します。

ルール 134:1 を有効にして、ルールが一時停止されるときにイベントを生成できます。また、ルール 134:2 を有効にして、一時停止されたルールが有効化されるときにイベントを生成できます。[侵入ルールの状態オプション \(1639 ページ\)](#) を参照してください。

表 188: ルール遅延しきい値構成のオプション

オプション	説明
しきい値 (Threshold)	ルールがパケットを検査する際に超えることができない時間をマイクロ秒単位で指定します。
ルール停止前の連続しきい値違反 (Consecutive Threshold Violations Before Suspending Rule)	ルールが一時停止される前に、ルールによるパケットの検査時間が [しきい値 (Threshold)] で設定された時間を超えることができる、連続した回数を指定します。
停止時間 (Suspension Time)	ルールのグループを一時停止する秒数を指定します。

システムパフォーマンスの測定に影響する要因は、CPU 速度、データ レート、パケット サイズ、プロトコルタイプなど多数あります。このためシスコは、ユーザ独自の計算によってご自身のネットワーク環境に合った設定を行うまで、次の表のしきい値設定を使用することを推奨します。

表 189: 最小のルール遅延しきい値設定

データ レート	最小しきい値設定 (マイクロ秒)
1 Gbps	500
100 Mbps	1250
5 Mbps	[5000]

独自の設定を計算する場合は、次の項目を決定します。

- 1秒あたりの平均パケット数
- 1パケットあたりの平均マイクロ秒数

ルールを不必要に一時停止することがないように、ネットワークの1パケットあたりの平均マイクロ秒数に重要な安全係数を乗算します。

## ルール遅延しきい値の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

- 
- ステップ 1** アクセス コントロール ポリシー エディタで、[詳細 (Advanced)] タブをクリックします。
  - ステップ 2** [遅延ベースのパフォーマンス設定 (Latency-Based Performance Settings)] の横にある編集アイコン (✎) をクリックします。  
  
代わりに表示アイコン (🔍) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。
  - ステップ 3** [遅延ベースのパフォーマンス設定 (Latency-Based Performance Settings)] ポップアップ ウィンドウで [ルール処理 (Rule Handling)] タブをクリックします。
  - ステップ 4** [ルール遅延しきい値構成の注記 \(1830 ページ\)](#) の任意のオプションを設定できます。
  - ステップ 5** [OK] をクリックします。
  - ステップ 6** [保存 (Save)] をクリックしてポリシーを保存します。
-

### 次のタスク

- イベントを生成するには、遅延ルール（134:1 と 134:2）を有効にします。詳細については、[侵入ルールの状態オプション（1639 ページ）](#) を参照してください。
- 設定変更を展開します。[設定変更の導入（350 ページ）](#) を参照してください。

## 侵入パフォーマンス統計情報のロギング設定

### [サンプル時間（秒）（Sample time (seconds)）] と [パケットの最小数（Minimum number of packets）]

パフォーマンス統計情報の各更新の間で指定した秒数が経過すると、システムは指定したパケット数を分析したかを検証します。分析していた場合、システムはパフォーマンス統計情報を更新します。それ以外の場合、システムは指定したパケット数を分析するまで待機します。

### トラブルシューティングオプション：[ログセッション/プロトコル分布（Log Session/Protocol Distribution）]

トラブルシューティングの電話中に、プロトコル分布、パケット長、およびポートの統計情報のログを取るようにサポートから依頼される場合があります。



**注意** サポートによって指示された場合を除き、[ログセッション/プロトコル分布（Log Session/Protocol Distribution）] を有効にしないでください。注：[ログセッション/プロトコル分布（Log Session/Protocol Distribution）] の有効化または無効化 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作（356 ページ）](#) を参照してください。

### トラブルシューティングオプション：[概要（Summary）]

トラブルシューティングの電話中に、Snort プロセスのシャットダウンまたは再起動時に限り、パフォーマンス統計情報を計算するようにシステムを設定するようにサポートから依頼される場合があります。このオプションを有効にするには、[ログセッション/プロトコル分布（Log Session/Protocol Distribution）] トラブルシューティングオプションも有効にする必要があります。



**注意** サポートから指示された場合を除き、[概要（Summary）] を有効にしないでください。

## 侵入パフォーマンス統計情報のロギングの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

### 手順

**ステップ 1** アクセスコントロールポリシーエディタで[詳細 (Advanced) ]タブをクリックし、[パフォーマンス設定 (Performance Settings) ]の横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔒) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する (Inherit from base policy) ]をオフにして、編集を有効にします。

**ステップ 2** 表示されるポップアップ ウィンドウの [パフォーマンス統計情報 (Performance Statistics) ] タブをクリックします。

**ステップ 3** 前述のように、[サンプル時間 (Sample time) ]または[パケットの最小数 (Minimum number of packets) ]を変更します。

**ステップ 4** 任意で、サポートによって求められた場合にのみ、[トラブルシューティング オプション (Troubleshoot Options) ]セクションを展開し、そのオプションを変更します。

**注意** [ログセッション/プロトコル配布 (Log Session/Protocol Distribution) ]を有効にするか、無効にする設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

**ステップ 5** [OK] をクリック

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。







## 第 **XIX** 部

### 高度なネットワーク分析と前処理

- ネットワーク分析/侵入ポリシーのための高度なアクセス制御の設定 (1837 ページ)
- ネットワーク分析ポリシーの使用を開始するには (1845 ページ)
- アプリケーション層プリプロセッサ (1855 ページ)
- SCADA プリプロセッサ (1939 ページ)
- トランスポート層およびネットワーク層プリプロセッサ (1945 ページ)
- 特定の脅威の検出 (1989 ページ)
- 適応型プロファイル (2013 ページ)





## 第 77 章

# ネットワーク分析/侵入ポリシーのための 高度なアクセス制御の設定

以下のトピックでは、ネットワーク分析ポリシーと侵入ポリシー用の高度な設定を行う手順を示します。

- [ネットワーク分析および侵入ポリシーのアクセスコントロールの詳細設定について \(1837 ページ\)](#)
- [デフォルトの侵入ポリシー \(1837 ページ\)](#)
- [ネットワーク分析プロファイルの詳細設定 \(1840 ページ\)](#)

## ネットワーク分析および侵入ポリシーのアクセスコントロールの詳細設定について

アクセス コントロール ポリシーにおける詳細設定の多くは、設定のために特定の専門知識を要する侵入検知設定と予防設定を制御します。通常、詳細設定はほとんど、あるいはまったく変更する必要がありません。詳細設定は導入環境ごとに異なります。

## デフォルトの侵入ポリシー

各アクセス コントロール ポリシーは、システムがトラフィックを検査する方法を正確に決定する前に、デフォルトの侵入ポリシーを使用してそのトラフィックを最初に検査します。これは、場合によってシステムがトラフィックを処理するアクセス コントロール ルール（存在する場合）を決定する前に、接続の最初の数パケットを処理し**通過を許可する**必要があるため必要となります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。デフォルトでは、デフォルトの侵入ポリシーでデフォルトの変数セットが使用されます。

システムはクライアントとサーバの間で接続が完全に確立される前にアプリケーションを識別したり URL をフィルタ処理することはできないので、デフォルトの侵入ポリシーは、アプリ

セッション制御およびURLフィルタリングを実行する場合に特に有用です。たとえば、パケットがアプリケーションまたはURL条件を持つアクセスコントロールルールのその他のすべての条件に一致する場合、そのパケットと後続のパケットは、接続が確立されてアプリケーションまたはURLの識別が完了するまで通過することを許可されます。通常は3～5パケットです。

システムはこれらの許可されたパケットをデフォルトの侵入ポリシーで検査し、これによってイベントを生成したり、インラインで配置されている場合は、悪意のあるトラフィックをブロックできます。システムが接続を処理する必要があるアクセスコントロールルールまたはデフォルトアクションを識別した後、接続内の残りのパケットが適宜処理され検査されます。

アクセスコントロールポリシーを作成する場合、そのデフォルトの侵入ポリシーは**最初に**選択したデフォルトアクションによって異なります。アクセスコントロールの初期のデフォルト侵入ポリシーは次のとおりです。

- [バランスの取れたセキュリティと接続 (Balanced Security and Connectivity)] (システムによって提供されるポリシー) は、最初に [侵入防御 (Intrusion Prevention)] デフォルトアクションを選択した場合のアクセスコントロールポリシーのデフォルトの侵入ポリシーです。
- 最初に [すべてのトラフィックをブロック (Block all traffic)] または [ネットワーク検出 (Network Discovery)] デフォルトアクションを選択した場合、アクセスコントロールポリシーのデフォルトの侵入ポリシーは No Rules Active になります。このオプションを選択すると、前述の許可されたパケットでの侵入インスペクションが無効になりますが、侵入データが必要なければ、パフォーマンスを向上できます。



---

(注) (たとえば、検出専用の導入において) 侵入インスペクションを実行していない場合は、デフォルトの侵入ポリシーとして No Rules Active ポリシーを保持してください。

---

アクセスコントロールポリシーを作成した後にデフォルトアクションを変更する場合、デフォルトの侵入ポリシーは自動的に変更され**ません**。手動で変更するには、アクセスコントロールポリシーの詳細オプションを使用します。

システムによって作成されたポリシーまたはユーザが作成したポリシーを選択できます。



---

(注) 最初に一致したネットワーク分析ルールに関連付けられているネットワーク分析ポリシーが、デフォルトの侵入ポリシーに対してトラフィックを前処理します。ネットワーク分析ルールがない場合、あるいはどのルールも一致しない場合は、デフォルトのネットワーク分析ポリシーが使用されます。

---

## デフォルトの侵入ポリシーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin



### 注意

アクセス コントロール ポリシーによって使用される侵入ポリシーの総数の変更 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。現在使用されていない侵入ポリシーを追加するか、侵入ポリシーの最後のインスタンスを削除することで、侵入ポリシーの総数を変更します。アクセス コントロール ルールで侵入ポリシーをデフォルトのアクションまたはデフォルトの侵入ポリシーとして使用できます。

### 手順

**ステップ 1** アクセス コントロール ポリシー エディタで、[詳細設定 (Advanced)] タブをクリックし、[ネットワーク分析と侵入ポリシー (Network Analysis and Intrusion Policies)] セクションの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。

**ステップ 2** [アクセス制御ルールが決定される前に使用されている侵入ポリシー (Intrusion Policy used before Access Control rule is determined)] ドロップダウン リストから、侵入ポリシーを選択します。

ユーザが作成したポリシーを選択した場合は、編集アイコン (✎) をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

**ステップ 3** 必要に応じて、[侵入ポリシーの変数セット (Intrusion Policy Variable Set)] ドロップダウン リストから別の変数セットを選択します。変数セットの横にある編集アイコン (✎) を選択して、変数セットを作成および編集することもできます。変数セットを変更しない場合、システムはデフォルトのセットを使用します。

**ステップ 4** [OK] をクリックします。

ステップ5 [保存 (Save) ]をクリックしてポリシーを保存します。

#### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[変数セット \(444 ページ\)](#)

## ネットワーク分析プロファイルの詳細設定

ネットワーク分析ポリシーは、特に侵入の試みの前兆となるかもしれない異常トラフィックに対し、そのトラフィックがさらに評価されるようにトラフィックをデコードおよび前処理する方法を制御します。トラフィックの前処理は、セキュリティインテリジェンスのブラックリスト登録およびトラフィックの復号化の後、侵入ポリシーによるパケットインスペクションの前に行われます。デフォルトでは、システム提供の [バランスの取れたセキュリティと接続 (Balanced Security and Connectivity) ] ネットワーク分析ポリシーが、デフォルトネットワーク分析ポリシーです。



#### ヒント

システムによって提供される [バランスの取れたセキュリティと接続 (Balanced Security and Connectivity) ] ネットワーク分析ポリシーおよび [バランスの取れたセキュリティと接続 (Balanced Security and Connectivity) ] 侵入ポリシーは共に機能し、侵入ルールの更新の際に両方とも更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。

前処理を調整する簡単な方法は、カスタムネットワーク分析ポリシーを作成し、それをデフォルトとして使用することです。複雑な環境での高度なユーザの場合は、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを別々に前処理するように調整することができます。さらに、トラフィックのセキュリティゾーン、ネットワーク、または VLAN に応じて前処理が制御されるようにこれらのポリシーを設定できます。

これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。ネットワーク分析ルールは、これらの条件に一致するトラフィックを前処理する方法を指定する設定および条件の単純なセットにすぎません。既存のアクセス コントロール ポリシーの詳細オプションでネットワーク分析ルールを作成および編集します。各ルールは1つのポリシーにのみ属します。

各ルールに含まれる内容は、次のとおりです。

- 一連のルール条件。前処理の対象となる特定のトラフィックを識別します
- 関連付けられたネットワーク分析ポリシー。すべてのルールの条件を満たすトラフィックを前処理するために使用できます

システムがトラフィックを前処理するときに、パケットはルール番号の上位から下位の順序でネットワーク分析ルールに照合されます。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

## デフォルトのネットワーク分析ポリシーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

システムによって作成されたポリシーまたはユーザが作成したポリシーを選択できます。



- (注) プリプロセッサを無効にしているが、システムは有効になっている侵入ルールまたはプリプロセッサルールと照合して前処理されたパケットを評価する必要がある場合、システムはプリプロセッサを自動的に有効にして使用します。しかし、ネットワーク分析ポリシー Web インターフェイスでは無効のままです。前処理の調整、特に複数のカスタムネットワーク分析ポリシーを使用して調整することは、**高度なタスク**です。前処理および侵入インスペクションは密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーが互いに補完することを許可する場合は慎重になる**必要があります**。

### 手順

- ステップ 1** アクセス コントロール ポリシー エディタで、[詳細設定 (Advanced)] タブをクリックし、[ネットワーク分析と侵入ポリシー (Network Analysis and Intrusion Policies)] セクションの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。

- ステップ 2** [デフォルトのネットワーク分析ポリシー (Default Network Analysis Policy)] ドロップダウンリストから、デフォルトのネットワーク分析ポリシーを選択します。

ユーザが作成したポリシーを選択した場合は、編集アイコン (✎) をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

**注意** アクセスコントロールポリシーによって使用されるネットワーク分析ポリシーの総数を変更すると設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。現在使用されていないポリシーを追加するか、ネットワーク分析ポリシーの最後のインスタンスを削除することで、ネットワーク分析ポリシーの総数を変更します。ネットワーク分析ポリシーは、ネットワーク分析ルールと一緒に使用することもできれば、デフォルトのネットワーク分析ポリシーとして使用することもできます。

**ステップ 3** [OK] をクリックします。

**ステップ 4** [保存 (Save) ] をクリックしてポリシーを保存します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[カスタム ポリシーの制限 \(1583 ページ\)](#)

## ネットワーク分析ルール

アクセスコントロールポリシーの詳細設定で、ネットワーク分析ルールを使用してネットワークトラフィックへの前処理設定を調整できます。

ネットワーク分析ルールには1から番号が付けられます。システムがトラフィックを前処理するときに、パケットはルール番号の昇順で上から順にネットワーク分析ルールに照合され、すべてのルールの条件が一致する最初のルールに従ってトラフィックが前処理されます。

ルールには、ゾーン、ネットワーク、VLAN タグの条件を追加できます。ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。たとえば、ネットワーク条件を持つがゾーン条件を持たないルールは、その入力または出力インターフェイスに関係なく、送信元または宛先 IP アドレスに基づいてトラフィックを評価します。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

### ネットワーク分析ルールの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin



## 手順

**ステップ 1** アクセス コントロール ポリシー エディタで [詳細 (Advanced) ] タブをクリックし、[ネットワーク分析 (Network Analysis) ] および [侵入ポリシー (Intrusion Policies) ] セクションの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する (Inherit from base policy) ] をオフにして、編集を有効にします。

**ヒント** [ネットワーク分析ポリシーリスト (Network Analysis Policy List) ] をクリックし、既存のカスタム ネットワーク分析ポリシーを表示および編集します。

**ステップ 2** [ネットワーク分析ルール (Network Analysis Rules) ] の横にある、所持しているカスタム ルールの数を示したステートメントをクリックします。

**ステップ 3** [ルールの追加 (Add Rule) ] をクリックします。

**ステップ 4** 追加する条件に対応するタブをクリックして、ルールの条件を設定します。[ルール条件タイプ \(371 ページ\)](#) を参照してください。

**ステップ 5** [ネットワーク分析 (Network Analysis) ] タブをクリックし、このルールに一致するトラフィックの前処理に使用する [ネットワーク分析ポリシー (Network Analysis Policy) ] を選択します。

編集アイコン (✎) をクリックして、新しいウィンドウでカスタム ポリシーを編集します。システムによって提供されたポリシーは編集できません。

**注意** アクセス コントロール ポリシーによって使用されるネットワーク分析ポリシーの総数を変更すると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。現在使用されていないポリシーを追加するか、ネットワーク分析ポリシーの最後のインスタンスを削除することで、ネットワーク分析ポリシーの総数を変更します。ネットワーク分析ポリシーは、ネットワーク分析ルールと一緒に使用することもできれば、デフォルトのネットワーク分析ポリシーとして使用することもできます。

**ステップ 6** [追加 (Add) ] をクリックします。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ネットワーク分析ルール管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

ネットワーク分析ルールは、これらの条件に一致するトラフィックを前処理する方法を指定する設定および条件の単純なセットにすぎません。既存のアクセスコントロールポリシーの詳細オプションでネットワーク分析ルールを作成および編集します。各ルールは1つのポリシーにのみ属します。

### 手順

**ステップ 1** アクセスコントロールポリシーエディタで、[詳細 (Advanced)] タブをクリックして、[侵入およびネットワーク分析ポリシー (Intrusion and Network Analysis Policies)] セクションの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベースポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。

**ステップ 2** [ネットワーク分析ルール (Network Analysis Rules)] の横にある、所持しているカスタムルールの数を示したステートメントをクリックします。

**ステップ 3** カスタムルールを編集します。次の選択肢があります。

- ルールの条件を編集する、またはルールによって呼び出されるネットワーク分析ポリシーを変更するには、ルールの横にある編集アイコン (✎) をクリックします。
- ルールの評価順序を変更するには、ルールをクリックして正しい位置にドラッグします。複数のルールを選択するには、Shift キーおよび Ctrl キーを使用します。
- ルールを削除するには、ルールの横にある削除アイコン (🗑️) をクリックします。

**ヒント** ルールを右クリックするとコンテキストメニューが表示され、新しいネットワーク分析ルールの切り取り、コピー、貼り付け、編集、削除、および追加を実行できます。

**ステップ 4** [OK] をクリックします。

**ステップ 5** [保存 (Save)] をクリックしてポリシーを保存します。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。



## 第 78 章

# ネットワーク分析ポリシーの使用を開始するには

ここでは、ネットワーク分析ポリシーの使用を開始する方法について説明します。

- [ネットワーク分析ポリシーの基本 \(1845 ページ\)](#)
- [ネットワーク分析ポリシーの管理 \(1846 ページ\)](#)

## ネットワーク分析ポリシーの基本

ネットワーク分析ポリシーは、多数のトラフィックの前処理オプションを制御し、アクセスコントロールポリシーの詳細設定で呼び出されます。ネットワーク分析に関連する前処理は、**Security Intelligence** によるブラックリスト化や SSL 復号化の後、侵入またはファイル検査の開始前に実行されます。

デフォルトでは、システムは *Balanced Security and Connectivity* ネットワーク分析ポリシーを使用して、アクセスコントロールポリシーによって処理されるすべてのトラフィックを前処理します。ただし、この前処理を実行するために別のデフォルトのネットワーク分析ポリシーを選択できます。便宜を図るため、システムによっていくつかの変更不可能なネットワーク分析ポリシーが提供されます。これらのポリシーは、Cisco Talos Security Intelligence and Research Group (Talos) によってセキュリティおよび接続の一定のバランスがとれるように調整されています。カスタム前処理設定を使用して、カスタムネットワーク分析ポリシーを作成することもできます。



### ヒント

システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。ネットワーク分析ポリシーと侵入ポリシーが連動してトラフィックを検査します。

複数のカスタムネットワーク分析ポリシーを作成し、それらに異なるトラフィックの前処理を割り当てることにより、特定のセキュリティゾーン、ネットワーク、VLAN用に前処理オプションを調整できます。（ただし、ASA FirePOWER VLANによる前処理を制限することはできないことに注意してください）。

## ネットワーク分析ポリシーの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin


マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** ネットワーク分析ポリシーを管理します。

- [比較 (Compare)] : [ポリシーの比較 (Compare Policies)] をクリックします ([ポリシーの比較 \(361 ページ\)](#) を参照)。
- 作成 : 新しいネットワーク分析ポリシーを作成する場合は、[ポリシーの作成 (Create Policy)] をクリックして、[カスタムネットワーク分析ポリシーの作成 \(1847 ページ\)](#) で説明する手順を実行します。
- 削除 : ネットワーク分析ポリシーを削除する場合は、削除アイコン () をクリックして、ポリシーの削除を確認します。アクセスコントロールポリシーが参照しているネットワーク分析ポリシーは削除できません。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- 展開 : [展開 (Deploy)] をクリックします ([設定変更の導入 \(350 ページ\)](#) を参照)。

- **編集:**既存のネットワーク分析ポリシーを編集する場合は、編集アイコン (✎) をクリックして、[ネットワーク分析ポリシーの設定とキャッシュされた変更 \(1849 ページ\)](#) で説明する手順を実行します。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- **[レポート (Report) ]:** レポート アイコン (📄) をクリックします ([現在のポリシー レポートの生成 \(363 ページ\)](#) を参照)。

## カスタム ネットワーク分析ポリシーの作成

新しいネットワーク分析ポリシーを作成するときは、一意の名前を付け、基本ポリシーを指定し、インライン モードを選択する必要があります。

基本ポリシーはネットワーク分析ポリシーのデフォルト設定を定義します。新しいポリシーの設定の変更は、基本ポリシーの設定を変更するのではなく、オーバーライドします。システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

ネットワーク分析ポリシーのインラインモードでは、プリプロセッサでトラフィックを変更 (正規化) したりドロップしたりして、攻撃者が検出を回避する可能性を最小限にすることができます。パッシブな展開では、インライン モードに関係なく、システムはトラフィック フローに影響を与えることができないことに注意してください。

### 関連トピック

[基本レイヤ \(1592 ページ\)](#)

[インライン導入でのプリプロセッサによるトラフィックの変更 \(1852 ページ\)](#)

[カスタム ネットワーク分析ポリシーの作成 \(1847 ページ\)](#)

[ネットワーク分析ポリシーの編集 \(1850 ページ\)](#)

## カスタム ネットワーク分析ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

## 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** [ポリシーの作成 (Create Policy)] をクリックします。別のポリシー内に未保存の変更が存在する場合は、[ネットワーク分析ポリシー (Network Analysis Policy)] ページに戻るかどうか尋ねられたときに [キャンセル (Cancel)] をクリックします。

**ステップ 3** [名前 (Name)] に一意の名前を入力します。

マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

**ステップ 4** 必要に応じて、[説明 (Description)] を入力します。

**ステップ 5** [基本ポリシー (Base Policy)] で最初の基本ポリシーを選択します。システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

**ステップ 6** プリプロセッサがインライン導入でのトラフィックに影響するようにする場合は、[インラインモード (Inline Mode)] を有効化します。

**ステップ 7** ポリシーを作成します。

- 新しいポリシーを作成して [ネットワーク分析ポリシー (Network Analysis Policy)] ページに戻るには、[ポリシーの作成 (Create Policy)] をクリックします。新しいポリシーには基本ポリシーと同じ設定項目が含まれています。
- ポリシーを作成し、高度なネットワーク分析ポリシーエディタでそれを開いて編集するには、[ポリシーの作成と編集 (Create and Edit Policy)] をクリックします。

## 関連トピック

[カスタム ユーザ ロールの作成 \(79 ページ\)](#)

## ネットワーク分析ポリシーの管理

[ネットワーク分析ポリシー (Network Analysis Policy)] ページ ([ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。、または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。) で、現在のカスタム ネットワーク分析ポリシーを次の情報とともに確認できます。

- ポリシーが最後に変更された日時 (ローカル時間) とそれを変更したユーザ

- プリプロセッサがトラフィックに影響を与えることを許可する [インラインモード (Inline Mode) ] 設定が有効になっているかどうか
- どのアクセス コントロール ポリシーとデバイスが、ネットワーク分析ポリシーを使用してトラフィックを前処理しているか
- ポリシーに保存されていない変更があるかどうか、およびポリシーを現在編集している人 (いれば) に関する情報

お客様が独自に作成するカスタム ポリシーに加えて、システムは初期インライン ポリシーと初期パッシブポリシーの2つのカスタムポリシーを提供しています。これら2つのネットワーク分析ポリシーは、基本ポリシーとして「Balanced Security and Connectivity」ネットワーク分析ポリシーを使用します。両者の唯一の相違点はインラインモードの設定です。インラインポリシーではプリプロセッサによるトラフィックの影響が有効化され、パッシブポリシーでは無効化されています。これらのシステム付属のカスタム ポリシーは編集して使用できます。

ただし、Firepowerシステムのユーザアカウントの権限が侵入ポリシーまたは修正侵入ポリシーに限定されている場合は、ネットワーク分析ポリシーに加えて、侵入ポリシーを作成して編集できます。

#### 関連トピック

[カスタム ネットワーク分析ポリシーの作成](#) (1847 ページ)

[ネットワーク分析ポリシーの編集](#) (1850 ページ)

## ネットワーク分析ポリシーの設定とキャッシュされた変更

新しいネットワーク分析ポリシーを作成すると、そのポリシーには基本ポリシーと同じ設定が付与されます。

ネットワーク分析ポリシーの調整時、特にプリプロセッサを無効化するときは、プリプロセッサおよび侵入ルールによっては、トラフィックを特定の方法で最初にデコードまたは前処理する必要がありますことに留意してください。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーのWebインターフェイスではプリプロセッサは無効のままになります。



- (注) 前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度なタスク**です。

システムは、ユーザごとに1つのネットワーク分析ポリシーをキャッシュします。ネットワーク分析ポリシーの編集中に、任意のメニューまたは別のページへの他のパスを選択した場合、変更内容はそのページを離れてもシステム キャッシュにとどまります。

#### 関連トピック

[ポリシーが侵入についてトラフィックを検査する仕組み](#) (1572 ページ)

[カスタム ポリシーの制限](#) (1583 ページ)

## ネットワーク分析ポリシーの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 設定するネットワーク分析ポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ネットワーク分析ポリシーを編集します。

- 基本ポリシーの変更：基本ポリシーを変更するには、[ポリシー情報 (Policy Information)] ページの [基本ポリシー (Base Policy)] ドロップダウンリストから、ポリシーを選択します。
- ポリシー階層の管理：ポリシー階層を管理するには、ナビゲーションパネルで [ポリシー層 (Policy Layers)] をクリックします。
- プリプロセッサの変更：プリプロセッサの設定有効または無効にするか、あるいは編集するには、ナビゲーションパネルで [設定 (Settings)] をクリックします。
- トラフィックの変更：プリプロセッサがトラフィックを変更またはドロップできるようにするには、[ポリシー情報 (Policy Information)] ページで [インラインモード (Inline Mode)] チェックボックスをオンにします。
- 設定の表示：基本ポリシーの設定を表示するには、[ポリシー情報 (Policy Information)] ページで [基本ポリシーの管理 (Manage Base Policy)] をクリックします。

**ステップ 4** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] を選択して、[変更を確定 (Commit Changes)] をクリックします。変更を確定せ



ずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

### 次のタスク

- プリプロセッサでイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、プリプロセッサのルールを有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

- [基本レイヤ \(1592 ページ\)](#)
- [ベースポリシーの変更 \(1595 ページ\)](#)
- [ネットワーク分析ポリシーでのプリプロセッサの設定 \(1851 ページ\)](#)
- [インライン導入でのプリプロセッサによるトラフィックの変更 \(1852 ページ\)](#)
- [レイヤの管理 \(1599 ページ\)](#)
- [競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## ネットワーク分析ポリシーでのプリプロセッサの設定

プリプロセッサは、トラフィックを正規化し、プロトコルの異常を識別することで、トラフィックの詳細な検査に備えます。プリプロセッサは、ユーザが設定したプリプロセッサオプションをパケットがトリガーしたときに、プリプロセッサイベントを生成できます。デフォルトで有効になるプリプロセッサや、それぞれのデフォルト設定は、ネットワーク分析ポリシーの基本ポリシーに応じて決まります。



- (注) 多くの場合、プリプロセッサの設定には特定の専門知識が必要で、通常は、ほとんどあるいはまったく変更を必要としません。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度なタスク**です。前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。

プリプロセッサの設定を変更するには、その設定とネットワークへの潜在的影響を理解する必要があります。

トランスポート/ネットワークプリプロセッサの詳細設定は、アクセスコントロールポリシーを展開するすべてのネットワーク、ゾーン、VLANにグローバルに適用されることに注意してください。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセスコントロールポリシーで設定します。

また、侵入ポリシーではASCIIテキストのクレジットカード番号や社会保障番号などの機密データを検出する機密データプリプロセッサを設定することにも注意してください。

## 関連トピック

- [DCE/RPC プリプロセッサ \(1856 ページ\)](#)
- [DNP3 プリプロセッサ \(1942 ページ\)](#)
- [DNS プリプロセッサ \(1869 ページ\)](#)
- [FTP/Telnet デコーダ \(1874 ページ\)](#)
- [GTP プリプロセッサ \(1910 ページ\)](#)
- [HTTP Inspect プリプロセッサ \(1883 ページ\)](#)
- [IMAP プリプロセッサ \(1912 ページ\)](#)
- [インライン正規化プリプロセッサ \(1951 ページ\)](#)
- [IP 最適化プリプロセッサ \(1960 ページ\)](#)
- [Modbus プリプロセッサ \(1939 ページ\)](#)
- [パケット デコーダ \(1966 ページ\)](#)
- [POP プリプロセッサ \(1916 ページ\)](#)
- [機密データ検出の基本 \(1661 ページ\)](#)
- [SIP プリプロセッサ \(1904 ページ\)](#)
- [SMTP プリプロセッサ \(1920 ページ\)](#)
- [SSH プリプロセッサ \(1927 ページ\)](#)
- [SSL プリプロセッサ \(1932 ページ\)](#)
- [Sun RPC プリプロセッサ \(1902 ページ\)](#)
- [TCP ストリームの前処理 \(1971 ページ\)](#)
- [UDP ストリームの前処理 \(1985 ページ\)](#)
- [カスタム ポリシーの制限 \(1583 ページ\)](#)

## インライン導入でのプリプロセッサによるトラフィックの変更

インライン導入（つまり、ルーテッド インターフェイス、スイッチド インターフェイス、トランスペアレント インターフェイス、あるいはインライン インターフェイスのペアを使用して関連する設定をデバイスに展開する導入）では、一部のプリプロセッサがトラフィックを変更およびブロックできます。次に例を示します。

- インライン正規化プリプロセッサは、パケットを正規化し、他のプリプロセッサおよび侵入ルールエンジンで分析されるようにパケットを準備します。ユーザは、プリプロセッサの [これらの TCP オプションを許可 (Allow These TCP Options) ] と [回復不能な TCP ヘッダーの異常をブロック (Block Unresolvable TCP Header Anomalies) ] オプションを使用して、特定のパケットをブロックすることもできます。
- システムは無効なチェックサムを持つパケットをドロップできます。
- システムはレート ベースの攻撃防御設定に一致するパケットをドロップできます。

ネットワーク分析ポリシーに設定したプリプロセッサがトラフィックに影響を与えるようにするには、プリプロセッサを有効にして正しく設定するとともに、管理対象デバイスをインラインで正しく展開する必要があります。最後に、ネットワーク分析ポリシーの [インライン モード (Inline Mode) ] 設定を有効にする必要があります。

## ネットワーク分析ポリシーの注記におけるプリプロセッサの設定

ネットワーク分析ポリシーのナビゲーション パネルで [設定 (Settings)] を選択すると、ポリシーによりタイプ別のプリプロセッサがリストされます。[設定 (Settings)] ページで、ネットワーク分析ポリシーのプリプロセッサを有効または無効にしたり、プリプロセッサの設定ページにアクセスしたりできます。

プリプロセッサを設定するには、それを有効にする必要があります。プリプロセッサを有効にすると、そのプリプロセッサに関する設定ページへのサブリンクがナビゲーションパネル内の [設定 (Settings)] リンクの下に表示され、この設定ページへの [編集 (Edit)] リンクが [設定 (Settings)] ページのプリプロセッサの横に表示されます。



**ヒント** プリプロセッサの設定を基本ポリシーの設定に戻すには、プリプロセッサ設定ページで [デフォルトに戻す (Revert to Defaults)] をクリックします。プロンプトが表示されたら、復元することを確認します。

プリプロセッサを無効にすると、サブリンクと [編集 (Edit)] リンクは表示されなくなります。設定は保持されます。特定の分析を実行するには、多くのプリプロセッサおよび侵入ルールで、トラフィックをまず特定の方法でデコードまたは前処理する必要があることに注意してください。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

実際にトラフィックを変更せずに、設定がインライン展開でどのように機能するかを評価する場合は、インラインモードを無効にできます。タップモードでのパッシブ展開またはインライン展開では、インラインモード設定に関係なくシステムがトラフィックに影響を及ぼすことはありません。



**(注)** インラインモードを無効にすることで、侵入イベントのパフォーマンス統計グラフに影響を及ぼす可能性があります。インライン展開でインラインモードが有効の場合、侵入イベントパフォーマンス ページ ([概要 (Overview)] > [概要 (Summary)] > [侵入イベントパフォーマンス (Intrusion Event Performance)]) には、正規化し、ブロックされたパケットを示すグラフが表示されます。インラインモードが無効の場合、またはパッシブ展開である場合、多くのグラフによりシステムが正規化するか、またはドロップするトラフィックに関するデータが表示されます。



**(注)** インライン展開では、インラインモードを有効にし、[TCP ペイロードの正規化 (Normalize TCP Payload)] オプションを有効にして、インライン正規化プリプロセッサを設定することをお勧めします。パッシブ展開では、アダプティブプロファイルの更新を使用することをお勧めします。

### 関連トピック

[トランスポート/ネットワーク プリプロセッサの詳細設定](#) (1946 ページ)

[チェックサム検証](#) (1949 ページ)

[インライン正規化プリプロセッサ](#) (1951 ページ)

[侵入イベントのパフォーマンス統計情報グラフの種類](#) (2604 ページ)



## 第 79 章

# アプリケーション層プリプロセッサ

次のトピックでは、アプリケーション層プリプロセッサおよびその設定方法について説明します。

- [アプリケーション層のプリプロセッサの概要 \(1855 ページ\)](#)
- [DCE/RPC プリプロセッサ \(1856 ページ\)](#)
- [DNS プリプロセッサ \(1869 ページ\)](#)
- [FTP/Telnet デコーダ \(1874 ページ\)](#)
- [HTTP Inspect プリプロセッサ \(1883 ページ\)](#)
- [Sun RPC プリプロセッサ \(1902 ページ\)](#)
- [SIP プリプロセッサ \(1904 ページ\)](#)
- [GTP プリプロセッサ \(1910 ページ\)](#)
- [IMAP プリプロセッサ \(1912 ページ\)](#)
- [POP プリプロセッサ \(1916 ページ\)](#)
- [SMTP プリプロセッサ \(1920 ページ\)](#)
- [SSH プリプロセッサ \(1927 ページ\)](#)
- [SSL プリプロセッサ \(1932 ページ\)](#)

## アプリケーション層のプリプロセッサの概要

アプリケーション層プロトコルにより、同一データをさまざまな方法で表すことができます。Firepower システムは、特定タイプのパケットデータを侵入ルールエンジンが分析可能なフォーマットに正規化する、アプリケーション層プロトコルデコーダを提供しています。アプリケーション層プロトコルエンコードを正規化することにより、ルールエンジンでさまざまなデータ形式のパケットに同じコンテンツ関連ルールを効果的に適用し、有意な結果を得ることができます。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。

ほとんどの場合、侵入ルールで関連するプリプロセッサルールが有効になっていないと、プリプロセッサはイベントを生成しません。

## DCE/RPC プリプロセッサ

DCE/RPC プロトコルにより、別々のネットワーク ホスト上のプロセスが、同一ホストに配置されている場合と同様に通信できます。通常、このようなプロセス間通信はホスト間で TCP および UDP 経由で転送されます。TCP 転送では、DCE/RPC が Windows Server Message Block (SMB) プロトコルまたは Samba でさらにカプセル化されることがあります。Samba は、Windows や UNIX/Linux 系のオペレーティングシステムから構成される混合環境でプロセス間通信に使用されるオープンソースの SMB 実装です。また、ネットワーク上の Windows IIS Web サーバでは IIS RPC over HTTP が使用されることがあります。IIS RPC over HTTP は、プロキシ TCP により伝送される DCE/RPC トラフィックに、ファイアウォールを介して分散通信を提供します。

DCE/RPC プリプロセッサ オプションとその機能の説明には、Microsoft による DCE/RPC の実装である MSRPC が含まれることに注意してください。SMB のオプションと機能についての説明は、SMB と Samba の両方に当てはまります。

ほとんどの DCE/RPC エクスプロイトは、DCE/RPC サーバ（ネットワーク上の Windows または Samba が稼働している任意のホスト）を対象とした DCE/RPC クライアント要求で発生します。またエクスプロイトはサーバ応答でも発生することがあります。DCE/RPC プリプロセッサは、TCP、UDP、および SMB トランスポートでカプセル化された DCE/RPC 要求と応答を検出します。これには、RPC over HTTP バージョン 1 を使用して TCP により伝送される DCE/RPC も含まれます。プリプロセッサは DCE/RPC データストリームを分析し、DCE/RPC トラフィックにおける異常な動作と回避技術を検出します。また、SMB データストリームを分析し、異常な SMB 動作と回避技術を検出します。

IP 最適化プリプロセッサによる IP 最適化および TCP ストリーム プリプロセッサによる TCP ストリームの再構成に加えて、DCE/RPC プリプロセッサは、SMB のセグメント化解除と DCE/RPC の最適化も行います。

最後に、DCE/RPC プリプロセッサはルールエンジンで処理できるように DCE/RPC トラフィックを正規化します。

## コネクションレス型およびコネクション型 DCE/RPC トラフィック

DCE/RPC メッセージは、2 種類の DCE/RPC Protocol Data Unit (PDU) の 1 つに準拠します。

### コネクション型 DCE/RPC PDU プロトコル

DCE/RPC プリプロセッサは、TCP、SMB、および RPC over HTTP トランスポートでコネクション型 DCE/RPC を検出します。

### コネクションレス型 DCE/RPC PDU プロトコル

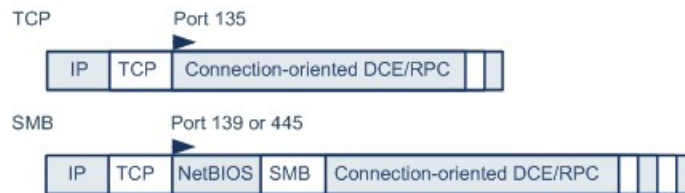
DCE/RPC プリプロセッサは、UDP トランスポートでコネクションレス型 DCE/RPC を検出します。

この 2 つの DCE/RPC PDU プロトコルには、それぞれ固有のヘッダーとデータ特性があります。たとえば、コネクション型 DCE/RPC のヘッダーの長さは通常は 24 バイトですが、コネク

コネクションレス型 DCE/RPC のヘッダーの長さは 80 バイト（固定）です。また、フラグメント化コネクションレス型 DCE/RPC のフラグメントの正しい順序は、コネクションレス型トランスポートでは処理できないため、代わりに、コネクションレス型 DCE/RPC ヘッダーの値によって維持する必要があります。これとは対照的に、コネクション型 DCE/RPC の正しいフラグメント順序はトランスポートプロトコルによって維持されます。DCE/RPC プリプロセッサは、これらや他のプロトコル固有の特性を使用して、両方のプロトコルで異常やその他の回避技術をモニタし、トラフィックをデコードおよび復号化してからルールエンジンに渡します。

次の図は、DCE/RPC プリプロセッサが各種トランスポートの DCE/RPC トラフィックの処理を開始するポイントを示します。

#### Connection-oriented DCE/RPC



#### Connectionless DCE/RPC



▶ = DCE/RPC preprocessor starts decoding

371939

この図の次の点に注意してください。

- ウェルノウン TCP または UDP ポート 135 は、TCP および UDP トランスポートの DCE/RPC トラフィックを特定します。
- この図には RPC over HTTP は含まれていません。

RPC over HTTP の場合、コネクション型 DCE/RPC は、図に示すように、HTTP を介した初期設定シーケンスの後、TCP 経由で直接伝送されます。

- DCE/RPC プリプロセッサは通常、NetBIOS セッション サービス用のウェルノウン TCP ポート 139 か、同様に実装されたウェルノウン Windows ポート 445 で SMB トラフィックを受信します。

SMB には DCE/RPC 伝送以外にも多数の機能があるため、プリプロセッサは SMB トラフィックが DCE/RPC トラフィックを伝送しているかどうかをまず検査します。伝送していない場合は処理を停止し、伝送している場合は処理を続行します。

- IP によりすべての DCE/RPC トランスポートがカプセル化されます。
- TCP は、すべてのコネクション型 DCE/RPC を伝送します。
- UDP はコネクションレス型 DCE/RPC を伝送します。

## DCE/RPC ターゲットベース ポリシー

Windows および Samba の DCE/RPC の実装は大きく異なります。たとえば、Windows のすべてのバージョンは、DCE/RPC トラフィックの最適化時に最初のフラグメントの DCE/RPC コンテキスト ID を使用しますが、Samba のすべてのバージョンは、最後のフラグメントのコンテキスト ID を使用します。また、特定の関数呼び出しを識別するために、Windows Vista では最初のフラグメントの `opnum` (操作番号) ヘッダーフィールドを使用しますが、Samba とその他のすべてのバージョンの Windows では最後のフラグメントの `opnum` フィールドを使用します。

Windows と Samba の SMB の実装にも、大きな違いがあります。たとえば、Windows は名前付きパイプの操作時に `SMB OPEN` および `READ` コマンドを認識しますが、Samba はこれらのコマンドを認識しません。

DCE/RPC プリプロセッサを有効にすると、デフォルトのターゲットベース ポリシーが自動的に有効になります。必要に応じて、異なる Windows や Samba バージョンを実行する他のホストを対象としたターゲットベース ポリシーを追加できます。デフォルトのターゲットベース ポリシーは、別のターゲットベース ポリシーに含まれていないホストに適用されます。

各ターゲットベースのポリシーでは次の設定が可能です。

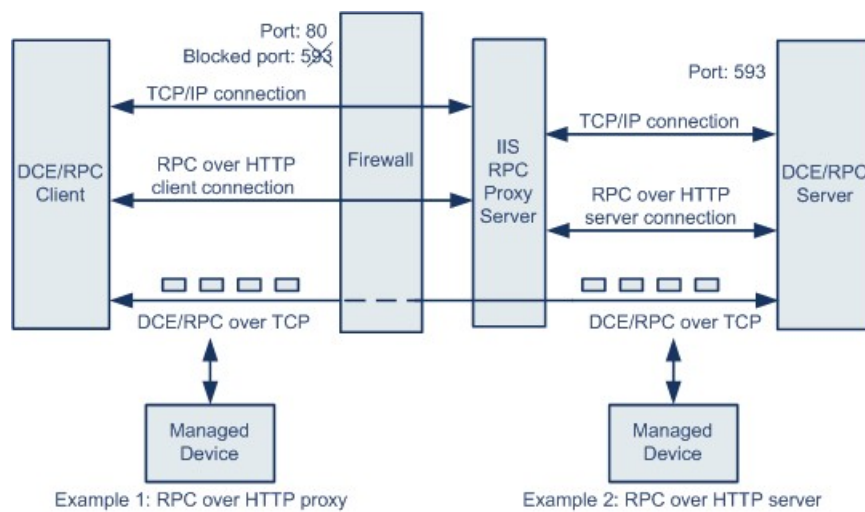
- 1 つ以上のポートを有効にし、それぞれについて検出ポートを指定します。
- 自動検出ポートを有効にして指定します。
- 指定した 1 つ以上の共有 SMB リソースへの接続が試行された場合にそのことを検出するように、プリプロセッサを設定します。
- SMB トラフィックでファイルを検出し、検出されたファイルで指定されたバイト数を検査するように、プリプロセッサを設定します。
- SMB プロトコルの知識を持つユーザだけが変更すべき拡張オプションを変更できます。このオプションでは、連結された `SMB AndX` コマンドの数が指定された最大数を超えた場合にそのことを検出するようにプリプロセッサを設定します。

DCE/RPC プリプロセッサで SMB トラフィック ファイル検出を有効にするほかに、オプションでこれらのファイルをキャプチャしてブロックするか、またはダイナミック分析のために Cisco AMP クラウドに送信するように、ファイルポリシーを設定できます。そのポリシー内で、[アクション (Action)] として [ファイル検出 (Detect Files)] または [ファイルブロック (Block Files)] を選択し、[アプリケーションプロトコル (Application Protocol)] として [任意 (Any)] または [NetBIOS-ssn (SMB)] を選択して、ファイルルールを作成する必要があります。

## RPC over HTTP トランスポート

Microsoft RPC over HTTP では、次の図に示すように、DCE/RPC トラフィックをトンネリングして、ファイアウォールを通過させることができます。DCE/RPC プリプロセッサは Microsoft RPC over HTTP バージョン 1 を検出します。





Microsoft IIS プロキシサーバと DCE/RPC サーバは、同じホストまたは別々のホストにインストールできます。いずれの場合でも、個別のプロキシオプションとサーバオプションがあります。この図の次の点に注意してください。

- DCE/RPC サーバはポート 593 で DCE/RPC クライアントトラフィックをモニタしますが、ファイアウォールはこのポート 593 をブロックします。  
通常、ファイアウォールではデフォルトでポート 593 がブロックされます。
- RPC over HTTP は、ファイアウォールによって許可される可能性が高いウェルノウン HTTP ポート 80 を使用して、HTTP 経由で DCE/RPC を伝送します。
- 例 1 のように、DCE/RPC クライアントと Microsoft IIS RPC プロキシサーバの間のトラフィックをモニタする場合は、[RPC over HTTP プロキシ (RPC over HTTP proxy)] オプションを選択します。
- 例 2 のように、Microsoft IIS RPC プロキシサーバと DCE/RPC サーバが異なるホスト上にあり、デバイスが2つのサーバ間のトラフィックをモニタしている場合は、[RPC over HTTP サーバ (RPC over HTTP server)] オプションを選択します。
- RPC over HTTP により DCE/RPC クライアントとサーバ間でのプロキシセットアップが完了した後、トラフィックは TCP を経由したコネクション型 DCE/RPC だけで構成されます。

## DCE/RPC グローバル オプション

グローバル DCE/RPC プリプロセッサオプションは、プリプロセッサの機能を制御します。[到達したメモリ容量 (Memory Cap Reached)] および [SMB セッションの自動検出ポリシー (Auto-Detect Policy on SMB Session)] オプション以外のオプションを変更すると、パフォーマンスまたは検出機能に悪影響を及ぼす可能性があります。プリプロセッサについて、またプリプロセッサと有効にされている DCE/RPC ルールとの間の相互作用について十分に理解していない場合は、これらのオプションを変更しないでください。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

### 最大フラグメント サイズ (Maximum Fragment Size)

[最適化の有効化 (Enable Defragmentation)] が選択されている場合、DCE/RPC フラグメントの許容最大長を指定します。これよりも大きなフラグメントの場合、プリプロセッサは処理のためにフラグメントの一部を切り捨て、指定のサイズにしてから最適化を行いますが、実際のパケットは変更されません。空白フィールドの場合、このオプションは無効になります。

[最大フラグメント サイズ (Maximum Fragment Size)] オプションは、ルールが検出する必要がある深さと同じかそれ以上にしてください。

### リアセンブリしきい値 (Reassembly Threshold)

[最適化の有効化 (Enable Defragmentation)] が選択されている場合、0 を指定するとこのオプションは無効になります。あるいは、フラグメント化された DCE/RPC の最小バイト数を、該当する場合は、再構成されたパケットをルールエンジンに送信する前にキューに入れるセグメント化 SMB のバイト数を指定します。低い値を指定すると、早期検出の可能性が高くなりますが、パフォーマンスに悪影響を及ぼす可能性があります。このオプションを有効にする場合は、パフォーマンスの影響をテストしておく必要があります。

[リアセンブリしきい値 (Reassembly Threshold)] オプションは、ルールが検出する必要がある深さと同じかそれ以上にしてください。

### 最適化の有効化 (Enable Defragmentation)

フラグメント化された DCE/RPC トラフィックを最適化するかどうかを指定します。無効にすると、プリプロセッサは引き続き異常を検出して DCE/RPC データをルールエンジンに送信しますが、フラグメント化された DCE/RPC データでのエクスプロイトを見落とすリスクがあります。

このオプションには、DCE/RPC トラフィックを最適化しないという柔軟性がありますが、ほとんどの DCE/RPC エクスプロイトでは、フラグメント化を利用してエクスプロイトを隠ぺいする試みが行われます。このオプションを無効にすると、ほとんどの既知のエクスプロイトがバイパスされ、検出漏れが大量に発生します。

### 到達したメモリ容量 (Memory Cap Reached)

プリプロセッサに割り当てられた最大メモリ制限に達したか、またはこの制限を超過したことを検出します。最大メモリ制限に達したか、またはこの制限を超過した場合、プリプロセッサはメモリキャップイベントを引き起こしたセッションに関連付けられているすべての保留データを解放し、セッションのそれ以降の部分を見捨てます。

ルール 133:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

### SMB セッションの自動検出ポリシー (Auto-Detect Policy on SMB Session)

SMB Session Setup AndX 要求および応答に指定されている Windows または Samba のバージョンを検出します。検出されたバージョンが、[ポリシー (Policy)] 設定オプションで設定されている Windows または Samba のバージョンと異なる場合、そのセッションに限り、検出されたバージョンが設定バージョンをオーバーライドします。

たとえば、[ポリシー (Policy)] に Windows XP を設定した場合に、プリプロセッサが Windows Vista を検出すると、プリプロセッサはそのセッションでは Windows Vista ポリシーを使用します。その他の設定は引き続き有効です。

DCE/RPC トランスポートが SMB ではない場合は (トランスポートが TCP または UDP の場合)、バージョンを検出できず、ポリシーを自動的に設定できません。

このオプションを有効にするには、ドロップダウン リストで次のいずれかを選択します。

- サーバ/クライアント トラフィックでポリシー タイプを検査するには、[クライアント (Client)] を選択します。
- クライアント/サーバ トラフィックでポリシー タイプを検査するには、[サーバ (Server)] を選択します。
- サーバ/クライアント トラフィックとクライアント/サーバ トラフィックの両方でポリシー タイプを検査するには、[両方 (Both)] を選択します。

### レガシー SMB 検査モード (Legacy SMB Inspection Mode)

検査する SMB バージョンを指定します。[レガシー SMB 検査モード (Legacy SMB Inspection Mode)] が有効になっている場合、DCE/RPC プリプロセッサは、SMB バージョン 1 のトラフィックのみを検査します。このオプションを無効にすると、DCE/RPC プリプロセッサは、SMB バージョン 1、2、および 3 を使用するトラフィックを調査します。

#### 関連トピック

[基本コンテンツおよび protected\\_content キーワードの引数 \(1714 ページ\)](#)

概要 : [byte\\_jump](#) および [byte\\_test](#) キーワード

## DCE/RPC ターゲットベース ポリシー オプション

各ターゲットベース ポリシーでは、TCP、UDP、SMB、および RPC over HTTP トランスポートのうち1つ以上を有効にできます。トランスポートを有効にする場合は、1つ以上の検出ポート (DCE/RPC トラフィックを伝送することがわかっているポート) を指定する必要があります。

シスコでは、デフォルトの検出ポート (ウェルノウンポートまたは各プロトコルで一般に使用されているポート) を使用することを推奨しています。検出ポートを追加するのは、デフォルト以外のポートで DCE/RPC トラフィックを検出した場合だけです。

Windows のターゲットベース ポリシーでは、ネットワークのトラフィックに一致するように、1つ以上の任意のトランスポートのポートを任意の組み合わせで指定できます。しかし、Samba のターゲットベース ポリシーでは SMB トランスポートのポートだけを指定できます。



- (注) 少なくとも1つのトランスポートが有効になっている DCE/RPC ターゲットベース ポリシーを追加した場合を除き、デフォルトのターゲットベースポリシーでは少なくとも1つの DCE/RPC トランスポートを有効にする必要があります。たとえば、すべての DCE/RPC 実装に対してホストを指定し、未指定のホストにはデフォルトのターゲットベースポリシーを展開したくない場合があります。そのような場合は、デフォルトのターゲットベースポリシーのトランスポートを有効化しないようにします。

(任意) 自動検出ポートを有効にして指定できます。プリプロセッサは、自動検出ポートとして指定されたポートを最初にテストして、そのポートが DCE/RPC トラフィックを伝送しているかどうかを判別し、DCE/RPC トラフィックを検出した場合にのみ処理を続行します。

自動検出ポートを有効にする場合は、エフェメラルポート範囲全体に対応するよう、自動検出ポートが 1025 から 65535 の範囲に設定されていることを確認してください。

自動検出は、トランスポート検出ポートによって識別されていないポートでのみ発生する点にも注意してください。

[RPC over HTTP プロキシ自動検出ポート (RPC over HTTP Proxy Auto-Detect Ports)] オプションまたは [SMB 自動検出ポート (SMB Auto-Detect Ports)] オプションで自動検出ポートを有効にしたり指定したりすることはほとんどありません。これは、指定されているデフォルト検出ポートを除き、どちらの場合もトラフィックが発生することはほとんどなく、その見込みも少ないためです。

各ターゲットベースポリシーでは、次に示すさまざまなオプションを指定できます。以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

### ネットワーク

DCE/RPC ターゲットベースサーバポリシーを展開するホストの IP アドレス。また、ターゲットベースポリシーを追加する場合は、[ターゲットの追加 (Add Target)] ポップアップウィンドウの [サーバアドレス (Server Address)] フィールドに指定した名前。

単一の IP アドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。デフォルトポリシーを含め、合計で最大255個のプロファイルを設定できます。



- (注) システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

デフォルトポリシーの default 設定では、別のターゲットベースポリシーでカバーされていないモニタ対象ネットワークセグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルトポリシーの IP アドレスまたは CIDR ブロック/プレフィックス

クス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、anyを表すアドレス表記(0.0.0.0/0または::/0)を使用したりすることはできません。

## ポリシー

モニタ対象ネットワーク セグメントのターゲット ホストが使用する Windows または Samba DCE/RPC の実装。

[SMB セッションの自動検出ポリシー (Auto-Detect Policy on SMB Session)] グローバル オプションを有効にすると、SMB が DCE/RPC トランスポートの場合に、このオプションの設定をセッションごとに自動的にオーバーライドできます。

## SMB の無効な共有 (SMB Invalid Shares)

指定した共有リソースへの接続が試行されると、プリプロセッサが検出する 1 つ以上の SMB 共有リソースを識別します。複数の共有をカンマで区切って指定できます。また必要に応じて、共有を引用符で囲むこともできます。これは、以前のソフトウェアバージョンでは必須でしたが、現在は必須ではありません。次に例を示します。

```
"C$", D$, "admin", private
```

[SMB ポート (SMB Ports)] が有効に設定されている場合、プリプロセッサは SMB トラフィックで無効な共有を検出します。

ほとんどの場合、Windows により名前が指定されたドライブを無効な共有として指定するには、このドライブにドル記号を付加する必要があることに注意してください。たとえば、ドライブ C は C\$ または "C\$" として指定します。

SMB の無効な共有を検出するには、[SMB ポート (SMB Ports)] か、[SMB 自動検出ポート (SMB Auto-Detect Ports)] を有効にする必要があることにも注意してください。

ルール 133:26 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

## SMB 最大 AndX チェーン (SMB Maximum AndX Chain)

連結された SMB AndX コマンドの許容最大数です。通常、多数の連結 AndX コマンドは異常な動作を表し、場合によっては回避試行を示している可能性があります。連結コマンドを許可しない場合は 1 を指定し、連結コマンドの数の検出を無効にするには 0 を指定します。

プリプロセッサは最初に連結コマンドの数をカウントし、関連する SMB プリプロセッサルールが有効であり、連結コマンドの数が設定されている値と等しいかそれ以上の場合にはイベントを生成することに注意してください。その後、処理が続行されます。



**注意** SMB プロトコルに詳しいユーザだけが [SMB AndX の最大チェーン (SMB Maximum AndX Chains)] オプションのデフォルト設定を変更するようにしてください。

ルール 133:20 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。 [侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

### RPC プロキシ トラフィックのみ (RPC proxy traffic only)

[RPC over HTTP プロキシ ポート (RPC over HTTP Proxy Ports) ] が有効である場合、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみであるか、または他の Web サーバ トラフィックを含んでいる可能性があるかどうかを示します。たとえば、ポート 80 はプロキシ トラフィックとその他の Web サーバ トラフィックの両方を伝送する可能性があります。

このオプションが無効になっている場合は、プロキシ トラフィックとその他の Web サーバ トラフィックの両方が想定されます。たとえばサーバが専用プロキシサーバである場合などに、このオプションを有効にします。有効にすると、プリプロセッサはトラフィックを調べて DCE/RPC を伝送しているかどうかを判別し、伝送していない場合はそのトラフィックを無視し、伝送している場合は処理を続行します。このオプションを有効にすることで機能が追加されるのは、[RPC over HTTP プロキシ ポート (RPC over HTTP Proxy Ports) ] チェック ボックスも有効にされている場合だけであることに注意してください。

### RPC over HTTP プロキシ ポート (RPC over HTTP Proxy Ports)

管理対象デバイスが DCE/RPC クライアントと Microsoft IIS RPC プロキシサーバの間に配置されている場合に、指定の各ポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの検出を有効にします。

有効である場合、DCE/RPC トラフィックが確認されるポートを追加できますが、Web サーバは一般に DCE/RPC トラフィックとその他のトラフィックの両方にデフォルト ポートを使用するため、この操作が必要になることはあまりありません。有効である場合、[RPC over HTTP プロキシ自動検出ポート (RPC over HTTP Proxy Auto-Detect Ports) ] は有効にしますが、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみであり、その他の Web サーバ トラフィックを含んでいない場合は、[RPC プロキシ トラフィックのみ (RPC Proxy Traffic Only) ] を有効にします。



(注) このオプションを選択することがあるとすれば、きわめて稀なケースです。

### RPC over HTTP サーバ ポート (RPC over HTTP Server Ports)

Microsoft IIS RPC プロキシサーバと DCE/RPC サーバが異なるホスト上に配置されており、デバイスがこの2つのサーバ間のトラフィックをモニタしている場合、指定の各ポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの検出を有効にします。

一般に、このオプションを有効にするときは、ネットワーク上のプロキシ Web サーバに注意を払わない場合でも、1025 ~ 65535 のポート範囲で [RPC over HTTP サーバ自動検出ポート (RPC over HTTP Server Auto-Detect Ports) ] も有効にする必要があります。場合によっては

RPC over HTTP サーバポートを再設定することがあり、その際には再設定したサーバポートをこのオプションのポートリストに追加する必要があることに注意してください。

### TCP ポート (TCP Ports)

指定の各ポートでの TCP の DCE/RPC トラフィックの検出を有効にします。

正当な DCE/RPC トラフィックとエクスプロイトは、さまざまなポートを使用する可能性があります。ポート 1024 より大きい番号のポートが一般的です。通常、このオプションを有効にする場合は、1025 ~ 65535 のポート範囲で [TCP 自動検出ポート (TCP Auto-Detect Ports)] も有効にする必要があります。

### UDP ポート

指定の各ポートでの UDP の DCE/RPC トラフィックの検出を有効にします。

正当な DCE/RPC トラフィックとエクスプロイトは、さまざまなポートを使用する可能性があります。ポート 1024 より大きい番号のポートが一般的です。通常、このオプションを有効にする場合は、1025 ~ 65535 のポート範囲で [UDP 自動検出ポート (UDP Auto-Detect Ports)] も有効にする必要があります。

### SMB ポート (SMB Ports)

指定の各ポートでの SMB の DCE/RPC トラフィックの検出を有効にします。

デフォルトの検出ポートを使用した SMB トラフィックが発生することがあります。他のポートはほとんどありません。通常はデフォルト設定を使用してください。

[SMB セッションの自動検出ポリシー (Auto-Detect Policy on SMB Session)] グローバル オプションを有効にすると、SMB が DCE/RPC トラnsポートの場合に、ターゲットポリシーに対して設定されているポリシータイプをセッションごとに自動的にオーバーライドできます。

### RPC over HTTP プロキシ自動検出ポート (RPC over HTTP Proxy Auto-Detect Ports)

管理対象デバイスが DCE/RPC クライアントと Microsoft IIS RPC プロキシサーバの間に配置されている場合に、指定のポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの自動検出を有効にします。

有効である場合は、一時ポート範囲全体をカバーするため、一般にポート範囲として 1025 から 65535 を指定します。

### RPC over HTTP サーバ自動検出ポート (RPC over HTTP Server Auto-Detect Ports)

Microsoft IIS RPC プロキシサーバおよび DCE/RPC サーバが異なるホスト上に配置されており、デバイスがこの 2 つのサーバ間のトラフィックをモニタしている場合、指定のポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの自動検出を有効にします。

### TCP 自動検出ポート (TCP Auto-Detect Ports)

指定のポートで TCP の DCE/RPC トラフィックの自動検出を有効にします。

### UDP 自動検出ポート (UDP Auto-Detect Ports)

指定の各ポートで UDP の DCE/RPC トラフィックの自動検出を有効にします。

### SMB 自動検出ポート (SMB Auto-Detect Ports)

SMB の DCE/RPC トラフィックの検出を有効にします。



(注) このオプションを選択することがあるとすれば、きわめて稀なケースです。

### SMB ファイル インспекション (SMB File Inspection)

ファイル検出のための SMB トラフィックのインспекションを有効にします。次の選択肢があります。

- ファイル インспекションを無効にするには、[オフ (Off)] を選択します。
- SMB でファイルデータを検査するが、DCE/RPC トラフィックは検査しない場合は、[ファイルのみ (Only)] を選択します。このオプションを選択すると、ファイルと DCE/RPC トラフィックの両方を検査する場合よりもパフォーマンスが向上する可能性があります。
- SMB でファイルと DCE/RPC トラフィックの両方を検査するには、[オン (On)] を選択します。このオプションを選択すると、パフォーマンスに影響する可能性があります。

SMB トラフィックでの次のファイルについてのインспекションはサポートされていません。

- このオプションを有効にしてポリシーを適用する前に確立された TCP または SMB セッションで転送されたファイル
- 1 つの TCP または SMB セッションで同時に転送されたファイル
- 複数の TCP または SMB セッションにわたって転送されたファイル
- メッセージ署名のネゴシエート時など、非連続データを使用して転送されたファイル
- 同一オフセットに異なるデータが含まれており、データがオーバーラップしている転送ファイル
- リモートクライアントがファイルサーバに保存し、そのクライアントで編集用に開かれたファイル

### SMB ファイル インспекションの深さ (SMB File Inspection Depth)

[SMB ファイル インспекション (SMB File Inspection)] が [ファイルのみ (Only)] または [オン (On)] に設定されている場合に、SMB トラフィックでファイルが検出された時に検査されるデータのバイト数です。次のいずれかを指定します。

- 正の値
- 0 : ファイル全体を検査する場合



- -1 : ファイルインスペクションを無効にする場合

アクセスコントロールポリシーの [詳細 (Advanced)] タブの [ファイルおよびマルウェアの設定 (File and Malware Settings)] セクションで定義された値以下になるように、このフィールドに値を入力します。[ファイルタイプを検知する前に検閲するバイト数制限 (Limit the number of bytes inspected when doing file type detection)] で定義されている値よりも大きい値をこのオプションに設定すると、アクセスコントロールポリシーの設定が、有効な最大値として使用されます。

[SMB ファイルインスペクション (SMB File Inspection)] が [オフ (Off)] に設定されている場合、このフィールドは無効になります。

#### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## トラフィックに関連する DCE/RPC ルール

ほとんどの DCE/RPC プリプロセッサルールでは、SMB、コネクション型 DCE/RPC、またはコネクションレス型 DCE/RPC のトラフィックで検出される異常や検知回避技術に対してトリガーします。トラフィックタイプ別に有効にできるルールを次の表に示します。

表 190: トラフィックに関連する DCE/RPC ルール

トラフィック	プリプロセッサルール GID:SID
SMB	133:2 ~ 133:26、133:48 ~ 133:57
コネクション型 DCE/RPC	133:27 ~ 133:39
コネクションレス型 DCE/RPC の検出	133:40 ~ 133:43

## DCE/RPC プリプロセッサの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

DCE/RPC プリプロセッサを設定するには、プリプロセッサの機能を制御するグローバルオプションを変更するか、IP アドレスと稼働している Windows または Samba のバージョンによってネットワーク上の DCE/RPC サーバを識別する 1 つ以上のターゲットベースサーバポリシーを指定します。ターゲットベースポリシー構成では、トランスポートプロトコルの有効化、DCE/RPC トラフィックをホストに伝送するポートの指定、およびその他のサーバ固有オプションの設定も行います。

システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

### 始める前に

- カスタムターゲットベースのポリシーで指定するネットワークが一致しているか、または親のネットワーク分析ポリシーで処理されるネットワーク、ゾーン、および VLAN のサブセットであることを確認します。詳細については、[ネットワーク分析プロファイルの詳細設定 \(1840 ページ\)](#) を参照してください。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** 左側のナビゲーションパネルで [設定 (Settings)] をクリックします。

**ステップ 4** [アプリケーション層プリプロセッサ (Application Layer Preprocessors)] の下の [DCE/RPC の構成 (DCE/RPC Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [DCE/RPC の構成 (DCE/RPC Configuration)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [グローバル設定 (Global Settings)] セクションのオプションを変更します。[DCE/RPC グローバル オプション \(1859 ページ\)](#) を参照してください。

**ステップ 7** 次の選択肢があります。

- サーバプロファイルの追加：[サーバ (Servers)] の横にある追加アイコン (+) をクリックします。1 つ以上の IP アドレスを [サーバアドレス (Server Address)] フィールドに指定し、[OK] をクリックします。
- サーバプロファイルの削除：ポリシーの横にある削除アイコン (🗑️) をクリックします。
- サーバプロファイルの編集：[サーバ (Servers)] の下にあるプロファイルの設定済みアドレスをクリックするか、[デフォルト (default)] をクリックします。[設定 (Configuration)] セクションの設定を変更できます。[DCE/RPC ターゲットベース ポリシー オプション \(1861 ページ\)](#) を参照してください。

**ステップ 8** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

#### 次のタスク

- 侵入イベントを生成する場合は、DCE/RPC プリプロセッサルール (GID 132 または 133) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#)、[DCE/RPC グローバルオプション \(1859 ページ\)](#)、[DCE/RPC ターゲットベースポリシーオプション \(1861 ページ\)](#)、およびトラフィックに関連する [DCE/RPC ルール \(1867 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

[ファイルおよびマルウェアのインスペクションパフォーマンスとストレージのオプション \(1564 ページ\)](#)

[DCE/RPC キーワード \(1771 ページ\)](#)

[レイヤの管理 \(1599 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## DNS プリプロセッサ

DNS プリプロセッサは、DNS ネーム サーバ応答を検査し、次に示す特定の 익스プロイトがあるかどうかを確認します。

- RData テキスト フィールドに対するオーバーフローの試行
- 古い DNS リソース レコード タイプ
- 試験的な DNS リソース レコード タイプ

最も一般的なタイプの DNS ネーム サーバ応答には、応答を求めたクエリ内のドメイン名に対応する 1 つ以上の IP アドレスが示されています。その他のタイプのサーバ応答には、たとえば、電子メールメッセージの宛先や、元のクエリの対象のサーバからは取得できない情報を提供できるネーム サーバの位置などが記述されています。

DNS 応答には以下の構成要素があります。

- メッセージ ヘッダー
- 1 つ以上の要求が含まれる [質問 (Question)] セクション
- [質問 (Question)] セクションの要求に回答する 3 つのセクション

- 応答
- 権限 (Authority)
- その他の情報 (Additional Information)

この3セクションの応答には、ネームサーバに保持されているリソースレコード (RR) の情報が反映されます。次の表で、これらの3つのセクションについて説明します。

表 191: DNS ネームサーバ RR 応答

セクション	内容	例
応答	クエリに対する特定の回答を提供する1つ以上のリソースレコード (オプション)	ドメイン名に対応する IP アドレス
権限	権威ネームサーバを指し示す1つ以上のリソースレコード (オプション)	応答の権威ネームサーバの名前
その他の情報	[応答 (Answer)] セクションに関連する追加情報を提供する1つ以上のリソースレコード (オプション)	クエリ対象の別のサーバの IP アドレス

さまざまなタイプのリソースレコードがありますが、これらはすべて一貫して次の構造を保っています。



理論上、すべてのタイプのリソースレコードを、ネームサーバ応答メッセージの [応答 (Answer)]、[権威 (Authority)]、または [追加情報 (Additional Information)] セクションで使用できます。DNS プリプロセッサは、検出されたエクスプロイトについて、3つの各応答セクションのすべてのリソースレコードを検査します。

[タイプ (Type)] および [RData] リソースレコードフィールドは、DNS プリプロセッサでは特に重要です。[タイプ (Type)] フィールドは、リソースレコードのタイプを示します。[RData] (リソースデータ) フィールドは、応答の内容を示します。[RData] フィールドのサイズと内容は、リソースレコードのタイプによって異なります。

DNS メッセージは通常、UDP トランスポートプロトコルを使用しますが、信頼性のある配信を必要とするメッセージタイプである場合や、メッセージサイズが UDP で処理可能なサイズを超えている場合は、TCP を使用します。DNS プリプロセッサは、UDP および TCP の両方のトラフィックで DNS サーバ応答を検査します。

DNS プリプロセッサは、ミッドストリームで検出された TCP セッションを検査せず、ドロップされたパケットが原因でセッションの状態が失われるとインスペクションを終了します。

## DNS プリプロセッサオプション

### ポート

このフィールドは、送信元ポート、または DNS プリプロセッサが DNS サーバ応答をモニタする必要があるポートを指定します。複数のポートを指定する場合は、カンマで区切ります。

DNS プリプロセッサ用に設定する一般的なポートは、ウェルノウンポート 53 です。これは、DNS ネーム サーバが UDP および TCP の両方で DNS メッセージに使用するポートです。

### RData テキスト フィールドでのオーバーフローの試行の検出

リソース レコードタイプが TXT (テキスト) の場合、RData フィールドは可変長の ASCII テキスト フィールドになります。

このオプションを選択した場合は、MITRE の Current Vulnerabilities and Exposures データベースの CVE-2006-3441 エントリで指定した特定の脆弱性を検出します。これは、Microsoft Windows 2000 Service Pack 4、Windows XP Service Pack 1 および Service Pack 2、Windows Server 2003 Service Pack 1 の既知の脆弱性です。攻撃者はこの脆弱性を悪用して、[RData] テキストフィールドの長さの誤算を引き起こし、結果としてバッファオーバーフローを発生させるよう悪意をもって作られたネームサーバ応答をホストに送信するか受信させることで、ホストを完全に制御できます。

アップグレードによってこの脆弱性が修正されていないオペレーティングシステムが稼働しているホストがネットワーク内に含まれている可能性がある場合は、このオプションを有効にする必要があります。

ルール 131:3 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### 古い DNS RR タイプの検知

RFC 1035 ではさまざまなリソース レコードタイプが古いタイプとして指定されています。これらは古いレコードタイプであるため、一部のシステムはこれらのレコードタイプに対応しておらず、エクスプロイトの対象となることがあります。このようなレコードタイプを含めるようにネットワークを意図的に設定している場合を除き、通常の DNS 応答でこのようなレコードタイプが検出されることは想定されません。

既知の古いリソース レコードタイプを検出するようにシステムを設定できます。次の表に、これらのレコードタイプとその説明を示します。

表 192:古い DNS リソース レコード タイプ

RR タイプ	コード (Code)	説明
3	MD	メールの宛先
4	MF	メールのフォワーダ

ルール 131:1 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### 試験的な DNS RR タイプの検出

RFC 1035 ではさまざまなリソース レコード タイプが試験的なタイプとして指定されています。これらは試験的なレコード タイプであるため、一部のシステムはこれらのレコード タイプに対応しておらず、エクスプロイトの対象となることがあります。このようなレコード タイプを含めるようにネットワークを意図的に設定している場合を除き、通常の DNS 応答でこのようなレコード タイプが検出されることは想定されません。

既知の試験的なレコード タイプを検出するようにシステムを設定できます。次の表に、これらのレコード タイプとその説明を示します。

表 193:試験的な DNS リソース レコード タイプ

RR タイプ	コード (Code)	説明
7	MB	メールボックスのドメイン名
8	MG	メール グループ メンバー
9	MR	メール リネーム ドメイン名
10	NUL	空白のリソース レコード

ルール 131:2 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

## DNS プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

## 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタムユーザーロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーションパネルで [設定 (Settings)] をクリックします。

**ステップ 4** [アプリケーション層プリプロセッサ (Application Layer Preprocessors)] の下の [DNS の構成 (DNS Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [DNS の構成 (DNS Configuration)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [DNS プリプロセッサ オプション \(1871 ページ\)](#) で説明されている設定を変更します。

**ステップ 7** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

## 次のタスク

- 侵入イベントを生成する場合は、DNS プリプロセッサルール (GID 131) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) および [DNS プリプロセッサ オプション \(1871 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 関連トピック

[侵入ポリシーおよびネットワーク分析ポリシーのレイヤ \(1591 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

# FTP/Telnet デコーダ

FTP/Telnet デコーダは FTP および Telnet データ ストリームを分析して、ルール エンジンによる処理の前に FTP および Telnet コマンドを正規化します。

## グローバル FTP および Telnet オプション

FTP/Telnet デコーダがパケットのステートフル インспекションまたはステートレス インспекションを実行するかどうか、デコーダが暗号化 FTP または Telnet セッションを検出するかどうか、およびデコーダが暗号化データの検出後にデータ ストリームの検査を続行するかどうかを決定するグローバル オプションを設定できます。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

### ステートフル インспекション (Stateful Inspection)

選択されている場合、FTP/Telnet デコーダは状態を保存し、各パケットにセッション コンテキストを提供し、再構成されたセッションだけを検査します。選択されていない場合、セッション コンテキストなしで個々のパケットを分析します。

FTP データ転送を検査するには、このオプションを選択する必要があります。

### 暗号化トラフィックの検出 (Detect Encrypted Traffic)

暗号化 Tenet および FTP セッションを検出します。

ルール 125:7 と 126:2 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### 暗号化データの検査を続行 (Continue to Inspect Encrypted Data)

プリプロセッサに対し、データ ストリームの暗号化後もデータ ストリームの検査を続行し、最終的に処理できるデコードされたデータを検索するように指示します。

## Telnet オプション

FTP/Telnet デコーダによる Telnet コマンドの正規化を有効または無効にし、特定の異常ケースを有効または無効にし、許容可能な Are You There (AYT) 攻撃数のしきい値を設定できます。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。



## ポート

Telnet トラフィックを正規化するポートを示します。通常、Telnet は TCP ポート 23 に接続します。インターフェイスで、複数のポートをカンマで区切って指定します。



**注意** 暗号化トラフィック (SSL) はデコードできないので、ポート 22 (SSH) を追加すると、予想外の結果が生じる可能性があります。

## 正規化 (Normalize)

指定のポートへの Telnet トラフィックを正規化します。

## 異常検知 (Detect Anomalies)

対応する SE (サブネゴシエーション終了) がない Telnet SB (サブネゴシエーション開始) の検出を有効にします。

Telnet がサポートするサブネゴシエーションは、SB (サブネゴシエーション開始) で開始し、SE (サブネゴシエーション終了) で終了していなければなりません。しかし、一部の Telnet サーバ実装では、対応する SE のない SB が無視されます。これは、回避事例につながるおそれのある異常な動作です。FTP はコントロール接続で Telnet プロトコルを使用するため、FTP もこの動作の影響を受けます。

ルール 126:3 を有効にすることでイベントを生成でき、インライン展開では、この異常が Telnet トラフィックで検出される場合に違反パケットをドロップできます。FTP コマンドチャンネルで検出される場合はルール 125:9 を有効にできます。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

## Are You There 攻撃のしきい値 (Are You There Attack Threshold Number)

連続する AYT コマンドの数が指定のしきい値を超えた場合にそのことを検出します。Cisco は、AYT しきい値としてデフォルト値以下の値を設定することを推奨します。

ルール 126:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

# サーバレベルの FTP オプション

複数の FTP サーバでデコード オプションを設定できます。作成する各サーバプロファイルには、トラフィックをモニタするサーバのサーバ IP アドレスとポートが含まれます。検証する FTP コマンドと、特定のサーバで無視する FTP コマンドを指定し、コマンドの最大パラメータ長を設定できます。また、デコーダが特定のコマンドで検証する特定のコマンド構文を設定し、代替最大コマンドパラメータ長を設定することもできます。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

## ネットワーク

FTP サーバの 1 つ以上の IP アドレスを指定するには、このオプションを使用します。

1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。設定できる最大文字数は 1024 文字です。デフォルト プロファイルを含め最大 255 個のプロファイルを設定できます。



- (注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン 展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの default 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたはアドレス ブロックは指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、any を表すアドレス表記 (0.0.0.0/0 または ::/0) を使用したりすることはできません。

## ポート

管理対象デバイスがトラフィックをモニタする FTP サーバのポートを指定するには、このオプションを使用します。インターフェイスで、複数のポートをカンマで区切って指定します。ポート 21 は FTP トラフィック用のウェルノウンポートです。

## File Get コマンド (File Get Commands)

サーバからクライアントにファイルを転送するために使用する FTP コマンドを定義するには、このオプションを使用します。サポートからの指示がない限り、これらの値を変更しないでください。



- 注意 サポートからの指示がない限り、[File Get コマンド (File Get Commands)] フィールドを変更しないでください。

## File Put コマンド (File Put Commands)

クライアントからサーバにファイルを転送するために使用する FTP コマンドを定義するには、このオプションを使用します。サポートからの指示がない限り、これらの値を変更しないでください。



- 注意 サポートからの指示がない限り、[File Put コマンド (File Put Commands)] フィールドを変更しないでください。

### 追加 FTP コマンド (Additional FTP Commands)

デコーダが検出するコマンドを追加で指定するには、この行を使用します。複数のコマンドを追加する場合は、コマンドをスペースで区切ってください。

追加できるコマンドには、XPWD、XCWD、XCUP、XMKD、XRMDがあります。これらのコマンドの詳細については、RFC 775 (Network Working Group によるディレクトリに基づく FTP コマンドの仕様) を参照してください。

### デフォルト最大パラメータ長 (Default Max Parameter Length)

代替最大パラメータ長が設定されていないコマンドの最大パラメータ長を検出するには、このオプションを使用します。代替最大パラメータ長は、必要な数だけ追加できます。

ルール 125:3 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

### 代替最大パラメータ長 (Alternate Max Parameter Length)

異なる最大パラメータ長を検出するコマンドを指定し、それらのコマンドの最大パラメータ長を指定するには、このオプションを使用します。[追加 (Add)] をクリックして行を追加し、特定のコマンドで検出する異なる最大パラメータ長を指定します。

### フォーマット文字列攻撃の検査コマンド (Check Commands for String Format Attacks)

指定されたコマンドでフォーマット文字列攻撃を検査するには、このオプションを使用します。

ルール 125:5 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

### コマンドの妥当性 (Command Validity)

特定のコマンドの有効な形式を入力するには、このオプションを使用します。[追加 (Add)] をクリックして、コマンド検証行を追加します。

ルール 125:2 と 125:4 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

### FTP 転送を無視 (Ignore FTP Transfers)

データ転送チャンネルで状態インスペクション以外のすべてのインスペクションを無効にして FTP データ転送のパフォーマンスを改善するには、このオプションを使用します。



(注) データ転送を検査するには、グローバル FTP/Telnet オプション [ステートフルインスペクション (Stateful Inspection)] を選択する必要があります。

### FTP コマンドでの Telnet エスケープ コードの検出 (Detect Telnet Escape Codes within FTP Commands)

FTP コマンドチャンネルで Telnet コマンドが使用された場合にそのことを検出するには、このオプションを使用します。

ルール 125:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

### 正規化時に消去コマンドを無視 (Ignore Erase Commands during Normalization)

[FTP コマンドでの Telnet エスケープ コードの検出 (Detect Telnet Escape Codes within FTP Commands)] が選択されている場合に、FTP トラフィックの正規化時に Telnet の文字および行の消去コマンドを無視するには、このオプションを使用します。この設定は、FTP サーバによる Telnet 消去コマンドの処理方法と一致する必要があります。一般に、新しい FTP サーバは Telnet 消去コマンドを無視しますが、ほとんどの古いサーバは Telnet 消去コマンドを処理する点に注意してください。

### トラブルシューティング オプション : FTP コマンドの検証設定のログを記録 (Troubleshooting Options : Log FTP Command Validation Configuration)

トラブルシューティングについてサポートに問い合わせた際に、サーバ用にリストされている FTP コマンドごとに設定情報を出力するように、システムを設定することを指示される場合があります。



**注意** サポートからの指示がない限り [FTP コマンドの検証設定のログを記録 (Log FTP Command Validation Configuration)] を有効にしないでください。

## FTP コマンドの検証ステートメント

FTP コマンドに対する検証ステートメントを設定するときには、複数の代替パラメータをスペースで区切って指定できます。2つのパラメータ間にバイナリ OR 関係を作成するには、検証ステートメントでこの2つのパラメータをパイプ文字 (|) で区切って指定します。パラメータを大カッコ ([]) で囲むと、これらのパラメータがオプションであることを示します。パラメータを中カッコ ({} ) で囲むと、これらのパラメータが必須であることを示します。

FTP 通信の一部として受信したパラメータの構文を検証する FTP コマンドパラメータ検証ステートメントを作成できます。

FTP コマンドパラメータ検証ステートメントに使用できるパラメータを次の表に示します。

表 194: FTP コマンドパラメータ

使用するパラメータ	実行される検証
int	示されるパラメータが整数である必要があります。

使用するパラメータ	実行される検証
number	示されるパラメータが 1～255 の範囲内の整数である必要があります。
char _chars	示されるパラメータが単一文字であり、かつ _chars 引数に指定した文字の 1 つである必要があります。  たとえば、検証引数 char SBC を使用して MODE のコマンド検証を定義すると、MODE コマンドのパラメータが、文字 s (Stream モードを示す)、文字 B (Block モードを示す)、または文字 c (Compressed モードを示す) を含んでいるかどうかを検証されます。
date _datefmt	_datefmt に # が含まれている場合、示されるパラメータは数値である必要があります。  _datefmt に c が含まれている場合、示されるパラメータは文字である必要があります。  _datefmt にリテラル文字列が含まれている場合、示されるパラメータはリテラル文字列に一致している必要があります。
string	示されるパラメータが文字列である必要があります。
host_port	示されるパラメータは、RFC 959 (Network Working Group による File Transfer Protocol 仕様) で定義されている有効なホストポート指定子である必要があります。

上記の表の構文を必要に応じて組み合わせることにより、トラフィックを検証する必要がある各 FTP コマンドを正しく検証するパラメータ検証ステートメントを作成できます。



- (注) TYPE コマンドに複合式を含める場合は、式をスペースで囲んでください。また、式内の各オペランドをスペースで囲んでください。たとえば、char A|B ではなく char A | B と入力します。

#### 関連トピック

- [サーバレベルの FTP オプション \(1875 ページ\)](#)
- [Firepower システムの IP アドレス表記法 \(14 ページ\)](#)
- [FTP コマンドの検証ステートメント \(1878 ページ\)](#)

## クライアントレベルの FTP オプション

カスタム FTP クライアント プロファイルを設定するには、これらのオプションを使用します。オプション記述にプリプロセッサルールが含まれない場合、そのオプションはプリプロセッサルールに関連付けられません。

### ネットワーク

FTP クライアントの 1 つ以上の IP アドレスを指定するには、このオプションを使用します。

1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト プロファイルを含め最大 255 個のプロファイルを設定できます。



- (注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの default 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたはアドレス ブロックは指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、any を表すアドレス表記 (0.0.0.0/0 または ::/0) を使用したりすることはできません。

### 最大応答長 (Max Response Length)

このオプションを使用して、クライアントが受け入れる FTP コマンドに許可される最大応答長を指定します。これにより、基本的なバッファ オーバーフローを検出できます。

ルール 125:6 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### FTP バウンス試行の検出 (Detect FTP Bounce Attempts)

FTP バウンス攻撃を検出するには、このオプションを使用します。

ルール 125:8 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### FTP バウンスの許可 (Allow FTP Bounce to)

FTP PORT コマンドを FTP バウンス攻撃として扱わない追加のホストとそれらのホスト上のポートのリストを設定するには、このオプションを使用します。

### FTP コマンドでの Telnet エスケープ コードの検出 (Detect Telnet Escape Codes within FTP Commands)

FTP コマンド チャネルで Telnet コマンドが使用された場合にそのことを検出するには、このオプションを使用します。

ルール 125:1 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### 正規化時に消去コマンドを無視 (Ignore Erase Commands during Normalization)

[FTP コマンドでの Telnet エスケープ コードの検出 (Detect Telnet Escape Codes within FTP Commands)] が選択されている場合に、FTP トラフィックの正規化時に Telnet の文字および行の消去コマンドを無視するには、このオプションを使用します。この設定は、FTP クライアントによる Telnet 消去コマンドの処理方法に一致する必要があります。一般に、新しい FTP クライアントは Telnet 消去コマンドを無視しますが、ほとんどの古いクライアントは Telnet 消去コマンドを処理する点に注意してください。

#### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## FTP/Telnet デコーダの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

クライアントからの FTP トラフィックをモニタするように、FTP クライアントのクライアント プロファイルを設定できます。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン 展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

#### 始める前に

- カスタム ターゲットベース ポリシーで識別するネットワークが、親ネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、および VLAN のサブセットと一致するか、サブセットであることを確認します。詳細については、[ネットワーク分析プロファイルの詳細設定 \(1840 ページ\)](#) を参照してください。

## 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション パネルで [設定 (Settings)] をクリックします。

**ステップ 4** [アプリケーション層プリプロセッサ (Application Layer Preprocessors)] の下の [FTP と Telnet の構成 (FTP and Telnet Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [FTP と Telnet の構成 (FTP and Telnet Configuration)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [グローバル FTP および Telnet オプション \(1874 ページ\)](#) の説明に従って、[グローバル設定 (Global Settings)] セクションのオプションを設定します。

**ステップ 7** [Telnet オプション \(1874 ページ\)](#) の説明に従って、[Telnet の設定 (Telnet Settings)] セクションのオプションを設定します。

**ステップ 8** FTP サーバ プロファイルを管理します。

- サーバ プロファイルの追加: [FTP サーバ (FTP Server)] の横にある追加アイコン (⊕) をクリックします。クライアントの 1 つ以上の IP アドレスを [サーバアドレス (Server Address)] フィールドに指定し、[OK] をクリックします。単一の IP アドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト ポリシーを含め最大 255 個のポリシーを設定できます。
- サーバ プロファイルの編集: [FTP サーバ (FTP Server)] の下にあるカスタム プロファイルの設定済みアドレスをクリックするか、[デフォルト (default)] をクリックします。[設定 (Configuration)] セクションの設定を変更できます。[サーバレベルの FTP オプション \(1875 ページ\)](#) を参照してください。
- サーバ プロファイルの削除: プロファイルの横にある削除アイコン (🗑️) をクリックします。

**ステップ 9** FTP クライアント プロファイルを管理します。

- クライアント プロファイルの追加: [FTP クライアント (FTP Client)] の横にある追加アイコン (⊕) をクリックします。クライアントの 1 つ以上の IP アドレスを [クライアントアドレス (Client Address)] フィールドに指定し、[OK] をクリックします。単一の IP ア



ドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト ポリシーを含め最大 255 個のポリシーを設定できます。

- クライアントプロファイルの編集：[FTP クライアント (FTP Client)] の下にあるプロファイルの設定済みアドレスをクリックするか、[デフォルト (default)] をクリックします。[設定 (Configuration)] ページエリアの設定を変更できます。[クライアントレベルの FTP オプション \(1880 ページ\)](#) を参照してください。
- クライアントプロファイルの削除：カスタムプロファイルの横にある削除アイコン (🗑️) をクリックします。

**ステップ 10** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

#### 次のタスク

- 侵入イベントを生成する場合は、FTP および telnet プリプロセッサルール (GID 125 および 126) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

[レイヤの管理 \(1599 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## HTTP Inspect プリプロセッサ

HTTP Inspect プリプロセッサは、次の処理を行います。

- ネットワーク上の Web サーバに送信される HTTP 要求と Web サーバから受信する HTTP 応答をデコードおよび正規化する。
- HTTP 関連の侵入ルールのパフォーマンス向上のために、Web サーバに送信されたメッセージを URI、非 cookie ヘッダー、cookie ヘッダー、メソッド、メッセージ本文の各コンポーネントに分ける。
- HTTP 関連の侵入ルールのパフォーマンス向上のために、Web サーバから受信したメッセージをステータスコード、ステータスメッセージ、非 set-cookie ヘッダー、cookie ヘッダー、応答本文の各コンポーネントに分ける。
- URI エンコード攻撃の可能性を検出する。

- 正規化データを追加ルール処理に使用できるようにする。

HTTP トラフィックはさまざまな形式でエンコードされている可能性があり、このことが、ルールによる適切な検査の実施を困難にしています。HTTP Inspect は 14 種類のエンコードをデコードし、HTTP トラフィックが最良のインスペクションを受けられるようにします。

HTTP Inspect のオプションは、グローバルに設定するか、1 つのサーバで設定するか、またはサーバリストに対して設定することができます。

プリプロセッサ エンジン は HTTP の正規化をステートレスに実行することに注意してください。つまり、パケット単位で HTTP 文字列を正規化し、TCP ストリーム プリプロセッサにより再構成された HTTP 文字列のみを処理できます。

## グローバル HTTP 正規化オプション

HTTP Inspect プリプロセッサのグローバル HTTP オプションは、プリプロセッサの機能を制御します。Web サーバポートとして指定されていないポートが HTTP トラフィックを受信する場合の HTTP 正規化を有効または無効にするには、このオプションを使用します。

次の点に注意してください。

- [無制限の圧縮解除 (Unlimited Decompression) ] を有効にすると、変更のコミット時に [圧縮データの最大深さ (Maximum Compressed Data Depth) ] および [圧縮解除データの最大深さ (Maximum Decompressed Data Depth) ] オプションが自動的に 65535 に設定されます。
- 最大値は、[圧縮データの最大深さ (Maximum Compressed Data Depth) ] または [圧縮解除データの最大深さ (Maximum Decompressed Data Depth) ] の値が異なる場合に使用されません。
  - デフォルトのネットワーク分析ポリシー
  - 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

### 異常な HTTP サーバの検出 (Detect Anomalous HTTP Servers)

Web サーバポートとして指定されていないポートに送信された HTTP トラフィックまたはこのポートで受信した HTTP トラフィックを検出します。



- (注) このオプションをオンにする場合は、[HTTP 設定 (HTTP Configuration)] ページで、HTTP トラフィックを受信するすべてのポートがサーバプロファイルにリストされていることを確認してください。確認せずにこのオプションと関連するプリプロセッサルールを有効にすると、サーバとの間の通常のトラフィックによってイベントが生成されます。デフォルトのサーバプロファイルには、HTTP トラフィックに一般に使用されるすべてのポートが含まれていますが、このプロファイルを変更した場合は、イベントの生成を防ぐために別のプロファイルにそれらのポートを追加する必要があります。

ルール 120:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

#### HTTP プロキシ サーバの検出 (Detect HTTP Proxy Servers)

[HTTP プロキシの使用を許可 (Allow HTTP Proxy Use)] オプションで定義されていないプロキシサーバを使用する HTTP トラフィックを検出します。

ルール 119:17 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

#### 圧縮データの最大深さ (Maximum Compressed Data Depth)

[圧縮データの検査 (Inspect Compressed Data)] (および任意で、[SWF ファイルの圧縮解除 (LZMA) (Decompress SWF File (LZMA))]、[SWF ファイルの圧縮解除 (Deflate) (Decompress SWF File (Deflate))]、または [PDF ファイルの圧縮解除 (Deflate) (Decompress PDF File (Deflate))] が有効な場合に、圧縮解除する圧縮データの最大サイズを設定します。

#### 圧縮解除データの最大深さ (Maximum Decompressed Data Depth)

[圧縮データの検査 (Inspect Compressed Data)] (および任意で、[SWF ファイルの圧縮解除 (LZMA) (Decompress SWF File (LZMA))]、[SWF ファイルの圧縮解除 (Deflate) (Decompress SWF File (Deflate))]、または [PDF ファイルの圧縮解除 (Deflate) (Decompress PDF File (Deflate))] が有効な場合に、正規化された圧縮データの最大サイズを設定します。

## サーバレベルの HTTP 正規化オプション

サーバレベルのオプションは、モニタ対象サーバごとに設定するか、すべてのサーバに対してグローバルに設定するか、またはサーバリストに対して設定することができます。また、事前定義のサーバプロファイルを使用してこれらのオプションを設定するか、またはご使用の環境のニーズに合わせて個別に設定することができます。これらのオプション、またはこれらのオプションを設定するデフォルトプロファイルの1つを使用して、トラフィックを正規化する

HTTP サーバポート、正規化するサーバ応答ペイロードの量、および正規化するエンコードのタイプを指定します。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

## ネットワーク

1 つ以上のサーバの IP アドレスを指定するには、このオプションを使用します。1 つの IP アドレスまたはアドレスブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。

デフォルト プロファイルを含めてプロファイルの合計数は最大 255 ですが、さらに、HTTP サーバリストに最大 496 文字（約 26 エントリ）を含めることができ、すべてのサーバプロファイルに対して合計 256 のアドレス エントリを指定できます。



- (注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの default 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、any を表すアドレス表記 (0.0.0.0/0 または ::/0) を使用したりすることはできません。

## ポート

プリプロセッサエンジンが HTTP トラフィックを正規化するポート。ポート番号が複数ある場合は、カンマで区切ります。

## サイズ超過のディレクトリ長 (Oversize Dir Length)

指定された値よりも長い URL ディレクトリを検出します。

ルール 119:15 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

## クライアントフローの深さ (Client Flow Depth)

[ポート (Ports)] で定義されているクライアント側 HTTP トラフィックについて、ルールで検査される raw HTTP パケットのバイト数 (ヘッダーとペイロードデータを含む) を指定します。ルール内の HTTP コンテンツ ルール オプションによって要求メッセージの特定の部分が検査される場合は、[クライアントフローの深さ (Client Flow Depth)] は適用されません。

次のいずれかを指定します。

- 正の値によって、最初のパケットで指定のバイト数が検査されます。最初のパケットのバイト数が指定のバイト数よりも少ない場合は、パケット全体が検査されます。指定された値は、セグメント化されたパケットと再構成されたパケットの両方に適用されることに注意してください。  
また、値300を指定すると、通常は、多くのクライアント要求ヘッダーの終わりにある大きな HTTP Cookie のインスペクションが排除されることにも注意してください。
- 0を指定すると、すべてのクライアント側トラフィックが検査されます。これにはセッション内の複数のパケットが含まれ、必要な場合にはバイトの上限を超えることもあります。この値はパフォーマンスに影響する可能性があることに注意してください。
- -1を指定すると、クライアント側のすべてのトラフィックが無視されます。

### サーバフローの深さ (Server Flow Depth)

[ポート (Ports)] で指定されているサーバ側 HTTP トラフィックについて、ルールで検査される raw HTTP パケットのバイト数を指定します。[HTTP 応答の検査 (Inspect HTTP Responses)] が無効である場合は raw ヘッダーとペイロードが検査され、[HTTP 応答の検査 (Inspect HTTP Response)] が有効である場合は、raw 応答ボディのみが検査されます。

[サーバフローの深さ (Server Flow Depth)] では、[ポート (Ports)] で定義されているサーバ側 HTTP トラフィックについて、ルールで検査されるセッション内の raw サーバ応答データのバイト数を指定します。このオプションを使用して、HTTP サーバ応答データのインスペクションのレベルとパフォーマンスのバランスを調整できます。ルール内の HTTP コンテンツ オプションによって要求メッセージの特定の部分が検査される場合は、Server Flow Depth は適用されません。

クライアントフローの深さ (Client Flow Depth) とは異なり、サーバフローの深さ (Server Flow Depth) では、ルールが検査するバイト数を、HTTP 要求パケットごとではなく、HTTP 応答ごとのバイト数として指定します。

次のいずれかの値を指定できます。

- 正の値 :

[HTTP 応答の検査 (Inspect HTTP Responses)] が**有効**である場合、raw HTTP 応答ボディのみが検査され、raw HTTP ヘッダーは検査されません。また、[圧縮データの検査 (Inspect Compressed Data)] が有効である場合は、圧縮解除データも検査されます。

[HTTP 応答の検査 (Inspect HTTP Responses)] が**無効**である場合、raw パケットヘッダーとペイロードが検査されます。

セッションの応答バイト数が指定の値よりも少ない場合は、そのセッションで、ルールにより (必要に応じて複数パケットにわたって) すべての応答パケットが完全に検査されます。セッションの応答バイト数が指定の値よりも多い場合、そのセッションで、ルールにより (必要に応じて複数パケットにわたって) 指定のバイト数だけが検査されます。

フローの深さ (Flow Depth) の値が小さいと、[ポート (Ports)] で定義されているサーバ側トラフィックを対象とするルールで、検出漏れが発生する可能性があります。これらの

ルールのほとんどはHTTPヘッダーまたはコンテンツ（通常、非ヘッダーデータの先頭の約 100 バイト以内）を対象とします。通常はヘッダーの長さは 300 バイト未満ですが、ヘッダー サイズは異なることがあります。

指定された値は、セグメント化されたパケットと再構成されたパケットの両方に適用されることにも注意してください。

- 0 を指定すると、[ポート (Port) ] で定義されているすべての HTTP サーバ側トラフィックでパケット全体が検査されます。これにはセッションでの 65535 バイトよりも大きな応答データも含まれます。

この値はパフォーマンスに影響する可能性があることに注意してください。

- -1

[HTTP 応答の検査 (Inspect HTTP Responses) ] が有効な場合、raw HTTP ヘッダーだけが検査され、raw HTTP 応答ボディは検査されません。

[HTTP 応答の検査 (Inspect HTTP Responses) ] が無効である場合、[ポート (Ports) ] で定義されているすべてのサーバ側トラフィックは無視されます。

#### 最大ヘッダー長 (Maximum Header Length)

[HTTP 応答の検査 (Inspect HTTP Responses) ] が有効である場合は、HTTP 要求、および HTTP 応答で、指定されている最大バイト数よりも長いヘッダーフィールドを検出します。値 0 を指定すると、このオプションが無効になります。これを有効にするため正の値を指定します。

ルール 119:19 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

#### 最大ヘッダー数 (Maximum Number of Headers)

HTTP 要求でヘッダー数がこの設定を超えている場合にそのことを検出します。値 0 を指定すると、このオプションが無効になります。これを有効にするため正の値を指定します。

ルール 119:20 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

#### 最大スペース数 (Maximum Number of Spaces)

折りたたみ行のスペースの数が HTTP 要求のこの設定と等しいか、超えている場合にそのことを検出します。値 0 を指定すると、このオプションが無効になります。これを有効にするため正の値を指定します。

ルール 119:26 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### HTTP クライアント ボディの抽出の深さ (HTTP Client Body Extraction Depth)

HTTP クライアント要求のメッセージボディから抽出するバイト数を指定します。侵入ルールを使用して抽出データを検査するには、`content` または `protected_content` キーワードを [HTTP クライアント ボディ (HTTP Client Body)] オプションと共に選択します。

クライアント ボディを無視するには、`-1` を指定します。クライアント ボディ全体を抽出するには、`0` を指定します。抽出対象のバイト数を指定すると、システムパフォーマンスが向上することがある点に注意してください。また、侵入ルールで [HTTP クライアントボディ (HTTP Client Body)] オプションが機能するためには、`0` か `0` より大きい値を指定する必要があることに注意してください。

### 小さいチャンク サイズ (Small Chunk Size)

チャンクが小さいとみなされるサイズの最大バイト数を指定します。正の値を指定します。値 `0` を指定すると、異常な小さなセグメントの連続の検出が無効になります。詳細については、[連続する小さいチャンク (Consecutive Small Chunks)] オプションを参照してください。

### 連続する小さいチャンク (Consecutive Small Chunks)

チャンク転送エンコードを使用するクライアント トラフィックまたはサーバ トラフィックで異常に大量であるとみなされる、連続する小さなチャンクの数を指定します。[小さいチャンク サイズ (Small Chunk Size)] オプションは、小さなチャンクの最大サイズを指定します。

たとえば、`10` バイト以下のチャンクが `5` つ連続していることを検出するには、[小さいチャンク サイズ (Small Chunk Size)] に `10` を設定し、[連続する小さいチャンク (Consecutive Small Chunks)] に `5` を設定します。

大量の小さなチャンクが検出される場合に イベントを生成し、インライン展開では、違反パケットをドロップします。するには、クライアント トラフィックの場合はプリプロセッサルール `119:27` を有効にし、サーバ トラフィックの場合はルール `120:7` を有効にします。[小さいチャンク サイズ (Small Chunk Size)] が有効であり、このオプションが `0` または `1` に設定されている場合にこれらのルールを有効にすると、指定されたサイズ以下のすべてのチャンクでイベントがトリガーとして使用されます。

### HTTP メソッド (HTTP Methods)

システムがトラフィックで検出すると予期される、`GET` および `POST` 以外の HTTP 要求メソッドを指定します。複数の値はカンマで区切ります。

侵入ルールでは、HTTP メソッドのコンテンツを検索するために、`content` または `protected_content` キーワードが **HTTP Method** 引数と共に使用されます。`GET`、`POST`、およびこのオプションで設定されているメソッド以外のメソッドがトラフィックで検出される場合 イベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール `119:31` を有効にします。 [侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### アラートなし (No Alerts)

関連するプリプロセッサルールが有効である場合に、侵入イベントを無効にします。



(注) このオプションは、HTTP の標準テキストルールと共有するオブジェクトルールを無効にしません。

### HTTP ヘッダーの正規化 (Normalize HTTP Headers)

[HTTP 応答の検査 (Inspect HTTP Responses)] が有効な場合は、要求ヘッダーと応答ヘッダーの非 cookie データの正規化が有効になります。[HTTP 応答の検査 (Inspect HTTP Responses)] が有効ではない場合は、要求ヘッダーと応答ヘッダーで cookie を含む HTTP ヘッダー全体の正規化が有効になります。

### HTTP Cookie の検査 (Inspect HTTP Cookies)

HTTP 要求ヘッダーからの cookie の抽出を有効にします。また、[HTTP 応答の検査 (Inspect HTTP Responses)] が有効な場合は、応答ヘッダーからの set-cookie データの抽出も有効になります。cookie の抽出が不要な場合は、このオプションを無効にするとパフォーマンスが向上します。

Cookie: および Set-Cookie: のヘッダー名、ヘッダー行の先頭のスペース、およびヘッダー行の末尾の CRLF は、cookie の一部ではなくヘッダーの一部として検査されます。

### HTTP ヘッダーの Cookie の正規化 (Normalize Cookies in HTTP headers)

HTTP 要求ヘッダーの cookie の正規化を有効にします。[HTTP 応答の検査 (Inspect HTTP Responses)] が有効な場合も、応答ヘッダーの set-cookie データの正規化を有効にします。このオプションを選択する前に、[HTTP Cookie の検査 (Inspect HTTP Cookies)] を選択する必要があります。

### HTTP プロキシの使用を許可 (Allow HTTP Proxy Use)

モニタ対象 Web サーバを HTTP プロキシとして使用できるようにします。このオプションは、HTTP 要求のインスペクションでのみ使用されます。

### URI のみの検査 (Inspect URI Only)

正規化された HTTP 要求パケットの URI 部分のみを検査します。

### HTTP 応答の検査 (Inspect HTTP Responses)

HTTP 応答の拡張インスペクションが有効になり、プリプロセッサは、HTTP 要求メッセージのデコードと正規化の他に、ルールエンジンによるインスペクションのために応答フィールドを抽出します。このオプションを有効にすると、応答ヘッダー、ボディ、ステータスコードなどがシステムにより抽出されます。また [HTTP Cookie の検査 (Inspect HTTP Cookies)] が有効な場合は、set-cookie データも抽出されます。

ルール 120:2 と 120:3 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。



### UTF エンコードの UTF-8 への正規化 (Normalize UTF Encodings to UTF-8)

[HTTP 応答の検査 (Inspect HTTP Responses)] が有効である場合、HTTP 応答で UTF-16LE、UTF-16BE、UTF-32LE、および UTF32-BE エンコードが検出され、UTF-8 に正規化されます。

ルール 120:4 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### 圧縮データの検査 (Inspect Compressed Data)

[HTTP 応答の検査 (Inspect HTTP Responses)] が有効な場合は、HTTP 応答ボディ内の gzip および deflate 互換圧縮データの圧縮解除と、正規化された圧縮解除データのインスペクションが有効になります。システムは、チャンク HTTP 応答データと非チャンク HTTP 応答データを検査します。システムは、必要に応じて複数のパケットにわたり圧縮解除データをパケット単位で検査します。つまり、システムが異なるパケットの圧縮解除データをインスペクションのために結合させることはありません。[圧縮データの最大深さ (Maximum Compressed Data Depth)]、[圧縮解除データの最大深さ (Maximum Decompressed Data Depth)]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除 (Unlimited Decompression)] を選択していない場合は、[サーバフローの深さ (Server Flow Depth)] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、file\_data ルールキーワードを使用できます。

ルール 120:6 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### 無制限の圧縮解除 (Unlimited Decompression)

[圧縮データの検査 (Inspect Compressed Data)] (および任意で、[SWF ファイルの圧縮解除 (LZMA) (Decompress SWF File (LZMA))]、[SWF ファイルの圧縮解除 (Deflate) (Decompress SWF File (Deflate))]、または [PDF ファイルの圧縮解除 (Deflate) (Decompress PDF File (Deflate))] ) が有効な場合、複数のパケットにわたって [圧縮解除データの最大深さ (Maximum Decompressed Data Depth)] がオーバーライドされます。つまり、このオプションにより、複数のパケットにわたる無制限の圧縮解除が有効になります。このオプションを有効にしても、単一パケット内での [圧縮データの最大深さ (Maximum Compressed Data Depth)] または [圧縮解除データの最大深さ (Maximum Decompressed Data Depth)] には影響しないことに注意してください。また、このオプションを有効にすると、変更のコミット時に、[圧縮データの最大深さ (Maximum Compressed Data Depth)] と [圧縮解除データの最大深さ (Maximum Decompressed Data Depth)] が 65535 に設定されることにも注意してください。

### Javascript の正規化 (Normalize Javascript)

[HTTP 応答の検査 (Inspect HTTP Responses)] が有効な場合、HTTP 応答ボディ内での Javascript の検出と正規化を有効にします。プリプロセッサは unescape 関数や decodeURI 関数、String.fromCharCode メソッドなどの難読化 Javascript データを正規化します。プリプロセッサは、unescape、decodeURI、および decodeURIComponent 関数内の次のエンコードを正規化します。

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

プリプロセッサは連続するスペースを検出し、1つのスペースに正規化します。このオプションが有効である場合、設定フィールドでは、難読化 Javascript データで許容する連続スペースの最大数を指定できます。入力できる値は、1～65535 です。値 0 を指定すると、このフィールドに関連付けられているプリプロセッサルール (120:10) が有効かどうかに関係なく、イベントの生成が無効になります。

プリプロセッサは、Javascript の正符号 (+) 演算子も正規化し、この演算子を使用して文字列を連結します。

file\_data 侵入ルール キーワードを使用して、正規化された Javascript データに対し侵入ルールを指し示すことができます。

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、次に示すように、ルール 120:9、120:10、および 120:11 を有効にします。

表 195: [Javascript の正規化 (Normalize Javascript) ] オプションのルール (Normalize Javascript Option Rules)

ルール	以下の場合にトリガーする
120:9	プリプロセッサ内の難読化レベルが 2 以上である。
120:10	Javascript 難読化データで連続するスペースの数が、許容される連続スペースの最大数として設定された値以上である。
120:11	エスケープされたデータまたはエンコードされたデータに、複数のエンコードタイプが含まれている。

### SWF ファイルの圧縮解除 (LZMA) (Decompress SWF File (LZMA) ) および SWF ファイルの圧縮解除 (Deflate) (Decompress SWF File (Deflate) )

[HTTP Inspect の応答 (HTTP Inspect Responses) ] が有効な場合、これらのオプションは、HTTP 要求の HTTP 応答ボディ内にあるファイルの圧縮部分を圧縮解除します。



(注) HTTP GET 応答で見つかったファイルの圧縮部分のみを圧縮解除できます。

- [SWF ファイルの圧縮解除 (LZMA) (Decompress SWF File (LZMA) ) ] は、Adobe ShockWave Flash (.swf) ファイルの LZMA 互換の圧縮部分を圧縮解除します。

- [SWF ファイルの圧縮解除 (Deflate) (Decompress SWF File (Deflate))] は、Adobe ShockWave Flash (.swf) ファイルの deflate 互換の圧縮部分を圧縮解除します。

[圧縮データの最大深さ (Maximum Compressed Data Depth)]、[圧縮解除データの最大深さ (Maximum Decompressed Data Depth)]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除 (Unlimited Decompression)] を選択していない場合は、[サーバフローの深さ (Server Flow Depth)] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、file\_data 侵入ルール キーワードを使用できません。

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、次に示すように、ルール 120:12 および 120:13 を有効にします。

表 196: [SWF ファイルの圧縮解除 (Decompress SWF File)] オプションのルール (Decompress SWF File Option Rules)

ルール	以下の場合にトリガーする
120:12	deflate ファイルの圧縮解除に失敗
120:13	LZMA ファイルの圧縮解除に失敗

### PDF ファイルの圧縮解除 (Deflate) (Decompress PDF File (Deflate))

[HTTP Inspect の応答 (HTTP Inspect Responses)] が有効な場合、[PDF ファイルの圧縮解除 (Deflate) (Decompress PDF File (Deflate))] は、HTTP 要求の HTTP 応答ボディ内にある Portable Document Format (.pdf) ファイルの deflate 互換の圧縮部分を圧縮解除します。システムは、/FlateDecode ストリーム フィルタが付いた PDF ファイルだけを圧縮解除できます。他のフィルタ (/FlateDecode /FlateDecode など) はサポートしていません。



(注) HTTP GET 応答で見つかったファイルの圧縮部分のみを圧縮解除できます。

[圧縮データの最大深さ (Maximum Compressed Data Depth)]、[圧縮解除データの最大深さ (Maximum Decompressed Data Depth)]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除 (Unlimited Decompression)] を選択していない場合は、[サーバフローの深さ (Server Flow Depth)] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、file\_data 侵入ルール キーワードを使用できません。

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、次に示すように、ルール 120:14、120:15、120:16、および 120:17 を有効にします。

表 197: [PDF ファイルの圧縮解除 (Deflate) (Decompress PDF File (Deflate))] オプションのルール (Decompress PDF File (Deflate) Option Rules)

ルール	以下の場合にトリガーする
120:14	ファイルの圧縮解除に失敗

ルール	以下の場合にトリガーする
120:15	圧縮タイプがサポート対象外のタイプであるため、ファイルの圧縮解除に失敗
120:16	PDF ストリーム フィルタがサポート対象外のフィルタであるため、ファイルの圧縮解除に失敗
120:17	ファイルの解析に失敗

### 元のクライアント IP アドレスの抽出 (Extract Original Client IP Address)

侵入検査中の、元のクライアント IP アドレスの調査を有効にします。システムは元のクライアント IP アドレスを、X-Forwarded-For (XFF)、True-Client-IP、または [XFF ヘッダーの優先順位 (XFF Header Priority)] オプションで定義したカスタム HTTP ヘッダーから抽出します。侵入イベントテーブルで、抽出された元のクライアント IP アドレスを表示できます。

ルール 119:23、119:29 および 119:30 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### XFF ヘッダーの優先順位 (XFF Header Priority)

HTTP 要求に複数のヘッダーが存在する場合は、システムが元のクライアント IP ヘッダーを処理する順序を指定します。デフォルトでは、システムはまず X-Forwarded-For (XFF) ヘッダーを、次に True-Client-IP ヘッダーを調査します。各ヘッダー タイプの横にある上下矢印アイコンを使用して、優先順位を調整します。

このオプションでも、抽出と評価のために、XFF または True-Client-IP 以外の元のクライアント IP ヘッダーを指定できます。[追加 (Add)] をクリックして、カスタムヘッダー名をプライオリティ リストに追加します。システムは、XFF または True-Client-IP ヘッダーと同じ構文を使用するカスタムヘッダーのみをサポートします。

このオプションを設定する場合は、次の点に留意してください。

- アクセス コントロールと侵入検査の両方で、システムは元のクライアント IP アドレスヘッダーを評価するときに、この優先順位を使用します。
- 元のクライアント IP ヘッダーが複数ある場合、システムは優先順位が最も高いヘッダーのみを処理します。
- XFF ヘッダーには、要求が渡されるプロキシサーバを表す IP アドレスのリストが含まれています。スプーフィングを防止するために、システムはリスト内の最後の IP アドレス (つまり、信頼されるプロキシにより追加されたアドレス) を、元のクライアント IP アドレスとして使用します。

### URI のログ (Log URI)

rawURI が存在する場合に、HTTP 要求パケットから rawURI を抽出できるようにし、このセッションで生成されるすべての侵入イベントにこの URI を関連付けます。

このオプションが有効である場合、侵入イベントテーブルビューの [HTTP URI] 列に、抽出された URI の先頭 50 文字を表示できます。パケットビューでは、URI 全体 (最大 2048 バイト) を表示できます。

### ホスト名のログ (Log Hostname)

ホスト名が存在する場合に、HTTP 要求の Host ヘッダーからホスト名を抽出できるようにし、このセッションで生成されるすべての侵入イベントにこのホスト名を関連付けます。複数の Host ヘッダーがある場合は、1 番目のヘッダーからホスト名を抽出します。

このオプションが有効である場合、侵入イベントテーブルビューの [HTTP ホスト名 (HTTP Hostname)] 列に、抽出されたホスト名の先頭 50 文字を表示できます。パケットビューでは、ホスト名全体 (最大 256 バイト) を表示できます。

ルール 119:25 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

有効にすると、このオプションの設定に関係なく、HTTP 要求で複数のホストヘッダーが検出された場合、ルール 119:24 がトリガーされます。

### プロファイル (Profile)

HTTP トラフィック向けに正規化されたエンコードのタイプを指定します。システムには、ほとんどのサーバに適用できるデフォルトプロファイル、Apache サーバと IIS サーバ用のデフォルトプロファイル、およびモニタ対象トラフィックのニーズに合わせて調整できるカスタムのデフォルト設定があります。

- すべてのサーバに対して適切な標準のデフォルト プロファイルを使用するには、[すべて (All)] を選択します。
- システムによって提供される IIS プロファイルを使用するには、[IIS] を選択します。
- システムによって提供される Apache プロファイルを使用するには、[Apache] を選択します。
- 独自のサーバ プロファイルを作成するには、[カスタム (Custom)] を選択します。

## サーバレベルの HTTP 正規化エンコードオプション

HTTP サーバレベルの [プロファイル (Profile)] オプションを Custom に設定すると、HTTP トラフィックに対して正規化されるエンコードタイプを指定できます。また、HTTP のプリプロセッサルールを有効にして、異なるエンコードタイプを含むトラフィックに対してイベントを生成できます。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

### ASCII エンコード

エンコードされた ASCII 文字をデコードし、ルールエンジンが ASCII エンコード URI でイベントを生成するかどうかを指定します。

ルール 119:1 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### UTF-8 エンコード

URI の標準 UTF-8 Unicode シーケンスをデコードします。

ルール 119:6 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### Microsoft %U エンコード

%u とその後に続く 4 文字を使用する IIS %u エンコードスキームをデコードします。この 4 文字は、IIS Unicode コードポイントに関連する 16 進数のエンコード値です。



**ヒント** 正規のクライアントが %u エンコードを使用することはほとんどないため、シスコは、%u エンコードによってエンコードされている HTTP トラフィックをデコードすることを推奨します。

ルール 119:3 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### ベアバイト UTF-8 エンコード

ベアバイトエンコードをデコードします。ベアバイトエンコードは、UTF-8 値のデコード時に非 ASCII 文字を有効な値として使用します。



**ヒント** ベアバイトエンコードにより、ユーザは IIS サーバをエミュレートし、非標準エンコードを正しく解釈することができます。正規のクライアントはこの方法で UTF-8 をエンコードしないため、シスコは、このオプションを有効にすることを推奨します。

ルール 119:4 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

## Microsoft IIS エンコード

Unicode コードポイント マッピングを使用してデコードします。



**ヒント** これは主に攻撃と回避の試行で見られるため、シスコはこのオプションを有効にすることを推奨します。

ルール 119:7 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。 [侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

## 二重符号化

要求 URI を 2 回通過し、それぞれでデコードを実行するようにすることで、IIS 二重エンコードトラフィックをデコードします。これは通常は攻撃シナリオでのみ検出されるため、シスコはこのオプションを有効にすることを推奨します。

ルール 119:2 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。 [侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

## マルチスラッシュ オブファスケーション

1 つの行内の複数のスラッシュを 1 つのスラッシュに正規化します。

ルール 119:8 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。 [侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

## IIS バックスラッシュ オブファスケーション

バックスラッシュをスラッシュに正規化します。

ルール 119:9 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。 [侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

## ディレクトリ トラバーサル

ディレクトリ トラバーサルおよび自己参照用ディレクトリを正規化します。一部の Web サイトはディレクトリ トラバーサルを使用してファイルを参照するため、このタイプのトラフィックに対してイベントを生成するために、関連するプリプロセッサルールを有効にすると、誤検出が発生する可能性があります。

ルール 119:10 と 119:11 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。 [侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

### タブオブファスケーション

スペース区切り記号としてタブを使用する非 RFC 標準を正規化します。Apache やその他の非 IIS Web サーバは、URL の区切り文字としてタブ文字 (0x09) を使用します。



(注) このオプションの設定に関係なく、空白文字 (0x20) がタブの前にある場合、HTTP Inspect プリプロセッサはそのタブをスペースとして扱います。

ルール 119:12 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。 [侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

### 無効な RFC 区切り文字

URI データの改行 (\n) を正規化します。

ルール 119:13 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。 [侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

### Webroot ディレクトリ トラバーサル

URL の初期ディレクトリを越えて横断するディレクトリ トラバーサルを検出します。

ルール 119:18 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。 [侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

### タブ区切り (URI)

URI の区切り文字としてタブ文字 (0x09) を有効にします。Apache、新しいバージョンの IIS、およびその他の一部の Web サーバは、URL の区切り文字としてタブ文字を使用します。



(注) このオプションの設定に関係なく、空白文字 (0x20) がタブの前にある場合、HTTP Inspect プリプロセッサはそのタブをスペースとして扱います。

### 非 RFC 文字

対応するフィールドに追加された非 RFC 文字リストが、着信または発信 URI データ内に含まれている場合にそれを検出します。このフィールドを変更する場合は、バイト文字を表す 16 進表記を使用します。このオプションを設定する場合は、値を慎重に設定してください。非常に一般的な文字を使用すると、イベントが大量に発生する可能性があります。

ルール 119:14 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。 [侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。



### チャンク形式の最大エンコード サイズ

URI データで異常に大きなチャンク サイズを検出します。

ルール 119:16 と 119:22 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### パイプライン デコードの無効化

パイプライン処理された要求の HTTP デコードを無効にします。このオプションが無効である場合、パイプラインで待機する HTTP 要求には、デコードおよび分析は行われず、汎用パターンマッチングを使用した検査のみが行われるため、パフォーマンスが向上します。

### Non-Strict URI 解析

Non-Strict URI 解析を有効にします。このオプションは、「GET /index.html abc xo qr \n」という形式の非標準 URI を受け入れるサーバでのみ使用します。このオプションを使用すると、デコーダは URI が 1 番目のスペースと 2 番目のスペースで囲まれているものと想定します。これは、2 番目のスペースの後に有効な HTTP 識別子がなくても同様です。

### 拡張 ASCII エンコード

HTTP 要求 URI の拡張 ASCII 文字の解析を有効にします。このオプションは、カスタム サーバプロファイルでのみ使用可能であり、Apache、IIS、またはすべてのサーバ向けに提供されるデフォルト プロファイルでは使用できないことに注意してください。

### 関連トピック

[概要：HTTP content および protected\\_content キーワードの引数 \(1719 ページ\)](#)

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## HTTP 検査プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

### 始める前に


- カスタム ターゲットベース ポリシーで識別するネットワークが、親ネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、および VLAN のサブセットと一致す


るか、サブセットであることを確認します。詳細については、[ネットワーク分析プロファイルの詳細設定（1840 ページ）](#)を参照してください。

## 手順

**ステップ 1** [ポリシー（Policies）]>[アクセスコントロール（Access Control）]、次に[ネットワーク分析ポリシー（Network Analysis Policy）]をクリックします。または[ポリシー（Policies）]>[アクセスコントロール（Access Control）]>[侵入（Intrusion）]、次に[ネットワーク分析ポリシー（Network Analysis Policy）]をクリックします。を選択します。


(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン () をクリックします。

代わりに表示アイコン () が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。



**ステップ 3** ナビゲーション パネルで [設定（Settings）] をクリックします。

**ステップ 4** [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [HTTP の設定（HTTP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

**ステップ 5** [HTTP の設定（HTTP Configuration）] の横にある編集アイコン () をクリックします。

**ステップ 6** [グローバル設定（Global Settings）] ページ エリアのオプションを変更します。[グローバル HTTP 正規化オプション（1884 ページ）](#)を参照してください。

**ステップ 7** 次の 3 つの選択肢があります。

- サーバプロファイルの追加：[サーバ（Servers）] セクションの追加アイコン () をクリックします。クライアントの 1 つ以上の IP アドレスを [サーバアドレス（Server Address）] フィールドに指定し、[OK] をクリックします。単一の IP アドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。リストに入力できる文字数は最大 496 文字、すべてのサーバプロファイルで指定できるアドレス項目の総数は 256、作成できるプロファイルの総数はデフォルトプロファイルを含めて 255 です。
- サーバプロファイルの編集：[サーバ（Servers）] の下で追加したプロファイルの設定済みアドレスをクリックするか、[デフォルト（default）] をクリックします。[設定（Configuration）] セクションの設定を変更できます。[サーバレベルの HTTP 正規化オプション（1885 ページ）](#)を参照してください。プロファイル値で [カスタム（Custom）] を選択した場合は、[サーバレベルの HTTP 正規化エンコードオプション（1895 ページ）](#)で説明されているエンコーディング オプションを変更することもできます。
- サーバプロファイルの削除：カスタム プロファイルの横にある削除アイコン () をクリックします。

**ステップ 8** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

### 次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。する場合は、HTTP プリプロセッサルール (GID 119) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[レイヤの管理 \(1599 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## その他の HTTP 検査プリプロセッサルール

特定の設定オプションに関連付けられていない HTTP Inspect プリプロセッサルールのイベントを生成するには、次の表の「プリプロセッサルール GID : SID」列のルールを有効にできません。

表 198: その他の HTTP 検査プリプロセッサルール

プリプロセッサルール GID:SID	説明
120:5	HTTP 応答トラフィックで UTF-7 エンコードが検出された場合にイベントが生成されます。UTF-7 は、SMTP トラフィックなどで 7 ビットパリティが必要な場合にのみ使用してください。
119:21	HTTP 要求ヘッダーに複数の content-length フィールドがある場合にイベントが生成されます。
119:24	HTTP 要求に複数の Host ヘッダーがある場合に、イベントが生成されます。
119:28 120:8	これらのルールを有効にする場合、イベントは生成されません。
119:32	トラフィックで HTTP バージョン 0.9 が検出されると、イベントが生成されます。TCP ストリームの設定も有効にする必要があることに注意してください。
119:33	エスケープされていないスペースが HTTP URI に含まれている場合に、イベントが生成されます。

プリプロセッサ ルール <b>GID:SID</b>	説明
119:34	TCP 接続に 24 以上のパイプライン処理された HTTP 要求が含まれている場合に、イベントが生成されます。

## Sun RPC プリプロセッサ

リモートプロシージャコール (RPC) の正規化では、フラグメント化された複数の RPC レコードを取得し、それらを1つのレコードに正規化するので、ルールエンジンがそのレコード全体を検査できます。たとえば、攻撃者が RPC `admin` が実行されているポートの検出を試行するとします。一部の UNIX ホストは、RPC `admin` を使用してリモート分散システムタスクを実行します。ホストが弱い認証を実行する場合、悪意のあるユーザがリモート管理のコントロールを獲得できることがあります。Snort ID (SID) 575 の標準テキストルール (GID : 1) では、特定のロケーションでコンテンツを検索して、不適切な `portmap` `GETPORT` 要求を特定することで、この攻撃を検出します。

## Sun RPC プリプロセッサのオプション

### ポート

トラフィックを正規化するポートを示します。インターフェイスで、複数のポートをカンマで区切って指定します。一般的な RPC ポートは 111 および 32771 です。ネットワークが他のポートに RPC トラフィックを送信する場合は、それらのポートの追加を検討してください。

### RPC フラグメント化レコードの検出 (**Detect fragmented RPC records**)

RPC フラグメント化レコードを検出します。

ルール 106:1 と 106:5 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

### 1 パケットの複数レコードの検出 (**Detect multiple records in one packet**)

パケット (または再構成されたパケット) ごとに、複数の RPC 要求を検出します。

ルール 106:2 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640ページ\)](#) を参照してください。

### 1 フラグメントを超えるフラグメント化レコード合計の検出 (**Detect fragmented record sums which exceed one fragment**)

現在のパケット長を超える再構成されたフラグメント化レコード長を検出します。

ルール 106:3 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。 [侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

### 1 パケットのサイズを超える単一フラグメントレコードの検出 (Detect single fragment records which exceed the size of one packet)

部分的なレコードを検出します。

ルール 106:4 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。 [侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。

## Sun RPC プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。 を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション パネルで [設定 (Settings)] をクリックします。

**ステップ 4** [アプリケーション層プリプロセッサ (Application Layer Preprocessors)] の下の [Sun RPC の構成 (Sun RPC Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [Sun RPC の構成 (Sun RPC Configuration)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [Sun RPC プリプロセッサのオプション \(1902 ページ\)](#) で説明されている設定を変更します。

**ステップ 7** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

### 次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。する場合は、Sun RPC プリプロセッサルール (GID 106) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[レイヤの管理 \(1599 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## SIP プリプロセッサ

Session Initiation Protocol (SIP) は、インターネット テレフォニー、マルチメディア会議、インスタントメッセージング、オンラインゲーム、ファイル転送などのクライアントアプリケーションの 1 人以上のユーザに対し、1 つ以上のセッションのコールのセットアップ、変更、およびティアダウンを提供します。各 SIP 要求の *method* フィールドは要求の目的を示し、Request-URI に要求の送信先が指定されます。各 SIP 応答のステータス コードは、要求されたアクションの結果を示します。

SIP を使用してコールがセットアップされた後、後続の音声およびビデオによる通信は Real-time Transport Protocol (RTP) により処理されます。セッションのこの部分は、コール チャネル、データ チャネル、または音声/ビデオ データ チャネルと呼ばれることがあります。RTP は、データチャネルパラメータ ネゴシエーション、セッション通知、およびセッションへの招待のために、SIP メッセージ ボディ内で Session Description Protocol (SDP) を使用します。

SIP プリプロセッサは次の処理を実行します。

- SIP 2.0 トラフィックのデコードおよび分析
- SDP データが存在する場合はこのデータを含む SIP ヘッダーとメッセージ ボディを抽出し、抽出したデータを今後のインスペクションのためにルール エンジンに受け渡す
- 次の状態が検出され、対応するプリプロセッサルールが有効な場合にイベントを生成する
  - SIP パケット内の異常と既知の脆弱性
  - 順序が間違っているコール シーケンスと無効なコール シーケンス
- コール チャネルの無視 (オプション)

プリプロセッサは、SIP メッセージ ボディに組み込まれている SDP メッセージに示されているポートに基づいて RTP チャンネルを識別しますが、RTP プロトコル インスペクションを実行しません。

SIP プリプロセッサを使用するときは、次の点に注意してください。

- UDP は通常、SIP でサポートされるメディア セッションを伝送します。UDP ストリームの前処理により、SIP プリプロセッサに対し SIP セッション トラッキングが提供されます。
- SIP ルール キーワードにより、SIP パケット ヘッダーまたはメッセージ ボディを指し示し、検出対象を特定の SIP メソッドまたはステータスコードのパケットに限定できます。

## SIP プリプロセッサのオプション

次のオプションでは、1 から 65535 バイトの正の値を指定するか 0 を指定して、関連するルールが有効にされているかどうかにかかわらず、オプションのイベント生成を無効にできます。

- 要求 URI の最大長 (**Maximum Request URI Length**)
- コール ID の最大長 (**Maximum Call ID Length**)
- 要求名の最大長 (**Maximum Request Name Length**)
- 送信元の最大長 (**Maximum From Length**)
- 送信先の最大長 (**Maximum To Length**)
- 経由の最大長 (**Maximum Via Length**)
- 連絡先の最大長 (**Maximum Contact Length**)
- コンテンツの最大長 (**Maximum Content Length**)

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

### ポート

SIP トラフィックを検査するポートを指定します。0 ~ 65535 の整数を指定できます。ポート番号が複数ある場合は、カンマで区切ります。

### 検査するメソッド (**Methods to Check**)

検出する SIP メソッドを指定します。次に示す現在定義されている SIP メソッドを指定できます。

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

メソッドでは大文字と小文字が区別されません。メソッド名には英字、数字、下線文字を使用できます。その他の特殊文字は使用できません。複数のメソッドはカンマで区切ります。

新しいSIPメソッドが今後定義される可能性があるため、設定には、現在定義されていない英字文字列を含めることができます。システムでは最大32個のメソッド（現在定義されている21個のメソッドと追加の11個のメソッド）がサポートされます。システムは、設定される未定義のメソッドをすべて無視します。

合計32個のメソッドには、このオプションに指定するメソッドの他に、侵入ルールで`sip_method`キーワードを使用して指定するメソッドも含まれることに注意してください。

### セッション内のダイアログ最大数 (Maximum Dialogs within a Session)

ストリームセッション内で許容されるダイアログの最大数を指定します。この数より多くのダイアログが作成されると、ダイアログの数が、指定されている最大数以下になるまで、最も古いダイアログから順に削除されます。1～4194303の整数を指定できます。

ルール140:27を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。[侵入ルール状態の設定 \(1640ページ\)](#)を参照してください。

### 要求URIの最大長 (Maximum Request URI Length)

[要求URI (Request-URI)]ヘッダーフィールドの最大許容バイト数を指定します。ルール140:3が有効である場合、URIが長いとイベントを生成し、インライン展開では、違反パケットをドロップします。。[要求URI (Request-URI)]フィールドは、要求の宛先のパスまたはページを示します。

### コールIDの最大長 (Maximum Call ID Length)

[要求または応答のコールID (request or response Call-ID)]ヘッダーフィールドの最大許容バイト数を指定します。ルール140:5が有効である場合、Call-IDが長いとイベントを生成し、インライン展開では、違反パケットをドロップします。。[コールID (Call-ID)]フィールドによって、要求や応答内のSIPセッションが一意に識別されます。

### 要求名の最大長 (Maximum Request Name Length)

要求名で許容される最大バイト数を指定します。要求名は、CSeqトランザクションIDに指定されるメソッドの名前です。ルール140:7が有効である場合、リクエスト名が長いとイベントを生成し、インライン展開では、違反パケットをドロップします。。

### 送信元の最大長 (Maximum From Length)

要求または応答の[送信元 (From)]ヘッダーフィールドで許容される最大バイト数を指定します。ルール140:9が有効である場合、[送信元 (From)]が長いとイベントを生成し、インライン展開では、違反パケットをドロップします。。[送信元 (From)]フィールドは、メッセージの発信側を識別します。



**送信先の最大長 (Maximum To Length)**

要求または応答の [送信先 (To) ] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:11 が有効である場合、[送信先 (To) ] が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[送信先 (To) ] フィールドは、メッセージの受信側を識別します。

**経由の最大長 (Maximum Via Length)**

要求または応答の [経由 (Via) ] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:13 が有効である場合、[経由 (Via) ] が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[経由 (Via) ] フィールドには要求がたどるパスが示され、応答の場合は受信者情報が示されます。

**連絡先の最大長 (Maximum Contact Length)**

要求または応答の [連絡先 (Contact) ] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:15 が有効である場合、[連絡先 (Contact) ] が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[連絡先 (Contact) ] フィールドには、後続のメッセージについての連絡先を指定する URI が示されます。

**コンテンツの最大長 (Maximum Content Length)**

要求または応答のメッセージ ボディのコンテンツで許容される最大バイト数を指定します。ルール 140:16 が有効である場合、コンテンツが長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。

**音声/ビデオ データ チャンルを無視 (Ignore Audio/Video Data Channel)**

データ チャンル トラフィックのインスペクションを有効または無効にします。このオプションを有効にすると、プリプロセッサはその他の非データチャンネル SIP トラフィックのインスペクションを続行するので注意してください。

**関連トピック**

[SIP キーワード](#) (1775 ページ)

## SIP プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

## 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析 ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション パネルで [設定 (Settings)] をクリックします。

**ステップ 4** [アプリケーション層プリプロセッサ (Application Layer Preprocessors)] の下の [SIP の設定 (SIP Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [SIP の設定 (SIP Configuration)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [SIP プリプロセッサのオプション \(1905 ページ\)](#) の説明に従ってオプションを変更します。

**ステップ 7** 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックし、[変更の確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

## 次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、SIP プリプロセッサルール (GID 140) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 関連トピック

[レイヤの管理 \(1599 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## その他の SIP プリプロセッサルール

次の表に示す SIP プリプロセッサルールは、特定の設定オプションに関連付けられていません。その他の SIP プリプロセッサルールと同様に、これらのルールによって イベントを生成し、インライン展開では、違反パケットをドロップします。する場合は、これらのルールを有効にする必要があります。

表 199: その他の SIP プリプロセッサルール

プリプロセッサルール <b>GID:SID</b>	以下の場合にトリガーする
140:1	プリプロセッサがモニタしている SIP セッションの数が、システムで許容される最大数である。
140:2	SIP 要求で [要求 URI (Request URI)] 必須フィールドが空である。
140:4	SIP 要求または応答の Call-ID ヘッダー フィールドが空である。
140:6	SIP 要求または応答の CSeq フィールドのシーケンス番号値が、231 未満の 32 ビット符号なし整数ではない。
140:8	SIP 要求または応答の [送信元 (From)] 必須フィールドが空である。
140:10	SIP 要求または応答の [送信先 (To)] ヘッダー フィールドが空である。
140:12	SIP 要求または応答の [経由 (Via)] ヘッダー フィールドが空である。
140:14	SIP 要求または応答で [連絡先 (Contact)] 必須フィールドが空である。
140:17	UDP トラフィック内の 1 つの SIP 要求または応答パケットに複数のメッセージが含まれている。SIP の旧バージョンでは複数メッセージがサポートされていますが、SIP 2.0 ではパケットあたり 1 メッセージだけがサポートされていることに注意してください。
140:18	UDP トラフィック内の SIP 要求または応答のメッセージ本文の実際の長さが SIP 要求または応答の [コンテンツ長 (Content-Length)] ヘッダー フィールドに指定されている値と一致しない。
140:19	プリプロセッサが SIP 応答の [CSeq] フィールドのメソッド名を認識しない。
140:20	SIP サーバが、認証済み招待メッセージに対してチャレンジを送信しない。これは InviteReplay 請求攻撃の場合に発生することに注意してください。
140:21	呼び出しが設定される前に、セッション情報が変更される。これは FakeBusy 請求攻撃の場合に発生することに注意してください。

プリプロセッサ ルール <b>GID:SID</b>	以下の場合にトリガーする
140:22	応答ステータス コードが 3 桁の数字でない。
140:23	[コンテンツ タイプ (Content-Type) ]ヘッダーフィールドにコンテンツ タイプが指定されておらず、メッセージ ボディにデータが含まれている。
140:24	SIP バージョンが 1、1.1、2.0 でない。
140:25	SIP 要求で、[CSeq] ヘッダーで指定されたメソッドとメソッド フィールドが一致しない。
140:26	プリプロセッサが SIP 要求のメソッド フィールドに指定されたメソッドを認識しない。

## GTP プリプロセッサ

General Packet Radio Service (GPRS) Tunneling Protocol (GTP) により、GTP コア ネットワークを介した通信が実現します。GTP プリプロセッサは、GTP トラフィックの異常を検出し、コマンドチャンネルシグナリングメッセージをインスペクションのためにルールエンジンに転送します。GTP コマンドチャンネルトラフィックでエクスプロイトがあるかどうかを検査するには、`gtp_version`、`gtp_type`、および `gtp_info` ルール キーワードを使用します。

1つの構成オプションで、プリプロセッサがGTPコマンドチャンネルメッセージを検査するポートのデフォルト設定を変更できます。

## GTP プリプロセッサ ルール

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、次の表に示す GTP プリプロセッサ ルールを有効にする必要があります。

表 200: GTP プリプロセッサ ルール

プリプロセッサ ルール <b>GID:SID</b>	説明
143:1	プリプロセッサが無効なメッセージの長さを検出すると、イベントが生成されます。
143:2	プリプロセッサが無効な情報要素の長さを検出すると、イベントが生成されます。
143:3	プリプロセッサが誤った順序の情報要素を検出すると、イベントが生成されます。

## GTP プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

GTP プリプロセッサが GTP コマンド メッセージをモニタするポートを変更するには、次の手順を使用します。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析 ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析 ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** 左側のナビゲーション パネルで [設定 (Settings)] をクリックします。

**ステップ 4** [アプリケーション層プリプロセッサ (Application Layer Preprocessors)] の下の [GTP コマンド チャネル構成 (GTP Command Channel Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [GTP コマンドチャネル構成 (GTP Command Channel Configuration)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** ポート値を入力します。

複数のポートを指定する場合は、カンマで区切ります。

**ステップ 7** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

### 次のタスク

- 侵入イベントを有効にする場合は、GTP プリプロセッサルール (GID 143) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## IMAP プリプロセッサ

Internet Message Application Protocol (IMAP) は、リモート IMAP サーバから電子メールを取得するときに使用されます。IMAP プリプロセッサはサーバクライアント IMAP4 トラフィックを検査し、関連するプリプロセッサルールが有効な場合は、異常なトラフィックがあるとイベントを生成します。プリプロセッサは、クライアント/サーバ IMAP4 トラフィックの電子メール添付ファイルを抽出してデコードし、添付ファイルデータをルールエンジンに送信することもできます。添付ファイルデータを指し示すには、侵入ルールで `file_data` キーワードを使用します。

抽出とデコードでは、複数の添付ファイル (存在する場合) や、複数パケットにまたがる大きな添付ファイルなども処理されます。

## IMAP プリプロセッサ オプション

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル (存在する場合) および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 デコーディングの深さ (Base64 Decoding Depth) ]、[7 ビット/8 ビット/バイナリのデコーディングの深さ (7-Bit/8-Bit/Binary Decoding Depth) ]、[Quoted-Printable (QP) のデコーディングの深さ (Quoted-Printable Decoding Depth) ]、または [Unix-to-Unix (UU) のデコーディングの深さ (Unix-to-Unix Decoding Depth) ] オプションの値が以下のポリシーで異なる場合は、最も大きい値が使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー



**注意** [Base64 復号の深さ (Base64 Decoding Depth) ]、[7 ビット/8 ビット/バイナリ復号化の深さ (7-Bit/8-Bit/Binary Decoding Depth) ]、[Quoted-Printable (QP) のデコーディングの深さ (Quoted-Printable Decoding Depth) ]、または [UNIX 間復号の深さ (Unix-to-Unix Decoding Depth) ] の値の変更設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

### ポート

IMAP トラフィックを検査するポートを指定します。0 ~ 65535 の整数を指定できます。ポート番号が複数ある場合は、カンマで区切ります。

### Base64 デコーディングの深さ (Base64 Decoding Depth)

各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはすべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

このオプションが有効である場合、ルール 141:4 を有効にすると、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます (エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります)。

### 7 ビット/8 ビット/バイナリのデコーディングの深さ (7-Bit/8-Bit/Binary Decoding Depth)

デコードを必要としない各 MIME 電子メール添付ファイルから抽出するデータの最大バイト数を指定します。これらの添付ファイルタイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ (プレーンテキスト、jpeg イメージ、mp3 ファイルなど) があります。正値またはパケット内のすべてのデータを抽出するには 0 を指定できます。非デコードデータを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 141:6 を有効にすると、抽出の失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます (たとえばデータの破損のために抽出が失敗することがあります)。

### Quoted-Printable (QP) のデコーディングの深さ (Quoted-Printable Decoding Depth)

各 quoted-printable (QP) エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはパケットのすべての QP エンコード済みデータを復号化する場合は 0 を指定します。QP エンコードデータを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 141:5 を有効にすると、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます (エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります)。

### Unix-to-Unix (UU) のデコーディングの深さ (Unix-to-Unix Decoding Depth)

各 Unix-to-Unix エンコード (UU エンコード) 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。パケットのすべての UU エンコードデータをデコードする

には、正値を指定するか、0 を指定できます。UU エンコード データを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 141:7 を有効にして、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

#### 関連トピック

[file\\_data キーワード](#) (1814 ページ)

## IMAP プリプロセッサの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin



**注意** [Base64 復号の深さ (Base64 Decoding Depth) ]、[7 ビット/8 ビット/バイナリ復号化の深さ (7-Bit/8-Bit/Binary Decoding Depth) ]、[Quoted-Printable (QP) のデコーディングの深さ (Quoted-Printable Decoding Depth) ]、または [UNIX 間復号の深さ (Unix-to-Unix Decoding Depth) ] の値の変更 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作](#) (356 ページ) を参照してください。

#### 手順

**ステップ 1** [ポリシー (Policies) ] > [アクセス コントロール (Access Control) ]、次に [ネットワーク分析 ポリシー (Network Analysis Policy) ] をクリックします。または [ポリシー (Policies) ] > [アクセス コントロール (Access Control) ] > [侵入 (Intrusion) ]、次に [ネットワーク分析ポリシー (Network Analysis Policy) ] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション パネルで [設定 (Settings) ] をクリックします。



**ステップ 4** [アプリケーション層プリプロセッサ (Application Layer Preprocessors)] の下の [IMAP の構成 (IMAP Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [IMAP の構成 (IMAP Configuration)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [IMAP プリプロセッサ オプション \(1912 ページ\)](#) で説明されている設定を変更します。

**ステップ 7** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

### 次のタスク

- 侵入イベントを有効にする場合は、IMAP プリプロセッサルール (GID 141) を有効にします。[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[侵入ポリシーおよびネットワーク分析ポリシーのレイヤ \(1591 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## その他の IMAP プリプロセッサルール

次の表に示す IMAP プリプロセッサルールは、特定の設定オプションに関連付けられていません。他の IMAP プリプロセッサルールの場合と同様に、これらのルールでイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルールを有効にする必要があります。

表 201: その他の IMAP プリプロセッサルール

プリプロセッサルール GID:SID	説明
141:1	プリプロセッサが RFC 3501 に定義されていないクライアントコマンドを検出すると、イベントが生成されます。
141:2	プリプロセッサが RFC 3501 に定義されていないサーバ応答を検出すると、イベントが生成されます。
141:3	プリプロセッサが使用しているメモリの量が、システムでの最大許容量に達している場合に、イベントが生成されます。この時点で、プリプロセッサはメモリが使用可能になるまでデコードを停止します。

# POP プリプロセッサ

Post Office Protocol (POP) は、リモート POP メール サーバから電子メールを取得するときに使用されます。POP プリプロセッサは、サーバからクライアントへの POP3 トラフィックを検査し、関連付けられているプリプロセッサルールが有効な場合は、異常なトラフィックについてのイベントを生成します。プリプロセッサは、クライアントからサーバへの POP3 トラフィック内の電子メールの添付ファイルを抽出して復号化（デコード）し、添付ファイルデータをルールエンジンに送信することもできます。添付ファイルデータを指し示すには、侵入ルールで `file_data` キーワードを使用します。

抽出とデコードでは、複数の添付ファイル（存在する場合）や、複数パケットにまたがる大きな添付ファイルなども処理されます。

## POP プリプロセッサ オプション

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 デコーディングの深さ (Base64 Decoding Depth) ]、[7 ビット/8 ビット/バイナリのデコーディングの深さ (7-Bit/8-Bit/Binary Decoding Depth) ]、[Quoted-Printable (QP) のデコーディングの深さ (Quoted-Printable Decoding Depth) ]、または [Unix-to-Unix (UU) のデコーディングの深さ (Unix-to-Unix Decoding Depth) ] オプションの値が以下のポリシーで異なる場合は、最も大きい値が使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー



**注意** [Base64 復号の深さ (Base64 Decoding Depth) ]、[7 ビット/8 ビット/バイナリ復号化の深さ (7-Bit/8-Bit/Binary Decoding Depth) ]、[Quoted-Printable (QP) のデコーディングの深さ (Quoted-Printable Decoding Depth) ]、または [UNIX 間復号の深さ (Unix-to-Unix Decoding Depth) ] の値の変更設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

## ポート

POP トラフィックを検査するポートを指定します。0～65535の整数を指定できます。ポート番号が複数ある場合は、カンマで区切ります。

### Base64 デコーディングの深さ (Base64 Decoding Depth)

各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはすべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

このオプションが有効である場合、ルール 142:4 を有効にして、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

### 7 ビット/8 ビット/バイナリのデコーディングの深さ (7-Bit/8-Bit/Binary Decoding Depth)

デコードを必要としない各 MIME 電子メール添付ファイルから抽出するデータの最大バイト数を指定します。これらの添付ファイルタイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ (プレーンテキスト、jpeg イメージ、mp3 ファイルなど) があります。正值またはパケット内のすべてのデータを抽出するには 0 を指定できます。非デコードデータを無視するには、-1 を指定します。

このオプションが有効であれば、抽出が失敗したときにルール 142:6 を有効にしてイベントを生成し、インライン展開では、違反パケットをドロップします。できます。抽出は、たとえば、データの破損により失敗することがあります。

### Quoted-Printable (QP) のデコーディングの深さ (Quoted-Printable Decoding Depth)

各 quoted-printable (QP) エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはパケットのすべての QP エンコード済みデータを復号化する場合は 0 を指定します。QP エンコードデータを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 142:5 を有効にして、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

### Unix-to-Unix (UU) のデコーディングの深さ (Unix-to-Unix Decoding Depth)

各 Unix-to-Unix エンコード (UU エンコード) 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。パケットのすべての UU エンコードデータをデコードするには、正值を指定するか、0 を指定できます。UU エンコードデータを無視するには、-1 を指定します。

このオプションが有効である場合、ルール142:7を有効にして、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

#### 関連トピック

[レイヤの管理](#) (1599 ページ)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー](#) (1587 ページ)

[file\\_data キーワード](#) (1814 ページ)

## POP プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin



**注意** [Base64 復号の深さ (Base64 Decoding Depth) ]、[7 ビット/8 ビット/バイナリ復号化の深さ (7-Bit/8-Bit/Binary Decoding Depth) ]、[Quoted-Printable (QP) のデコーディングの深さ (Quoted-Printable Decoding Depth) ]、または [UNIX 間復号の深さ (Unix-to-Unix Decoding Depth) ]の値の変更設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作](#) (356 ページ) を参照してください。

#### 手順

**ステップ 1** [ポリシー (Policies) ] > [アクセス コントロール (Access Control) ]、次に [ネットワーク分析ポリシー (Network Analysis Policy) ] をクリックします。または [ポリシー (Policies) ] > [アクセス コントロール (Access Control) ] > [侵入 (Intrusion) ]、次に [ネットワーク分析ポリシー (Network Analysis Policy) ] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション パネルで [設定 (Settings) ] をクリックします。

**ステップ 4** [アプリケーション層プリプロセッサ (Application Layer Preprocessors) ] の下の [POP の構成 (POP Configuration) ] が無効になっている場合は、[有効化 (Enabled) ] をクリックします。

**ステップ 5** [POP の構成 (POP Configuration) ] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [POP プリプロセッサ オプション \(1916 ページ\)](#) で説明されている設定を変更します。

**ステップ 7** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information) ] をクリックして、[変更を確定 (Commit Changes) ] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

### 次のタスク

- 侵入イベントを有効にする場合は、POP プリプロセッサルール (GID 142) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[レイヤの管理 \(1599 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## その他の POP プリプロセッサルール

次の表に示す POP プリプロセッサルールは、特定の設定オプションに関連付けられていません。その他の POP プリプロセッサルールと同様に、これらのルールによってイベントを生成し、インライン展開では、違反パケットをドロップします。する場合は、これらのルールを有効にする必要があります。

表 202: その他の POP プリプロセッサルール

プリプロセッサルール GID:SID	説明
142:1	プリプロセッサが RFC 1939 に定義されていないクライアントコマンドを検出すると、イベントが生成されます。
142:2	プリプロセッサが RFC 1939 に定義されていないサーバ応答を検出すると、イベントが生成されます。
142:3	プリプロセッサが使用しているメモリの量が、システムでの最大許容量に達している場合に、イベントが生成されます。この時点で、プリプロセッサはメモリが使用可能になるまでデコードを停止します。

# SMTP プリプロセッサ

SMTP プリプロセッサはルールエンジンに対し、SMTP コマンドを正規化するように指示します。このプリプロセッサは、クライアントからサーバへのトラフィック内の電子メールの添付ファイルを抽出して復号化（デコード）することもできます。またソフトウェアのバージョンによっては、SMTP トラフィックによりトリガーされた侵入イベントの表示時にコンテキストを提供するために、電子メールのファイル名、アドレス、およびヘッダー データも抽出します。

## SMTP プリプロセッサのオプション

正規化を有効または無効にし、SMTP デコーダが検出する異常トラフィックのタイプを制御するオプションを設定できます。

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 デコーディングの深さ (Base64 Decoding Depth) ]、[7 ビット/8 ビット/バイナリのデコーディングの深さ (7-Bit/8-Bit/Binary Decoding Depth) ]、[Quoted-Printable (QP) のデコーディングの深さ (Quoted-Printable Decoding Depth) ]、または [Unix-to-Unix (UU) のデコーディングの深さ (Unix-to-Unix Decoding Depth) ] オプションの値が以下のポリシーで異なる場合は、最も大きい値が使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー



**注意** [Base64 復号の深さ (Base64 Decoding Depth) ]、[7 ビット/8 ビット/バイナリ復号化の深さ (7-Bit/8-Bit/Binary Decoding Depth) ]、[Quoted-Printable (QP) のデコーディングの深さ (Quoted-Printable Decoding Depth) ]、または [UNIX 間復号の深さ (Unix-to-Unix Decoding Depth) ] の値の変更 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

## ポート

SMTP トラフィックを正規化するポートを指定します。0以上の値を指定できます。複数のポートを指定する場合は、カンマで区切ります。

## ステートフル インスペクション (Stateful Inspection)

選択されている場合、SMTP デコーダは状態を保存し、各パケットのセッションコンテキストを提供し、再構成されたセッションだけを検査します。選択されていない場合、セッションコンテキストなしで個々のパケットを分析します。

## 正規化 (Normalize)

[すべて (All)] に設定すると、すべてのコマンドが正規化されます。コマンドの後に複数のスペース文字があるかどうかを確認します。

[なし (None)] に設定すると、コマンドは正規化されません。

[Cmds] に設定すると、[カスタム コマンド (Custom Commands)] にリストされているコマンドが正規化されます。

## カスタム コマンド (Custom Commands)

[正規化 (Normalize)] が [Cmds] に設定されている場合に、リストされているコマンドが正規化されます。

正規化する必要があるコマンドをテキストボックスに指定します。コマンドの後に複数のスペース文字があるかどうかを確認します。

スペース文字 (ASCII 0x20) とタブ文字 (ASCII 0x09) は、正規化のためにスペース文字としてカウントされます。

## データを無視 (Ignore Data)

メールデータを処理せず、MIME メールヘッダーデータだけを処理します。

## TLS データを無視 (Ignore TLS Data)

Transport Layer Security プロトコルで暗号化されたデータを処理しません。

## アラートなし (No Alerts)

関連するプリプロセッサルールが有効である場合に、侵入イベントを無効にします。

## 不明なコマンドの検出 (Detect Unknown Commands)

SMTP トラフィックで不明なコマンドを検出します。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 124:5 を有効にできます。

### コマンドラインの最大長 (Max Command Line Len)

SMTP コマンドラインがこの値より長い場合にそのことを検出します。コマンドラインの長さを検出しない場合は、0 を指定します。

RFC 2821 (Network Working Group による Simple Mail Transfer Protocol 仕様) では、コマンドラインの最大長として 512 が推奨されています。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 124:1 を有効にできます。

### ヘッダ行の最大長 (Max Header Line Len)

SMTP データ ヘッダ行がこの値より長い場合にそのことを検出します。データ ヘッダ行の長さを検出しない場合は、0 を指定します。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 124:2 および 124:7 を有効にします。

### 応答行の最大長 (Max Response Line Len)

SMTP 応答行がこの値より長い場合にそのことを検出します。応答行の長さを検出しない場合は、0 を指定します。

RFC 2821 では、応答行の最大長として 512 が推奨されています。

ルール 124:3 を有効にすると、このオプションに関して、および [代替のコマンドラインの最大長 (Alt Max Command Line Len) ] オプション (有効になっている場合) に関してイベントを生成し、インライン展開では、違反パケットをドロップします。を行うことができます。

### 代替のコマンドラインの最大長 (Alt Max Command Line Len)

指定のコマンドの SMTP コマンドラインがこの値より長い場合にそのことを検出します。指定したコマンドのコマンドライン長を検出しない場合は、0 を指定します。多数のコマンドに対して、さまざまなデフォルト ライン長が設定されています。

この設定は、指定されたコマンドの [コマンドラインの最大長 (Max Command Line Len) ] の設定をオーバーライドします。

ルール 124:3 を有効にすると、このオプションに関して、および [応答行の最大長 (Max Response Line Len) ] オプション (有効になっている場合) に関してイベントを生成し、インライン展開では、違反パケットをドロップします。を行うことができます。

### 無効なコマンド (Invalid Commands)

これらのコマンドがクライアント側から送信された場合にそのことを検出します。

ルール 124:6 を有効にすると、このオプションに関して、および [無効なコマンド (Invalid Commands) ] に関してイベントを生成し、インライン展開では、違反パケットをドロップします。を行うことができます。



### 有効なコマンド (Valid Commands)

このリストのコマンドを許可します。

このリストが空の場合でも、プリプロセッサにより許可される有効なコマンドは、ATR N AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR です。



(注) RCPT TO および MAIL FROM は SMTP コマンドです。プリプロセッサ設定では、コマンド名 RCPT と MAIL がそれぞれ使用されます。プリプロセッサはコード内で RCPT および MAIL を正しいコマンド名にマッピングします。

ルール 124:4 を有効にすると、このオプションに関して、および [無効なコマンド (Invalid Commands)] オプション (設定済みの場合) に関して イベントを生成し、インライン展開では、違反パケットをドロップします。を行うことができます。

### データ コマンド (Data Commands)

RFC 5321 に基づく SMTP DATA コマンドによるデータの送信と同じ方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

### バイナリ データ コマンド (Binary Data Commands)

RFC 3030 に基づく BDAT コマンドによるデータの送信と類似の方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

### 認証コマンド (Authentication Commands)

クライアントおよびサーバ間で認証交換を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

### xlink2state の検出 (Detect xlink2state)

X-Link2State Microsoft Exchange バッファ データ オーバーフロー攻撃の一部であるパケットを検出します。インライン展開では、システムはこれらのパケットをドロップすることもできます。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 124:8 を有効にできます。

### Base64 デコーディングの深さ (Base64 Decoding Depth)

[データを無視 (Ignore Data)] が無効である場合、各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。正の値から指定するか 0 を指定して、すべての Base64 データをデコードします。Base64 データを無視するには、-1 を指

定めます。[データを無視 (Ignore Data)] が選択されている場合、プリプロセッサはデータをデコードしません。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

このオプションが有効である場合、ルール 124:10 を有効にすると、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。を行うことができます (エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります)。

このオプションは、廃止されたオプション [MIME デコーディングの有効化 (Enable MIME Decoding)] および [MIME デコーディングの最大の深さ (Maximum MIME Decoding Depth)] の代わりに使用されます。廃止されたこれらのオプションは、既存の侵入ポリシーでは後方互換性を維持する目的で引き続きサポートされています。

### 7 ビット/8 ビット/バイナリのデコーディングの深さ (7-Bit/8-Bit/Binary Decoding Depth)

[データを無視 (Ignore Data)] が無効である場合、デコードを必要としない各 MIME 電子メール添付ファイルから抽出する最大バイト数を指定します。これらの添付ファイルタイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパートコンテンツタイプ (プレーンテキスト、jpeg イメージ、mp3 ファイルなど) があります。正値またはパケット内のすべてのデータを抽出するには 0 を指定できます。非デコードデータを無視するには、-1 を指定します。[データを無視 (Ignore Data)] が選択されている場合、プリプロセッサはデータを抽出しません。

### Quoted-Printable (QP) のデコーディングの深さ (Quoted-Printable Decoding Depth)

[データを無視 (Ignore Data)] が無効な場合、各 quoted-printable (QP) エンコード MIME 電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。

1 ~ 65535 バイトを指定するか、または、パケットのすべての QP エンコードデータをデコードする場合は 0 を指定します。QP エンコードデータを無視するには、-1 を指定します。[データを無視 (Ignore Data)] が選択されている場合、プリプロセッサはデータをデコードしません。

このオプションが有効である場合、ルール 124:11 を有効にすると、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます (エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります)。

### Unix-to-Unix (UU) のデコーディングの深さ (Unix-to-Unix Decoding Depth)

[データを無視 (Ignore Data)] が無効な場合、各 UNIX 間エンコード (UU エンコード) 電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。1 ~ 65535 バイトを指定するか、または、パケットのすべての UU エンコードデータをデコードする場合は 0 を指定します。UU エンコードデータを無視するには、-1 を指定します。[データを無視 (Ignore Data)] が選択されている場合、プリプロセッサはデータをデコードしません。

このオプションが有効である場合、ルール 124:13 を有効にすると、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

### MIME 添付ファイル名のログ (Log MIME Attachment Names)

MIME Content-Disposition ヘッダーからの MIME 添付ファイル名の抽出を有効にして、セッションで生成されるすべての侵入イベントにこのファイル名を関連付けます。複数ファイル名がサポートされています。

このオプションが有効である場合、侵入イベントのテーブルビューの[電子メール添付 (Email Attachment)] 列に、イベントに関連付けられているファイル名が表示されます。

### 受信者アドレスのログ (Log To Addresses)

SMTP RCPT TO コマンドからの受信者の電子メールアドレスの抽出を有効にし、セッションで生成されるすべての侵入イベントにこの受信者アドレスに関連付けます。複数の受信者がサポートされます。

このオプションが有効である場合、侵入イベントのテーブルビューの[電子メール受信者 (Email Recipient)] 列に、イベントに関連付けられている受信者が表示されます。

### 送信者アドレスのログ (Log From Addresses)

SMTP MAIL FROM コマンドからの送信者の電子メールアドレスの抽出を有効にし、セッションで生成されるすべての侵入イベントにこの送信者アドレスに関連付けます。複数の送信者アドレスがサポートされます。

このオプションが有効である場合、侵入イベントのテーブルビューの[電子メール送信者 (Email Sender)] 列に、イベントに関連付けられている送信者が表示されます。

### ヘッダーのログ (Log Headers)

電子メールヘッダーの抽出を有効にします。抽出されるバイト数は、[ヘッダーのログの深さ (Header Log Depth)] に指定されている値によって決まります。

キーワード `content` または `protected_content` を使用して、電子メールヘッダーデータをパターンとして使用する侵入ルールを作成できます。侵入イベントパケットビューに、抽出された電子メールヘッダーが表示されます。

### ヘッダーのログの深さ (Header Log Depth)

[ヘッダーのログ (Log Headers)] が有効である場合、抽出する電子メールヘッダーのバイト数を指定します。0 ~ 20480 バイトを指定できます。値 0 を指定すると、[ヘッダーのログ (Log Headers)] が無効になります。

### 関連トピック

[基本コンテンツおよび `protected\_content` キーワードの引数](#) (1714 ページ)

## SMTP デコードの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。



**注意** [Base64 復号の深さ (Base64 Decoding Depth)]、[7 ビット/8 ビット/バイナリ復号化の深さ (7-Bit/8-Bit/Binary Decoding Depth)]、[Quoted-Printable (QP) のデコーディングの深さ (Quoted-Printable Decoding Depth)]、または [UNIX 間復号の深さ (Unix-to-Unix Decoding Depth)] の値の変更設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション ウィンドウで [設定 (Settings)] をクリックします。

**ステップ 4** [アプリケーション層プリプロセッサ (Application Layer Preprocessors)] の下の [SMTP の設定 (SMTP Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [SMTP の設定 (SMTP Configuration)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [SMTP プリプロセッサのオプション \(1920 ページ\)](#) の説明に従ってオプションを変更します。

**ステップ 7** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

### 次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、SMTP プリプロセッサルール (GID 124) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

- [レイヤの管理 \(1599 ページ\)](#)
- [競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## SSH プリプロセッサ

SSH プリプロセッサでは、次の攻撃を検出します。

- チャレンジレスポンス バッファ オーバーフロー エクスプロイト
- CRC-32 エクスプロイト
- SecureCRT SSH クライアント バッファ オーバーフロー エクスプロイト
- プロトコル不一致
- 不正な SSH メッセージの方向
- バージョン 1 または 2 以外のすべてのバージョン文字列

チャレンジレスポンス バッファ オーバーフロー攻撃と CRC--32 攻撃はいずれもキー交換の後に発生するので、暗号化されています。いずれの攻撃でも、20 KB を超える普通よりも大きなペイロードが認証チャレンジ直後にサーバに送信されます。CRC--32 攻撃の対象となるのは SSH バージョン 1 のみであり、チャレンジレスポンス バッファ オーバーフロー エクスプロイトの対象となるのは SSH バージョン 2 のみです。バージョン文字列は、セッションの開始時に読み取られます。バージョン文字列の違いを除き、この両方の攻撃は同様に扱われます。

SecureCRT SSH エクスプロイトとプロトコル不一致攻撃は、鍵交換前に接続をセキュリティで保護しようとするときに発生します。SecureCRT エクスプロイトでは、非常に長いプロトコル ID 文字列がクライアントに送信され、これが原因でバッファ オーバーフローが発生します。プロトコル不一致は、非 SSH クライアントアプリケーションがセキュア SSH サーバに接続しようとした場合、またはサーバとクライアントのバージョン番号が一致しない場合に発生します。

SSH プリプロセッサは、指定のポートまたはポートのリストでトラフィックを検査するか、または SSH トラフィックを自動的に検出するように設定できます。指定バイト数に達するまで

に指定数の暗号化パケットが渡されたか、指定パケット数に達するまでにバイト数が指定最大バイト数を超えるまで、SSHトラフィックの検査が続行されます。最大バイト数を超えた場合は、CRC--32 (SSHバージョン1) 攻撃またはチャレンジレスポンスバッファオーバーフロー (SSHバージョン2) 攻撃が発生したとみなされます。プリプロセッサは、設定していない場合でもバージョン1または2以外のバージョン文字列を検出することに注意してください。

SSHプリプロセッサでは、ブルートフォース攻撃が処理されないことにも注意してください。

## SSH プリプロセッサのオプション

次のいずれかが発生すると、プリプロセッサはセッションのトラフィックの検査を停止します。

- この数の暗号化パケットで、サーバとクライアント間で有効な交換が行われた場合。接続は続行します。
- 検査対象の暗号化パケットの数に達する前に、[サーバ応答がないまま送信されたバイト数 (Number of Bytes Sent Without Server Response) ]に達した場合。この場合、攻撃があったものと想定されます。

[検査する暗号化パケットの数 (Number of Encrypted Packets to Inspect) ]に達するまでの有効な各サーバ応答により、[サーバ応答がないまま送信されたバイト数 (Number of Bytes Sent Without Server Response) ]がリセットされ、パケットカウントが続行します。

次に示す SSH のプリプロセッサの設定例で説明します。

- [サーバポート (Server Ports) ] : 22
- [自動検出ポート (Autodetect Ports) ] : off
- [プロトコルバージョンストリングの最大長 (Maximum Length of Protocol Version String) ] : 80
- [検査する暗号化パケットの数 (Number of Encrypted Packets to Inspect) ] : 25
- [サーバ応答がないまま送信されたバイト数 (Number of Bytes Sent Without Server Response) ] : 19,600
- 検出オプションはすべて有効です。

この例では、プリプロセッサはポート 22 のトラフィックだけを検査します。つまり、自動検出が無効であるため、指定されたポートでのみ検査をします。

また、次のいずれかが発生すると、この例のプリプロセッサはトラフィックの検査を停止します。

- クライアントが 25 個の暗号化パケットを送信したが、すべてのパケットのデータ合計が 19,600 バイト以下であった。攻撃はなかったと想定されます。
- クライアントが、25 個の暗号化パケットで 19,600 バイトを超えるデータを送信した。この場合、この例のセッションは SSH バージョン 2 セッションであるため、プリプロセッサはこの攻撃がチャレンジレスポンスバッファオーバーフロー攻撃であるとみなします。

この例のプリプロセッサは、トラフィックの処理時に以下の状況が発生しているかどうかを検出します。

- 80 バイトより長いバージョン文字列によりトリガーとして使用されるサーバ オーバーフロー（これは SecureCRT エクスプロイトを示します）
- プロトコルの不一致
- 誤った方向に流れるパケット

最後に、プリプロセッサは、バージョン1または2以外のすべてのバージョン文字列を自動的に検出します。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

### サーバポート (Server Ports)

SSH プリプロセッサがトラフィックを検査する必要があるポートを指定します。

1つのポート、または複数のポートをカンマで区切ったリストを設定できます。

### 自動検出ポート (Autodetect Ports)

SSH トラフィックを自動的に検出するようにプリプロセッサを設定します。

このオプションが選択されている場合、プリプロセッサはすべてのトラフィックで SSH バージョン番号を検査します。クライアント パケットにもサーバ パケットにもバージョン番号が含まれていない場合は、処理が停止します。無効である場合、プリプロセッサは [サーバポート (Server Ports)] オプションで指定されているトラフィックだけを検査します。

### 検査する暗号化パケットの最大数 (Number of Encrypted Packets to Inspect)

セッションあたりの検査対象の暗号化パケットの数を指定します。

このオプションをゼロに設定すると、すべてのトラフィックの通過が許可されます。

検査対象の暗号化パケットの数を減らすと、一部の攻撃が検出されなくなることがあります。検査対象の暗号化パケットの数を増やすと、パフォーマンスに悪影響を及ぼす可能性があります。

### サーバ応答がないまま送信されたバイト数 (Number of Bytes Sent Without Server Response)

SSH クライアントが、応答なしでサーバに送信できる最大バイト数を指定します。この最大バイト数を超えると、チャレンジレスポンス バッファ オーバーフロー攻撃または CRC-32 攻撃が想定されます。

プリプロセッサがチャレンジレスポンス バッファ オーバーフローまたは CRC-32 エクスプロイトを誤検出する場合は、このオプションの値を増やしてください。

**プロトコルバージョンストリングの最大長 (Maximum Length of Protocol Version String)**

サーバのバージョン文字列の最大許容バイト数を指定します。この値を超えると、SecureCRT エクスプロイトとみなされます。

**チャレンジレスポンスバッファオーバーフロー攻撃の検出 (Detect Challenge-Response Buffer Overflow Attack)**

チャレンジレスポンスバッファオーバーフローエクスプロイトの検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 128:1 を有効にできます。

**SSH1 CRC-32 攻撃の検出 (Detect SSH1 CRC-32 Attack)**

CRC-32 エクスプロイトの検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 128:2 を有効にできます。

**サーバオーバーフローの検出 (Detect Server Overflow)**

SecureCRT SSH クライアントバッファオーバーフローエクスプロイトの検出を有効または無効にします。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 128:3 を有効にします。

**プロトコル不一致の検出 (Detect Protocol Mismatch)**

プロトコル不一致の検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 128:4 を有効にできます。

**正しくないメッセージ方向の検出 (Detect Bad Message Direction)**

トラフィックのフロー方向が正しくない場合（つまり、推定されるサーバがクライアントトラフィックを生成したり、クライアントがサーバトラフィックを生成したりした場合）の検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 128:5 を有効にできます。

**特定のペイロードに正しくないペイロードサイズの検出 (Detect Payload Size Incorrect for the Given Payload)**

SSH パケットに指定された長さが IP ヘッダーに指定されている合計長と矛盾する場合や、メッセージが切り捨てられる場合、つまり完全な SSH ヘッダーを形成できる十分なデータがない場合などの、誤ったペイロードサイズのパケットの検出を有効または無効にします。



このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 128:6 を有効にできます。

#### 正しくないバージョンストリングの検出 (Detect Bad Version String)

有効である場合、プリプロセッサは、設定していない場合でもバージョン 1 または 2 以外のバージョン文字列を検出することに注意してください。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 128:7 を有効にできます。

## SSH プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション パネルで [設定 (Settings)] をクリックします。

**ステップ 4** [アプリケーション層プリプロセッサ (Application Layer Preprocessors)] の下の [SSH の構成 (SSH Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [SSH の構成 (SSH Configuration)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [SSH プリプロセッサのオプション \(1928 ページ\)](#) の説明に従ってオプションを変更します。

**ステップ 7** 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックし、[変更の確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

### 次のタスク

- 侵入イベントを有効にする場合は、SSH プリプロセッサルール (GID 128) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[レイヤの管理 \(1599 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## SSL プリプロセッサ

SSL プリプロセッサでは、SSL インスペクション (検査) を設定できます。SSL インスペクションでは、暗号化トラフィックのブロック、暗号化トラフィックの復号化、またはアクセスコントロール (アクセス制御) によるトラフィックの検査を実行します。SSL インスペクションが設定されているかどうかに関係なく、SSL プリプロセッサでは、トラフィックで検出された SSL ハンドシェイク メッセージも分析し、セッションを暗号化するタイミングを決定します。暗号化トラフィックを識別することにより、システムは暗号化ペイロードの侵入およびファイルインスペクションを停止できます。これによって、誤検出が減少し、パフォーマンスが向上します。

SSL プリプロセッサは、暗号化トラフィックを検査して Heartbleed バグを悪用する試みを検出し、そのような悪用の検出時にイベントを生成することもできます。

セッションが暗号化されると、侵入およびマルウェアに対するトラフィックの検査を一時停止できます。SSL インスペクションを設定した場合、SSL プリプロセッサでは、ユーザがアクセスコントロールによってブロック、復号化、または検査を行える暗号化トラフィックも識別します。

SSL プリプロセッサを使用して暗号化トラフィックを復号化するために、ライセンスは必要ありません。マルウェアおよび侵入に対する暗号化ペイロードのインスペクションの停止、Heartbleed バグの悪用の検出など、他のすべての SSL プリプロセッサ機能には保護ライセンスが必要です。

## SSL 前処理の仕組み

SSL インスペクションを設定すると、SSL プリプロセッサは暗号化データに対する侵入およびファイルインスペクションを停止して、SSL ポリシーにより暗号化トラフィックを検査します。これにより誤検出を排除できます。SSL プリプロセッサは、SSL ハンドシェイクを検査するときに状態情報を保持し、そのセッションの状態と SSL バージョンの両方を追跡します。セッションの状態が暗号化されていることをプリプロセッサが検出すると、そのセッションのトラフィックは暗号化されているものとしてシステムによりマークされます。暗号化が確定した場合に暗号化セッションにおけるすべてのパケット処理を停止し、Heartbleed のバグを悪用する試みが検出された場合にイベントを生成するように、システムを設定できます。

パケットごとに、IP ヘッダー、TCP ヘッダー、および TCP ペイロードがトラフィックに含まれており、このトラフィックが SSL 前処理用に指定されているポートで発生することが SSL プリプロセッサにより確認されます。次に示す状況では、対象トラフィックについて、トラフィックが暗号化されているかどうかを判別されます。

- システムがセッションのすべてのパケットを監視し、[サーバ側のデータを信頼する (Server side data is trusted)] が有効にされておらず、サーバとクライアントの両方からの完了メッセージ、および Application レコードが存在するが Alert レコードがない各側からの 1 つ以上のパケットが、セッションに含まれている。
- システムがトラフィックの一部を検出せず、[サーバ側のデータを信頼する (Server side data is trusted)] が有効にされておらず、Alert レコードによる応答がない Application レコードが存在する各側からの 1 つ以上のパケットが、セッションに含まれている。
- システムがセッションのすべてのパケットを監視し、[サーバ側のデータを信頼する (Server side data is trusted)] が有効であり、クライアントからの完了メッセージ、および Application レコードが存在するが Alert レコードがないクライアントからの 1 つ以上のパケットが、セッションに含まれている。
- システムがトラフィックの一部を検出せず、[サーバ側のデータを信頼する (Server side data is trusted)] が有効であり、Alert レコードによる応答がない Application レコードが存在するクライアントからの 1 つ以上のパケットが、セッションに含まれている。

暗号化トラフィックの処理を停止することを選択する場合、セッションが暗号化されているものとしてマークされると、そのセッションのその後のパケットは無視されます。

また、SSL ハンドシェイク時、プリプロセッサはハートビート要求と応答をモニタします。プリプロセッサは、以下を検出したときにイベントを生成します。

- ペイロード自体よりも大きいペイロード長の値を含むハートビート要求
- [ハートビートの最大長 (Max Heartbeat Length)] フィールドに格納されている値よりも大きいハートビート応答



(注) ルール内で SSL 状態またはバージョン情報を使用するには、キーワード `ssl_state` および `ssl_version` をルールに追加します。

#### 関連トピック

[SSL キーワード \(1765 ページ\)](#)

[SSL インспекションの要件 \(1441 ページ\)](#)

## SSL プリプロセッサのオプション



- (注) システム付属のネットワーク分析ポリシーは、デフォルトでSSLプリプロセッサを有効にします。暗号化トラフィックがネットワークを通過することを予想している場合、シスコは、カスタム展開でSSLプリプロセッサを無効にしないことを推奨します。

SSLインスペクションを設定しないと、システムは暗号化トラフィックを復号化せずに、マルウェアと侵入について暗号化トラフィックの検査を試行します。SSLプリプロセッサを有効にすると、セッションが暗号化されたときにそのことを検出します。SSLプリプロセッサが有効にされると、ルールエンジンがこのプリプロセッサを呼び出し、SSLの状態およびバージョン情報を取得できるようになります。侵入ポリシーでキーワード `ssl_state` および `ssl_version` を使用してルールを有効にする場合は、そのポリシーでSSLプリプロセッサも有効にする必要があります。

### ポート

SSLプリプロセッサは、暗号化されたセッションのトラフィックをモニタする必要があるポートを、カンマで区切って指定します。このフィールドで指定されるポートでのみ、暗号化トラフィックが検査されます。



- (注) SSLプリプロセッサは、SSLモニタの対象として指定されたポートでSSL以外のトラフィックを検出すると、そのトラフィックをSSLトラフィックとしてデコードすることを試みた後、破損しているものとしてマークします。

### 暗号化トラフィックの検査を停止する (Stop inspecting encrypted traffic)

セッションが暗号化されているとしてマークされた後、セッションのトラフィックの検査を有効または無効にします。

暗号化されたセッションの検査を無効化しリアセンブルするには、このオプションを有効にします。SSLプリプロセッサによりセッションの状態が維持されるため、セッションのすべてのトラフィックのインスペクションを無効にできます。システムは、次の両方の場合に、暗号化されたセッションのトラフィックの検査のみを停止します。

- SSLの前処理が有効にされている
- このオプションが選択されている

このオプションをクリアすると、[サーバ側のデータを信頼する (Server side data is trusted)] オプションを変更できません。

**サーバ側のデータを信頼する (Server side data is trusted)**

[暗号化トラフィックの検査を停止する (Stop inspecting encrypted traffic)] が有効にされており、クライアント側のトラフィックにのみ基づいて暗号化されたトラフィックの識別を有効にすると、

**ハートビートの最大長 (Max Heartbeat Length)**

バイト数を指定して、ハートビートバグ悪用の試みに対する SSL ハンドシェイク内のハートビート要求と応答の検査を有効にします。1 ~ 65535 の整数を指定できます。このオプションを無効にする場合は 0 を入力します。

プリプロセッサがハートビート要求を検出し、このペイロード長が実際のペイロード長より大きく、ルール 137:3 が有効にされている場合、または、ルール 137:4 が有効にされている際に、このオプションに設定された値よりハートビート応答のサイズが大きい場合は、プリプロセッサはイベントを生成し、インライン展開では、違反パケットをドロップします。。

## SSL プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

**手順**

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション パネルで [設定 (Settings)] をクリックします。

**ステップ 4** [アプリケーション層プリプロセッサ (Application Layer Preprocessors)] の下の [SSL 設定 (SSL Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [SSL 設定 (SSL Configuration)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [SSL プリプロセッサのオプション \(1934 ページ\)](#) に示されている任意の設定を変更します。

- [ポート (Ports) ]フィールドに値を入力します。複数の値を指定する場合は、カンマで区切ります。
- [暗号化トラフィックの検査の停止 (Stop inspecting encrypted traffic) ]チェックボックスをオンまたはオフにします。
- [暗号化トラフィックの検査の停止 (Stop inspecting encrypted traffic) ]チェックボックスをオンにした場合は、[サーバ側データは信頼済み (Server side data is trusted) ]チェックボックスをオンまたはオフにします。
- [最大ハートビート長 (Max Heartbeat Length) ]フィールドに値を入力します。  
ヒント 値 0 を指定すると、このオプションが無効になります。

**ステップ 7** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information) ]をクリックして、[変更を確定 (Commit Changes) ]をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

#### 次のタスク

- 侵入イベントを有効にする場合は、SSL プリプロセッサ ルール (GID 137) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[レイヤの管理 \(1599 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

[SSL インスペクションの要件 \(1441 ページ\)](#)

## SSL プリプロセッサ ルール

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、SSL プリプロセッサ ルール (GID 137) を有効にします。

次の表に、有効にできる SSL プリプロセッサ ルールを示します。

表 203: SSL プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
137:1	ServerHello メッセージの後の ClientHello メッセージを検出します。これは無効であり、異常な動作とみなされません。

プリプロセッサルール <b>GID:SID</b>	説明
137:2	SSL プリプロセッサ オプション [サーバ側のデータを信頼する (Server side data is trusted) ] が無効な場合に、ClientHello メッセージのない ServerHello メッセージを検出します。これは無効であり、異常な動作としてみなされます。
137:3	SSL プリプロセッサ オプション [ハートビートの最大長 (Max Heartbeat Length) ] にゼロ以外の値が含まれている場合に、ペイロード自体よりも大きいペイロード長の値を含むハートビート要求を検出します。このようなハートビート要求は、Heartbleed バグを悪用する試みを示しています。
137:4	SSL プリプロセッサ オプション [ハートビートの最大長 (Max Heartbeat Length) ] で指定されているゼロ以外の値よりも大きいハートビート応答を検出します。このようなハートビート応答は、Heartbleed バグを悪用する試みを示しています。







## 第 80 章

# SCADA プリプロセッサ

以下のトピックでは、遠隔監視制御・情報取得（SCADA）プロトコルのプリプロセッサとその設定方法について説明します。

- [SCADA プリプロセッサの概要（1939 ページ）](#)
- [Modbus プリプロセッサ（1939 ページ）](#)
- [DNP3 プリプロセッサ（1942 ページ）](#)

## SCADA プリプロセッサの概要

Supervisory Control and Data Acquisition（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャプロセス、および設備プロセスからのデータをモニタ、制御、取得します。Firepower システムは、ネットワーク分析ポリシーの一部として設定できる Modbus および DNP3 SCADA プロトコル用のプリプロセッサを提供します。

対応する侵入ポリシーで Modbus または DNP3 キーワードを含むルールを有効にすると、Modbus または DNP3 プロセッサがその現在の設定で自動的に使用されます。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

## Modbus プリプロセッサ

Modbus プロトコルは 1979 年に Modicon が初めて発表した、広く利用されている SCADA プロトコルです。Modbus プリプロセッサは、Modbus トラフィックの異常を検出し、ルールエンジンによる処理のために Modbus プロトコルをデコードします。ルールエンジンは Modbus キーワードを使用して特定のプロトコルフィールドにアクセスします。

1 つの構成オプションで、プリプロセッサが Modbus トラフィックを検査するポートのデフォルト設定を変更できます。

### 関連トピック

- [SCADA キーワード（1790 ページ）](#)

## Modbus プリプロセッサ ポート オプション

### ポート

プリプロセッサが Modbus トラフィックを検査するポートを指定します。複数のポートを指定する場合は、カンマで区切ります。

## Modbus プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

ネットワークに Modbus 対応デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション パネルで [設定 (Settings)] をクリックします。

**ステップ 4** [SCADA プリプロセッサ (SCADA Preprocessors)] の下の [Modbus の構成 (Modbus Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [Modbus の構成 (Modbus Configuration)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [ポート (Ports)] フィールドに値を入力します。

複数の値を指定する場合は、カンマで区切ります。

**ステップ7** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

#### 次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、Modbus プリプロセッサルール (GID 144) を有効にします。詳細については、[侵入ルール状態の設定 \(1640ページ\)](#) および [Modbus プリプロセッサルール \(1941ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350ページ\)](#) を参照してください。

#### 関連トピック

[レイヤの管理 \(1599 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## Modbus プリプロセッサルール

次の表に示す Modbus プリプロセッサルールによって イベントを生成し、インライン展開では、違反パケットをドロップします。するには、これらのルールを有効にする必要があります。

表 204: Modbus プリプロセッサルール

プリプロセッサルール GID:SID	説明
144:1	Modbus の見出しの長さが、Modbus 機能コードに必要な長さとは一致していない場合に、イベントが生成されます。  各 Modbus 機能の要求と応答には期待される形式があります。メッセージの長さが、期待される形式と一致しない場合に、このイベントが生成されます。
144:2	Modbus プロトコル ID がゼロ以外の場合に、イベントが生成されます。プロトコル ID フィールドは、Modbus と共にその他のプロトコルを多重伝送するために使用されます。プリプロセッサはこのような他のプロトコルを処理しないため、代わりにこのイベントが生成されます。
144:3	プリプロセッサが予約済み Modbus 機能コードを検出すると、イベントが生成されます。

## DNP3 プリプロセッサ

Distributed Network Protocol (DNP3) は、当初は発電所間で一貫性のある通信を実現する目的で開発された SCADA プロトコルです。DNP3 も、水処理、廃棄物処理、輸送などさまざまな産業分野で幅広く利用されるようになっていきます。

DNP3 プリプロセッサは、DNP3 トラフィックの異常を検出し、ルールエンジンによる処理のために DNP3 プロトコルをデコードします。ルールエンジンは、DNP3 キーワードを使用して特定のプロトコルフィールドにアクセスします。

### 関連トピック

[DNP3 キーワード](#) (1791 ページ)

## DNP3 プリプロセッサ オプション

### ポート

指定された各ポートでの DNP3 トラフィックのインスペクションを有効にします。1 つのポートを指定するか、複数のポートをカンマで区切ったリストを指定できます。

### 無効な CRC を記録 (Log bad CRCs)

DNP3 リンク層フレームに含まれているチェックサムを検証します。無効なチェックサムを含むフレームは無視されます。

ルール 145:1 を有効にすると、無効なチェックサムが検出されたときにイベントを生成し、インライン展開では、違反パケットをドロップします。 できます。

## DNP3 プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

ネットワークに DNP3 対応デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

## 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション パネルで [設定 (Settings)] をクリックします。

**ステップ 4** [SCADA プリプロセッサ (SCADA Preprocessors)] の下の [DNP3 の構成 (DNP3 Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [DNP3 の構成 (DNP3 Configuration)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** ポートの値を入力します。

複数の値を指定する場合は、カンマで区切ります。

**ステップ 7** [不良 CRC の記録 (Log bad CRCs)] チェックボックスをオンまたはオフにします。

**ステップ 8** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

## 次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、DNP3 プリプロセッサルール (GID 145) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#)、[DNP3 プリプロセッサオプション \(1942 ページ\)](#)、および [DNP3 プリプロセッサルール \(1944 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 関連トピック

[レイヤの管理 \(1599 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## DNP3 プリプロセッサルール

次の表に示すDNP3プリプロセッサルールによってイベントを生成し、インライン展開では、違反パケットをドロップします。するには、これらのルールを有効にする必要があります。

表 205: DNP3 プリプロセッサルール

プリプロセッサルール <b>GID:SID</b>	説明
145:1	[無効な CRC を記録 (Log bad CRC) ] が有効である場合に、無効なチェックサムを含むリンク層フレームがプリプロセッサにより検出されると、イベントが生成されます。
145:2	無効な長さのDNP3リンク層フレームがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:3	再構成中に無効なシーケンス番号のトランスポート層セグメントがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:4	完全なフラグメントを再構成する前に DNP3 再構成バッファがクリアされると、イベントが生成されます。このことは、FIRフラグを送送するセグメントが、他のセグメントがキューに入れられた後で現れる場合に発生します。
145:5	予約済みアドレスを使用するDNP3リンク層フレームをプリプロセッサが検出すると、イベントが生成されます。
145:6	予約済み機能コードを使用するDNP3要求または応答をプリプロセッサが検出すると、イベントが生成されます。



## 第 81 章

# トランスポート層およびネットワーク層プリプロセッサ

以下のトピックでは、トランスポート層およびネットワーク層プリプロセッサとそれらの設定方法について説明します。

- [トランスポート層およびネットワーク層のプリプロセッサの概要 \(1945 ページ\)](#)
- [トランスポート/ネットワーク プリプロセッサの詳細設定 \(1946 ページ\)](#)
- [チェックサム検証 \(1949 ページ\)](#)
- [インライン正規化プリプロセッサ \(1951 ページ\)](#)
- [IP 最適化プリプロセッサ \(1960 ページ\)](#)
- [パケット デコーダ \(1966 ページ\)](#)
- [TCP ストリームの前処理 \(1971 ページ\)](#)
- [UDP ストリームの前処理 \(1985 ページ\)](#)

## トランスポート層およびネットワーク層のプリプロセッサの概要

トランスポート層およびネットワーク層のプリプロセッサは、IPフラグメンテーション、チェックサム検証、TCP および UDP セッションの前処理を悪用する攻撃を検出します。パケットがプリプロセッサに送信される前に、パケット デコーダはパケット ヘッダーとペイロードを、プリプロセッサおよび侵入ルールエンジンで簡単に使用できるフォーマットに変換し、パケット ヘッダー内でさまざまな変則的動作を検出します。インライン正規化プリプロセッサは、パケットをデコードした後、他のプリプロセッサにパケットを送信する前に、インライン型展開を対象にトラフィックを正規化します。

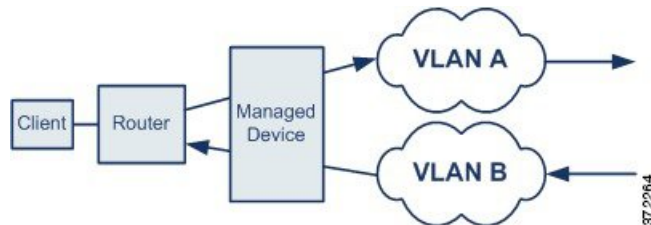
侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。

# トランスポート/ネットワークプリプロセッサの詳細設定

トランスポート/ネットワークプリプロセッサの詳細設定は、アクセスコントロールポリシーを展開するすべてのネットワーク、ゾーン、VLANにグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセスコントロールポリシーで設定します。

## 無視される VLAN ヘッダー

同じ接続で異なる方向に流れるトラフィックの VLAN タグが異なると、トラフィックのリアセンブルやルールの処理に影響を与える場合があります。たとえば、以下の図では、同じ接続のトラフィックを VLAN A で送信し、VLAN B で受信できます。



展開でパケットを正しく処理するため、VLANヘッダーを無視するようにシステムを設定できます。



(注) このオプションは、ASA FirePOWER ではサポートされません。

## 侵入廃棄ルールでのアクティブ応答

廃棄ルールは、ルール状態が [ドロップしてイベントを生成する (Drop and Generate Events) ] に設定された侵入ルールまたはプリプロセッサルールです。インライン展開では、システムは TCP または UDP 廃棄ルールに反応するために、トリガーしたパケットをドロップし、そのパケットが開始されたセッションをブロックします。パッシブ展開の場合、システムがパケットをドロップすることはできません。また、セッションをブロックすることはありませんが、アクティブ応答を使用する場合はその限りではありません。



**ヒント** UDP データ ストリームは一般にセッションという観点では考慮されないため、ストリーム プリプロセッサはカプセル化 IP データグラム ヘッダーの送信元と宛先の IP アドレス フィールドと UDP ヘッダーのポート フィールドを使用してフローの方向を判別し、UDP セッションを識別します。



問題のあるパケットによって TCP または UDP 廃棄ルールがトリガーされた時点で、1 つ以上のアクティブ応答を開始して、より正確かつ明示的に TCP 接続または UDP セッションを閉じるようにシステムを設定することができます。

インライン展開でアクティブ応答が有効にされている場合、システムは TCP 廃棄ルールへの応答として、トリガーしたパケットをドロップし、クライアントとサーバの両方のトラフィックに TCP リセット (RST) パケットを挿入します。システムはパッシブ展開でパケットをドロップできません。アクティブ応答がパッシブ展開で有効になっている場合、システムは TCP 接続のクライアント側とサーバ側の両方に TCP リセットを送信することによって TCP 廃棄ルールに応答します。インライン展開またはパッシブ展開でアクティブ応答が有効にされていると、システムはセッションの両端に ICMP 到達不能パケットを送信することによって UDP セッションを閉じます。リセットは接続やセッションに影響を与えるのに間に合うまでに到着する可能性が高いため、アクティブ応答はインライン展開で最も効果を発揮します。

設定内容によっては、接続またはセッションのいずれかの側からさらにトラフィックが発生しているようであれば、システムが追加のアクティブ応答を開始することもできます。システムは、指定された間隔 (秒数) で、指定された最大回数まで追加のアクティブ応答を開始します。

## トランスポート/ネットワーク プリプロセッサの詳細オプション

### 接続の追跡時に VLAN ヘッダーを無視する (Ignore the VLAN header when tracking connections)

トラフィックの識別時に VLAN ヘッダーを無視するか、それとも考慮するかを指定します。次のようになります。

- このオプションを選択すると、VLAN ヘッダーが無視されます。この設定は、異なる方向に移動するトラフィックで同じ接続について異なる VLAN タグを検出する可能性がある展開済みデバイスに使用します。
- このオプションを無効にすると、VLAN ヘッダーが考慮されます。この設定は、異なる方向に移動するトラフィックで同じ接続について異なる VLAN タグを検出しない展開済みデバイスに使用します。



(注) このオプションは、ASA FirePOWER ではサポートされていません。

### アクティブ応答の最大数 (Maximum Active Responses)

TCP 接続あたりのアクティブ応答の最大数を指定します。アクティブ応答が開始された接続でさらにトラフィックが発生し、前のアクティブ応答を送信してから [最小応答秒数 (Minimum Response Seconds)] を超えるトラフィックが発生した場合、システムは指定された最大数に達するまで、別のアクティブ応答を送信します。0 を設定すると、廃棄ルールによってトリガーされるアクティブ応答が無効になり、**resp** または **react** ルールによってトリガーされる追加のアクティブ応答も無効になります。

このオプションの設定とは関係なく、**resp** または **react** ルールがトリガーされた場合にも、アクティブ応答が開始されることに注意してください。ただし、このオプションは、ドロップルールでアクティブ応答の最大数を制御するのと同じ方法で、**resp** および **react** ルールで追加のアクティブ応答をシステムが開始するかどうかを制御します。

`config response` コマンドを使用して、使用するアクティブ応答インターフェイス、およびパッシブ展開で試行する TCP リセットの回数を設定することもできます。

#### 最小応答時間（秒）（Minimum Response Seconds）

[最大アクティブ応答数（Maximum Active Responses）] に達するまで、システムがアクティブ応答を開始した接続で発生した追加のトラフィックに対して次のアクティブ応答を送信するまで待機する時間を指定します。

#### トラブルシューティングオプション：セッション終了ログギングしきい値（Troubleshooting Options: Session Termination Logging Threshold）



**注意** [セッション終了ログギングしきい値（Session Termination Logging Threshold）] は、サポート担当から指示されない限り変更しないでください。

トラブルシューティングの電話中に、個別の接続が指定したしきい値を超えた場合にメッセージを記録するようにシステムを設定することをサポートから依頼される場合があります。このオプションの設定を変更するとパフォーマンスに影響するので、必ずサポートのガイダンスに従って実行してください。

このオプションは、ログに記録されるメッセージのバイト数を指定します。セッションが終了し、メッセージが指定のバイト数を超えた場合は、ログに記録されます。



(注) 上限は 1 GB ですが、管理対象デバイスでストリーム処理のために割り当てられるメモリの量によっても制限されます。

#### 関連トピック

[アクティブ応答のキーワード](#)（1796 ページ）

## トランスポート/ネットワーク プリプロセッサの詳細設定の構成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

## 手順

- 
- ステップ1** アクセスコントロールポリシーエディタで、[詳細 (Advanced)] タブをクリックします。
- ステップ2** [トランスポート/ネットワークレイヤ設定 (Transport/Network Layer Settings)] セクションの横にある編集アイコン (✎) をクリックします。
- ステップ3** トラブルシューティングオプション [セッション終了のロギングしきい値 (Session Termination Logging Threshold)] を除き、[トランスポート/ネットワークプリプロセッサの詳細オプション \(1947 ページ\)](#) の説明に従ってオプションを変更します。
- (注) [接続のトラッキング時はVLANヘッダーを無視 (Ignore the VLAN header when tracking connectons)] オプションは、ASA FirePOWER モジュールでは使用できません。
- 注意 [セッション終了のロギングしきい値 (Session Termination Logging Threshold)] は、サポートからの指示がない限り変更しないでください。
- ステップ4** [OK] をクリックします。
- 

## 次のタスク

- 必要に応じて、[アクセスコントロールポリシーの編集 \(1331 ページ\)](#) の説明に従ってさらにポリシーを設定します。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

# チェックサム検証

システムは、あらゆるプロトコルレベルのチェックサムを検証することで、IP、TCP、UDP、およびICMPによる送信データが完全に受信されていることを確認できます。さらに基本的なレベルで、パケットが転送中に改ざんされたり、誤って変更されたりしていないことも確認できます。チェックサムはアルゴリズムを使用して、パケットでのプロトコルの整合性を検証します。システムが終端のホストでパケットに書き込まれた値を計算し、それがチェックサムと同じであれば、そのパケットは変更されていないと見なされます。

チェックサムの検証を無効にすると、ネットワークが侵入攻撃にさらされる危険があります。システムは、チェックサム検証イベントを生成しないことに注意してください。インライン展開では、パケットのチェックサムが正しくない場合、そのパケットをドロップするようにシステムを設定できます。

## チェックサム検証オプション

次のオプションは、いずれも、パッシブ展開またはインライン展開で[有効 (Enabled)]または[無効 (Disabled)]に設定することができます。インライン展開では[ドロップ (Drop)]に設定することもできます。

- ICMP チェックサム (ICMP Checksums)
- IP チェックサム (IP Checksums)
- TCP チェックサム (TCP Checksums)
- UDP チェックサム (UDP Checksums)

違反パケットをドロップするには、オプションを[ドロップ (Drop)]に設定するだけでなく、関連付けられているネットワーク分析ポリシーの[インラインモード (Inline Mode)]を有効にし、確実にデバイスがインラインで展開されるようにする必要があります。

パッシブ展開またはタップモードでのインライン展開で、これらのオプションを[ドロップ (Drop)]に設定することは、[有効 (Enabled)]に設定するのと同じです。

すべてのチェックサム検証オプションは、デフォルトで、[有効 (Enabled)]になっています。ただし、Firepower Threat Defense ルーテッドトランスペアレントインターフェイスでは、IP チェックサム検証に失敗したパケットは常にドロップされます。Firepower Threat Defense ルーテッドおよびトランスペアレントインターフェイスが、パケットを Snort プロセスに渡す前に、正しくないチェックサムを使用して UDP パケットを修正することに注意してください。

### 関連トピック

[インライン導入でのプリプロセッサによるトラフィックの変更 \(1852 ページ\)](#)

## チェックサムの確認

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

### 手順

- ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。 を選択します。

(注) カスタム ユーザー ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーションパネルで [設定 (Settings)] をクリックします。

**ステップ 4** [トランスポート層/ネットワーク層のプロセッサ (Transport/Network Layer Preprocessors)] の下にある [チェックサムの確認 (Checksum Verification)] が無効になっている場合、[有効 (Enabled)] をクリックします。

**ステップ 5** [チェックサムの確認 (Checksum Verification)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [チェックサム検証 \(1949 ページ\)](#) で説明されているオプションを変更します。

**ステップ 7** 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックし、[変更の確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

---

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[レイヤ管理 \(1597 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## インライン正規化プリプロセッサ

インライン正規化プリプロセッサは、インライン展開で攻撃者が検出を免れる可能性を最小限にするために、トラフィックを正規化します。



- (注) システムでトラフィックに影響を与えるには、ルーテッド、スイッチド、またはトランスペアレント インターフェイスあるいはインライン インターフェイス ペアを使用して、関連する設定を管理対象デバイスに展開する必要があります。

IPv4、IPv6、ICMPv4、ICMPv6、TCP トラフィックを任意に組み合わせて正規化を指定できます。ほとんどの正規化は、パケット単位で行われ、インライン正規化プリプロセッサによって処理されます。ただし、TCP ストリームプリプロセッサは、TCP ペイロードの正規化を含む、ほとんどの状態関連パケットおよびストリームの正規化を処理します。

インライン正規化は、パケットデコーダによるデコードの直後に行われます。その後で、別のプリプロセッサによる処理が行われます。正規化は、パケット層の内部から外部への方向で行われます。

インライン正規化プリプロセッサはイベントを生成しません。インライン正規化プリプロセッサの役割は、インライン展開の別のプリプロセッサおよびルールエンジンで使用できるようにパケットを準備することです。また、システムが処理するパケットが、ネットワーク上のホストで受信したパケットと同じであるようにする役割もあります。



- (注) インライン展開では、インライン モードを有効にし、[TCP ペイロードの正規化 (Normalize TCP Payload) ] オプションを有効にして、インライン正規化プリプロセッサを設定することをお勧めします。パッシブ展開では、アダプティブプロファイルの更新を使用することをお勧めします。

#### 関連トピック

[インライン導入でのプリプロセッサによるトラフィックの変更 \(1852 ページ\)](#)  
[アダプティブプロファイルについて \(2013 ページ\)](#)

## インライン正規化オプション

### 最小 TTL (Minimum TTL)

[TTL のリセット (Reset TTL) ] がこのオプションに設定する値以上の値に設定されている場合、このオプションは以下を指定します。

- [IPv4 の正規化 (Normalize IPv4) ] が有効にされている場合は、[IPv4 存続可能時間 (TTL) (IPv4 Time to Live (TTL)) ] フィールドの最小許容値。TTL のパケット値がこの値を下回る場合、[TTL のリセット (Reset TTL) ] に設定された値に正規化されます。
- [IPv6 の正規化 (Normalize IPv6) ] が有効にされている場合は、[IPv6 ホップリミット (IPv6 Hop Limit) ] フィールドの最小許容値。ホップリミットの値がこの値を下回る場合、[TTL のリセット (Reset TTL) ] に設定された値に正規化されます。

このフィールドが空白の場合、システムは値が 1 であると想定します。



- (注) Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスの場合、[最小 TTL (Minimum TTL) ] および [TTL のリセット (Reset TTL) ] オプションは無視されます。接続の最大 TTL は最初のパケットの TTL によって決定します。後続パケットの TTL は削減できますが、増やすことはできません。システムは、TTL をその接続の以前の最小 TTL にリセットします。これにより、TTL 回避攻撃を阻止します。

パケット復号化の [プロトコル ヘッダー異常の検出 (Detect Protocol Header Anomalies) ] オプションが有効になっている場合、デコーダ ルール カテゴリで次のルールを有効にして、この

オプションに関する イベントを生成し、インライン展開では、違反パケットをドロップします。を行うことができます。

- 指定の最小値を下回る TTL が設定された IPv4 パケットが検出された場合にトリガーするには、ルール 116:428 を有効にします。
- 指定の最小値を下回るホップ リミットが設定された IPv6 パケットが検出された場合にトリガーするには、ルール 116:270 を有効にします。

### TTL のリセット (Reset TTL)

[最小 TTL (Minimum TTL) ]の値以上の値を設定した場合、以下のフィールドが正規化されません。

- [IPv4 の正規化 (Normalize IPv4) ]が有効にされている場合は、[IPv4 TTL] フィールド
- [IPv6 の正規化 (Normalize IPv6) ]が有効にされている場合は、[IPv6 ホップリミット (IPv6 Hop Limit) ]フィールド

パケット値が [最小 TTL (Minimum TTL) ]を下回る場合、システムはパケットの TTL またはホップリミットの値をこのオプションに対して設定された値に変更して、パケットを正規化します。このフィールドを空白のままにするか、0 に設定するか、または [最小 TTL (Minimum TTL) ]未満の値に設定すると、このオプションは無効になります。

### IPv4 の正規化 (Normalize IPv4)

IPv4 トラフィックの正規化を有効にします。システムは、以下の場合にも必要に応じて TTL フィールドを正規化します。

- このオプションが有効になっていて、さらに、
- [TTL のリセット (Reset TTL) ]に設定された値によって TTL の正規化が有効になっている。

このオプションを有効にすると、追加の IPv4 オプションを有効にすることもできます。

このオプションを有効にすると、システムは以下の基本の IPv4 正規化を実行します。

- 過剰なペイロードを持つパケットを、IP ヘッダーに指定されたデータグラム長まで切り捨てます。
- [差別化サービス (DS) (Differentiated Services (DS)) ]フィールド (旧称 [タイプオブサービス (TOS) (Type of Service (TOS)) ]フィールド) をクリアします。
- すべてのオプション オクテットを 1 ([操作なし (No Operation) ]) に設定します。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。Firepower Threat Defense デバイスは、各ルーテッドまたはトランスペアレント インターフェイスのルータ アラート、End of Options List (EOOL) 、およびオペレーションなし (NOP) オプションを持つ RSVP パケットをドロップします。

### フラグメント禁止ビットの正規化 (Normalize Don't Fragment Bit)

[IPv4 フラグ (IPv4 Flags)] ヘッダー フィールドの単一ビットの [フラグメント禁止 (Don't Fragment)] サブフィールドをクリアします。このオプションを有効にすると、ダウンストリームのルータがパケットをドロップする代わりに、必要に応じてパケットをフラグメント化できます。また、このオプションを有効にすることで、ドロップされるパケットを巧妙に作成してポリシーを回避する試みを防ぐこともできます。このオプションを選択するには、[IPv4 の正規化 (Normalize IPv4)] を有効にする必要があります。

### リザーブドビットの正規化 (Normalize Reserved Bit)

[IPv4 フラグ (IPv4 Flags)] ヘッダー フィールドの単一ビットの [予約済み (Reserved)] サブフィールドをクリアします。通常は、このオプションを有効にします。このオプションを選択するには、[IPv4 の正規化 (Normalize IPv4)] を有効にする必要があります。

### TOS ビットの正規化 (Normalize TOS Bit)

1 バイトの [差別化サービス (Differentiated Services)] (旧称 [タイプオブ サービス (Type of Service)]) フィールドをクリアします。このオプションを選択するには、[IPv4 の正規化 (Normalize IPv4)] を有効にする必要があります。

### 余剰ペイロードの正規化 (Normalize Excess Payload)

過剰なペイロードを持つパケットを、IP ヘッダーに指定されたデータグラム長にレイヤ2 (たとえば、イーサネット) ヘッダーを合計した長さまで切り捨てます。ただし、最小フレーム長より小さく切り捨てることはしません。このオプションを選択するには、[IPv4 の正規化 (Normalize IPv4)] を有効にする必要があります。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。過剰なペイロードを持つパケットは、常にこれらのインターフェイスでドロップされます。

### IPv6 の正規化 (Normalize IPv6)

[ホップバイホップ オプション (Hop-by-Hop Options)] および [宛先オプション (Destination Options)] 拡張ヘッダーに含まれるすべてのオプションタイプフィールドを 00 (スキップして処理を続行) に設定します。このオプションが有効にされていて、[TTL のリセット (Reset TTL)] に設定された値がホップリミット正規化を有効にしている場合、システムは必要に応じてホップリミットフィールドも正規化します。

### ICMPv4 の正規化 (Normalize ICMPv4)

ICMPv4 トラフィックのエコー (要求) およびエコー応答メッセージで8ビットのコードフィールドをクリアします。

### ICMPv6 の正規化 (Normalize ICMPv6)

ICMPv6 トラフィックのエコー (要求) およびエコー応答メッセージで8ビットのコードフィールドをクリアします。



**予約済みビットの正規化またはクリア (Normalize/Clear Reserved Bits)**

TCP ヘッダーの予約ビットをクリアします。

**オプションパディングバイトの正規化またはクリア (Normalize/Clear Option Padding Bytes)**

TCP オプションのパディングバイトをクリアします。

**URG=0 の場合に緊急ポインタをクリア (Clear Urgent Pointer if URG=0)**

緊急 (URG) 制御ビットが設定されていない場合、16 ビットの TCP ヘッダー [緊急ポインタ (Urgent Pointer) ] フィールドをクリアします。

**空のペイロードに設定された緊急ポインタまたは URG をクリア (Clear Urgent Pointer/URG on Empty Payload)**

ペイロードがない場合、TCP ヘッダー [緊急ポインタ (Urgent Pointer) ] フィールドおよび URG 制御ビットをクリアします。

**緊急ポインタが設定されていない場合 URG をクリア (Clear URG if Urgent Pointer is Not Set)**

緊急ポインタが設定されていない場合、TCP ヘッダー URG 制御ビットをクリアします。

**緊急ポインタの正規化 (Normalize Urgent Pointer)**

ポインタがペイロード長を上回る場合、2 バイトの TCP ヘッダー [緊急ポインタ (Urgent Pointer) ] フィールドをペイロード長に設定します。

**TCP ペイロードの正規化 (Normalize TCP Payload)**

再送信されるデータの一貫性が確保されるように [TCP データ (TCP Data) ] フィールドの正規化を有効にします。正しく再構成できないセグメントはすべてドロップされます。

**SYN に関するデータを削除 (Remove Data on SYN)**

TCP オペレーティングシステムポリシーが MacOS 以外の場合、同期 (SYN) パケットのデータを削除します。

また、このオプションにより、TCP ストリーム プリプロセッサの [ポリシー (Policy) ] オプションが [Mac OS] に設定されていない場合にトリガー可能なルール 129:2 もまた無効になります。

**RST に関するデータを削除 (Remove Data on RST)**

TCP リセット (RST) パケットからデータを削除します。

**データをウィンドウにトリミング (Trim Data to Window)**

[TCP データ (TCP Data) ] フィールドを [ウィンドウ (Window) ] フィールドに指定されたサイズにまで切り捨てます。

### データを MSS にトリミング (Trim Data to MSS)

ペイロードが MSS より長い場合、[TCP データ (TCP Data) ] フィールドを最大セグメント サイズ (MSS) にまで切り捨てます。

### 解決不可能な TCP ヘッダーの異常をブロック (Block Unresolvable TCP Header Anomalies)

このオプションを有効にすると、システムは無効になり受信ホストによってブロックされる可能性が高い異常な TCP パケット (正規化されている場合) をブロックします。たとえば、システムは確立されたセッションの後に送信された SYN パケットをブロックします。

また、システムは、ルールが有効にされているかどうかに関係なく、以下に示す TCP ストリーム プリプロセッサ ルールのいずれかに一致するパケットもドロップします。

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 ~ 129:19

[ブロックされたパケットの合計 (Total Blocked Packets) ] パフォーマンス グラフには、インライン展開でブロックされたパケットの数が示され、パッシブ展開とタップモードでのインライン展開の場合は、インライン展開でブロックされる予想数が示されます。

### 明示的な混雑通知 (ECN) (Explicit Congestion Notification)

明示的輻輳通知 (ECN) フラグのパケット単位またはストリーム単位の正規化を以下のように有効にします。

- [パケット (Packet) ] を選択すると、ネゴシエーションに関係なく、パケット単位で ECN フラグがクリアされます。
- [ストリーム (Stream) ] を選択すると、ECN の使用がネゴシエートされていない場合、ストリーム単位で ECN フラグがクリアされます。

[ストリーム (Stream) ] を選択した場合、この正規化が実行されるようにするには、TCP ストリーム プリプロセッサの [TCP 3 ウェイ ハンドシェイク 必須 (Require TCP 3-Way Handshake) ] オプションも有効にされている必要があります。

### 既存の TCP オプションをクリア (Clear Existing TCP Options)

[これらの TCP オプションを許可 (Allow These TCP Options) ] を有効にします。

### これらの TCP オプションを許可 (Allow These TCP Options)

トラフィックで許可する特定の TCP オプションの正規化を無効にします。

明示的に許可されたオプションは、正規化されません。オプションを [操作なし (No Operation) ] (TCP オプション 1) に設定して明示的に許可していないオプションは、正規化されます。

[これらの TCP オプションを許可 (Allow These TCP Options) ] の設定に関係なく、次のオプションは最適な TCP パフォーマンスに一般的に使用されるため、システムは常にこれらのオプションを許可します。

- 最大セグメント サイズ (MSS) (Maximum Segment Size (MSS))
- ウィンドウ スケール (Window Scale)
- タイム スタンプ TCP (Time Stamp TCP)

他のそれほど一般的に使用されないオプションについては、システムは自動的に許可しません。

特定のオプションを許可するには、オプションキーワード、オプション番号、またはこの両方のカンマ区切りリストを設定します。以下に、一例を示します。

```
sack, echo, 19
```

オプションキーワードを指定するということは、そのキーワードと関連付けられた1つ以上の TCP オプションの番号を指定することと同じです。たとえば、sack を指定することは、TCP オプション 4 ([選択的確認応答を許可 (Selective Acknowledgment Permitted) ]) および TCP オプション 5 ([選択的確認応答 (Selective Acknowledgment) ]) を指定することと同じです。オプション キーワードでは、大文字と小文字が区別されません。

また、any を指定すると、すべての TCP オプションが許可されるため、実質的にすべての TCP オプションの正規化が無効にされます。

次の表に、許可する TCP オプションを指定する方法を要約します。フィールドを空のままにすると、システムは MSS、ウィンドウ スケール、およびタイムスタンプのオプションのみを許可します。

指定する内容	許可されるオプション
sack	TCP オプション 4 (Selective Acknowledgment Permitted) および 5 (Selective Acknowledgment)
エコー	TCP オプション 6 (Echo Request) および 7 (Echo Reply)
partial_order	TCP オプション 9 (Partial Order Connection Permitted) および 10 (Partial Order Service Profile)
conn_count	TCP 接続数オプション 11 (CC) 、 12 (CC.New) 、 および 13 (CC.Echo)
alt_checksum	TCP オプション 14 (Alternate Checksum Request) および 15 (Alternate Checksum)

指定する内容	許可されるオプション
md5	TCP オプション 19 (MD5 Signature)
オプション番号 2 ~ 255	キーワードのないオプションを含む、特定のオプション
任意	すべての TCP オプション (この設定は、実質的に TCP オプションの正規化を無効にします)

このオプションに any を指定しない場合、正規化には次のものが含まれます。

- MSS、ウィンドウ スケール、タイムスタンプ、およびその他の明示的に許可されたオプションを除き、すべてのオプションのバイトを [操作なし (No Operation) ] (TCP オプション 1) に設定します。
- タイムスタンプは存在していても無効な場合、あるいは有効であってもネゴシエートされない場合、タイムスタンプ オクテットを [操作なし (No Operation) ] に設定します。
- タイムスタンプがネゴシエートされるものの、存在しない場合、パケットをブロックします。
- 確認応答 (ACK) 制御ビットが設定されていない場合、[タイムスタンプ エコー応答 (TSecr) (Time Stamp Echo Reply (TSecr))] オプションフィールドをクリアします。
- SYN 制御ビットが設定されていない場合、[MSS] および [ウィンドウ スケール (Window Scale) ] オプションを [操作なし (No Operation) ] (TCP オプション 1) に設定します。

#### 関連トピック

[侵入イベントのパフォーマンス統計情報グラフの種類](#) (2604 ページ)

## インライン正規化の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

#### 始める前に

- 問題を起こすパケットを正規化またはドロップするには、[インライン導入でのプリプロセッサによるトラフィックの変更 \(1852 ページ\)](#) の説明に従って [インラインモード (Inline Mode) ] を有効にします。また、管理対象デバイスは、インラインで展開する必要があります。

## 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション パネルで [設定 (Settings)] をクリックします。

**ステップ 4** [トランスポートまたはネットワーク レイヤプリプロセッサ (Transport/Network Layer Preprocessors)] で [インライン正規化 (Inline Normalization)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [インライン正規化 (Inline Normalization)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [インライン正規化プリプロセッサ \(1951 ページ\)](#) で説明されているオプションを設定します。

**ステップ 7** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

## 次のタスク

- インライン正規化 [最小 TTL (Minimum TTL)] オプションで侵入イベントを生成する場合は、パケットデコーダルール 116:429 (IPv4) と 116:270 (IPv6) のいずれかまたは両方を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) および [インライン正規化オプション \(1952 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 関連トピック

[レイヤ管理 \(1597 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## IP 最適化プリプロセッサ

最大伝送ユニット (MTU) より大きいために IP データグラムが複数の小さい IP データグラムに分割されると、その IP データグラムはフラグメント化されたことになります。単一の IP データグラムフラグメントには、隠れた攻撃を識別するのに十分な情報が含まれない場合があります。そのため、攻撃者はエクスプロイトの検出を免れるために、フラグメント化されるパケットで攻撃データを送信する可能性があります。IP 最適化プリプロセッサは、ルールエンジンが IP データグラムに対してルールを実行する前に、パケットに仕込まれた攻撃をルールで識別しやすくするために、フラグメント化された IP データグラムを再構成します。フラグメント化されたデータグラムを再構成できない場合、それらのデータグラムに対しては、ルールが実行されません。

## IP フラグメンテーション エクスプロイト

IP最適化を有効にすると、ネットワーク上のホストに対する攻撃（ティアドロップ攻撃など）や、システム自体に対するリソース消費攻撃（Jolt2 攻撃など）を検出するのに役立ちます。

ティアドロップ攻撃は、特定のオペレーティングシステムのバグを悪用して、そのオペレーティングシステムがオーバーラップした IP フラグメントを再構成しようとするクラッシュするように仕掛けます。IP最適化プリプロセッサを有効にして、オーバーラップしたフラグメントを識別するように設定すれば、該当するフラグメントを識別できます。IP最適化プリプロセッサは、ティアドロップ攻撃などのオーバーラップフラグメント攻撃で、最初のパケットを検出するだけで、同じ攻撃での後続のパケットは検出しません。

Jolt2 攻撃では、IP最適化機能を酷使させるという方法でサービス妨害攻撃を仕掛けるために、フラグメント化された同じ IP パケットのコピーを大量に送信します。IP最適化プリプロセッサでは、メモリ使用量の上限によって、このような攻撃を阻止し、包括的検査においてシステムを自己防衛状態にします。システムは攻撃によって過負荷にならず、運用可能な状態を維持し、ネットワークトラフィックの検査を続行します。

フラグメント化されたパケットを再構成する方法は、オペレーティングシステムによって異なります。ホストがどのオペレーティングシステムで実行されているのかを攻撃者が特定できれば、その攻撃者はターゲットホストが特定の方法で再構成するように不正なパケットをフラグメント化することも可能です。モニタ対象のネットワーク上でホストを実行しているオペレーティングシステムは、システムには不明です。したがって、プリプロセッサがパケットを誤った方法で再構成して検査し、それによってエクスプロイトが検出されないままパススルーする可能性があります。このような攻撃を軽減するために、ネットワーク上のホストごとに適切な方法でパケットを最適化するよう、最適化プリプロセッサを設定できるようになっています。

パッシブ展開でアダプティブプロファイルの更新を使用することで、パケットのターゲットホストのホストオペレーティングシステム情報に応じて、IP最適化プリプロセッサに適用するターゲットベースのポリシーが動的に選択されるようにすることもできます。

## ターゲットベースの最適化ポリシー

ホストのオペレーティングシステムは以下の3つの基準を使用して、パケットを再構成する際に優先するパケットフラグメントを決定します。

- オペレーティングシステムがフラグメントを受信した順序
- フラグメントのオフセット（パケットの先頭からのそのフラグメントの距離（バイト単位））
- オーバーラップしているフラグメントとの相対開始位置と相対終了位置

これらの基準はすべてのオペレーティングシステムで使用されているものの、フラグメント化されたパケットを再構成するときに優先するフラグメントは、オペレーティングシステムによって異なります。したがって、ネットワーク上で異なるオペレーティングシステムを使用する2台のホストが、同じオーバーラップフラグメントをまったく異なる方法で再構成する場合も考えられます。

いずれかのホストのオペレーティングシステムを認識している攻撃者が、オーバーラップしたパケットフラグメントに不正なコンテンツを忍ばせて送信することによって、エクスプロイトの検出を免れ、そのホストを悪用する可能性があります。このパケットが他のホストで再構成されて検査されても、パケットに害はないように見えますが、ターゲットホストで再構成される場合には不正なエクスプロイトが含まれています。ただし、モニタ対象のネットワークセグメントで稼働するオペレーティングシステムを認識するようにIP最適化プリプロセッサを設定すれば、このプリプロセッサがターゲットホストと同じ方法でフラグメントを再構成することによって、攻撃を識別できます。

## IP最適化オプション

IP最適化を有効または無効にすることだけを選択することもできますが、シスコでは、それよりも細かいレベルで、有効にするIP最適化プリプロセッサの動作を指定することを推奨しています。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

次のグローバルオプションを構成できます。

### 事前に割り当てられたフラグメント（Preallocated Fragments）

プリプロセッサが一度に処理できる個々のフラグメントの最大数。事前割り当てするフラグメントノードの数を指定すると、静的メモリ割り当てが有効になります。



#### 注意

個々のフラグメントの処理には、約1550バイトのメモリが使用されます。プリプロセッサで個々のフラグメントを処理するために必要なメモリが、管理対象デバイスに事前定義された使用可能なメモリ量の制限を上回る場合は、管理対象デバイスのメモリ制限が優先されます。

IP 最適化ポリシーごとに、以下のオプションを設定できます。

### ネットワーク

最適化ポリシーを適用するホスト（複数可）の IP アドレス。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。デフォルトポリシーを含め、合計で最大255個のプロファイルを指定できます。



- (注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの default 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、any を表すアドレス表記 (0.0.0.0/0 または ::/0) を使用したりすることはできません。

### ポリシー

モニタ対象ネットワーク セグメント上のホスト一式に使用する最適化ポリシー。

ターゲットホストのオペレーティングシステムに応じて、7つの最適化ポリシーの1つを選択できます。以下の表に、7つのポリシーと、それぞれのポリシーを使用するオペレーティングシステムを記載します。First と Last というポリシー名は、これらのポリシーが元のオーバーラップ パケットまたは後続のオーバーラップ パケットのどちらを優先するかを反映しています。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

表 206: ターゲットベースの最適化ポリシー

ポリシー	オペレーティング システム
BSD	AIX FreeBSD IRIX VAX/VMS
BSD-right	HP JetDirect



ポリシー	オペレーティング システム
ファースト	Mac OS HP-UX
Linux	Linux OpenBSD
Last	Cisco IOS
Solaris	SunOS
Windows	Windows

### Timeout

プリプロセッサエンジンがフラグメント化されたパケットを再構成する際に使用できる最大時間（秒数）を指定します。指定された時間内にパケットを再構成できない場合、プリプロセッサエンジンはパケットの再構成試行を停止し、受信したフラグメントを破棄します。

### 最小 TTL (Min TTL)

パケットに許容される最小 TTL 値を指定します。このオプションは、TTL ベースの挿入攻撃を検出します。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 123:11 を有効にします。

### 異常検知 (Detect Anomalies)

オーバーラップフラグメントのようなフラグメンテーション問題を識別します。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、次のルールを有効にすることができます：

- 123:1 ~ 123:4
- 123:5 (BSD ポリシー)
- 123:6 ~ 123:8

### オーバーラップ範囲 (Overlap Limit)

セッション内で重複しているセグメントの設定された数が検出されると、そのセッションの最適化を停止することを指定します。

このオプションを設定するには、[異常検知 (Detect Anomalies)] を有効にする必要があります。値が空白の場合、このオプションは無効になります。値0は、無制限の重複セグメント数を指定します。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。重複フラグメントは、それらのインターフェイスでは常にドロップされます。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 123:12 を有効にできます。

### 最小フラグメント サイズ (Minimum Fragment Size)

設定されたバイト数より小さい最後でないフラグメントが検出された場合、そのパケットは悪意のあるものとみなされることを指定します。

このオプションを設定するには、[異常検知 (Detect Anomalies)] を有効にする必要があります。値が空白の場合、このオプションは無効になります。値0は、無制限のバイト数を指定します。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 123:13 を有効にできます。

### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## IP 最適化の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

### 始める前に

- カスタム ターゲットベース ポリシーで識別するネットワークが、親ネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、および VLAN のサブセットと一致するか、サブセットであることを確認します。詳細については、[ネットワーク分析プロファイルの詳細設定 \(1840 ページ\)](#) を参照してください。

## 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション パネルで [設定 (Settings)] をクリックします。

**ステップ 4** [トランスポートまたはネットワーク レイヤプリプロセッサ (Transport/Network Layer Preprocessors)] で [IP 最適化 (IP Defragmentation)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [IP 最適化 (IP Defragmentation)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** 必要に応じて、[事前割り当て済みフラグメント (Preallocated Fragments)] フィールドに値を入力します。

**ステップ 7** 次の選択肢があります。

- サーバプロファイルの追加：ページの左側の [サーバ (Servers)] の横にある追加アイコン (➕) をクリックし、[ホストアドレス (Host Address)] フィールドに値を入力して、[OK] をクリックします。単一の IP アドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。デフォルトポリシーを含め、合計で最大 255 個のターゲットベースのポリシーを作成できます。
- サーバプロファイルの編集：ページの左側の [サーバ (Servers)] で設定済みのアドレスをクリックするか、[デフォルト (default)] をクリックします。
- プロファイルの削除：ポリシーの横にある削除アイコン (🗑️) をクリックします。

**ステップ 8** IP 最適化オプション (1961 ページ) の説明に従ってオプションを変更します。

**ステップ 9** 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックし、[変更の確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

### 次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、IP最適化ルール (GID 123) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) および [IP 最適化オプション \(1961 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

[レイヤの基本 \(1591 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## パケット デコーダ

キャプチャしたパケットをプリプロセッサに送信する前に、システムはパケットをパケットデコーダに送信します。パケットデコーダは、プリプロセッサやルールエンジンが容易に使用できる形式に、パケットヘッダーおよびペイロードを変換します。データリンク層から開始して、ネットワーク層、トランスポート層へと、各スタック層が順にデコードされます。

## パケット デコーダ オプション

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

### GTP データ チャネルのデコード (Decode GTP Data Channel)

カプセル化された GTP (General Packet Radio Service (GPRS) トンネリング プロトコル) データ チャネルをデコードします。デフォルトでは、デコーダはポート 3386 ではバージョン 0 のデータをデコードし、ポート 2152 ではバージョン 1 のデータをデコードします。GTP\_PORTS デフォルト変数を使用して、カプセル化された GTP トラフィックを識別するポートを変更できます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:297 および 116:298 を有効にします。

### [標準外ポートで Teredo を検知 (Detect Teredo on Non-Standard Ports)]

ポート 3544 以外の UDP ポートで識別される IPv6 トラフィックの Teredo トンネリングを検査します。

IPv6 トラフィックが存在する場合、システムは常にこのトラフィックを検査します。デフォルトでは、IPv6 インスペクションには 4in6、6in4、6to4、および 6in6 トンネリング方式が含まれます。また、UDP ヘッダーがポート 3544 を指定している場合は、Teredo トンネリングも含まれます。

IPv4 ネットワークでは、IPv4 ホストが Teredo プロトコルを使用して、IPv4 ネットワーク アドレス変換 (NAT) デバイスを介して IPv6 トラフィックをトンネリングできます。Teredo は、IPv6 パケットを IPv4 UDP データグラムにカプセル化して、IPv4 NAT デバイスの背後で IPv6 接続を許可します。システムは通常、UDP ポート 3544 を使用して Teredo トラフィックを識別します。ただし、攻撃者が検出を免れるために標準以外のポートを使用する可能性も考えられます。[非標準ポートでの Teredo の検出 (Detect Teredo on Non-Standard Ports)] を有効にすることで、システムに Teredo トンネリングのすべての UDP ペイロードを検査させることができます。

Teredo のデコードは、外側のネットワーク層に IPv4 が使用されている場合に限り、最初の UDP ヘッダーに対してのみ行われます。UDP データが IPv6 データにカプセル化されるため、Teredo IPv6 層の後に 2 つ目の UDP 層が存在する場合、ルール エンジン は UDP 侵入ルールを使用して、内側および外側の両方の UDP 層を分析します。

**policy-other** ルール カテゴリの侵入ルール 12065、12066、12067、および 12068 は Teredo トラフィックを検出しますが、デコードは行わないので注意してください。(任意) これらのルールを使用してインライン展開で Teredo トラフィックをドロップすることができます。ただし、[非標準ポートでの Teredo の検出 (Detect Teredo on Non-Standard Ports)] を有効にする場合は、これらのルールを無効化するか、トラフィックをドロップせずにイベントを生成するように設定する必要があります。

#### [余長値の検知 (Detect Excessive Length Value)]

パケットヘッダーが実際のパケット長を超えるパケット長を指定しているかどうかを検出します。

このオプションは、Firepower Threat Defense ルーテッド、トランスペアレント、およびインラインインターフェイスでは無視されます。超過ヘッダー長を持つパケットは常にドロップされます。ただし、このオプションは Firepower Threat Defense インライン タップおよびパッシブインターフェイスに適用されます。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 116:6、116:47、116:97、および 116:275 を有効にできます。

#### [間違いな IP オプションを検知 (Detect Invalid IP Options)]

無効な IP オプションを使用したエクスプロイトを識別するために、無効な IP ヘッダー オプションを検出します。たとえば、ファイアウォールに対するサービス妨害攻撃は、システムをフリーズさせる原因になります。ファイアウォールが無効なタイムスタンプおよび IP セキュリティ オプションを解析しようとして、ゼロ長のチェックに失敗すると、回復不可能な無限ループが発生します。ルールエンジンはゼロ長のオプションを識別し、ファイアウォールでの攻撃を軽減するために使用できる情報を提供します。

Firepower Threat Defense デバイスは、各ルーテッドまたはトランスペアレントインターフェイスのルータ アラート、End of Options List (EOOL)、およびオペレーションなし (NOP) オプションを持つ RSVP パケットをドロップします。インライン、インラインタップ、またはパッシブインターフェイスについては、IP オプションは上記のように処理されます。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 116:4 および 116:5 を有効にします。

#### [実験的 TCP オプションを検知 (Detect Experimental TCP Options) ]

試験的な TCP オプションが設定された TCP ヘッダーを検出します。以下の表は、それらのオプションを示しています。

TCP オプション	説明
9	半順序接続許可 (Partial Order Connection Permitted)
10	半順序サービス プロファイル (Partial Order Service Profile)
18	Alternate Checksum Request
15	Alternate Checksum Data
18	Trailer Checksum
20	Space Communications Protocol Standards (SCPS)
21	Selective Negative Acknowledgements (SCPS)
22	Record Boundaries (SCPS)
23	Corruption (SPCS)
24	SNAP
26	TCP 圧縮フィルタ (TCP Compression Filter)

これらのオプションは試験的なものであるため、一部のシステムでは考慮されず、悪用される恐れがあります。



- (注) 上記の表に記載されている試験的オプションに加えて、26 より大きいオプション番号を持つ TCP オプションは、試験的オプションと見なされます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:58 を有効にします。

#### 廃止された TCP オプションを検知

廃止された TCP オプションが設定された TCP ヘッダーを検出します。これらのオプションは廃止されたものであるため、一部のシステムでは考慮されず、悪用される恐れがあります。以下の表は、それらのオプションを示しています。

TCP オプション	説明
[6]	エコー (Echo)
7	エコー応答 (Echo Reply)
16	Skeeter
17	Bubba
19	MD5 Signature (MD5 認証)
25	Unassigned (未定義)

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:57 を有効にします。

#### [T または TCP を検知 (Detect T/TCP) ]

CC.ECHO オプションが設定された TCP ヘッダーを検出します。CC.ECHO オプションは、TCP for Transactions (T/TCP) が使用されていることを確認します。T/TCP ヘッダー オプションは幅広く使用されていないため、一部のシステムでは考慮されず、悪用される恐れがあります。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:56 を有効にします。

#### [その他の TCP オプションを検知 (Detect Other TCP Options) ]

他の TCP デコード イベント オプションでは検出されない無効な TCP オプションが設定された TCP ヘッダーを検出します。たとえば、このオプションは、無効な長さ、またはオプション データが TCP ヘッダーに収まらない長さの TCP オプションを検出します。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。無効な TCP オプションを持つパケットは常にドロップされます。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、ルール 116:54、116:55、および 116:59 を有効にできます。

#### [プロトコルヘッダの異常を検知 (Detect Protocol Header Anomalies) ]

より具体的な IP および TCP デコーダ オプションでは検出されない他のデコードエラーを検出します。たとえば、このデコーダは、不正な形式のデータ リンク プロトコル ヘッダーを検出する場合があります。

このオプションは、Firepower Threat Defense ルーテッド、トランスペアレント、およびインライン インターフェイスでは無視されます。ヘッダー異常があるパケットは常にドロップされます。ただし、このオプションは Threat Defense インライン タップ および パッシブ インターフェイスに適用されます。

このオプションに関する イベント を生成し、インライン展開では、違反パケットをドロップします。を行うには、次のルールを有効にすることができます。

GID:SID	該当する場合にイベントを生成
116:467	パケットが Cisco FabricPath ヘッダーにカプセル化されるパケットの最小サイズより小さい。
116:468	ヘッダーの Cisco メタデータ (CMD) フィールドに、有効なCMDヘッダの最小サイズより小さいヘッダー長が含まれている。CMD フィールドは、Cisco TrustSec プロトコルと関連付けられています。
116:469	ヘッダーのCMDフィールドに、無効なフィールド長が含まれている。
116:470	ヘッダーのCMDフィールドに、無効なセキュリティグループタグ (SGT) オプションのタイプがあります。
116:471	ヘッダーのCMDフィールドに、値が予約されている SGT が含まれています。

その他のパケットデコーダオプションに関連付けられていないパケットデコーダルールを有効にすることもできます。

#### 関連トピック

[定義済みデフォルト変数](#) (447 ページ)

## パケット復号化の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

#### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。



代わりに表示アイコン (🔒) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション パネルで [設定 (Settings)] をクリックします。

**ステップ 4** [トランスポートまたはネットワーク レイヤプリプロセッサ (Transport/Network Layer Preprocessors)] の下の [パケット復号化 (Packet Decoding)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [パケット復号化 (Packet Decoding)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [パケットデコーダオプション \(1966 ページ\)](#) で説明されているオプションを有効または無効にします。

**ステップ 7** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

#### 次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、パケットデコーダルール (GID 116) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) および [パケットデコーダオプション \(1966 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[レイヤの基本 \(1591 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

## TCP ストリームの前処理

TCP プロトコルは、接続で生じ得るさまざまな状態を定義します。各 TCP 接続は、送信元と宛先の IP アドレス、および送信元と宛先のポートによって識別されます。TCP では、接続パラメータ値が同じ接続は、一度に 1 つしか存在できません。

### 状態に関連する TCP エクスプロイト

侵入ルールに `established` 引数と組み合わせた `flow` キーワードを追加すると、侵入ルールエンジンはステートフル モードでルールとフロー ディレクティブに一致するパケットを検査します。ステートフル モードでは、クライアントとサーバの間で正当な 3 ウェイ ハンドシェイクによって確立された TCP セッションの一部となっているトラフィックだけが評価されます。

確立された TCP セッションの一部として識別できない TCP トラフィックをプリプロセッサが検出するようにシステムを設定することは可能です。しかし、このようなイベントは、システムをすぐに過負荷状態に陥らせ、しかも意味のあるデータを提供しないため、通常の使用法では推奨されません。

Stick や Snot などの攻撃では、システムの自身に対する広範なルールセットとパケットインスペクションを悪用します。これらのツールは、Snort ベースの侵入ルールのパターンに基づいてパケットを生成し、ネットワークに送信します。ステートフルインスペクションに対して設定するルールに `flow` または `flowbits` キーワードを含めなければ、パケットのそれぞれがルールをトリガーするため、システムが過負荷状態になります。ステートフルインスペクションを使用することで、確立された TCP セッションに含まれず、意味のある情報を提供しないこれらのパケットを無視できます。ステートフルインスペクションを実行すると、ルールエンジンは確立された TCP セッションに含まれる攻撃のみを検出するため、アナリストが stick や snot によって大量に生成されるイベントに時間を取られることがなくなります。

## ターゲットベースのTCPポリシー

オペレーティングシステムによって、TCP の実装方法は異なります。たとえば、セッションをリセットするために、Windows やその他のオペレーティングシステムの一部では TCP リセットセグメントに正確な TCP シーケンス番号を割り当てる必要があるのに対し、Linux や他のオペレーティングシステムではシーケンス番号の範囲を使用できます。この例の場合、ストリームプリプロセッサは、シーケンス番号に基づき、宛先ホストがリセットにどのように応答するかを正確に把握しなければなりません。ストリームプリプロセッサがセッションの追跡を停止するのは、宛先ホストがリセットが有効であると見なした場合のみです。したがって、プリプロセッサがストリームの検査を停止した後は、パケットを送信することによって攻撃が検出を免れることはできません。TCP の実装方法の違いには、オペレーティングシステムで TCP タイムスタンプオプションを採用しているかどうか、採用している場合にはどのようにタイムスタンプを処理するか、そしてオペレーティングシステムで SYN パケットのデータを受け入れるか、無視するかどうか含まれます。

また、オーバーラップ TCP セグメントを再構成する方法も、オペレーティングシステムによって異なります。オーバーラップ TCP セグメントは、確認応答済み TCP トラフィックの通常の再送信を反映する場合があります。あるいは、ホストのオペレーティングシステムを認識している攻撃者が、エクスプロイトの検出を免れるためにオーバーラップセグメントに不正なコンテンツを忍ばせて送信し、そのホストを悪用しようとしている場合もあります。ただし、モニタ対象のネットワークセグメント上で稼働するオペレーティングシステムを認識するようにストリームプリプロセッサを設定すれば、そのプリプロセッサがターゲットホストと同じ方法でセグメントを再構成することによって、攻撃を識別できます。

モニタ対象のネットワークセグメント上のさまざまなオペレーティングシステムに合わせて TCP ストリームインスペクションおよび再構成を調整するために、1 つ以上の TCP ポリシーを作成することができます。ポリシーごとに、13 のオペレーティングシステムポリシーのうち 1 つを特定します。異なるオペレーティングシステムを使用するホストのいずれか、あるいはすべてを識別するために必要な数だけ TCP ポリシーを使用し、各 TCP ポリシーを特定の IP アドレスまたはアドレスブロックにバインドします。デフォルトの TCP ポリシーは、他の TCP ポリシーで指定されていないモニタ対象ネットワーク上のすべてのホストに適用されま

す。したがって、デフォルトの TCP ポリシーに IP アドレスまたはアドレス ブロックを指定する必要はありません。

パッシブ展開でアダプティブ プロファイルの更新を使用することで、パケットのターゲットホストのホストオペレーティングシステム情報に応じて、TCP ストリーム プリプロセッサに適用するターゲットベースのポリシーが動的に選択されるようにすることもできます。

## TCP ストリームの再構成

ストリームプリプロセッサは、TCPセッションでのサーバからクライアントへの通信ストリーム、クライアントからサーバへの通信ストリーム、またはその両方の通信ストリームに含まれるすべてのパケットを収集して再構成します。これにより、ルールエンジンは、特定のストリームに含まれる個々のパケットだけを検査するのではなく、ストリームを再構成された単一のエンティティとして検査できます。

ストリームの再構成により、ルールエンジンは、個々のパケットを検査する場合には検出できない可能性のあるストリームベースの攻撃を識別できます。ルールエンジンの再構成対象とする通信ストリームは、ネットワークのニーズに応じて指定できます。たとえば、Webサーバ上のトラフィックをモニタする際に、独自の Web サーバから不正なトラフィックを受信する可能性がほとんどないため、クライアントトラフィックだけを検査するという場合もあります。

各 TCP ポリシーに、ストリームプリプロセッサが再構成するトラフィックを識別するポートのカンマ区切りのリストを指定できます。アダプティブ プロファイルの更新が有効にされている場合、再構成するトラフィックを識別するサービスを、ポートの代わりとして、あるいはポートと組み合わせてリストすることもできます。

ポート、サービス、またはその両方を指定できます。クライアントポート、サーバポート、またはその両方を任意に組み合わせた個別のポートリストを指定できます。また、クライアントサービス、サーバサービス、またはその両方を任意に組み合わせた個別のサービスリストを指定することもできます。たとえば、以下を再構成する必要があります。

- クライアントからの SMTP (ポート 25) トラフィック
- FTP サーバ応答 (ポート 21)
- 両方向の Telnet (ポート 23) トラフィック

この場合、以下のように設定できます。

- クライアントポートとして、23, 25 を指定
- サーバポートとして、21, 23 を指定

あるいは、以下のように設定することもできます。

- クライアントポートとして、25 を指定
- サーバポートとして、21 を指定
- 両方のポートとして、23 を指定

さらに、ポートとサービスを組み合わせた以下の設定例は、アダプティブプロファイルの更新が有効にされている場合、有効になります。

- クライアントポートとして、23 を指定
- クライアントサービスとして、smtp を指定
- サーバポートとして、21 を指定
- サーバサービスとして、telnet を指定

ポートを否定すると（180 など）、そのポートのトラフィックがTCPストリームプリプロセッサで処理されなくなり、パフォーマンスが向上します。

all を引数として指定して、すべてのポートに対して再構成を指定することもできますが、ではポートを all に設定しないよう推奨しています。この設定では、このプリプロセッサで検査するトラフィックの量が増え、不必要にパフォーマンスが低下するためです。

TCP再構成には、自動的かつ透過的にその他のプリプロセッサに追加するポートが含まれています。しかし、他のプリプロセッサの設定に追加したTCP再構成リストにポートを明示的に追加する場合は、これらの追加したポートは通常処理されます。これには、次のプリプロセッサのポートリストが含まれています。

- FTP/Telnet（サーバレベルFTP）
- DCE/RPC
- HTTP Inspect
- SMTP
- Session Initiation Protocol
- POP
- IMAP
- SSL

追加のトラフィックタイプ（クライアント、サーバ、両方）を再構成すると、リソースの需要が増大することに注意してください。

## TCP ストリームのプリプロセスオプション

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

次のグローバルTCPオプションを構成できます。

### パケットタイプパフォーマンスの向上（Packet Type Performance Boost）

送信元ポートおよび宛先ポートの両方を any に設定したTCPルールで、flow または flowbits オプションが使用されている場合を除き、有効化された侵入ルールに指定されていないポートおよびアプリケーションプロトコルのすべてについて、TCPトラフィックを無視するように

設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。

TCP ポリシーごとに、以下のオプションを設定できます。

### ネットワーク (Network)

TCP ストリーム再構成ポリシーを適用するホストの IP アドレスを指定します。

単一の IP アドレスまたはアドレスブロックを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを指定できます。



- (注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの default 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、any を表すアドレス表記 (0.0.0.0/0 または ::/0) を使用したりすることはできません。

### ポリシー

TCP ポリシーを適用するターゲット ホスト (複数可) のオペレーティング システムを識別します。[MacOS] 以外のポリシーを選択すると、システムは同期 (SYN) パケットからデータを削除し、ルール 129:2 に対するイベントの生成を無効にします。インライン正規化プリプロセッサの [SYN に関するデータを削除 (Remove Data on SYN)] オプションを有効にすると、ルール 129:2 も無効になることに注意してください。

以下の表に、オペレーティング システム ポリシーとそれを使用するホスト オペレーティング システムをリストします。

表 207: TCP オペレーティング システム ポリシー

ポリシー	オペレーティング システム
ファースト	不明な OS
Last	Cisco IOS
BSD	AIX FreeBSD OpenBSD

ポリシー	オペレーティング システム
Linux	Linux 2.4 カーネル Linux 2.6 カーネル
Old Linux	Linux 2.2 以前のカーネル
Windows	Windows 98 Windows NT Windows 2000 Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista
Solaris	Solaris OS SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 以降
HPUX 10	HP-UX 10.2 以前
Mac OS	Mac OS 10 (Mac OS X)



**ヒント** First オペレーティング システム ポリシーは、ホストのオペレーティング システムが不明な場合にはある程度の保護対策になります。ただし、攻撃を見逃す可能性もあります。オペレーティング システムが既知であれば、ポリシーを編集して、その正しいオペレーティング システムを指定してください。

### Timeout

侵入ルール エンジンが非アクティブなストリームを状態テーブルで保持する秒数（1 ～ 86400 秒）。指定された期間内にストリームが再構成されない場合、侵入ルールエンジンはそのストリームを状態テーブルから削除します。



(注) ネットワーク トラフィックがデバイスの帯域幅制限に到達しやすいセグメントに、管理対象デバイスが展開されている場合は、処理のオーバーヘッド量を削減するために、この値を大きい値（たとえば、600 秒）に設定することを検討する必要があります。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

### 最大 TCP ウィンドウ (Maximum TCP Window)

受信側ホストで指定されている TCP ウィンドウの最大許容サイズを 1 ~ 1073725440 バイトの範囲で指定します。値を 0 に設定すると、TCP ウィンドウ サイズのチェックが無効になります。



#### 注意

上限は RFC で許可される最大ウィンドウ サイズです。これは、攻撃者が検出を回避できないようにすることを目的としていますが、あまりにも大きな最大ウィンドウ サイズを設定すると、システム自体がサービス妨害を招く可能性があります。

[ステートフル インスペクションの異常 (Stateful Inspection Anomalies)] が有効になっている場合は、ルール 129:6 を有効にして、このオプションに対しイベントを生成し、インライン展開では、違反パケットをドロップします。することができます。

### オーバーラップ範囲 (Overlap Limit)

セッションで許容するオーバーラップ セグメントの数を 0 (無制限) ~ 255 の範囲で指定します。セッションで、この指定された値に達すると、セグメントの再構成が停止します。[ステートフル インスペクションの異常 (Stateful Inspection Anomalies)] が有効にされていて、それに付随するプリプロセッサ ルールが有効にされている場合、イベントも生成されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:7 を有効にします。

### ファクタをフラッシュ (Flush Factor)

インライン展開では、ここで設定するサイズ減少なしのセグメントの数 (1 ~ 2048) の後にサイズが減少したセグメントが検出されると、システムは検出用に累積されたセグメントデータをフラッシュします。値を 0 に設定すると、要求または応答の終わりを示す可能性のあるこのセグメントパターンの検出が無効になります。このオプションを有効にするには、インライン正規化の [TCP ペイロードの正規化 (Normalize TCP Payload)] オプションを有効にする必要があることに注意してください。

### ステートフル インスペクションの異常 (Stateful Inspection Anomalies)

TCP スタックの異常な動作を検出します。付随するプリプロセッサ ルールが有効にされている場合、TCP/IP スタックが不完全に作成されていると、多数のイベントが生成される可能性があります。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、次のルールを有効にすることができます：

- 129:1 ~ 129:5
- 129:6 (Mac OS のみ)
- 129:8 ~ 129:11
- 129:13 ~ 129:19

次の点に注意してください。

- ルール 129:6 でトリガーするには、さらに [最大 TCP ウィンドウ (Maximum TCP Window) ] に 0 より大きい値を設定する必要があります。
- ルール 129:9 および 129:10 でトリガーするには、さらに [TCP セッションのハイジャック (TCP Session Hijacking) ] を有効にする必要があります。

### TCP セッションのハイジャック (TCP Session Hijacking)

3 ウェイ ハンドシェイク中に TCP 接続の両端から検出されたハードウェア (MAC) アドレスの有効性を、セッションで受信した後続のパケットに照合して検査することにより、TCP セッションハイジャックを検出します。[ステートフルインスペクションの異常 (Stateful Inspection Anomalies) ] が有効にされていて、2 つの対応するプリプロセッサルールのいずれかが有効にされている場合、接続のどちらかの側の MAC アドレスが一致しないと、システムがイベントを生成します。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションに対しイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:9 および 129:10 を有効にします。これらのルールのいずれかを使用してイベントを生成するには、[ステートフルインスペクションの異常 (Stateful Inspection Anomalies) ] を有効にする必要があります。

### 連続した小型セグメント (Consecutive Small Segments)

[ステートフルインスペクションの異常 (Stateful Inspection Anomalies) ] が有効にされている場合、連続する小さな TCP セグメントの許容数を 1 ~ 2048 の範囲で指定します。値を 0 に設定すると、連続する小さなセグメントのチェックが無効になります。

このオプションは、[小さなセグメントサイズ (Small Segment Size) ] オプションと同時に設定し、両方とも無効にするか、両方にゼロ以外の値を設定する必要があります。通常は、それぞれのセグメントの長さが 1 バイトであったとしても、ACK が介在することなく 2000 個もの連続するセグメントを受信することはないので注意してください。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:12 を有効にします。



### 小型セグメントのサイズ (Small Segment Size)

[ステートフル インспекションの異常 (Stateful Inspection Anomalies)] が有効にされている場合、小さいと見なされる TCP セグメントのサイズを 1 ~ 2048 バイトの範囲で指定します。値を 0 に設定すると、小さいセグメントのサイズの指定が無効になります。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションは、[連続する小さなセグメント (Consecutive Small Segments)] オプションと同時に設定し、両方とも無効にするか、両方にゼロ以外の値を設定する必要があります。2048 バイトの TCP セグメントは、標準的な 1500 バイトのイーサネットフレームより大きいことに注意してください。

### 小型セグメントを無視したポート (Ports Ignoring Small Segments)

[ステートフル インспекションの異常 (Stateful Inspection Anomalies)]、[連続する小さなセグメント (Consecutive Small Segments)]、および [小さなセグメント サイズ (Small Segment Size)] が有効になっている場合は、小さい TCP セグメントの検出を無視する 1 つ以上のポートのカンマ区切りリストを指定します。このオプションを空白のままにすると、ポートはすべて無視されないように指定されます。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

リストには任意のポートを追加できますが、このリストが適用されるのは、TCP ポリシーの [ストリーム再構成を実行 (Perform Stream Reassembly on)] ポート リストに指定されているポートのみです。

### TCP 3 ウェイ ハンドシェイク 必須 (Require TCP 3-Way Handshake)

TCP スリーウェイ ハンドシェイクの完了時に確立されたセッションだけを処理することを指定します。パフォーマンスを向上させ、SYN フラッド攻撃から保護し、部分的に非同期の環境での運用を可能にするには、このオプションを無効にします。確立された TCP セッションには含まれていない情報を送信して誤検出を発生させようとする攻撃を回避するには、このオプションを有効にします。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:20 を有効にします。

### 3 ウェイ ハンドシェイク タイムアウト (3-Way Handshake Timeout)

[TCP 3 ウェイ ハンドシェイク 必須 (Require TCP 3-Way Handshake)] が有効にされている場合、ハンドシェイクを完了するまでの時間制限を 0 (無制限) ~ 86400 秒 (24 時間) の範囲で指定します。このオプションの値を変更するには、[TCP 3 ウェイ ハンドシェイク 必須 (Require TCP 3-Way Handshake)] を有効にする必要があります。

Firepower ソフトウェア デバイスと Firepower Threat Defense インライン、インラインタップ、およびパッシブ インターフェイスの場合、デフォルトは 0 です。Firepower Threat Defense の

ルーティッド インターフェイスおよびトランスペアレント インターフェイスの場合、タイムアウトは常に 30 秒であり、ここで設定した値は無視されます。

### パケット サイズ パフォーマンスの向上 (Packet Size Performance Boost)

再構成バッファで大きいパケットをキューに入れないようにプリプロセッサを設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。1~20 バイトの小さなパケットを使用した検出回避の試行から保護するには、このオプションを無効にします。すべてのトラフィックが非常に大きなパケットからなるため、そのような攻撃は起こらないと確信できる場合は、このオプションを有効にします。

### レガシー再構成 (Legacy Reassembly)

パケットを再構成する際に、廃止されたストリーム4プリプロセッサをエミュレートするようにストリームプリプロセッサを設定します。これにより、ストリームプリプロセッサで再構成されたイベントを、ストリーム4プリプロセッサで再構成された、同じデータストリームに基づくイベントと比較できます。

### 非同期ネットワーク (Asynchronous Network)

モニタ対象ネットワークが非同期ネットワーク (システムにトラフィックの半分だけが見えるネットワーク) であるかどうかを指定します。このオプションを有効にすると、システムは TCP ストリームを再構成しないため、パフォーマンスが向上します。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

### クライアントポートでのストリーム再構成の実行 (Perform Stream Reassembly on Client Ports)

接続のクライアント側のポートに基づくストリームの再構成を有効にします。つまり、Web サーバ、メールサーバ、または一般に \$HOME\_NET で指定された IP アドレスによって定義されたその他の IP アドレスを宛先とするストリームが再構成されます。不正なトラフィックがクライアントから発生する可能性がある場合は、このオプションを使用します。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

### クライアントサービスでのストリーム再構成の実行 (Perform Stream Reassembly on Client Services)

接続のクライアント側のサービスに基づくストリーム再構成を有効にします。不正なトラフィックがクライアントから発生する可能性がある場合は、このオプションを使用します。

選択するクライアントサービスごとに、1つ以上のクライアントディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。関連するクライアントアプリケーションに有効にされているディテクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタをアプリケーションに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーションに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

#### サーバポートでのストリーム再構成の実行 (Perform Stream Reassembly on Server Ports)

接続のサーバ側のポートに基づくストリーム再構成のみを有効にします。つまり、Web サーバ、メールサーバ、または一般に \$EXTERNAL\_NET で指定された IP アドレスによって定義されたその他の IP アドレスから発信されたストリームが再構成されます。サーバ側の攻撃を監視する必要がある場合は、このオプションを使用します。ポートを指定しないことによって、このオプションを無効にできます。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。



- (注) 一部の Web サーバの場合、シームレスなアクセスを行うには、このフィールドでポート番号 80 を指定するだけでは不十分です。[サーバサービスでのストリーム再構成の実行 (Perform Stream Reassembly on Server Services) ] フィールドに「**HTTP**」サービスを追加することも必要になります。

#### サーバサービスでのストリーム再構成の実行 (Perform Stream Reassembly on Server Services)

接続のサーバ側のサービスに基づくストリーム再構成のみを有効にします。サーバ側の攻撃を監視する必要がある場合は、このオプションを使用します。サービスを指定しないことによって、このオプションを無効にできます。

1 つ以上のディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。サービスに有効にされているディテクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタを関連するアプリケーションプロトコルに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーションプロトコルに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

#### 両方のポートでのストリーム再構成の実行 (Perform Stream Reassembly on Both Ports)

接続のクライアント側とサーバ側の両方のポートに基づくストリーム再構成を有効にします。同じポートで、不正なトラフィックがクライアントとサーバ間のいずれの方向でも移動する可能性がある場合は、このオプションを使用します。ポートを指定しないことによって、このオプションを無効にできます。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

**両方のサービスでのストリーム再構成の実行 (Perform Stream Reassembly on Both Services)**

接続のクライアント側とサーバ側の両方のサービスに基づくストリーム再構成を有効にします。同じサービスで、不正なトラフィックがクライアントとサーバ間のいずれの方向でも移動する可能性がある場合は、このオプションを使用します。サービスを指定しないことによって、このオプションを無効にできます。

1 つ以上のディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。関連するクライアントアプリケーションまたはアプリケーションプロトコルに対して有効になっているディテクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタをアプリケーションまたはアプリケーションプロトコルに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーションまたはアプリケーションプロトコルに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

このオプションは、Firepower Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

**トラブルシューティング オプション : 最大キューイング バイト (Troubleshooting Options: Maximum Queued Bytes)**

トラブルシューティングの電話中に、TCP 接続の片側でキューイングできるデータの量を指定するようにサポートから依頼される場合があります。値 0 は、無制限のバイト数を指定します。



**注意** このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイドンスに従って実行してください。

---

**トラブルシューティング オプション : 最大キューイング セグメント (Troubleshooting Options : Maximum Queued Segments)**

トラブルシューティングの電話中に、TCP 接続の片側でキューイングできるデータ セグメントの最大バイト数を指定するようにサポートから依頼される場合があります。値 0 は、無制限のデータ セグメント バイト数を指定します。



**注意** このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイドンスに従って実行してください。

---

**関連トピック**

[Firepower システムの IP アドレス表記法](#) (14 ページ)

[ディテクタのアクティブおよび非アクティブの設定](#) (2118 ページ)

[レイヤ管理](#) (1597 ページ)

[競合と変更 : ネットワーク分析ポリシーと侵入ポリシー](#) (1587 ページ)

## TCP ストリームの前処理の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

### 始める前に

- カスタムターゲットベースのポリシーで指定するネットワークが一致しているか、または親のネットワーク分析ポリシーで処理されるネットワーク、ゾーン、および VLAN のサブセットであることを確認します。詳細については、[ネットワーク分析プロファイルの詳細設定 \(1840 ページ\)](#) を参照してください。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 変更するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。


**ステップ 3** 左側のナビゲーション パネルで [設定 (Settings)] をクリックします。

**ステップ 4** [トランスポートまたはネットワーク レイヤプリプロセッサ (Transport/Network Layer Preprocessors)] の下の [TCP ストリームの構成 (TCP Stream Configuration)] 設定が無効になっている場合は、[有効化 (Enabled)] をクリックして有効にします。

**ステップ 5** [TCP ストリームの構成 (TCP Stream Configuration)] の横にある編集アイコン (✎) をクリックします。


**ステップ 6** [グローバル設定 (Global Settings)] セクションの [パケット タイプ パフォーマンス ブースト (Packet Type Performance Boost)] チェックボックスをオンまたはオフにします。

**ステップ 7** 次の操作を実行できます。

- ターゲットベースのポリシーの追加：[ターゲット (Targets) ] セクションの [ホスト (Hosts) ] の横にある追加アイコン (  ) をクリックします。[ホストアドレス (Host Address) ] フィールドに 1 つまたは複数の IP アドレスを指定します。単一の IP アドレスまたはアドレス ブロックを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のターゲットベースのポリシーを作成できます。作業が完了したら [OK] をクリックします。
- 既存のターゲットベースのポリシーの編集：[ホスト (Hosts) ] の下で、編集するポリシーのアドレスをクリックするか、またはデフォルトの構成値を編集します。
- TCP ストリームの前処理オプションの変更：[TCP ストリームのプリプロセス オプション \(1974 ページ\)](#) を参照してください。

**注意** サポートから指示がない限り、[最大キュー済みバイト (Maximum Queued Bytes) ] または [最大キュー済みセグメント (Maximum Queued Segments) ] を変更しないでください。

**ヒント** クライアント サービス、サーバ サービス、またはその両方に基づくストリーム リアセンブル設定を変更するには、変更するフィールドの内側をクリックするか、そのフィールドの横にある [編集 (Edit) ] をクリックします。ポップアップ ウィンドウで矢印ボタンを使用して、サービスを [利用可能 (Available) ] リストと [有効化 (Enabled) ] リスト間で移動し、[OK] をクリックします。

- 既存のターゲットベースのポリシーの削除：削除するポリシーの横にある削除アイコン (  ) をクリックします。

**ステップ 8** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information) ] をクリックして、[変更を確定 (Commit Changes) ] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

### 次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、SMTP ストリーム プリプロセッサ ルール (GID 129) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) および [TCP ストリームのプリプロセス オプション \(1974 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[レイヤ管理 \(1597 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## UDP ストリームの前処理

UDP ストリームの前処理が行われるのは、ルール エンジンがパケットを処理するために使用する UDP ルールに、以下の引数のいずれかを使用した `flow` キーワードが含まれる場合です。

- `Established`
- `To Client`
- `From Client`
- `To Server`
- `From Server`

UDP データストリームは一般に、セッションという観点で考慮されません。UDP は接続レス型プロトコルであり、2つのエンドポイントが通信チャネルを確立してデータを交換し、チャネルを終了する手段は提供していません。ただし、ストリームプリプロセッサは、カプセル化 IP データグラム ヘッダーの送信元および宛先 IP アドレス フィールドと、UDP ヘッダーのポートフィールドを使用して、フローの方向を判断し、セッションを識別します。セッションが終了するのは、設定可能なタイマーの時間を超えた場合、または一方のエンドポイントで、もう一方のエンドポイントが到達不能、あるいは要求されたサービスが利用不可という内容の ICMP メッセージを受け取った場合です。

システムは UDP ストリームの前処理に関連するイベントを生成しないことに注意してください。ただし、関連するパケット デコーダ ルールを有効にすることで、UDP プロトコル ヘッダーの異常を検出することができます。

### 関連トピック

[TCP ヘッダー値とストリーム サイズ \(1760 ページ\)](#)

## UDP ストリームのプリプロセス オプション

### Timeout

プリプロセッサが非アクティブなストリームを状態テーブルに保持する秒数を指定します。指定した時間内に追加のデータグラムが現れなかった場合、プリプロセッサはそのストリームを状態テーブルから削除します。

Firepower Threat Defense ルーテッドインターフェイスおよびトランスペアレントインターフェイスの場合、この値は無視されます。代わりに、デバイスに適用されているプラットフォーム設定ポリシーで定義された UDP タイムアウトによってタイムアウトが決まります。プラットフォーム設定ポリシーのデフォルトは 2 分です。

### パケット タイプ パフォーマンスの向上 (Packet Type Performance Boost)

送信元および宛先ポートの両方を `any` に設定した UDP ルールで `flow` または `flowbits` オプションが使用されている場合を除き、有効化されたルールに指定されていないポートおよびアプリ

ケーションプロトコルのすべてについて、UDP トラフィックを無視するようにプリプロセッサを設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。

## UDP ストリームの前処理の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーションパネルで [設定 (Settings)] をクリックします。

**ステップ 4** [トランスポートまたはネットワーク レイヤプリプロセッサ (Transport/Network Layer Preprocessors)] の下の [UDP ストリームの構成 (UDP Stream Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [UDP ストリームの構成 (UDP Stream Configuration)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** [UDP ストリームのプリプロセスオプション \(1985 ページ\)](#) で説明されているオプションを設定します。

**ステップ 7** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。



### 次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、関連するパケット デコーダ ルール (GID 116) を有効にします。詳細については、[侵入ルール状態の設定 \(1640 ページ\)](#) および [パケット デコーダ \(1966 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[レイヤ管理 \(1597 ページ\)](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー \(1587 ページ\)](#)





## 第 82 章

# 特定の脅威の検出

次のトピックでは、特定の脅威を検出するためにネットワーク分析ポリシーでプリプロセッサを使用する方法について説明します。

- [特定の脅威の検出の概要 \(1989 ページ\)](#)
- [Back Orifice の検出 \(1989 ページ\)](#)
- [ポートスキャン検出 \(1991 ページ\)](#)
- [レート ベースの攻撃防御 \(2000 ページ\)](#)

## 特定の脅威の検出の概要

ネットワーク分析ポリシーでさまざまなプリプロセッサを使用して、モニタ対象ネットワークへの特定の攻撃、たとえば、Back Orifice 攻撃、複数のポートスキャンタイプ、過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃などを検出できます。ただし、侵入ルールまたはルールの引数が無効化されたプリプロセッサを必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。

侵入ポリシーで設定する機密データ検出を使用して、センシティブな数値データの保護なし送信を検出することもできます。

## Back Orifice の検出

Firepower システムは、Back Orifice プログラムの存在を検出するプリプロセッサを提供しています。Back Orifice プログラムにより Windows ホストに対する管理者アクセス権を取得される可能性があります。

## Back Orifice 検出プリプロセッサ

Back Orifice プリプロセッサは、UDP トラフィックを分析し、Back Orifice マジック クッキー「!\*QWTY?」を調べます。このクッキーは、パケットの最初の 8 バイトにあり、XOR で暗号化されています。

## Back Orifice の検出

Back Orifice プリプロセッサには設定ページがありますが、設定オプションはありません。Back Orifice プリプロセッサが有効になっていても、プリプロセッサルールを有効にしなければ、イベントを生成し、インライン展開では、違反パケットをドロップします。

表 208: Back Orifice GID:SID

プリプロセッサルール GID:SID	説明
105:1	Back Orifice トラフィック検出
105:2	Back Orifice クライアント トラフィック検出
105:3	Back Orifice サーバ トラフィック検出
105:4	Back Orifice Snort バッファ攻撃検出

## Back Orifice の検出

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

## 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析 ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析 ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

**ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ナビゲーション ウィンドウで [設定 (Settings)] をクリックします。

**ステップ 4** [特定の脅威の検出 (Specific Threat Detection)] の下の [Back Orifice の検出 (Back Orifice Detection)] が無効になっている場合は、[有効 (Enabled)] をクリックします。

(注) Back Orifice にユーザが設定できるオプションはありません。

**ステップ 5** 最後のポリシーの確定以降にこのポリシーに加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

#### 次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、Back Orifice 検出ルール 105:1、105:2、105:3、または 105:4 を有効にします。詳細については、[侵入ルールの状態 \(1639 ページ\)](#) および [Back Orifice 検出プリプロセッサ \(1989 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ポートスキャン検出

ポートスキャンとは、攻撃者が攻撃の準備段階としてよく使用する、ネットワーク調査の形式です。ポートスキャンでは、攻撃者が特別に細工したパケットをターゲットホストに送信します。攻撃者は多くの場合、ホストが応答するパケットを調べることで、ホストでどのポートが開かれているか、そして開かれているポートでどのアプリケーションプロトコルが実行されているかを、直接あるいは推論によって判断できます。

ポートスキャンは、それ自体では攻撃の証拠になりません。実際、攻撃者が使用するポートスキャン手法の中には、正当なユーザがネットワークで使用する可能性があるものもあります。Cisco のポートスキャンディテクタは、アクティビティのパターンを検出するという方法で、悪意のあるポートスキャンの可能性のあるポートスキャンを判別できるように設計されています。

## ポートスキャンタイプ、プロトコル、フィルタリング感度レベル

攻撃者がネットワークを調査するために複数の手法を使用することはよくあります。通常、攻撃者は異なる複数のプロトコルを使用して、ターゲットホストからさまざまな応答を引き出します。その目的は、ブロックされた特定タイプのプロトコルを基に、使用できる可能性のあるプロトコルを絞り込んでいくことです。

表 209: プロトコルタイプ

プロトコル	説明
[TCP]	TCP プローブを検出します。たとえば、SYN スキャン、ACK スキャン、TCP connect() スキャン、および Xmas tree、FIN、NULL といった異常なフラグを組み合わせたスキャンなどです。

プロトコル	説明
UDP	ゼロバイトUDPパケットなどのUDPプローブを検出します。
ICMP	ICMPエコー要求(ping)を検出します。
IP	IPプロトコルスキャンを検出します。これらのスキャンは、攻撃者が開いているポートを見つけようとしているのではなく、ターゲットホストでサポートされているIPプロトコルを発見しようとするためのスキャンであるため、TCPスキャンおよびUDPスキャンとは異なります。

一般に、ターゲットホストの数、スキャン側ホストの数、およびスキャン対象のポートの数に応じて、ポートスキャンは4つのタイプに分けられます。

表 210: ポートスキャンタイプ

タイプ (Type)	説明
ポートスキャン検出	<p>攻撃者が少数のホストを使用して、1つの対象ホスト上で複数のポートをスキャンする1対1ポートスキャン。</p> <p>1対1ポートスキャンは次のような特徴があります：</p> <ul style="list-style-type: none"> <li>• 少数のホストを使用してスキャン</li> <li>• 単一のホストをスキャン</li> <li>• 多数のポートをスキャン</li> </ul> <p>このオプションでは、TCP、UDP、およびIPポートスキャンが検出されます。</p>
ポートスイープ	<p>攻撃者が少数のホストを使用して、複数の対象ホスト上で1つのポートをスキャンする1対複数のポートスイープ。</p> <p>ポートスイープには次のような特徴があります。</p> <ul style="list-style-type: none"> <li>• 少数のホストを使用してスキャン</li> <li>• 多数のホストをスキャン</li> <li>• 少数の固有のポートをスキャン</li> </ul> <p>このオプションでは、TCP、UDP、ICMP、およびIPポートスイープが検出されます。</p>

タイプ (Type)	説明
デコイ ポートスキャン	<p>攻撃者がスプーフィングされた送信元 IP アドレスと実際にスキャンされた IP アドレスとを組み合わせた1対1ポートスキャン。</p> <p>デコイ ポートスキャンには次のような特徴があります。</p> <ul style="list-style-type: none"> <li>• 多数のホストを使用してスキャン</li> <li>• 少数のポートを一度だけスキャン</li> <li>• 単一 (または少数) のホストをスキャン</li> </ul> <p>デコイ ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。</p>
分散型ポートスキャン	<p>複数のホストが開いているポートに対して1つのホストをクエリする複数対1のポートスキャン。</p> <p>分散型ポートスキャンには次のような特徴があります。</p> <ul style="list-style-type: none"> <li>• 多数のホストを使用してスキャン</li> <li>• 多数のポートを一度だけスキャン</li> <li>• 単一 (または少数) のホストをスキャン</li> </ul> <p>分散型ポートスキャンオプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。</p>

ポートスキャンディテクタは、主にプローブ対象ホストからの否定応答に基づいて、プローブに関する情報を取得します。たとえば、Web クライアントが Web サーバに接続するときに、クライアントはサーバのポート 80/tcp が開いていることを頼りに、そのポートを使用します。ただし、攻撃者がサーバをプローブする場合、そのサーバがウェブサービスを提供するかどうかを攻撃者があらかじめ知っていることはありません。ポートスキャンディテクタは否定応答 (つまり、ICMP 到達不能または TCP RST パケット) を見つけると、その応答を潜在的ポートスキャンとして記録します。否定応答をフィルタリングするデバイス (ファイアウォールやルータなど) の向こう側にターゲットホストがある場合、このプロセスはさらに困難になります。この場合、ポートスキャンディテクタは、選択された機密レベルに基づいてフィルタリングされたポートスキャンイベントを生成することができます。

表 211: 感度レベル

水準器	説明
低 (Low)	<p>ターゲット ホストからの否定応答だけが検出されます。誤検出を抑えるためには、この機密レベルを選択します。ただし、特定のタイプのポートスキャン（時間をかけたスキャン、フィルタリングされたスキャン）が見逃される可能性があることに注意してください。</p> <p>このレベルを使用すると、ポートスキャン検出の所要時間が最短になります。</p>
中 (Medium)	<p>ホストへの接続数に基づいてポートスキャンが検出されます。したがって、フィルタリングされたポートスキャンを検出できます。ただし、ネットワーク アドレス変換プログラムやプロキシなど、ホストが非常にアクティブな場合は、誤検出が発生する可能性があります。</p> <p>[スキャン済みの無視 (Ignore Scanned) ]フィールドに、アクティブなホストの IP アドレスを追加すると、そのような誤検出を軽減できます。</p> <p>このレベルを使用すると、ポートスキャン検出の所要時間が長くなります。</p>
高 (High)	<p>時間帯に基づいてポートスキャンを検出します。つまり、時間を基準としたポートスキャンを検出できます。ただし、このオプションを使用する場合は、[スキャン済みの無視 (Ignore Scanned) ]および[スキャナの無視 (Ignore Scanner) ]フィールドに IP アドレスを指定するという方法で、時間をかけて慎重にディテクタを調整してください。</p> <p>このレベルを使用すると、ポートスキャン検出の所要時間が大幅に長くなります。</p>

## ポートスキャンイベント生成

ポートスキャン検出が有効の場合、ジェネレータ ID (GID) 122 および SID 1~27 の Snort ID (SID) によりルールを有効にして、それぞれ有効化したポートスキャンタイプのイベントを生成し、インライン展開では、違反パケットをドロップします。する必要があります。





(注) イベントがポートスキャン接続ディテクタによって生成され場合、プロトコル番号は255に設定されます。デフォルトでは、ポートスキャンに特定のプロトコルは関連付けられません。したがって、Internet Assigned Numbers Authority (IANA) にはプロトコル番号が割り当てられません。IANA では255を予約番号として指定しているため、ポートスキャンイベントでは、そのイベントに関連付けられている番号がないことを示すために、この番号が使用されます。

表 212: ポートスキャン検出 SID (GID 122)

ポートスキャンタイプ	[プロトコル (Protocol) ]:	機密レベル	プリプロセッサルール SID
ポートスキャン検出	[TCP]	低 (Low)	1
	UDP	中または高	5
	ICMP	低 (Low)	17
	IP	中または高	21
		低 (Low)	イベントを生成しません。
		中または高	イベントを生成しません。
		低 (Low)	9
		中または高	13
ポートスweep	[TCP]	低 (Low)	3、27
	UDP	中または高	7
	ICMP	低 (Low)	19
	IP	中または高	23
		低 (Low)	25
		中または高	26
		低 (Low)	11
		中または高	15

ポートスキャンタイプ	[プロトコル (Protocol) ]:	機密レベル	プリプロセッサルール SID
デコイ ポートスキャン	[TCP]	低 (Low)	2
	UDP	中または高	[6]
	ICMP	低 (Low)	18
	IP	中または高	22
		低 (Low)	イベントを生成しません。
		中または高	イベントを生成しません。
		低 (Low)	10
		中または高	18
分散型ポートスキャン	[TCP]	低 (Low)	4
	UDP	中または高	8
	ICMP	低 (Low)	20
	IP	中または高	24
		低 (Low)	イベントを生成しません。
		中または高	イベントを生成しません。
		低 (Low)	12
		中または高	16

## ポートスキャンイベントパケットビュー

関連するプリプロセッサルールを有効にすると、ポートスキャンディテクタによって侵入イベントが生成されるようになります。生成されたイベントは、他のすべての侵入イベントと同じように表示できます。ただし、ポートスキャンイベントのパケットビューに表示される情報は、他のタイプの侵入イベントとは異なります。

侵入イベントビューを出発点に、ポートスキャンイベントのパケットビューまでドリルダウンします。各ポートスキャンイベントは複数のパケットに基づくため、単一のポートスキャンパケットをダウンロードすることはできません。ただし、ポートスキャンパケットビューで、使用可能なすべてのパケット情報を確認できます。

任意の IP アドレスをクリックしてコンテキストメニューを表示し、[whois (whois)] を選択して、その IP アドレスでルックアップを実行するか、[ホストプロファイルの表示 (View Host Profile)] を選択して、そのホストのホストプロファイルを表示できます。

表 213: ポートスキャンパケットビュー

情報	説明
Device	イベントを検出したデバイス。
時刻 (Time)	イベントが発生した時刻。
メッセージ (Message)	プリプロセッサによって生成されたイベントメッセージ。
ソース IP	スキャン側ホストの IP アドレス。
宛先 IP (Destination IP)	スキャンされたホストの IP アドレス。
プライオリティ カウント (Priority Count)	スキャンされたホストからの否定応答 (TCP RST、ICMP 到達不能など) の数。否定応答の数が多ければ多いほど、プライオリティ カウントが高くなります。
接続数 (Connection Count)	ホスト上でアクティブな接続数。この値は、TCP および IP など接続ベースのスキャンではさらに正確です。
IP カウント (IP Count)	スキャン対象のホストに接続する IP アドレスが変更された回数。たとえば、最初の IP アドレスが 10.1.1.1、2 番目の IP アドレスが 10.1.1.2、3 番目の IP アドレスが 10.1.1.1 の場合、IP カウントは 3 となります。  プロキシや DNS サーバなどのアクティブ ホストでは、この数値はそれほど正確ではありません。
スキャナ/スキャン対象 IP 範囲 (Scanner/Scanned IP Range)	スキャン対象ホストまたはスキャン側ホスト (スキャンのタイプに依存) の IP アドレスの範囲。ポートスweepの場合、このフィールドにはスキャン対象ホストの IP アドレス範囲が示されます。ポートスキャンの場合は、スキャン側ホストの IP アドレス範囲が示されます。
ポート/プロトコル カウント (Port/Proto Count)	TCP および UDP ポートスキャンの場合は、スキャン対象のポートが変更された回数です。たとえば、スキャンされた最初のポートが 80、2 番目のポートが 8080、3 番目のポートが再び 80 の場合、ポート カウントは 3 となります。  IP プロトコル ポートスキャンの場合は、スキャン対象ホストに接続するために使用されたプロトコルが変更された回数です。

情報	説明
ポート/プロトコル範囲 (Port/Proto Range)	TCP および UDP ポートスキャンの場合は、スキャンされたポートの範囲です。  IP プロトコル ポートスキャンの場合は、スキャン対象ホストへの接続試行で使用された IP プロトコル番号の範囲です。
開いているポート (Open Ports)	スキャン対象ホストで開かれた TCP ポート。このフィールドは、ポートスキャンで1つ以上の開かれたポートが検出された場合にのみ表示されます。

## 関連トピック

[侵入イベントについて](#) (2555 ページ)

## ポートスキャン検出の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

ポートスキャン検出の設定オプションを使用して、ポートスキャンディテクタによるスキャンアクティビティのレポート方法を微調整できます。

システムは、各リーフドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

## 手順

- ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

- ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- ステップ 3** [設定 (Settings)] をクリックします。
- ステップ 4** [特定の脅威検出 (Specific Threat Detection)] の下の [ポートスキャン検出 (Portscan Detection)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。
- ステップ 5** [ポートスキャン検出 (Portscan Detection)] の横にある編集アイコン (✎) をクリックします。
- ステップ 6** [プロトコル (Protocol)] フィールドで、有効にするプロトコルを指定します。
- (注) TCP を介してスキャンを検出するには TCP ストリーム処理が有効になっていること、UDP を介してスキャンを検出するには UDP ストリーム処理が有効になっていることを確認する必要があります。
- ステップ 7** [スキャンタイプ (Scan Type)] フィールドで、検出するポートスキャンタイプを指定します。
- ステップ 8** [重要度レベル (Sensitivity Level)] リストからレベルを選択します。[ポートスキャンタイプ、プロトコル、フィルタリング感度レベル \(1991 ページ\)](#) を参照してください。
- ステップ 9** 特定のホストのポートスキャンアクティビティのサインをモニタする場合は、[IP の監視 (Watch IP)] フィールドにホストの IP アドレスを入力します。
- 単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。すべてのネットワークトラフィックを監視するには、フィールドを空白のままにします。
- ステップ 10** ホストをスキャナとして無視するには、[スキャナの無視 (Ignore Scanners)] フィールドにホストの IP アドレスを入力します。
- 単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。
- ステップ 11** ホストをスキャンのターゲットとして無視するには、[スキャン対象の無視 (Ignore Scanned)] フィールドにホストの IP アドレスを入力します。
- 単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。
- ヒント** 特にアクティブなネットワーク上のホストを示すには、[スキャナの無視 (Ignore Scanners)] と [スキャン対象の無視 (Ignore Scanned)] を使用します。このホストリストは、時間経過とともに変更しなければならない場合があります。
- ステップ 12** ミッドストリームでピックアップされたセッションのモニタリングを中断するには、[ACK スキャンの検出 (Detect Ack Scans)] チェックボックスをオフにします。
- (注) ミッドストリームセッションの検出は ACK スキャンの識別に役立ちますが、大量のトラフィックとパケットのドロップが発生するネットワークでは、誤ってイベントが生成される可能性があります。
- ステップ 13** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] をクリックして、[変更を確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

### 次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。するためにポートスキャン検出を行う場合は、ルール 122:1 ~ 122:27 を有効にします。詳細については、[侵入ルールの状態 \(1639 ページ\)](#) および [ポートスキャンイベント生成 \(1994 ページ\)](#) を参照してください。
- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## レートベースの攻撃防御

レートベース攻撃とは、接続の頻度または攻撃を行うための反復試行に依存する攻撃のことです。レートベースの検出基準を使用することで、レートベース攻撃が行われていることを検出し、攻撃が発生するごとに対応できます。また、攻撃が収まった後は、通常の設定に戻すことができます。

レートベースフィルタを含めたネットワーク分析ポリシーを設定することで、ネットワーク上のホストを対象とした過剰なアクティビティを検出できます。インラインモードで展開されている管理対象デバイスでこの機能を使用すると、指定の期間だけレートベース攻撃をブロックし、その後イベントだけを生成してトラフィックをドロップしない状態に戻せます。

ネットワークのホストを SYN フラッドから保護するには、SYN 攻撃防止オプションを利用します。一定期間中に認められたパケットの数を基準に、個々のホストまたはネットワーク全体を保護することができます。パッシブ導入のデバイスでは、イベントを生成できます。インライン導入のデバイスでは、不正なパケットをドロップすることもできます。タイムアウト期間の満了時にレート条件に達しなくなっていれば、イベントの生成およびパケットのドロップが停止します。

たとえば、1つの IP アドレスからの SYN パケットの最大許容数を設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

ネットワーク上のホストでの TCP/IP 接続数を制限することで、サービス妨害 (DoS) 攻撃や、ユーザによる過剰なアクティビティを防止できます。システムが、指定の IP アドレスまたはアドレス範囲で正常に行われている接続が設定された許容数に達したことを検出すると、以降の接続に対してイベントを生成します。タイムアウト期間が満了するまでは、レート条件に達しなくなっても、レートベースのイベント生成が続行されます。インライン導入では、レート条件がタイムアウトになるまでパケットをドロップするように設定できます。

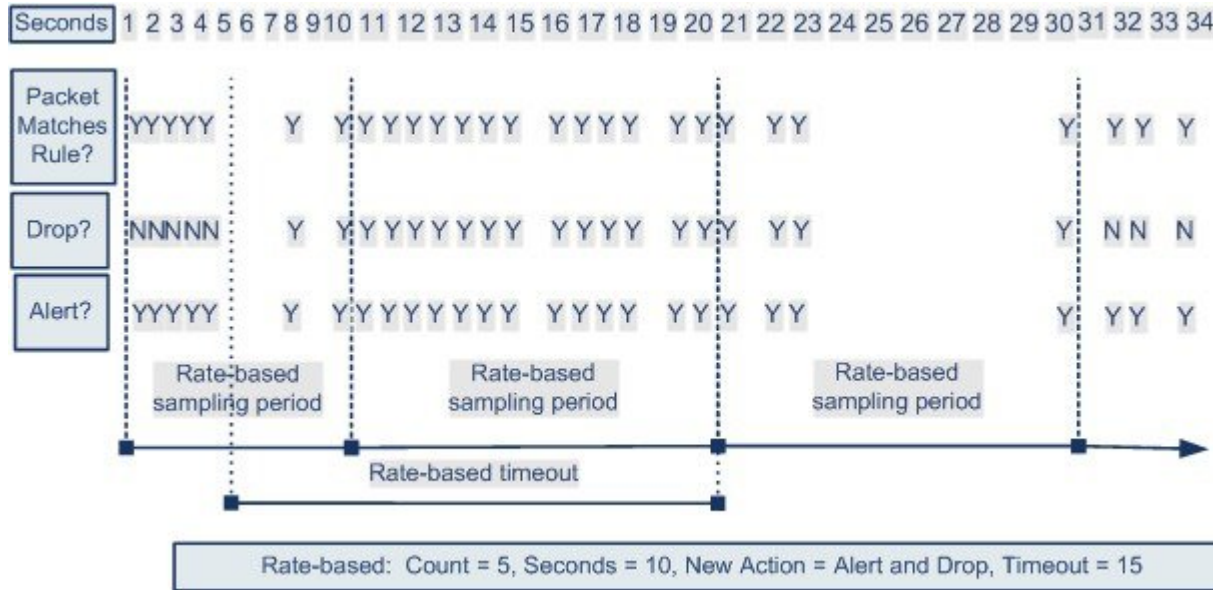
たとえば、1つの IP アドレスからの同時接続の最大許容数を 10 に設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。



(注) デバイスは内部リソース全体でインスペクションのロードバランスを行います。レートベースの攻撃の防御を設定すると、デバイスごとではなく、リソースごとのトリガーレートを設定します。レートベースの攻撃の防御が適切に作動しなければ、トリガーレートを低減する必要があります。正しいレートを決定する際に支援が必要な場合は、サポートに連絡してください。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。繰り返しパスワードを特定しようとする試みが、レートベースの攻撃防止が設定されたルールをトリガーします。レートベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [ドロップしてイベントを生成する (Drop and Generate Events)] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリングレートが現在または過去のサンプリング期間のしきい値を上回っている場合は、新しいアクションが継続されます。新しいアクションが元の「イベントの生成」アクションに戻されるのは、サンプリング期間の完了時にサンプリングレートがしきい値を下回っている場合のみです。



関連トピック  
[動的侵入ルール状態 \(1649 ページ\)](#)

## レートベースの攻撃防御の例

トラフィック自体またはシステムが生成するイベントをフィルタリングする手段としては、`detection_filter` キーワード、しきい値および抑制機能も使用できます。レートベースの攻撃防御は、単独で使用することも、しきい値構成、抑制、または `detection_filter` キーワードと任意に組み合わせて使用することもできます。

detection\_filter キーワード、しきい値構成または抑制、およびレートベースの基準のすべてが同じトラフィックに適用される場合もあります。抑制をルールに適用すると、レートベースの変更が発生しても、指定の IP アドレスに対するイベントの生成は抑制されます。

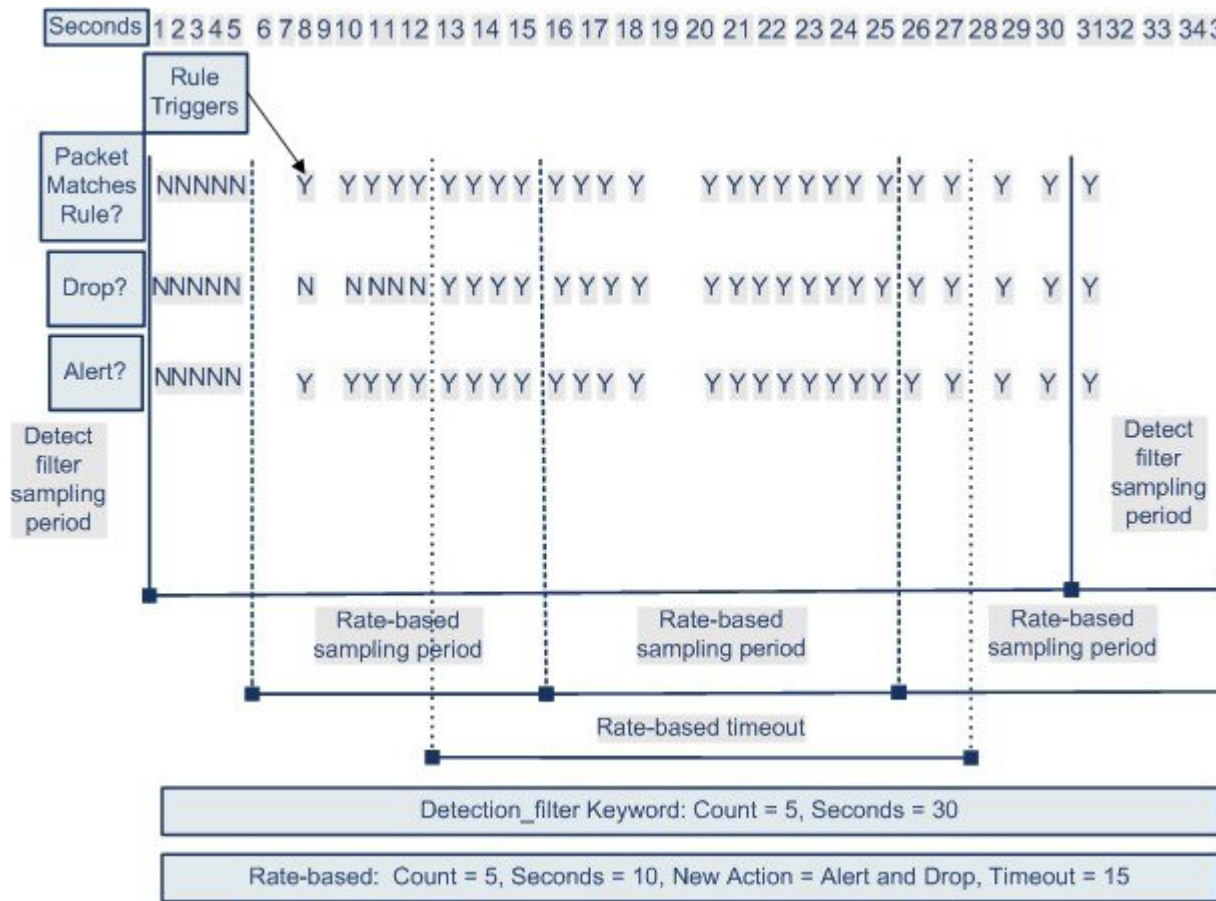
## detection\_filter キーワードの例

以下に、攻撃者がブルートフォースログインを仕掛ける例を示します。パスワードの検出試行が繰り返されると、カウントが5に設定された detection\_filter キーワードも含むルールがトリガーされます。このルールには、レートベース攻撃防止が設定されています。10秒以内にルールに5回ヒットすると、レートベースの設定により、ルール属性が20秒間、[ドロップしてイベントを生成する (Drop and Generate Events)] に変更されます。

図に示されているように、最初の5個の packets がルールに一致しても、イベントは生成されません。それは、レートが detection\_filter キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに5個の packets が通過するまでは、レートベースの基準によって新しいアクション [ドロップしてイベントを生成する (Drop and Generate Events)] がトリガーされることはありません。

レートベースの基準に一致すると、イベントが生成されて、packet がドロップされます。これは、レートベースのタイムアウト期間が満了し、かつレートがしきい値未満になるまで続きます。20秒が経過すると、レートベースアクションがタイムアウトになります。タイムアウト後も、その packet は後続のレートベースのサンプリング期間にドロップされることに注意してください。タイムアウトが発生した時点で、サンプリングされたレートは前のサンプリング期間のしきい値レートを超過しているため、レートベースのアクションは続行されます。





この例には示されていませんが、[ドロップしてイベントを生成する (Drop and Generate Events)] ルール状態を `detection_filter` キーワードと組み合わせることで、ルールのヒット数が指定のレートに達するとトラフィックのドロップが開始されるようにすることができます。ルールにレートベースの設定を使用するかどうかを決定する際は、ルールを [ドロップしてイベントを生成する (Drop and Generate Events)] に設定した場合の結果と `detection_filter` キーワードを含めた場合の結果が同じであるかどうか、あるいは侵入ポリシーでレートとタイムアウトの設定を管理する必要があるかどうかを検討してください。

関連トピック

[侵入ルールの状態 \(1639 ページ\)](#)

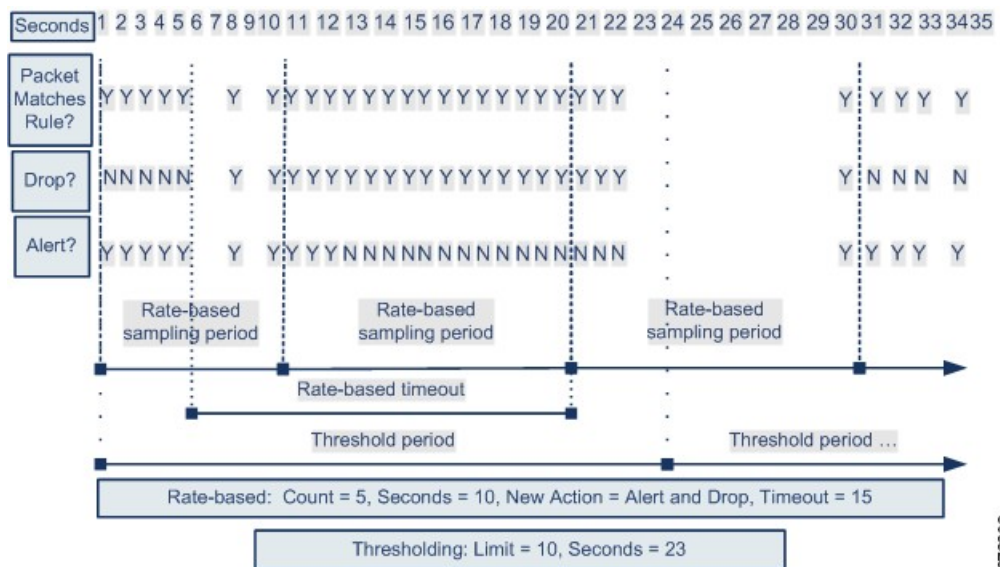
### ダイナミック ルール状態のしきい値構成または抑制の例

以下に、攻撃者がブルートフォースログインを仕掛ける例を示します。パスワードを特定する試みが繰り返されると、レートベースの攻撃防止が設定されているルールがトリガーされます。10秒以内にルールに5回ヒットすると、レートベースの設定により、ルール属性が15秒間、[ドロップしてイベントを生成する (Drop and Generate Events)] に変更されます。さらに、上限しきい値により、ルールで生成可能なイベントの数が23秒間で10に制限されます。

図に示されているように、最初の5個の packets が一致すると、ルールはイベントを生成します。5個の packets がルールに一致した後、レートベースの基準が新しいアクションとして [ド

ドロップしてイベントを生成する（Drop and Generate Events）]をトリガーし、次の5個のパケットがルールに一致した時点でイベントが生成され、パケットをドロップします。10個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成することなくドロップします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリングレートが現在または前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが実行されます。新しいアクションが元の[イベントを生成する（Generate Events）]アクションに戻されるのは、サンプリング期間の完了時にサンプリングレートがしきい値を下回っている場合のみです。



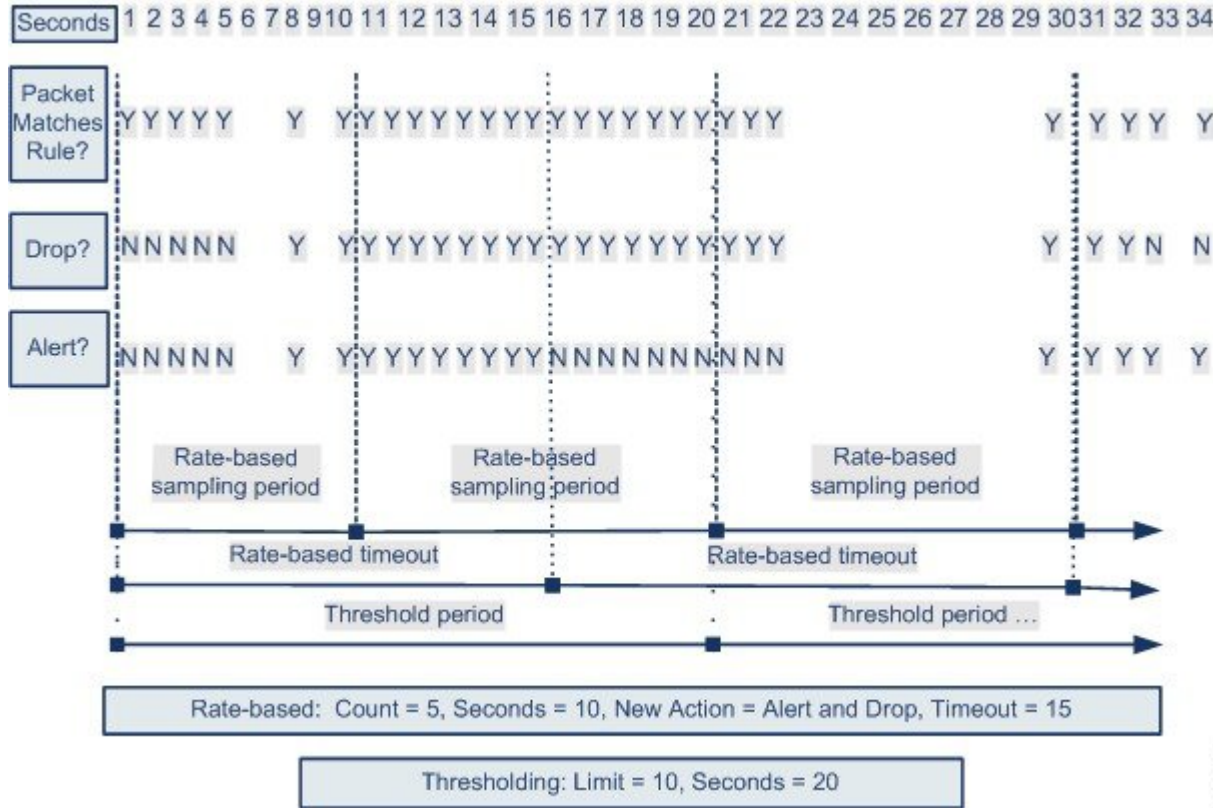
この例には示されていませんが、しきい値に達した後に、レートベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の10に達してシステムがイベントの生成を停止し、14番目のパケットでアクションが[イベントを生成する（Generate Events）]から[ドロップしてイベントを生成する（Drop and Generate Events）]に変更されると、システムはアクションが変更されたことを示す11番目のイベントを生成します。

## ポリシー全体のレート ベース検出としきい値構成または抑制の例

以下に、ネットワーク上のホストに対して、攻撃者がサービス妨害（DoS）攻撃を仕掛ける例を示します。同じ送信元から多数のホストに対して同時接続が行われると、ポリシー全体の[同時接続の制御（Control Simultaneous Connections）]設定がトリガーされます。この設定は、1つの送信元からの接続数が10秒間で5つに達すると、イベントを生成して悪意のあるトラフィックをドロップします。さらに、グローバル上限しきい値により、ルールまたは設定で生成可能なイベントの数が20秒間で10件に制限されます。

この図に示されているように、ポリシー全体の設定により、一致する最初の10個のパケットに対してイベントが生成され、トラフィックがドロップされます。10個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリングされたレートが、現在または前のサンプリング期間のしきい値レートを超過している場合、レートベースのアクションによるイベントの生成とトラフィックのドロップが続行されます。レートベースアクションが停止するのは、サンプリング期間が完了した時点で、サンプリングされたレートがしきい値レートを下回っている場合のみです。



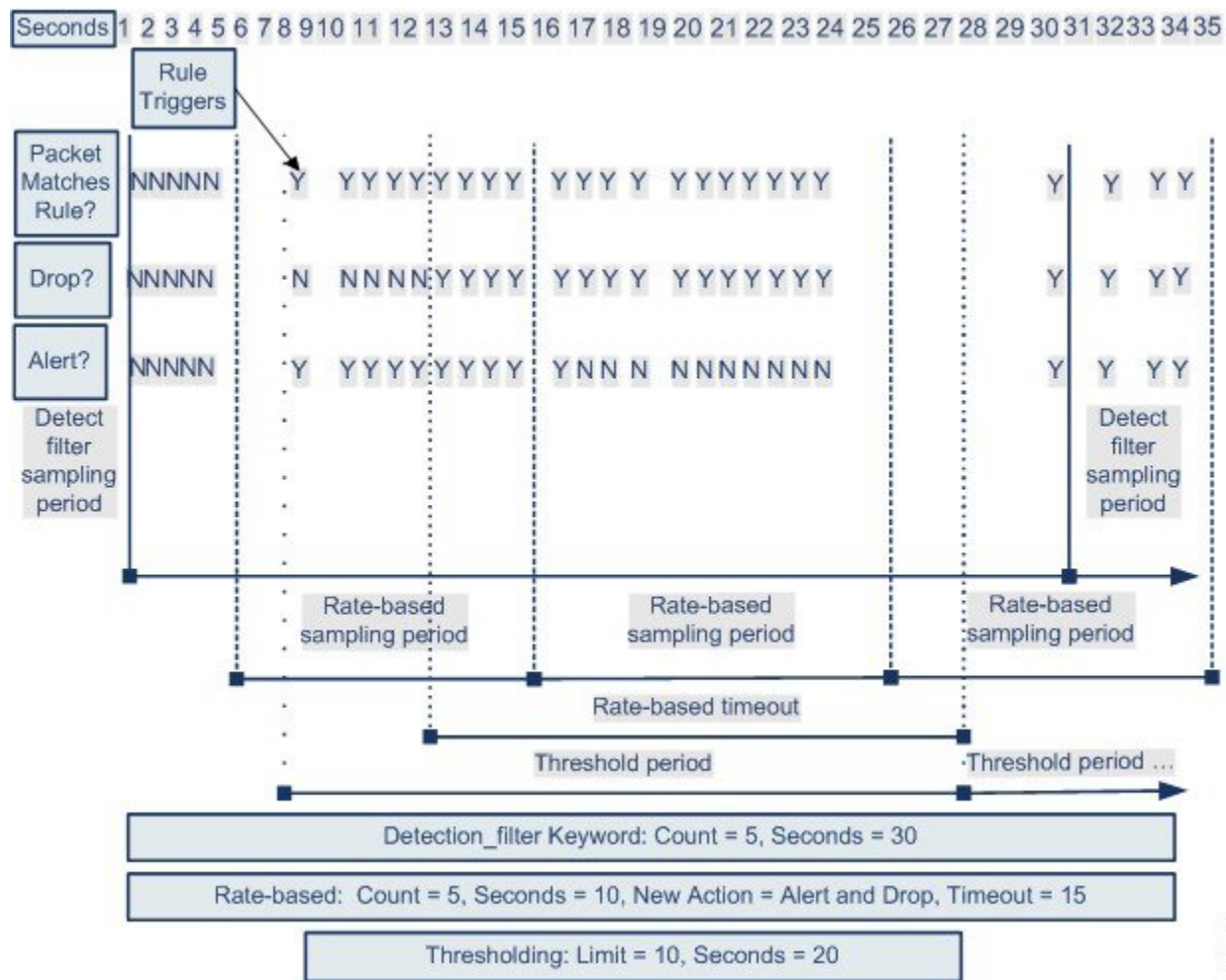
この例には示されていませんが、しきい値に達した後に、レートベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の10に達してシステムがイベントの生成を停止し、14番目のパケットでアクションが[ドロップしてイベントを生成する (Drop and Generate Events)]に変更されると、システムはアクションが変更されたことを示す11番目のイベントを生成します。

### 複数のフィルタリング方法によるレートベース検出の例

以下に、攻撃者がブルートフォースログインを仕掛ける例で、`detection_filter` キーワード、レートベースのフィルタリング、およびしきい値が相互作用する場合を説明します。パスワードの検出試行が繰り返されると、カウントが5に設定された`detection_filter` キーワードを含むルールがトリガーされます。このルールには、レートベースの攻撃防御も設定されています。その設定では、15秒間にルールのヒット数が5に達すると、ルール属性が30秒間、[ドロップしてイベントを生成する (Drop and Generate Events)]に変更されます。さらに、上限しきい値により、ルールによって生成されるイベントは30秒間で10件に制限されます。

図に示されているように、最初の5個の packets がルールに一致しても、イベント通知は行われません。それは、`detection_filter` キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに5個の packets が通過するまでは、レートベースの基準によって新しいルールとして [ドロップしてイベントを生成する (Drop and Generate Events)] がトリガーされることはありません。レートベースの基準が満たされると、システムは11個目から15個目の packets に対してイベントを生成し、 packets をドロップします。15個目の packets がルールに一致すると、上限しきい値に達するため、システムは残りの packets についてはイベントを生成せずにドロップします。

レートベースのタイムアウトが発生した後は、それに続くレートベースのサンプリング期間中、 packets が引き続きドロップされることに注意してください。サンプリングレートが前回のサンプリング期間中にしきい値レートを越えた場合は、新しいアクションが実行されます。



372201

## レートベースの攻撃防御オプションと設定

レートベース攻撃の防御では、異常なトラフィックパターンを識別して、そのトラフィックが正当な要求に与える影響を最小限に抑えるようにします。一般に、レートベース攻撃には次のいずれかの特性があります。

- 任意のトラフィックに、ネットワーク上のホストに対して過剰な未完了接続が含まれています。これは、SYNフラッド攻撃を意味します。
- 任意のトラフィックには、ネットワーク上のホストに対して過剰な接続が含まれています。これは、TCP/IP接続フラッド攻撃を意味します。
- 1つ以上の特定の宛先IPアドレスへのトラフィック、または1つ以上の特定の送信元IPアドレスからのトラフィックで、ルールとの一致が過剰に発生します。
- すべてのトラフィックで、特定のルールとの一致が過剰に発生します。

ネットワーク分析ポリシーでは、ポリシー全体に対してSYNフラッドまたはTCP/IP接続フラッドのいずれかの検出を設定することができます。または個々の侵入ルールもしくはプリプロセッサルールに対してレートベースフィルタを設定できます。GID 135ルールに手動でレートベースフィルタを追加すること、またはルールの状態を変更することはできない点に注意してください。GID 135のルールでは、クライアントを送信元の値、サーバを宛先の値として使用します。



- (注) 内部リソースのデバイスの負荷分散試験。レートベースの攻撃の防御を設定すると、デバイスごとではなく、リソースごとのトリガーレートを設定します。レートベースの攻撃の防御が適切に作動しなければ、トリガーレートを低減する必要があります。正しいレートを決定する場合は、サポートチームにご連絡ください。

[SYN攻撃の防御 (SYN Attack Prevention)] オプションを有効にすると、ルール 135:1 もアクティブになります。このルールを手動でアクティブにしても効果はありません。ルール状態は常に [無効 (Disabled)] として表示され、変更されることはありません。このオプションを有効にすると、定義されたレート条件を超過した時点で、ルールによってイベントが生成されません。

[同時接続の制御 (Control Simultaneous Connections)] オプションを有効にすると、ルール 135:2 および 135:3 もアクティブになります。このルールを手動でアクティブにしても効果はありません。ルール状態は常に [無効 (Disabled)] として表示され、変更されることはありません。定義されたレート条件を超過した時点で、135:2 のルールによってイベントが生成されます。セッションが終了するかタイムアウトすると、ルール 135:3 はイベントを生成します。

各レートベースフィルタには、以下のコンポーネントが含まれます。

- ポリシー全体またはルールベースの送信元/宛先の設定の場合、ネットワークアドレスの指定
- 特定の秒数以内のルール一致のカウンタとして設定されるルール一致率

- レートを超過した場合に実行する新しいアクション

ポリシー全体に対してレートベースを設定すると、システムはレートベース攻撃を検出した時点でイベントを生成します。インライン展開では、トラフィックをドロップすることもできます。個々のルールにレートベースアクションを設定する場合は、[イベントの生成 (Generate Events)]、[イベントのドロップと作成 (Drop and Generate Events)]、[無効 (Disable)] の3つの利用可能なアクションから選択できます。

- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウト期間が満了し、レートがしきい値を下回っている場合、ルールのアクションはそのルールに最初に設定されたアクションに戻ります。ポリシー全体に適用される設定の場合、アクションは、トラフィックと一致する個々のルールのアクションに戻ります。一致するアクションがなければ、アクションは停止されます。

インライン展開のレートベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レートベースの設定が使用されていない場合、ルールが[イベントの生成 (Generate Events)] に設定されていればイベントが生成されますが、そのルールのパケットがドロップされることはありません。ただし、攻撃トラフィックが、レートベースの基準が設定されているルールに一致した場合、それらのルールが当初[イベントのドロップおよび生成 (Drop and Generate Events)] に設定されていないとしても、レートアクションがアクティブである期間は、パケットがドロップされる場合があります。



- (注) レートベースアクションでは、無効にされたルールを有効にすることも、無効にされたルールに一致するトラフィックをドロップすることもできません。ただし、ポリシーレベルでレートベースフィルタを設定すると、指定した期間内の過剰な数のSYNパケットまたはSYN/ACKインタラクションを含むトラフィックに対してイベントを生成するか、イベントを生成してトラフィックをドロップすることができます。

同じルールに複数のレートベースフィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2つのレートベースフィルタアクションが競合する場合は、最初のレートベースフィルタのアクションが実行されることに注意してください。同様に、ポリシー全体に対するレートベースフィルタと個々のルールに設定されたレートベースフィルタが競合する場合は、ポリシー全体のレートベースフィルタが優先されます。

#### 関連トピック

[\[ルール \(Rule\)\] ページからの動的ルール状態の設定](#) (1651 ページ)

## レートベースの攻撃防御、検出フィルタリング、しきい値処理または抑制

キーワード `detection_filter` により、ルールに一致するしきい値が指定の時間内に発生するまで、ルールのトリガーを阻止します。ルールに `detection_filter` キーワードが含まれている場合、システムは指定の期間、ルールのパターンに一致する着信パケットの数を追跡します。シ

システムはそのルールについて、特定の送信元 IP アドレスからのヒット数、または特定の宛先 IP アドレスからのヒット数をカウントできます。レートがルールのレートを超過すると、そのルールに関するイベント通知が開始されます。

しきい値処理と抑制を用いて、ルール、送信元または宛先に関するイベント通知数を制限することまたはそのルールをすべて一緒に通知を抑制することで、過剰なイベントを低減できます。また、オーバーライドする特定のしきい値がない各ルールに適用するグローバルルールのしきい値を設定できます。

ルールに抑制を提供する場合、ポリシー全体またはルールにより指定されたレートベースの設定であるため、レートベースでアクションの変更が発生した場合でも、システムは、すべての適用可能な IP アドレスのそのルールのイベント通知を抑制します。

#### 関連トピック

[侵入イベントのしきい値](#) (1641 ページ)

[侵入ポリシーの抑制の設定](#) (1646 ページ)

[グローバルルールのしきい値の基本](#) (1677 ページ)

## レートベース攻撃防止の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

ポリシー レベルでレートベース攻撃防止を設定することで、SYN フラッド攻撃を阻止できます。特定の送信元からの過剰な接続、または特定の宛先への過剰な接続を阻止することもできます。

#### 手順

- ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [侵入 (Intrusion)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。を選択します。

(注) カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

- ステップ 2** 編集するポリシーの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- ステップ 3** [設定 (Settings)] をクリックします。

**ステップ 4** [特定の脅威検出 (Specific Threat Detection)] の下の [レートベース攻撃防止 (Rate-Based Attack Prevention)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

**ステップ 5** [レートベース攻撃防止 (Rate-Based Attack Prevention)] の横にある編集アイコン (✎) をクリックします。

**ステップ 6** 次の 2 つの選択肢があります。

- ホストのフラッディングを目的とする不完全な接続を防ぐには、[SYN 攻撃の防止 (SYN Attack Prevention)] の下にある [追加 (Add)] をクリックします。
- 過剰な数の接続を防ぐには、[同時接続の制御 (Control Simultaneous Connections)] の下にある [追加 (Add)] をクリックします。

**ステップ 7** トラフィックを追跡する方法を指定します。

- 特定の送信元または送信元の範囲からのすべてのトラフィックを追跡するには、[追跡対象 (Track By)] ドロップダウンリストから [送信元 (Source)] を選択し、[ネットワーク (Network)] フィールドに単一の IP アドレスまたはアドレスブロックを入力します。
- 特定の宛先または宛先の範囲へのすべてのトラフィックを追跡するには、[追跡対象 (Track By)] ドロップダウンリストから [宛先 (Destination)] を選択し、[ネットワーク (Network)] フィールドに単一の IP アドレスまたはアドレスブロックを入力します。

(注) システムは、[ネットワーク (Network)] フィールドに含まれる各 IP アドレスのトラフィックを個別に追跡します。ある特定の IP アドレスからの設定されたレートを超過するトラフィックがある場合、その IP アドレスに関するイベントだけが生成されることとなります。例として、ネットワーク設定で 10.1.0.0/16 の送信元 CIDR ブロックを設定し、10 個の同時接続が開始された時点でイベントを生成するようにシステムを設定するとします。10.1.4.21 から 8 つの接続が開始され、10.1.5.10 から 6 つの接続が開始されている場合、いずれの送信元も開始されている接続がトリガーを引き起こす数になっていないため、システムはイベントを生成しません。一方、10.1.4.21 から 11 個の同時接続が開始されている場合、システムは 10.1.4.21 からの接続に対してだけイベントを生成します。

システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

**ステップ 8** レート追跡設定をトリガーとして使用するレートを指定します。

- SYN 攻撃に対する構成の場合は、[レート (Rate)] フィールドに、一定の秒数あたりの SYN パケット数を入力します。
- 同時接続に対する構成の場合は、[カウント (Count)] フィールドに、接続数を入力します。

デバイスは、内部リソースにインスペクションの負荷を分散させます。レートベースの攻撃の防御を設定すると、デバイスごとではなく、リソースごとのトリガーレートを設定します。



レートベースの攻撃の防御が適切に作動しなければ、トリガーレートを低減する必要があります。正しいレートの決定する方法については、サポートにお問い合わせください。

**ステップ 9** レートベース攻撃防止設定に一致するパケットをドロップするには、[ドロップ (Drop)] チェックボックスをオンにします。

**ステップ 10** [タイムアウト (Timeout)] フィールドに、イベント生成のタイムアウト期間を入力します。この期間を経過すると、SYNまたは同時接続のパターンに一致するトラフィックに対するイベント生成が（該当する場合はドロップも）停止されます。

**注意** インライン展開では、大きいタイムアウト値を指定するとホストへの接続が完全にブロックされる可能性があります。

**ステップ 11** [OK] をクリックします。

**ステップ 12** 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックし、[変更の確定 (Commit Changes)] をクリックします。変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

---

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)





## 第 83 章

# 適応型プロファイル

ここでは、適応型プロファイルの設定方法について説明します。

- [アダプティブプロファイルについて \(2013 ページ\)](#)
- [アダプティブプロファイルの更新 \(2014 ページ\)](#)
- [アダプティブプロファイルの更新および Firepower 推奨ルール \(2014 ページ\)](#)
- [適応型プロファイルのオプション \(2015 ページ\)](#)
- [適応型プロファイルの設定 \(2016 ページ\)](#)

## アダプティブプロファイルについて

アダプティブプロファイルを使うと、次の操作を実行できます。

- アクセスコントロールルールはAMPを含むアプリケーション制御およびファイル制御が可能になり、侵入ルールはサービスメタデータを使用できるようになります。



**注意** アクセスコントロールルールがAMPを含むアプリケーション制御およびファイル制御を行い、侵入ルールがサービスメタデータを使用するためには、[適応型プロファイルの設定 \(2016ページ\)](#) で説明されているように、アダプティブプロファイルが**必ず**有効になっている (デフォルト状態) 必要があります。

- パッシブ展開では、アダプティブプロファイルの更新を有効にして、宛先ホストのオペレーティングシステムに従ってIPトラフィックに最適化とリアセンブルを行います。



**(注)** インライン展開では、アダプティブプロファイルの更新を有効にする代わりに、インライン正規化プリプロセッサを設定し、[TCPペイロードの正規化 (Normalize TCP Payload) ]オプションを有効にすることを推奨します。

## アダプティブプロファイルの更新

通常、システムはネットワーク分析ポリシーの静的な設定を使用して、トラフィックの前処理と分析を行います。アダプティブプロファイルの更新では、ネットワーク検出で検出したホスト情報またはサードパーティからインポートしたホスト情報に合わせて、システムが処理動作を変更します。

プロファイルの更新ネットワーク分析ポリシーに手動で設定可能なターゲットベースプロファイルと同様に、ターゲットホストのオペレーティングシステムと同じ方法で、IPパケットの最適化およびストリームのリアセンブルを行うのに役立ちます。その後、侵入ルールエンジンは宛先ホストによって使用されるものと同じ形式でデータを分析します。

手動で設定されたターゲットベースプロファイルは、選択したデフォルトオペレーティングシステムプロファイルまたは特定のホストにバインドしたプロファイルのいずれかに適用されます。プロファイルの更新では、ターゲットホストのホストプロファイル内のオペレーティングシステムに基づいて、適切なオペレーティングシステムプロファイルに切り替えを行います。

10.6.0.0/16 サブネット向けにプロファイルの更新を設定し、Linux にデフォルトの IP 最適化ターゲットベースポリシーを設定するシナリオを考えてみます。設定を構成する Firepower Management Center には 10.6.0.0/16 サブネットを含むネットワークマップがあります。

- システムが 10.6.0.0/16 サブネットにないホスト A からのトラフィックを検出すると、Linux ターゲットベースポリシーを使用して IP フラグメントのリアセンブルを行います。
- システムが 10.6.0.0/16 サブネット上にあるホスト B からのトラフィックを検出すると、ネットワークマップからホスト B のオペレーティングシステムデータを取得します。システムは、このオペレーティングシステムに基づいたプロファイルを使用し、ホスト B を宛先とするトラフィックを最適化します。

## アダプティブプロファイルの更新および Firepower 推奨ルール

アダプティブプロファイルの更新機能は、アクセスコントロールポリシーの詳細設定で、そのアクセスコントロールポリシーによって呼び出されるすべての侵入ポリシーにグローバルに適用されます。Firepower 推奨ルールの機能は、設定する個々の侵入ポリシーに適用されません。

Firepower 推奨ルールと同様に、プロファイルの更新はルールのメタデータをホスト情報と比較し、ルールを特定のホストに適用すべきかどうかを判別します。ただし、Firepower 推奨ルールがその情報を使用してルールの有効化または無効化を行うための推奨事項を提供するのに対して、プロファイルの更新はその情報を使用して特定のトラフィックに特定のルールを適用します。

Firepower 推奨ルールでは、提案された変更をルール状態に実装するために、ユーザの対話が必要になります。一方、プロファイルの更新は侵入ポリシーを変更しません。プロファイル更新に基づくルールの処理は、パケット単位で行われます。

さらに、Firepower 推奨ルールによって、無効なルールが有効化される可能性があります。プロファイルの更新は、対照的に、侵入ポリシーですでに有効になっているルールの適用にだけ影響します。プロファイルの更新がルール状態を変更することはありません。

プロファイルの更新と Firepower 推奨ルールは組み合わせて使用できます。侵入ポリシーを展開すると、プロファイルの更新はルールの状態を使用して適用の候補に含めるかどうかを判別し、推奨事項の承認または拒否はそのルール状態に反映されます。両方の機能を使用して、監視対象の各ネットワークに最適なルールを有効化または無効化することができ、特定のトラフィックに対する有効化したルールの適用を最も効率的に行うことができます。

#### 関連トピック

[Firepower 推奨ルールについて](#) (1655 ページ)

## 適応型プロファイルのオプション

### 有効 (Enable)

次のことを可能にします。

- アクセスコントロールルールで AMP を含めたアプリケーションとファイルの制御を実行する
- 侵入ルールでサービス メタデータを使用する

### プロファイルの更新を有効にする (Enable Profile Updates)

パッシブ展開で、プロファイルの更新を有効にして、ネットワーク マップでホストが使用するオペレーティング システムのプロファイルに応じて IP トラフィックがデフラグおよびリアセンブルされるようにします。

### アダプティブ プロファイル - 属性の更新間隔 (Adaptive Profiles - Attribute Update Interval)

プロファイルの更新を有効にすると、Firepower Management Center から管理対象デバイスに対するネットワーク マップデータの同期の頻度を分単位で制御することができます。システムはデータを使用して、トラフィックを処理する際に使用するプロファイルを判別します。このオプションの値を大きくすると、大規模なネットワークでパフォーマンスを向上させることができます。

### アダプティブ プロファイル - ネットワーク (Adaptive Profiles - Networks)

任意で、プロファイルの更新を有効にすると、IP アドレス、アドレス ブロック、およびネットワーク変数のカンマ区切りリストに対するプロファイルの更新を制限して、パフォーマンスを向上させることができます。ネットワーク変数を使用すると、アクセスコントロールポ

リシーのデフォルトの侵入ポリシーにリンクされている変数セットの変数の値が使用されるようになります。たとえば、**192.168.1.101**、**192.168.4.0/24**、**\$HOME\_NET** 这样就可以入力することができます。



- (注) システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上位ポリシーでプロファイルの更新を有効にして適用する場合、Cisco では、デフォルトのネットワークの制約 **0.0.0.0/0** を保持するか、または値 `any` を指定してネットワーク変数を使用することをお勧めしています。この設定により、すべてのサブドメインのすべてのモニタ対象ホストにプロファイルの更新が適用されるようになります。

#### 関連トピック

[デフォルトの侵入ポリシー](#) (1837 ページ)

[Firepower システムの IP アドレス表記法](#) (14 ページ)

[変数セット](#) (444 ページ)

## 適応型プロファイルの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

パッシブ展開では、アダプティブプロファイルの更新を設定することをお勧めします。インライン展開の場合、インライン正規化プリプロセッサの設定で [TCP ペイロードの正規化 (Normalize TCP Payload) ] オプションを有効にします。



- 注意** アクセスコントロールルールが AMP を含むアプリケーション制御およびファイル制御を行い、侵入ルールがサービスメタデータを使用するためには、この手順で説明されているように、アダプティブプロファイルが**必ず**有効になっている (デフォルト状態) 必要があります。アダプティブプロファイルを有効化または無効化すると設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作](#) (356 ページ) を参照してください。

## 手順

---

**ステップ 1** アクセス コントロール ポリシー エディタで [詳細 (Advanced) ] タブをクリックし、[検出拡張の設定 (Detection Enhancement Settings) ] セクションの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する (Inherit from base policy) ] をオフにして、編集を有効にします。

**ステップ 2** [適応型プロファイルのオプション \(2015ページ\)](#) の説明に従って適応型プロファイルのオプションを設定します。

**ステップ 3** [OK] をクリックします。

**ステップ 4** [保存 (Save) ] をクリックしてポリシーを保存します。

---

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 関連トピック

[インライン正規化プリプロセッサ \(1951 ページ\)](#)

[Snort® の再起動シナリオ \(354 ページ\)](#)







## 第 **XX** 部

# 検出とアイデンティティ

- [ネットワーク検出とアイデンティティの概要 \(2021 ページ\)](#)
- [ホスト ID ソース \(2039 ページ\)](#)
- [アプリケーションの検出 \(2097 ページ\)](#)
- [ユーザアイデンティティ ソース \(2121 ページ\)](#)
- [ネットワーク検出ポリシー \(2147 ページ\)](#)
- [レルムとアイデンティティ ポリシー \(2177 ページ\)](#)





## 第 84 章

# ネットワーク検出とアイデンティティの概要

次のトピックでは、ネットワーク検出およびアイデンティティポリシーとデータの概要を示します。

- [ホスト、アプリケーション、ユーザの検出 \(2021 ページ\)](#)
- [ホスト、アプリケーション、およびユーザ検出とアイデンティティ データの使用 \(2022 ページ\)](#)
- [ホストおよびアプリケーション検出の基礎 \(2023 ページ\)](#)
- [ユーザアイデンティティについて \(2031 ページ\)](#)
- [Firepower システムのホストとユーザの制限 \(2035 ページ\)](#)

## ホスト、アプリケーション、ユーザの検出

Firepower システムは、ネットワーク検出およびアイデンティティポリシーを使用して、ネットワークトラフィックのホスト、アプリケーション、およびユーザのデータを収集します。特定のタイプの検出およびアイデンティティデータを使用すると、ネットワークアセットの包括的なマップを作成し、フォレンジック分析、動作プロファイリング、アクセス制御を行い、組織が影響を受ける脆弱性およびエクスプロイトに対応して軽減することができます。

### ホストおよびアプリケーション データ

ホストやアプリケーションデータは、ネットワーク検出ポリシーの設定に従ってホストのアイデンティティソースとアプリケーションディテータによって収集されます。管理対象デバイスは、指定したネットワークセグメントのトラフィックを確認します。

詳細については、[ホストおよびアプリケーション検出の基礎 \(2023 ページ\)](#) を参照してください。

### ユーザ データ (User Data)

ユーザデータはネットワーク検出およびアイデンティティポリシーの設定に従ってユーザのアイデンティティソースによって収集されます。データはユーザ認識とユーザ制御のために使用できます。

詳細については、[ユーザアイデンティティについて \(2031 ページ\)](#) を参照してください。

#### 関連トピック

[ホスト ID ソース \(2039 ページ\)](#)

[アプリケーションの検出 \(2097 ページ\)](#)

[ユーザアイデンティティ ソース \(2121 ページ\)](#)

## ホスト、アプリケーション、およびユーザ検出とアイデンティティ データの使用

検出データとアイデンティティ データをロギングすることにより、次のような Firepower システムのさまざまな機能を活用できます。

- ネットワーク アセットとトポロジの詳細を示すネットワーク マップを表示します。その際、ホストとネットワーク デバイス、ホスト属性、アプリケーション プロトコル、または脆弱性をグループ化して表示できます。
- アプリケーション、レルム、ユーザ、ユーザグループ、および ISE 属性の各条件を使ってアクセス コントロール ルールを作成することにより、アプリケーション制御およびユーザ制御を実行します。
- 検出されたホストで利用可能なすべての情報の完全なビューであるホストプロファイルを表示します。
- (さまざまな機能の 1 つとして) ネットワーク アセットとユーザ アクティビティの概要を示すダッシュボードを表示します。
- システムによって記録された検出イベントとユーザ アクティビティに関する詳細情報を表示します。
- ホストおよびそこで実行されているサーバ/クライアントと、被害を及ぼす可能性のあるエクスプロイトとを関連付けます。  
これにより、脆弱性を特定して軽減したり、ネットワークに対する侵入イベントの影響を評価したり、ネットワーク アセットを最大限に保護できるように侵入ルール状態を調整したりできます。
- システムで特定の影響フラグ付きの侵入イベントまたは特定のタイプの検出イベントが生成された場合に、電子メール、SNMP トラップ、または syslog によるアラートを発行します。
- 許可されたオペレーティング システム、クライアント、アプリケーション プロトコル、およびプロトコルのホワイトリストを使用して組織のコンプライアンスをモニタします。
- システムが検出イベントを生成するかユーザ アクティビティを検出したときにトリガーして関連イベントを生成するルールを使って、関連ポリシーを作成します。
- 該当する場合、NetFlow 接続をロギングして使用します。

# ホストおよびアプリケーション検出の基礎

ネットワーク検出ポリシーを設定すると、ホストおよびアプリケーション検出を実行できます。

詳細については、[概要：ホストのデータ収集（2039ページ）](#) および [概要：アプリケーション検出（2097ページ）](#) を参照してください。

## オペレーティング システムおよびホスト データのパッシブ検出

パッシブ検出は、システムがネットワークトラフィック（およびエクスポートされた NetFlow データ）を分析してネットワークマップにデータを取り込む際のデフォルト方式です。パッシブ検出では、ネットワークアセットに関するコンテキスト情報（オペレーティングシステムや実行中のアプリケーションなど）が提供されます。

モニタ対象のホストからのトラフィックが、ホストで実行されているオペレーティングシステムを示す決定的証拠とならない場合、使用されている可能性が最も高いオペレーティングがネットワークマップに表示されます。たとえば、複数のホストが NAT デバイスの「背後」にあることから、NAT デバイスが複数のオペレーティングシステムを実行しているように表示される場合があります。この最も可能性の高いオペレーティングを決定するためにシステムが使用するのには、検出された各オペレーティングシステムに割り当てられた信頼度の値と、検出されたオペレーティングシステムの中でその特定のオペレーティングシステムが使用されていることを裏付けるデータの量です。



(注) この決定を行う際、システムは「unknown」として報告されたアプリケーションとオペレーティングシステムを考慮しません。

パッシブ検出でネットワークアセットが正確に識別されない場合は、管理対象デバイスの配置について検討してください。また、システムのパッシブ検出機能をオペレーティングシステムのカスタムフィンガープリントとカスタムアプリケーションディテクタで増補することもできます。あるいは、アクティブ検出を使用するという方法もあります。アクティブ検出では、トラフィック分析をベースとするのではなく、スキャン結果やその他の情報ソースを使用して直接ネットワークマップを更新できます。

## オペレーティング システムおよびホスト データのアクティブ検出

アクティブ検出では、アクティブソースによって収集されたホスト情報をネットワークマップに追加します。たとえば、Nmap スキャナを使用して、ネットワーク上の対象ホストをアクティブにスキャンできます。Nmap は、ホストでオペレーティングシステムおよびアプリケーションを検出します。

さらに、ホスト入力機能によって、ネットワークマップにホスト入力データをアクティブに追加することができます。ホスト入力データには 2 種類のカテゴリがあります。

- ユーザ入力データ：FirePOWER システム ユーザ インターフェイスで追加されたデータ。このユーザ インターフェイスを使用して、ホストのオペレーティング システムやアプリケーションの ID を変更できます。
- ホスト インポート入力データ：コマンドライン ユーティリティを使用してインポートされたデータ。

システムは、それぞれのアクティブソースに対して1個のIDを保持します。たとえば、Nmap スキャンインスタンスを実行すると、以前のスキャンの結果は新しいスキャン結果に置き換えられます。ただし、Nmap スキャンを実行し、それらの結果をクライアントからのデータ（コマンドラインを使用してインポートした結果）と交換する場合、システムは Nmap の結果の ID とインポートクライアントの ID の両方を保持します。システムは、ネットワーク検出ポリシーで設定された優先順位を使用して、現在の ID として使用するアクティブ ID を判別します。

複数のユーザが入力したとしても、ユーザ入力は1ソースと見なされることに注意してください。たとえば、UserA がホストプロファイルを使用してオペレーティングシステムを設定し、UserB がホストプロファイルを使用してその定義を変更した場合、UserB によって設定された定義が保持され、UserA によって設定された定義は破棄されます。また、ユーザ入力によって、他のアクティブソースすべてが上書きされ、存在する場合、現在の ID として使用されることに注意してください。

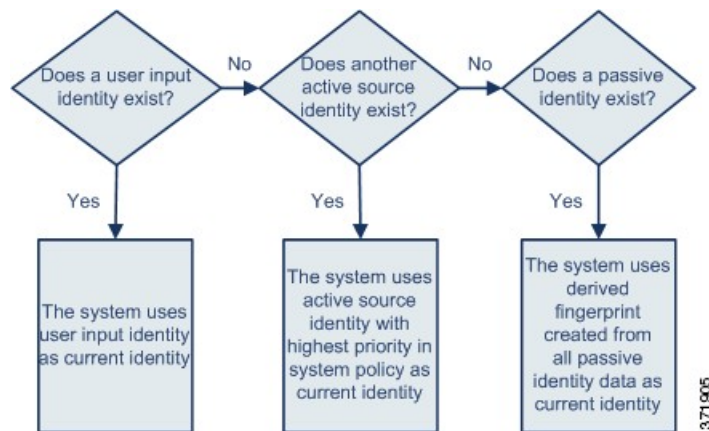
## アプリケーションおよびオペレーティングシステムの現在の ID

ホストのアプリケーションまたはオペレーティングシステムの現在の ID は、ホストが最も正しい可能性が高いと認識する ID です。

システムは、以下の目的で、オペレーティングシステムまたはアプリケーションの現在の ID を使用します。

- 脆弱性のホストへの割り当て
- 影響評価
- オペレーティングシステムの識別、ホストプロファイルの認定、およびコンプライアンスのホワイトリストに対して記述された関連ルールの評価
- ワークフローのホストおよびサーバのテーブルビューでの表示
- ホストプロファイルでの表示
- [検出統計情報 (Discovery Statistics) ] ページでのオペレーティングシステムとアプリケーションの統計の計算

システムは、ソースの優先順位を使用して、アプリケーションまたはオペレーティングシステムの現在の ID として使用するアクティブ ID を判別します。



たとえば、ユーザがホストでオペレーティングシステムを Windows 2003 Server に設定した場合、Windows 2003 Server が現在の ID になります。そのホストの Windows 2003 Server の脆弱性を狙った攻撃により大きな影響力があると見なされ、ホストプロファイルのそのホストについてリストされた脆弱性に、Windows 2003 Server の脆弱性が含まれます。

データベースは、ホストのオペレーティングシステムや特定のアプリケーションに関する複数のソースからの情報を保持する場合があります。

データのソースに最も高いソースの優先順位が付けられている場合に、システムはオペレーティングシステムまたはアプリケーションの ID を現在の ID として扱います。使用される可能性のあるソースには、次の優先順位があります。

- 1 : ユーザ
- 2 : スキャナとアプリケーション (ネットワーク検出ポリシーで設定)
- 3 : 管理対象デバイス
- 4 : NetFlow レコード

新しい優先順位の高いアプリケーション ID は、現在のアプリケーション ID ほど詳細でない場合、現在の ID を上書きしません。

また、ID の競合が発生した場合、競合の解決はネットワーク検出ポリシーの設定または手動解決によります。

## 現在のユーザ ID

システムは、同じホストに対して異なるユーザによる複数のログインを検出すると、特定のホストにログインするユーザは一度に1人だけであり、ホストの現在のユーザが最後の権限のあるユーザログインであると見なします。権限のないユーザログインだけがホストにログインしている場合は、最後にログインしたものが現在のユーザと見なされます。複数のユーザがリモートセッション経由でログインしている場合は、サーバによって報告された最後のユーザが Firepower Management Center に報告されるユーザです。

システムは、同じホストに対して異なるユーザによる複数のログインを検出すると、ユーザが初めて特定のホストにログインした時点を記録し、それ以降のログインを無視します。ある

ユーザが特定のホストにログインしている唯一の人物の場合は、システムが記録する唯一のログインがオリジナルのログインです。

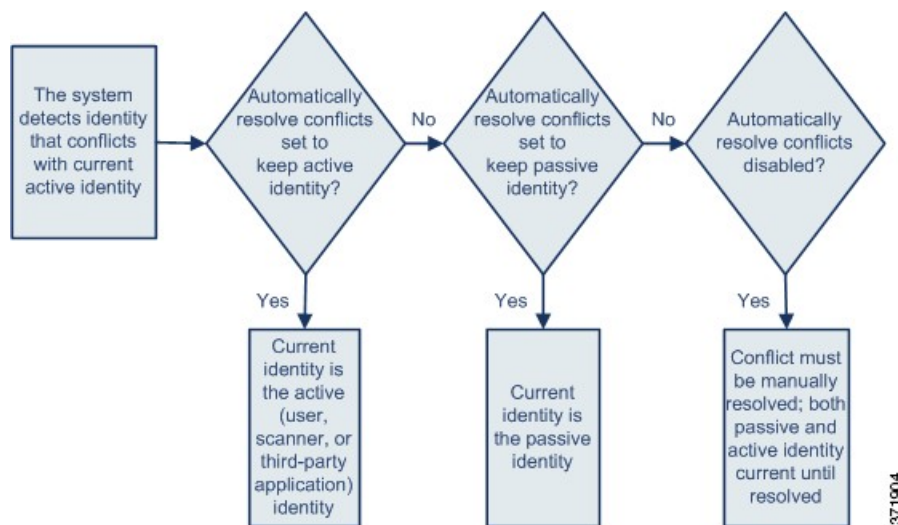
ただし、そのホストに別のユーザがログインした時点で、システムは新しいログインを記録します。その後で、オリジナルのユーザが再度ログインすると、その人物の新しいログインが記録されます。

## アプリケーションおよびオペレーティングシステムの ID の競合

現在のアクティブ ID および以前に報告されたパッシブ ID と競合する新しいパッシブ ID が報告されると、ID の競合が発生します。たとえば、オペレーティングシステムの以前のパッシブ ID は Windows 2000 と報告され、Windows XP のアクティブ ID が現在の ID になります。次に、システムが Ubuntu Linux 8.04.1 の新しいパッシブ ID を検出します。Windows XP と Ubuntu Linux の ID が競合状態になります。

ホストのオペレーティングシステムまたはホスト上のいずれかのアプリケーションの ID に対して ID の競合が存在する場合、システムは現在の ID として競合する両方の ID をリストし、競合が解決されるまで影響評価に両方の ID を使用します。

管理者特権を持つユーザは、パッシブ ID を常に使用するか、またはアクティブ ID を常に使用するかを選択することによって、自動的に ID の競合を解決できます。ID の競合の自動解決を無効にしない限り、ID の競合は常に自動的に解決されます。



管理者特権を持つユーザは、ID の競合が発生した場合に、イベントを生成するようにシステムを設定することもできます。そのユーザは、関連応答として Nmap スキャンを使用する相関ルールで相関ポリシーを設定できます。イベントが発生すると、Nmap はホストをスキャンして、更新されたホストのオペレーティングシステムとアプリケーションデータを取得します。



## Firepower システムの NetFlow データ

NetFlow は、ルータを通過するパケットの統計情報を提供する、Cisco IOS アプリケーションの 1 つです。NetFlow は Cisco ネットワーキング デバイスで使用できます。また、Juniper、FreeBSD、OpenBSD デバイ스에組み込むことも可能です。

NetFlow がネットワーク デバイスで有効にされている場合、そのデバイス上のデータベース (NetFlow キャッシュ) に、ルータを通過するフローのレコードが格納されます。Firepower システムで接続と呼ばれるフローは、特定のポート、プロトコル、およびアプリケーションプロトコルを使用する送信元ホストと宛先ホスト間のセッションを表すパケットのシーケンスです。この NetFlow データをエクスポートするようにネットワーク デバイスを設定できます。本書では、そのように設定されたネットワーク デバイスを NetFlow エクスポートと呼びます。

Firepower システムの管理対象デバイスは、NetFlow エクスポートからレコードを収集して、それらのレコードに含まれるデータに基づいて単方向の接続終了イベントを生成し、それらのイベントを接続イベントデータベースに記録するために Firepower Management Center に送信するように設定できます。また、NetFlow 接続内の情報に基づいて、ホストとアプリケーションプロトコルに関する情報をデータベースに追加するためのネットワーク検出ポリシーを設定することもできます。

この検出データと接続データを使用して、管理対象デバイスによって直接収集されたデータを補完できます。これは、管理対象デバイスでモニタできないネットワークを NetFlow エクスポートにモニタさせる場合には特に有効です。

### NetFlow データを使用するための要件

NetFlow データを分析するために Firepower System を設定する前に、ルータまたは使用する他の NetFlow が有効なネットワーク デバイス上で NetFlow 機能を有効にし、管理対象デバイスのセンシングインターフェイスを接続する宛先ネットワークへ NetFlow データをブロードキャストするようにデバイスを設定する必要があります。

Firepower System では、NetFlow バージョン 5 レコードと NetFlow バージョン 9 レコードをいずれも解析できます。Firepower System にデータをエクスポートするには、NetFlow エクスポートがいずれかのバージョンを使用する必要があります。さらに、このシステムでは、特定のフィールドがエクスポートされた NetFlow テンプレートとレコードに存在する必要があります。NetFlow エクスポートがカスタマイズ可能なバージョン 9 を使用している場合は、エクスポートされたテンプレートとレコードに次のフィールドが任意の順序で含まれていることを確認する必要があります。

- IN\_BYTES (1)
- IN\_PKTS (2)
- PROTOCOL (4)
- TCP\_FLAGS (6)
- L4\_SRC\_PORT (7)
- IPV4\_SRC\_ADDR (8)
- L4\_DST\_PORT (11)

- IPV4\_DST\_ADDR (12)
- LAST\_SWITCHED (21)
- FIRST\_SWITCHED (22)
- IPV6\_SRC\_ADDR (27)
- IPV6\_DST\_ADDR (28)

Firepower System は管理対象デバイスを使用して NetFlow データを分析するため、NetFlow エクスポートの監視可能な1つ以上の管理対象デバイスを展開に含める必要があります。この管理対象デバイス上の1つ以上のセンシング インターフェイスを、エクスポートされた NetFlow データを収集可能なネットワークに接続する必要があります。通常、管理対象デバイス上のセンシング インターフェイスには IP アドレスが割り当てられないため、システムは NetFlow レコードの直接収集をサポートしません。

一部のネットワーク デバイス上で使用可能な Sampled NetFlow 機能は、デバイスを通るパケットのサブセットだけに基づく NetFlow 統計情報を収集することに注意してください。この機能を有効にすると、ネットワーク デバイス上の CPU 使用率が改善される可能性があります。Firepower System で分析するために収集されている NetFlow データに影響する場合があります。

## NetFlow データと管理対象デバイス データの違い

Firepower システムは、NetFlow データによって表されるトラフィックを直接分析しません。代わりに、エクスポートした NetFlow レコードを接続ログおよびホストとアプリケーションのプロトコル データに変換します。

その結果、変換された NetFlow データと、管理対象デバイスによって直接収集された検出および接続データにはいくつかの違いがあります。以下のことを必要とする分析を実行する場合には、これらの違いを意識しなければなりません。

- 検出された接続数に基づく統計情報
- オペレーティング システムとその他のホスト関連情報（脆弱性を含む）
- クライアント情報、Web アプリケーション情報、ベンダーおよびバージョン サーバ情報を含むアプリケーション データ
- 接続内の発信側のホストと応答側のホストの認識

### ネットワーク検出ポリシーとアクセス コントロール ポリシーの違い

接続ロギングを含む NetFlow データ収集は、ネットワーク検出ポリシー内のルールを使用して設定します。これを、アクセスコントロールルールごとに設定した FirePOWER システム管理対象デバイスによって検出された接続の接続ロギングと比較してください。

### 接続イベントのタイプ

NetFlow データ収集はアクセスコントロールルールではなくネットワークにリンクされているため、システムがログに記録する NetFlow 接続をきめ細かく制御することはできません。

NetFlow データは、セキュリティ インテリジェンス イベントを生成することはできません。

NetFlow ベースの接続イベントは、接続イベント データベースにのみ保存できます。システム ログまたは SNMP トラップ サーバに送信することはできません。

### モニタ対象セッションごとに生成される接続イベントの数

管理対象デバイスによって直接検出された接続の場合は、アクセスコントロールルールを設定して、接続の最初か最後またはその両方で双方向接続イベントをログに記録できます。

それに対し、エクスポートされた NetFlow レコードには単方向接続データが含まれているため、システムは処理する各 NetFlow レコードに対し少なくとも2つの接続イベントを生成します。これは、概要の接続数が NetFlow データに基づいた接続ごとに2ずつ増加することも意味しており、ネットワーク上で実際に発生している接続数が急増することになります。

接続がまだ実行中であっても、NetFlow エクスポートは固定間隔でレコードを出力するため、長時間実行しているセッションの場合は複数のエクスポートされたレコードが生成される場合があります。たとえば、NetFlow エクスポートが5分ごとにエクスポートする場合に、特定の接続が12分間続いている場合、システムはそのセッションに対し6つの接続イベントを生成します。

- 最初の5分間の1つのイベント ペア
- 次の5分間の1つのペア
- 接続が終了した時点の最後のペア

### ホスト データとオペレーティング システム データ

NetFlow データからのネットワーク マップに追加されたホストには、オペレーティング システム、NetBIOS、またはホストタイプ（ホストまたはネットワーク デバイス）の情報がありません。ただし、ホスト入力機能を使用してホストのオペレーティング システム ID を手動で設定できます。

### アプリケーション データ

管理対象デバイスによって直接検出された接続の場合は、接続内のパケットを検査することによって、システムはアプリケーションプロトコル、クライアント、および Web アプリケーションを識別できます。

システムは NetFlow レコードを処理するときに、`/etc/sf/services` 内のポート関連付けを使用して、アプリケーションプロトコル ID を推測します。ただし、これらのアプリケーションプロトコルに関するベンダーまたはバージョン情報が存在しないため、接続ログにはセッションで使用されるクライアントまたは Web アプリケーションに関する情報が含まれません。しかし、ホスト入力機能を使用してこの情報を手動で提供できます。

単純なポート関連付けでは、非標準ポート上で動作しているアプリケーションプロトコルが特定されないまたは誤認される可能性があることに注意してください。加えて、関連付けが存在しない場合は、システムがそのアプリケーションプロトコルを接続ログで unknown としてマークします。

### 脆弱性マッピング

システムは、ホスト入力機能を使用してホストのオペレーティングシステム ID またはアプリケーションプロトコル ID を手動で設定しない限り、NetFlow エクスポートによってモニタされるホストに脆弱性をマッピングできません。NetFlow 接続内にクライアント情報が存在しないため、クライアントの脆弱性を NetFlow データから作成されたホストに関連付けることはできないことに注意してください。

### 接続内の発信側情報と応答側情報

管理対象デバイスによって直接検出された接続の場合、システムは発信側または送信元のホストと応答側または宛先のホストを識別できます。ただし、NetFlow データには発信側または応答側の情報が含まれていません。

Firepower システムは、NetFlow レコードを処理するときに、それぞれのホストが使用しているポートとそれらのポートが既知かどうかに基づいて、この情報を判断するアルゴリズムを使用します。

- 使用されているポートの両方が既知のポートの場合、または、どちらも既知のポートでない場合、システムは番号の小さい方のポートを使用しているホストを応答側と見なします。
- どちらかのホストだけが既知のポートを使用している場合は、システムがそのホストを応答側と見なします。

したがって、既知のポートは、1～1023 の番号が割り当てられたポートまたは管理対象デバイス上の `/etc/sf/services` にアプリケーションプロトコル情報が保存されているポートです。

さらに、管理対象デバイスによって直接検出された接続の場合、システムは対応する接続イベントの 2 バイト数を記録します。

- [イニシエータ バイト数 (Initiator Bytes)] フィールドは送信バイト数を記録します。
- [レスポнда バイト数 (Responder Bytes)] フィールドは受信バイト数を記録します。

単方向 NetFlow レコードに基づく接続イベントには、1 バイト数しか含まれておらず、ポートベースアルゴリズムに応じて、システムが [イニシエータ バイト数 (Initiator Bytes)] または [レスポнда バイト数 (Responder Bytes)] に割り当てます。システムによって他のフィールドは 0 に設定されます。NetFlow レコードの接続の概要 (集約接続データ) を表示している場合に、両方のフィールドに値が読み込まれる場合があることに注意してください。

### NetFlow のみの接続イベント フィールド

いくつかのフィールドは、NetFlow レコードから生成された接続イベントでのみ表示されます (接続イベント フィールドで利用可能な情報 (2541 ページ) を参照)。

### 関連トピック

[接続イベント フィールドで利用可能な情報](#) (2541 ページ)

## ユーザアイデンティティについて

ユーザアイデンティティ情報を使用すると、ポリシー違反、攻撃、ネットワークの脆弱性の発生源を特定し、特定のユーザまで遡って追跡することができます。たとえば、以下について決定できます。

- 脆弱（レベル1：赤）影響レベルの侵入イベントの対象になっているホストの所有者。
- 内部攻撃またはポートスキャンを開始した人物。
- 特定のホストへの不正アクセスを試みている人物。
- 過度に大量の帯域幅を使用している人物。
- 重要なオペレーティング システム更新を適用しなかった人物。
- 会社のポリシーに違反してインスタント メッセージング ソフトウェアまたはピアツーピア ファイル共有アプリケーションを使用している人物。

この情報を入手すれば、Firepower システムの他の機能を使用して、リスクを低減し、アクセス制御を実行し、他のユーザを破壊行為から保護するためのアクションを実行できます。これらの機能により、監査制御が大幅に改善され、規制の順守が促進されます。

ユーザアイデンティティ ソースを設定してユーザ データを収集すると、ユーザ認識とユーザ制御を実行できます。

### 関連トピック

[アイデンティティの用語](#) (2031 ページ)

[アイデンティティ導入](#) (2032 ページ)

## アイデンティティの用語

このトピックでは、ユーザアイデンティティおよびユーザ制御の一般的な用語について説明します。

### ユーザ認識

アイデンティティ ソース（ユーザ エージェントや TS エージェントなど）を使用して、ネットワーク上のユーザを識別します。ユーザ認識によって、権限のあるソース（Active Directory など）および権限のないソース（アプリケーションベース）の両方からユーザを識別できます。Active Directory をアイデンティティ ソースとして使用するには、レルムおよびディレクトリを設定する必要があります。詳細については、[ユーザアイデンティティ ソースについて](#) (2121 ページ) を参照してください。

## ユーザ制御

アクセス コントロール ポリシーに関連付けるアイデンティティ ポリシーを構成します。(アイデンティティ ポリシーは、アクセス コントロール サブポリシーと呼ばれるようになります。) アイデンティティ ポリシーはアイデンティティ ソースを指定し、オプションで、そのソースに属するユーザおよびグループを指定します。

アイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けることで、ネットワークのトラフィックでユーザまたはユーザアクティビティをモニタ、信頼、ブロックまたは許可するかどうかを決定します。詳細については、[アクセスコントロールポリシーの開始 \(1321 ページ\)](#) を参照してください。

## 権限のあるアイデンティティ ソース

信頼できるサーバによってユーザ ログインが検証されています (たとえば、Active Directory)。権限のあるログインから取得したデータを使用すると、ユーザ認識とユーザ制御を実行できます。権限のあるユーザログインは、パッシブ認証とアクティブ認証から得られます。

- パッシブ認証は、ユーザが外部サーバ経由で認証されるときに発生します。ユーザエージェント、ISE、および TS エージェントは、Firepower システムでサポートされるパッシブ認証方式です。
- アクティブ認証は、ユーザが事前設定済みの管理対象デバイス経由で認証されるときに発生します。Firepower システムでサポートされているアクティブ認証方式は、キャプティブ ポータルだけです。

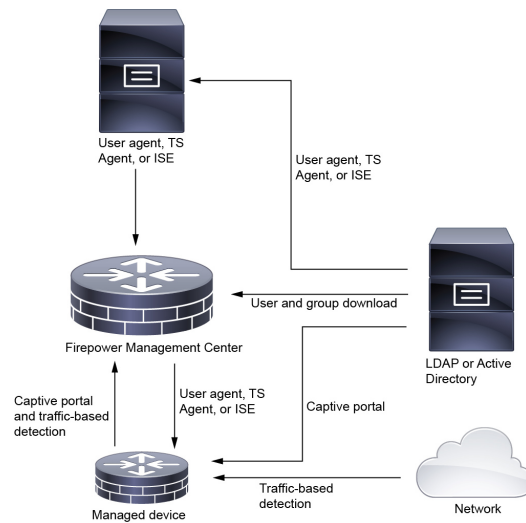
## 権限のないアイデンティティ ソース

ユーザ ログインの検証を行った不明または信頼できないサーバ。トラフィック ベースの検出は、Firepower システムでサポートされている唯一の権限のないアイデンティティ ソースです。権限のないログインから取得されたデータを使用すると、ユーザ認識を実行できません。

# アイデンティティ導入

システムがユーザ ログイン、またはアイデンティティ ソースからのユーザデータを検出すると、そのログインからのユーザは、Firepower Management Center ユーザデータベース内のユーザのリストに照らしてチェックされます。ログインユーザが既存のユーザと一致した場合は、ログインからのデータがそのユーザに割り当てられます。ログインがSMTPトラフィック内に存在しない場合は、既存のユーザと一致しないログインによって新しいユーザが作成されます。SMTPトラフィック内の一致しないログインは破棄されます。

次の図は、Firepower システムがユーザデータをどのように収集して保存するかを示しています。



## ユーザ アクティビティ データベース

Firepower Management Center のユーザ アクティビティ データベースには、設定されたすべてのアイデンティティ ソースによって検出または報告されたネットワーク上のユーザ アクティビティのレコードが含まれています。システムがイベントを記録するのは以下のような状況です。

- 個別のログインまたはログオフを検出したとき。
- 新しいユーザを検出したとき。
- システム管理者が手動でユーザを削除したとき。
- データベース内に存在しないユーザをシステムが検出したものの、ユーザ数の制限に達したためにそのユーザを追加できなかったとき。



(注) TS エージェントが別のパッシブ認証のアイデンティティ ソース (ユーザ エージェントや ISE など) と同じユーザをモニタする場合、Firepower Management Center では TS エージェントのデータを優先します。TS エージェントと別のパッシブのソースが同じ IP アドレスからの同じアクティビティを報告した場合、TS エージェントのデータだけが Firepower Management Center に記録されます。

システムで検出されたユーザ アクティビティは、Firepower Management Center Web インターフェイスを使用して表示できます。([分析 (Analysis)] > [ユーザ (Users)] > [ユーザ アクティビティ (User Activity)])。

## ユーザ データベース

Firepower Management Center のユーザ データベースには、設定されたすべてのアイデンティティソースによって検出または報告されたユーザごとのレコードが含まれています。権限のあるソースから取得したデータをユーザ制御に使用できます。

サポートされている権限のないアイデンティティソースと権限のあるアイデンティティソースの詳細については、[ユーザアイデンティティソースについて \(2121 ページ\)](#) を参照してください。

[Firepower システムのユーザの制限 \(2036 ページ\)](#) で説明されているように、Firepower Management Center で保存できるユーザの合計数は、Firepower Management Center のモデルごとに異なります。ユーザ制限に達した後、システムは、アイデンティティソースに基づいて未検出ユーザデータを次のように優先順位付けします。

- 新しいユーザが権限のないアイデンティティソースからである場合、ユーザはデータベースに追加されません。新規ユーザを追加できるようにするには、手動またはデータベースの消去によってユーザを削除する必要があります。
- 新しいユーザが権限のあるアイデンティティソースからである場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザを削除し、データベースに新しいユーザを追加します。

アイデンティティソースが特定のユーザ名を除外するように設定されている場合、それらのユーザ名のユーザ アクティビティ データは Firepower Management Center に報告されません。これらの除外されたユーザ名はデータベースに残りますが、IP アドレスに関連付けられません。システムによって保存されるデータのタイプの詳細については、[ユーザ データ \(User Data\) \(2746 ページ\)](#) を参照してください。

Firepower Management Center ハイアベイラビリティが設定済みで、プライマリに障害が発生した場合、ユーザエージェント、ISE、またはキャプティブポータルデバイスから報告されるログインはフェールオーバーダウンタイム中に識別不能になります（たとえユーザが以前に確認されて Firepower Management Center にダウンロードされた場合でも）。未確認のユーザは Firepower Management Center には不明なユーザとして記録されます。ダウンタイム後、不明のユーザはアイデンティティポリシーのルールに従って再確認され、処理されます。



- (注) TS エージェントが別のパッシブ認証のアイデンティティソース（ユーザエージェントまたは ISE）と同じユーザをモニタする場合、Firepower Management Center では TS エージェントのデータを優先します。TS エージェントと別のパッシブのソースが同じ IP アドレスからの同じアクティビティを報告した場合、TS エージェントのデータだけが Firepower Management Center に記録されます。

システムが新しいユーザセッションを検出すると、そのユーザセッションのデータは、次のいずれかが発生するまでユーザデータベースに残ります。

- Firepower Management Center のユーザが手動でユーザセッションを削除した。



- アイデンティティ ソースがそのユーザ セッションのログオフを報告した。
- レルムがレルムの [ユーザセッションのタイムアウト：認証されたユーザ (User Session Timeout: Authenticated Users) ] 設定、[ユーザセッションのタイムアウト：認証に失敗したユーザ (User Session Timeout: Failed Authentication Users) ] 設定、または [ユーザセッションのタイムアウト：ゲストユーザ (User Session Timeout: Guest Users) ] 設定で指定されているユーザ セッションを終了した。

## Firepower システムのホストとユーザの制限

Firepower Management Center モデルにより、展開でモニタできる個別のホストの数、モニタし、ユーザ制御を実行するために使用できるユーザの数が決定されます。

### 関連トピック

[Management Center データベースからのデータの消去](#) (243 ページ)

## Firepower システムのホスト制限

システムは (ネットワーク検出ポリシーで定義されている) モニタ対象ネットワークで IP アドレスに関連付けられたアクティビティを検出すると、ネットワーク マップにホストを追加します。Firepower Management Center がモニタでき、ネットワーク マップに保存できるホストの数。モデルによって異なります。

表 214: Firepower Management Center モデル別のホスト制限

Management Center モデル	ホスト
MC750	2,000
MC1500	50,000
FS2000	150,000
MC3500	300,000
MC4000	600,000
仮想	50,000

ネットワーク マップに存在しないホストのコンテキスト データは表示できません。ただし、アクセス制御は実行できます。たとえば、コンプライアンスホワイトリストを使用してホストのネットワーク コンプライアンスをモニタできない場合でも、ネットワーク マップに存在しないホストとの間のトラフィックでアプリケーション制御を実行できます。



- (注) システムでは、IPアドレスとMACアドレスの両方によって識別されるホストとは別に、MAC専用ホストがカウントされます。1つのホストに関連付けられているすべてのIPアドレスは、まとめて1つのホストとしてカウントされます。

#### ホスト制限への到達とホストの削除

ホスト制限に到達した後新しいホストを検出すると、ネットワーク検出ポリシーが制御を行います。新しいホストをドロップするか、または非アクティブになっている期間が最も長いホストを置換することができます。また、システムが非アクティブであるためネットワークからホストを削除するまでの期間を設定できます。ホスト、サブネット全体、またはすべてのホストをネットワークマップから手動で削除できますが、システムは、削除されたホストに関連付けられたアクティビティを検出した場合は、ホストを再追加します。

マルチドメイン展開では、各リーフドメインに自身のネットワーク検出ポリシーがあります。したがって、各リーフドメインによって、システムが新しいホストを検出したときの独自の動作が決定されます。

#### 関連トピック

[ドメインのプロパティ](#) (341 ページ)

[ネットワーク検出のデータストレージ設定](#) (2170 ページ)

## Firepower システムのユーザの制限

Firepower Management Center モデルにより、モニタできる個々のユーザ数が決まります。システムが新しいユーザのアクティビティを検出すると、そのユーザは Firepower Management Center の Users データベースに追加されます。任意のアイデンティティソースを使用して、ユーザを検出できます。

検討するユーザ制限には2つのタイプがあります。

- 権限のあるユーザ数の制限。データベースに保存でき、アクセス制御に使用できる、アクセス制御されたユーザの数です。権限のあるユーザデータは、ユーザエージェント、ISE、TS エージェント、およびキャプティブポータルによって収集されます。
- ユーザ総数の制限。データベースに保存できる、権限のあるユーザと権限のないユーザの数です。この制限には、すべての権限のあるユーザデータとトラフィックベースの検出を使用して収集された権限のないユーザデータが含まれます。

表 215: Firepower Management Center モデル別のユーザ制限

Management Center モデル	権限のあるユーザ	ユーザ総数
MC750	2,000	2,000
MC1500	50,000	50,000

Management Center モデル	権限のあるユーザ	ユーザ総数
FS2000	64,000	150,000
MC3500	64,000	300,000
MC4000	64,000	600,000
仮想	50,000	50,000

制限に達してから、新しい、以前検出されなかったユーザをシステムが検出すると、アイデンティティソースに基づいてユーザデータに優先順位が付けられます。

- 新しいユーザが権限のないアイデンティティソースからである場合、ユーザはデータベースに追加されません。新規ユーザを追加できるようにするには、手動またはデータベースの消去によってユーザを削除する必要があります。
- 新しいユーザが権限のあるアイデンティティソースからである場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザを削除し、データベースに新しいユーザを追加します。



(注) 展開に ASDM によって管理される ASA FirePOWER モジュールが含まれる場合、Firepower Management Center モデルに関係なく、最大 2,000 の権限のあるユーザを保存できます。



ヒント トラフィックベースの検出を使用している場合、プロトコルによるユーザログインを制限すると、ユーザ名の散乱を最小限に抑え、データベースのスペースを残しておくことができます。たとえば、システムが AIM、POP3、および IMAP トラフィックで検出されたユーザを追加できないようにすることができます（モニタを望んでいない特定の契約業者または訪問者からのトラフィックであることがわかっているため）。





## 第 85 章

# ホスト ID ソース

次のトピックでは、ホスト ID ソースについて説明します。

- [概要：ホストのデータ収集 \(2039 ページ\)](#)
- [システムが検出できるホスト オペレーティング システムの判別 \(2040 ページ\)](#)
- [ホスト オペレーティング システムの識別 \(2040 ページ\)](#)
- [カスタムフィンガープリント \(2041 ページ\)](#)
- [ホスト入力データ \(2052 ページ\)](#)
- [Nmap スキャン \(2065 ページ\)](#)

## 概要：ホストのデータ収集

Firepower システムはネットワークを通過するトラフィックを受動的に監視するため、ネットワーク トラフィックからの特定の packets ヘッダー値とその他の固有データを設定された定義と比較して (フィンガープリントと呼ばれる)、ネットワーク上のホストに関する次の情報を判断します。

- ホストの台数と種類 (ブリッジ、ルータ、ロード バランサ、NAT デバイスなどのネットワーク デバイスを含む)
- ネットワーク上の検出ポイントからホストまでのホップ数を含む、基本的なネットワーク ポロジデータ
- ホスト上で実行中のオペレーティング システム
- ホスト上のアプリケーションとそのアプリケーションに関連付けられているユーザ

システムがホストのオペレーティング システムを特定できない場合、カスタムのクライアントまたはサーバのフィンガープリントを作成できます。システムはこれらのフィンガープリントを使用して新しいホストを特定します。フィンガープリントを脆弱性データベース (VDB) 内のシステムにマップすることにより、カスタムフィンガープリントを使用してホストが特定されるたびに適切な脆弱性情報を表示できます。



- (注) システムはモニタ対象のネットワークトラフィックからだけでなく、エクスポートされた NetFlow レコードからもホストデータを収集することができ、また Nmap スキャンやホスト入力機能を使用してアクティブにホストデータを追加することもできます。

## システムが検出できるホストオペレーティングシステムの判別

システムがどのオペレーティングシステムのフィンガープリントを作成できるかを確認するには、カスタム OS フィンガープリントの作成プロセス中に表示される、使用可能なフィンガープリントの一覧を表示します。

### 手順

- ステップ 1 [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。
- ステップ 2 [カスタム OS (Custom Operating Systems)] をクリックします。
- ステップ 3 [カスタム フィンガープリントの作成 (Create Custom Fingerprint)] をクリックします。
- ステップ 4 [OS 脆弱性マッピング (OS Vulnerability Mappings)] セクションにあるドロップダウンリスト内のオプションのリストを表示します。これらのオプションが、システムがフィンガープリントを作成できるオペレーティングシステムになります。

### 次のタスク

必要に応じて、[ホストオペレーティングシステムの識別 \(2040ページ\)](#) を参照してください。

## ホストオペレーティングシステムの識別

システムがホストのオペレーティングシステムを正しく識別しない場合（たとえばホストプロファイル「不明」を示したり間違って識別したりする場合は）、下記の方法を試してください。

### 手順

次のいずれかの方法を試します。

- ネットワーク検出アイデンティティ競合設定を確認します。
- ホストのカスタム フィンガープリントを作成します。

- ホストに対して Nmap スキャンを実行します。
- ホスト入力機能を使用して、ネットワーク マップにデータをインポートします。
- オペレーティング システム情報を手動で入力します。

## カスタムフィンガープリント

Firepower システムには、検出された各ホストのオペレーティング システムを識別するためにシステムが使用するオペレーティング システムのフィンガープリントが含まれます。しかし、オペレーティング システムに一致するフィンガープリントがないため、システムがホスト オペレーティング システムを識別できない、または誤って識別することがあります。この問題を解決するために、不明または誤認されたオペレーティング システムに固有のオペレーティング システム特性のパターンを提供するカスタムフィンガープリントを作成し、識別用のオペレーティング システムの名前を提供することができます。

システムはオペレーティング システムのフィンガープリントから各ホストの脆弱性リストを取得するため、システムがホストのオペレーティング システムを照合できない場合、ホストの脆弱性を識別することはできません。たとえば、システムが Microsoft Windows を実行中のホストを検出した場合、そのシステムには保存された Microsoft Windows の脆弱性リストが存在します。このリストは、検出した Windows オペレーティング システムに基づいて、そのホストのホスト プロファイルに追加されます。

たとえば、ネットワーク上に Microsoft Windows の新しいベータ バージョンを実行中の複数のデバイスがある場合、システムはそのオペレーティング システムを識別できず、脆弱性をそれらのホストにマッピングすることもできません。しかし、システムに Microsoft Windows に関する脆弱性のリストがあるならば、同じオペレーティング システムを実行中の他のホストを識別できるように、いずれか 1 台のホストに対してカスタム フィンガープリントを作成できます。フィンガープリントに Microsoft Windows の脆弱性リストのマッピングを含め、フィンガープリントに一致する各ホストとそのリストを関連付けることができます。

カスタムフィンガープリントを作成すると Firepower Management Center は、同じオペレーティング システムを実行中のすべてのホストに関するそのフィンガープリントに関連付けられた脆弱性のセットをリストします。ユーザが作成したカスタムフィンガープリントに脆弱性マッピングが 1 つも存在しない場合、システムはフィンガープリントを使用して、フィンガープリントで提供するカスタム オペレーティング システムの情報を割り当てます。以前に検出されたホストからの新しいトラフィックが確認されると、システムはそのホストを新しいフィンガープリント情報で更新します。さらに、そのオペレーティング システムを実行する新しいホストの最初の検出時に、新しいフィンガープリントを使用して識別します。

カスタムフィンガープリントを作成する前に、ホストが正しく識別されない理由を特定して、カスタムフィンガープリントが実行可能なソリューションであるかどうかを判断する必要があります。

以下の 2 種類のフィンガープリントを作成できます。

- クライアントのフィンガープリント。ネットワーク上の別のホストで実行中の TCP アプリケーションに接続されている場合、ホストが送信する SYN パケットに基づいてオペレーティング システムを識別します。
- サーバのフィンガープリント。実行中の TCP アプリケーションへの着信接続に応答するためにホストが使用する SYN-ACK パケットに基づいてオペレーティング システムを識別します。



(注) クライアントとサーバの両方のフィンガープリントが同じホストに一致する場合、クライアントのフィンガープリントが使用されます。

フィンガープリントを作成した後、システムがフィンガープリントをホストに関連付けるには、その前に、フィンガープリントを有効化する必要があります。

#### 関連トピック

[クライアント用のカスタム フィンガープリントの作成](#) (2046 ページ)

[サーバ用のカスタム フィンガープリントの作成](#) (2049 ページ)

## フィンガープリントの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

フィンガープリントを作成してアクティブにした後、フィンガープリントを編集して変更を加えたり、脆弱性マッピングを追加したりできます。

#### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。


マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [カスタム OS (Custom Operating Systems)] をクリックします。システムがフィンガープリントを作成するデータを待機している場合、フィンガープリントが作成されるまで 10 秒ごとに自動的に更新されます。

**ステップ 3** カスタムのフィンガープリントを管理します。

- アクティブ化/非アクティブ化：フィンガープリントをアクティブ化または非アクティブ化します。詳細については、[フィンガープリントのアクティブおよび非アクティブの設定](#) (2043 ページ) を参照してください。



- 作成：フィンガープリントを作成します。詳細については、[クライアント用のカスタムフィンガープリントの作成（2046ページ）](#) および [サーバ用のカスタムフィンガープリントの作成（2049ページ）](#) を参照してください。
- 編集：フィンガープリントを編集します。詳細については、[アクティブなフィンガープリントの編集（2044ページ）](#) および [非アクティブなフィンガープリントの編集（2045ページ）](#) を参照してください。
- 削除：削除するフィンガープリントの横にある削除アイコン（）をクリックして、確認のために [OK] をクリックします。削除できるのは、非アクティブ化したフィンガープリントのみです。

## フィンガープリントのアクティブおよび非アクティブの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

ホストを識別するためにシステムがカスタムフィンガープリントを使用できるようにするには、その前に、カスタムフィンガープリントをアクティブにする必要があります。新しいフィンガープリントがアクティブにされた後は、以前に検出したホストを再識別し、新しいホストを検出するために使用されます。

フィンガープリントの使用を停止する場合は、それを非アクティブにすることができます。フィンガープリントを非アクティブにすると、フィンガープリントは使用できなくなりますが、システム上で維持できます。フィンガープリントを非アクティブにすると、オペレーティングシステムは、フィンガープリントを使用しているホストに対して不明としてマークされます。ホストが再度検出され、別のアクティブなフィンガープリントに一致すると、ホストはそのアクティブなフィンガープリントによって識別されます。

フィンガープリントを削除すると、システムから完全に削除されます。フィンガープリントを非アクティブにした後に削除できます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [カスタム OS (Custom Operating Systems)] をクリックします。

**ステップ 3** アクティブまたは非アクティブにするフィンガープリントの横にあるスライダをクリックします。

(注) アクティブ化オプションは、作成したフィンガープリントが有効である場合に限り使用できます。スライダが使用できない場合、フィンガープリントを再作成してください。

## アクティブなフィンガープリントの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

フィンガープリントがアクティブである場合、フィンガープリントの名前、説明、オペレーティングシステムのカスタム表示の変更、および追加の脆弱性のフィンガープリントへのマッピングを行えます。

フィンガープリントの名前、説明、オペレーティングシステムのカスタム表示の変更、および追加の脆弱性のフィンガープリントへのマッピングを行えます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [カスタム オペレーティング システム (Custom Operating Systems)] をクリックします。

**ステップ 3** 編集するフィンガープリントの横にある編集アイコン (✎) をクリックします。

**ステップ 4** 必要に応じて、フィンガープリントの名前、説明、およびカスタム OS 表示を変更します。

**ステップ 5** 脆弱性マッピングを削除する場合は、ページの [事前定義された OS 製品マップ (Pre-Defined OS Product Maps)] セクションのマッピングの横にある [削除 (Delete)] をクリックします。

**ステップ 6** 脆弱性マッピングにその他のオペレーティングシステムを追加する場合は、[製品 (Product)] を選択し (該当する場合は [メジャーバージョン (Major Version)]、[マイナーバージョン (Minor Version)]、[リビジョンバージョン (Revision Version)]、[ビルド (Build)]、[パッチ (Patch)]、および [拡張 (Extension)] も選択します)、[OS 定義の追加 (Add OS Definition)] をクリックします。

脆弱性マッピングが、[事前定義された OS 製品マップ (Pre-Defined OS Product Maps)] リストに追加されます。

**ステップ 7** [保存 (Save)] をクリックします。

## 非アクティブなフィンガープリントの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

フィンガープリントが非アクティブである場合は、フィンガープリントのすべての要素を変更し、それらを Firepower Management Center に再送信できます。これには、フィンガープリントのタイプ、ターゲットの IP アドレスとポート、脆弱性マッピングなど、フィンガープリントの作成時に指定したすべてのプロパティが含まれます。非アクティブのフィンガープリントを編集および送信すると、システムに再送信されます。また、それがクライアントのフィンガープリントである場合、アクティブにする前に、アプライアンスにトラフィックを再送信する必要があります。非アクティブのフィンガープリントに対して選択できる脆弱性マッピングは 1 つだけであることに注意してください。フィンガープリントをアクティブにした後、追加のオペレーティングシステムおよびバージョンを脆弱性リストにマッピングすることができます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [カスタム OS (Custom Operating Systems)] をクリックします。

**ステップ 3** 編集するフィンガープリントの横にある編集アイコン (✎) をクリックします。

**ステップ 4** 必要に応じてフィンガープリントを変更します。

- クライアントのフィンガープリントを変更している場合は、[クライアント用のカスタムフィンガープリントの作成 \(2046 ページ\)](#) を参照してください。
- サーバのフィンガープリントを変更している場合は、[サーバ用のカスタムフィンガープリントの作成 \(2049 ページ\)](#) を参照してください。

**ステップ 5** [保存 (Save)] をクリックします。

### 次のタスク

- クライアントのフィンガープリントを変更した場合は、ホストからフィンガープリントを収集しているアプライアンスにトラフィックを必ず送信してください。

## クライアント用のカスタムフィンガープリントの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

クライアントのフィンガープリントは、クライアントがネットワーク上の別のホストで実行する TCP アプリケーションに接続されている場合、ホストが送信する SYN パケットに基づいてオペレーティングシステムを識別します。

Firepower Management Center が監視対象ホストと直接通信することがない場合は、クライアントのフィンガープリントのプロパティを指定するときに、Management Center によって管理され、フィンガープリントを作成するホストに最も近いデバイスを指定することができます。

フィンガープリント作成プロセスを開始する前に、フィンガープリントを作成するホストに関する次の情報を取得します。

- ホストとフィンガープリントを取得するために使用する Firepower Management Center またはデバイスの間のネットワーク ホップの数。（Cisco では、ホストが接続されている同じサブネットに Firepower Management Center またはデバイスを直接接続することを強く推奨します）。
- ホストが存在するネットワークに接続されているネットワークインターフェイス（Firepower Management Center またはデバイス上）。
- ホストの実際のオペレーティングシステムベンダー、製品、バージョン。
- クライアントトラフィックを生成するためのホストへのアクセス。

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [カスタム OS (Custom Operating Systems)] をクリックします。

**ステップ 3** [カスタムフィンガープリントの作成 (Create Custom Fingerprint)] をクリックします。

**ステップ 4** [デバイス (Device)] ドロップダウンリストから、フィンガープリントを収集するために使用する Firepower Management Center またはデバイスを選択します。

**ステップ 5** [フィンガープリント名 (Fingerprint Name)] を入力します。

**ステップ 6** [フィンガープリントの説明 (Fingerprint Description)] を入力します。

**ステップ 7** [フィンガープリントタイプ (Fingerprint Type)] リストから、[クライアント (Client)] を選択します。

**ステップ 8** [ターゲット IP アドレス (Target IP Address)] フィールドで、フィンガープリントを作成するホストの IP アドレスを入力します。

フィンガープリントは、ホストに他の IP アドレスが存在していても、ユーザが指定したホスト IP アドレスから送受信されるトラフィックにのみ基づくことに注意してください。

**ステップ 9** [ターゲット距離 (Target Distance)] フィールドで、前の手順で選択したフィンガープリントを収集するデバイスとホストの間のネットワーク ホップ数を入力します。

**注意** これは、ホストへの実際の物理ネットワーク ホップ数である必要があります。システムによって検出されるホップ数と同じになる場合も、同じにならない場合もあります。

**ステップ 10** [インターフェイス (Interface)] リストから、ホストが存在するネットワーク セグメントに接続されているネットワーク インターフェイスを選択します。

**注意** Cisco では、いくつかの理由でフィンガープリントの作成に管理対象デバイスのセンシングインターフェイスを使用しないことを推奨します。まず、フィンガープリントは、センシング インターフェイスが SPAN ポート上にあると機能しません。また、デバイスでセンシングインターフェイスを使用する場合、デバイスはフィンガープリントを収集している間、ネットワークの監視を停止します。ただし、フィンガープリントの収集を実行するために、管理インターフェイスまたはその他の使用可能なネットワークインターフェイスを使用できます。どのインターフェイスがデバイスのセンシングインターフェイスであるかがわからない場合は、フィンガープリントの作成に使用している特定のモデルのインストレーション ガイドを参照してください。

**ステップ 11** フィンガープリントを作成したホストのホスト プロファイルのカスタム情報を表示する場合（またはフィンガープリントを作成するホストが [OS 脆弱性マッピング (OS Vulnerability Mappings)] セクションに存在しない場合）、[カスタム OS 表示の使用 (Use Custom OS Display)] を選択して、次に示すように表示する値を指定します。

- [ベンダー文字列 (Vendor String)] フィールドに、オペレーティング システムのベンダー名を入力します。たとえば、Microsoft Windows のベンダーは「Microsoft」になります。
- [製品文字列 (Product String)] フィールドに、オペレーティング システムの製品名を入力します。たとえば、Microsoft Windows 2000 の製品名は「Windows」になります。
- [バージョン文字列 (Version String)] フィールドに、オペレーティング システムのバージョン番号を入力します。たとえば、Microsoft Windows 2000 のバージョン番号は「2000」になります。

**ステップ 12** [OS 脆弱性マッピング (OS Vulnerability Mappings)] セクションで、脆弱性マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します。

フィンガープリントを使用して一致するホストの脆弱性を識別する場合、またはオペレーティング システムのカスタム表示情報を割り当てない場合、このセクションで [ベンダー (Vendor)] と [製品 (Product)] の値を指定する必要があります。

オペレーティング システムのすべてのバージョンの脆弱性をマッピングするには、[ベンダー (Vendor)] および [製品 (Product)] の値のみを指定します。

(注) [メジャーバージョン (Major Version)]、[マイナーバージョン (Minor Version)]、[リビジョンバージョン (Revision Version)]、[ビルド (Build)]、[パッチ (Patch)]、および [拡張 (Extension)] ドロップダウンリストのオプションの中には、選択したオペレーティングシステムに該当しないものもあります。また、フィンガープリントを作成するオペレーティングシステムに一致するリストに表示される定義がない場合は、それらの値を空のままにすることができます。フィンガープリントで OS の脆弱性マッピングを作成しない場合、システムはそのフィンガープリントを使用して、脆弱性リストをフィンガープリントによって識別されるホストに割り当てることはできないことに注意してください。

例：

たとえば、カスタムフィンガープリントで Redhat Linux 9 の脆弱性リストを一致するホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、メジャーバージョンとして [9] を選択します。

例：

Palm OS のすべてのバージョンを追加するには、[ベンダー (Vendor)] リストから [PalmSource, Inc.]、[製品 (Product)] リストから [Palm OS] を選択し、その他のすべてのリストはデフォルトの設定のままにします。

**ステップ 13** [作成 (Create)] をクリックします。

ステータスは一時的に [新規 (New)] になってから、[保留中 (Pending)] に切り替わります。フィンガープリントのトラフィックが確認されるまで、このステータスが維持されます。トラフィックが確認されると、[使用可 (Ready)] に切り替わります。

当該のホストからデータを受信するまで、[カスタムフィンガープリント (Custom Fingerprint)] ステータス ページは 10 秒ごとに更新されます。

**ステップ 14** ターゲット IP アドレスとして指定した IP アドレスを使用して、フィンガープリントを作成しようとしているホストにアクセスし、アプライアンスへの TCP 接続を開始します。

正確なフィンガープリントを作成するためには、トラフィックがフィンガープリントを収集するアプライアンスで認識される必要があります。スイッチを経由して接続している場合は、アプライアンス以外のシステムへのトラフィックはシステムによって認識されない場合があります。

例：

フィンガープリントを作成しようとしているホストから Firepower Management Center の Web インターフェイスにアクセスするか、ホストから SSH で Management Center にアクセスします。SSH を使用する場合は、次に示すコマンドを使用します。このコマンドの localIPv6address は、現在ホストに割り当てられているステップ 7 で指定した IPv6 アドレスです。

DCmanagementIPv6address は、Management Center の管理 IPv6 アドレスです。[カスタムフィンガープリント (Custom Fingerprint)] ページが [使用可 (Ready)] ステータスでリロードされるようになります。

```
ssh -b localIPv6address DCmanagementIPv6address
```

### 次のタスク

- [フィンガープリントのアクティブおよび非アクティブの設定 \(2043 ページ\)](#) で説明するように、フィンガープリントをアクティブにします。

## サーバ用のカスタム フィンガープリントの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

サーバのフィンガープリントは、実行中の TCP アプリケーションへの着信接続に応答するためにホストが使用する SYN-ACK パケットに基づいてオペレーティング システムを識別します。開始する前に、フィンガープリントを作成するホストに関する次の情報を取得します。

- ホストとフィンガープリントを取得するために使用するアプライアンスの間のネットワーク ホップの数。Cisco では、ホストが接続されている同じサブネットにアプライアンスの使用されていないインターフェイスを直接接続することを強く推奨します。
- ホストが存在するネットワークに接続されているネットワーク インターフェイス (アプライアンス上)。
- ホストの実際のオペレーティング システム ベンダー、製品、バージョン。
- 現在未使用の、ホストが存在するネットワーク上で許可されている IP アドレス。



**ヒント** Firepower Management Center が監視対象ホストと直接通信することがない場合は、サーバのフィンガープリントのプロパティを指定するときに、フィンガープリントを作成するホストに最も近い管理対象デバイスを指定することができます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [カスタム OS (Custom Operating Systems)] をクリックします。

**ステップ 3** [カスタム フィンガープリントの作成 (Create Custom Fingerprint)] をクリックします。

- ステップ 4** [デバイス (Device) ] リストから、フィンガープリントを収集するために使用する Firepower Management Center または管理対象デバイスを選択します。
- ステップ 5** [フィンガープリント名 (Fingerprint Name) ] を入力します。
- ステップ 6** [フィンガープリントの説明 (Fingerprint Description) ] を入力します。
- ステップ 7** [フィンガープリントタイプ (Fingerprint Type) ] リストから、サーバのフィンガープリント作成オプションを表示する [サーバ (Server) ] を選択します。
- ステップ 8** [ターゲット IP アドレス (Target IP Address) ] フィールドで、フィンガープリントを作成するホストの IP アドレスを入力します。

フィンガープリントは、ホストに他の IP アドレスが存在していても、ユーザが指定したホスト IP アドレスから送受信されるトラフィックにのみ基づくことに注意してください。

**注意** Firepower システムのバージョン 5.2 以降を実行するアプライアンスでのみ IPv6 フィンガープリントをキャプチャできます。

- ステップ 9** [ターゲット距離 (Target Distance) ] フィールドで、前の手順で選択したフィンガープリントを収集するデバイスとホストの間のネットワーク ホップ数を入力します。

**注意** これは、ホストへの実際の物理ネットワーク ホップ数である必要があります。システムによって検出されるホップ数と同じになる場合も、同じにならない場合もあります。

- ステップ 10** [インターフェイス (Interface) ] リストから、ホストが存在するネットワーク セグメントに接続されているネットワーク インターフェイスを選択します。

**注意** Cisco では、いくつかの理由でフィンガープリントの作成に管理対象デバイスのセンシングインターフェイスを使用しないことを推奨します。まず、フィンガープリントは、センシング インターフェイスが SPAN ポート上にあると機能しません。また、デバイスでセンシングインターフェイスを使用する場合、デバイスはフィンガープリントを収集している間、ネットワークの監視を停止します。ただし、フィンガープリントの収集を実行するために、管理インターフェイスまたはその他の使用可能なネットワークインターフェイスを使用できます。どのインターフェイスがデバイスのセンシングインターフェイスであるかがわからない場合は、フィンガープリントの作成に使用している特定のモデルのインストレーションガイドを参照してください。

- ステップ 11** [アクティブ ポートの取得 (Get Active Ports) ] をクリックします。

- ステップ 12** [サーバポート (Server Port) ] フィールドに、フィンガープリントを収集するように選択したデバイスが通信を開始するポートを入力します。または、[アクティブポートの取得 (Get Active Ports) ] ドロップダウンリストからポートを選択します。

ホストでオープンしていると判明しているすべてのサーバポートを使用できます (たとえば、ホストで Web サーバを実行している場合は 80) 。

- ステップ 13** [送信元 IP アドレス (Source IP Address) ] フィールドで、ホストとの通信を試行するために使用する IP アドレスを入力します。



ネットワークでの使用が許可されていて、現在未使用の送信元 IP アドレス（たとえば、現在使用されていない DHCP プール アドレス）を使用する必要があります。これにより、フィンガープリントの作成中に、別のホストを一時的にオフラインにすることを防ぎます。

フィンガープリントを作成している間は、その IP アドレスをネットワーク検出ポリシーでモニタリングから除外する必要があります。そうしていないと、ネットワークマップおよびディスカバリ イベント ビューに、その IP アドレスによって表されるホストに関する不正確な情報が混在することになります。

- ステップ 14** [送信元サブネット マスク (Source Subnet Mask)] フィールドには、ユーザが使用している IP アドレスのサブネット マスクを入力します。
- ステップ 15** [送信元ゲートウェイ (Source Gateway)] フィールドが表示されたら、ホストへのルートを確立するために使用するデフォルトのゲートウェイ IP アドレスを入力します。
- ステップ 16** フィンガープリントを作成したホストのホストプロファイルのカスタム情報を表示する場合、または使用するフィンガープリントの名前が [OS 定義 (OS Definition)] セクションに存在しない場合、[カスタム OS 表示 (Custom OS Display)] セクションの [カスタム OS 表示の使用 (Use Custom OS Display)] を選択します。

以下のように、ホストプロファイルで表示する値を入力します。

- [ベンダー文字列 (Vendor String)] フィールドに、オペレーティング システムのベンダー名を入力します。たとえば、Microsoft Windows のベンダーは「Microsoft」になります。
- [製品文字列 (Product String)] フィールドに、オペレーティング システムの製品名を入力します。たとえば、Microsoft Windows 2000 の製品名は「Windows」になります。
- [バージョン文字列 (Version String)] フィールドに、オペレーティング システムのバージョン番号を入力します。たとえば、Microsoft Windows 2000 のバージョン番号は「2000」になります。

- ステップ 17** [OS 脆弱性マッピング (OS Vulnerability Mappings)] セクションで、脆弱性マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します。

フィンガープリントを使用して一致するホストの脆弱性を識別する場合、またはオペレーティング システムのカスタム表示情報を割り当てない場合、このセクションでベンダーと製品名を指定する必要があります。

オペレーティング システムのすべてのバージョンの脆弱性をマッピングするには、ベンダーおよび製品名のみを指定します。

- (注) [メジャーバージョン (Major Version)]、[マイナーバージョン (Minor Version)]、[リビジョンバージョン (Revision Version)]、[ビルド (Build)]、[パッチ (Patch)]、および[拡張 (Extension)] ドロップダウンリストのオプションの中には、選択したオペレーティング システムに該当しないものもあります。また、フィンガープリントを作成するオペレーティング システムに一致するリストに表示される定義がない場合は、それらの値を空のままにすることができます。フィンガープリントで OS の脆弱性マッピングを作成しない場合、システムはそのフィンガープリントを使用して、脆弱性リストをフィンガープリントによって識別されるホストに割り当てることはできないことに注意してください。

例：

カスタムフィンガープリントで Redhat Linux 9 の脆弱性リストを一致するホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

例：

Palm OS のすべてのバージョンを追加するには、[ベンダー (Vendor)] リストから [PalmSource, Inc.]、[製品 (Product)] リストから [Palm OS] を選択し、その他のすべてのリストはデフォルトの設定のままにします。

**ステップ 18** [作成 (Create)] をクリックします。  
[カスタムフィンガープリント (Custom Fingerprint)] ステータス ページは 10 秒ごとに更新され、[使用可 (Ready)] ステータスでリロードされます。

(注) ターゲットシステムがフィンガープリント作成プロセス中に応答を停止した場合、ステータスにはメッセージ「エラー：応答がありません (ERROR: No Response)」が表示されます。このメッセージが表示された場合は、フィンガープリントを再度送信します。3～5 分間（時間はターゲットシステムによって異なる場合があります）待機して、編集アイコン (✎) をクリックし、[カスタムフィンガープリント (Custom Fingerprint)] ページにアクセスしてから [作成 (Create)] をクリックします。

---

### 次のタスク

- [フィンガープリントのアクティブおよび非アクティブの設定 \(2043 ページ\)](#) で説明するように、フィンガープリントをアクティブにします。

## ホスト入力データ

サードパーティからネットワーク マップ データをインポートすることで、ネットワーク マップを強化することができます。また、Web インターフェイスを使用して、オペレーティング システムまたはアプリケーションの ID を変更するか、アプリケーション プロトコル、プロトコル、ホスト属性、クライアントを削除することによって、ホスト入力機能を使用することができます。

システムは複数のソースからのデータを照合して、オペレーティング システムまたはアプリケーションの現行 ID を判別できます。

ネットワーク マップから影響を受けるホストを削除すると、サードパーティの脆弱性を除くすべてのデータは破棄されます。スクリプトまたはインポート ファイルの設定方法の詳細については、『*Firepower System Host Input API Guide*』を参照してください。

影響の関連付けにインポートしたデータを含めるには、データベースのオペレーティング システムおよびアプリケーション定義にデータをマッピングする必要があります。

## サードパーティのデータを使用するための要件

ネットワーク上のサードパーティのシステムから検出データをインポートできます。ただし、Firepower の推奨、アダプティブ プロファイルの更新、影響評価などの侵入データおよび検出データを共に使用する機能を有効にするには、対応する定義に対して、可能な限り多くのエレメントをマッピングする必要があります。サードパーティのデータを使用するには、以下の要件を考慮してください：

- サードパーティのシステムにネットワークアセット上に特定のデータがある場合、ホスト入力機能によりそのデータをインポートできます。しかし、サードパーティが異なる製品名をつける可能性があることから、対応する Cisco 製品の定義に対して、サードパーティベンダー、製品、バージョンをマッピングする必要があります。製品をマッピング後、Firepower Management Center 設定の影響を評価するために脆弱性のマッピングを有効にして、影響相関を可能にします。バージョンまたはベンダーに関係のないアプリケーションプロトコルでは、Firepower Management Center 設定におけるアプリケーションプロトコルの脆弱性をマッピングする必要があります。
- サードパーティからパッチ情報をインポートし、そのパッチで修正されたすべての脆弱性に無効とマークする場合は、サードパーティの修正名をデータベースの修正定義にマッピングする必要があります。修正によって解決された脆弱性はすべて、その修正を加えるホストから排除されます。
- オペレーティングシステムやアプリケーションプロトコルの脆弱性をサードパーティからインポートし、これらに影響相関に使用する場合、サードパーティの脆弱性識別文字列をデータベース内の脆弱性にマッピングする必要があります。多くのクライアントは、脆弱性と関連があり、影響評価に使用されますが、サードパーティのクライアントの脆弱性をインポートし、マッピングすることはできない点にご注意ください。脆弱性のマッピング後、Firepower Management Center 設定の影響評価のためにサードパーティの脆弱性のマッピングを有効にします。ベンダー情報やバージョン情報のないアプリケーションプロトコルを脆弱性にマッピングするには、管理ユーザは、Firepower Management Center 設定のアプリケーションの脆弱性もマッピングする必要があります。
- アプリケーションデータをインポートし、そのデータを影響相関に使用する場合、各アプリケーションプロトコルのベンダー文字列を対応する Cisco アプリケーションプロトコルの定義にマッピングする必要があります。

### 関連トピック

[サードパーティの製品のマッピング \(2054 ページ\)](#)

[サードパーティ製品の修正のマッピング \(2056 ページ\)](#)

[サードパーティの脆弱性のマッピング \(2057 ページ\)](#)

[サーバの脆弱性のマッピング \(988 ページ\)](#)

[カスタム製品マッピングの作成 \(2059 ページ\)](#)

## サードパーティ製品のマッピング

ユーザ入力機能を使用して各サードパーティからのデータをネットワークマップに追加する場合、サードパーティで使用するベンダー、製品、およびバージョンの各名前を Cisco 製品定義にマッピングする必要があります。各製品を Cisco の定義にマッピングすると、これらの定義に基づいて脆弱性が割り当てられます。

同様に、パッチ管理製品などのサードパーティからのパッチ情報をインポートする場合、その修正の名前をデータベース内の適切なベンダー、製品、および対応する修正にマッピングする必要があります。

### サードパーティの製品のマッピング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

サードパーティからデータをインポートする場合、そのデータを使用して脆弱性を指定したり、影響の関連付けを行ったりするために、シスコの製品をサードパーティの名前にマッピングする必要があります。製品をマッピングすることにより、シスコの脆弱性情報をサードパーティ製品の名前に関連付けます。これにより、システムはそのデータを使用して影響の関連付けを行うことができます。

ホスト入力のインポート機能を使用してデータをインポートする場合、AddScanResult 機能を使用して、インポート中にサードパーティ製品をオペレーティングシステムとアプリケーションの脆弱性にマッピングすることもできます。

たとえば、Apache Tomcat をアプリケーションとしてリストしているサードパーティのデータをインポートする場合で、それがバージョン 6 の Apache Tomcat であれば、以下のように設定し、サードパーティのマッピングを追加します。

- ベンダー名を [Apache] に設定します。
- プロダクト名に [Tomcat] 設定します。
- ベンダーのドロップダウンリストから [Apache] を選択します。
- 製品のドロップダウンリストから [Tomcat] を選択します。
- バージョンのドロップダウンリストから [6] を選択します。

このマッピングによって、Apache Tomcat 6 のすべての脆弱性が、Apache Tomcat をアプリケーションとしてリストアップするホストに割り当てられます。

バージョン情報やベンダー情報のないアプリケーションの場合、Firepower Management Center 構成のアプリケーションタイプで脆弱性をマッピングする必要があります。多くのクライアントには関連付けられた脆弱性があり、クライアントが影響アセスメントに使用されますが、サードパーティのクライアントの脆弱性をインポートしてマッピングすることはできないことに注意してください。



**ヒント** すでに別のFirepower Management Center にサードパーティのマッピングを作成している場合、そのマッピングをエクスポートして、このManagement Center にインポートすることができます。その後、必要に応じてインポートしたマッピングを編集できます。

## 手順

- ステップ 1** [ポリシー (Policies) ] > [アプリケーション デテクタ (Application Detectors) ] を選択します。
- ステップ 2** [ユーザ サードパーティ マッピング (User Third-Party Mappings) ] をクリックします。
- ステップ 3** 次の 2 つの選択肢があります。
- [作成 (Creat) ] : 新しいマップセットを作成するには、[製品マップセットの作成 (Create Product Map Set) ] をクリックします。
  - [編集 (Edit) ] : 既存のマップセットを編集するには、そのマップセットの横にある編集アイコン (✎) をクリックします。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 4** [マッピングセット名 (Mapping Set Name) ] を入力します。
- ステップ 5** [説明 (Description) ] を入力します。
- ステップ 6** 次の 2 つの選択肢があります。
- [作成 (Creat) ] : サードパーティ製品をマッピングするには、[製品マップの追加 (Add Product Map) ] をクリックします。
  - [編集 (Edit) ] : 既存のサードパーティの製品のマッピングを編集するには、そのマッピングの横にある編集アイコン (✎) をクリックします。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 7** サードパーティの製品で使用される [ベンダーの文字列 (Vendor String) ] を入力します。
- ステップ 8** サードパーティの製品で使用される [製品の文字列 (Product String) ] を入力します。
- ステップ 9** サードパーティの製品で使用される [バージョン文字列 (Version String) ] を入力します。
- ステップ 10** 製品マッピング セクションで、ベンダーの脆弱性のマッピングに使用するオペレーティングシステム、製品、製品バージョンを、以下の項目から選択します。[ベンダー (Vendor) ]、[製品 (Product) ]、[メジャーバージョン (Major Version) ]、[マイナーバージョン (Minor Version) ]、[改訂バージョン (Revision Version) ]、[ビルド (Build) ]、[パッチ (Patch) ]、[拡張子 (Extension) ]。
- 例 :**
- 名前がサードパーティの文字列で構成される製品を実行するホストで Red Hat Linux 9 の脆弱性マッピングを使用する場合、ベンダーとして [Redhat, Inc.]、製品として [Red Hat Linux]、バージョンとして [9] を選択します。

ステップ 11 [保存 (Save) ] をクリックします。

#### 関連トピック

[サーバの脆弱性のマッピング](#) (988 ページ)

## サードパーティ製品の修正のマッピング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

修正名をデータベースの特定の修正セットにマッピングする場合、サードパーティのパッチ管理アプリケーションからデータをインポートし、修正を一連のホストに適用することができます。修正名がホストにインポートされると、システムはその修正によって解決されるすべての脆弱性をそのホストに対して無効としてマークします。

#### 手順

ステップ 1 [ポリシー (Policies) ] > [アプリケーションディテクタ (Application Detectors) ] を選択します。

ステップ 2 [ユーザ サードパーティ マッピング (User Third-Party Mappings) ] をクリックします。

ステップ 3 次の 2 つの選択肢があります。

- [作成 (Creat) ] : 新しいマップセットを作成するには、[製品マップセットの作成 (Create Product Map Set) ] をクリックします。
- [編集 (Edit) ] : 既存のマップセットを編集するには、そのマップセットの横にある編集アイコン (✎) をクリックします。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [マッピングセット名 (Mapping Set Name) ] を入力します。

ステップ 5 [説明 (Description) ] を入力します。

ステップ 6 次の 2 つの選択肢があります。

- 作成 : サードパーティ製品をマッピングするには、[修正マップの追加 (Add Fix Map) ] をクリックします。
- 編集 : 既存のサードパーティ製品マップを編集するには、その横にある編集アイコン (✎) をクリックします。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 7 [サードパーティの修正名 (Third-Party Fix Name) ] フィールドにマッピングする修正の名前を入力します。

ステップ 8 [製品マッピング (Product Mappings) ] セクションで、次のフィールドから修正マッピングに使用するオペレーティングシステム、製品、およびバージョンを選択します。

- ベンダー
- 製品
- メジャーバージョン (Major Version)
- マイナーバージョン (Minor Version)
- リビジョンバージョン (Revision Version)
- ビルド (Build)
- パッチ (Patch)
- 内線番号

例：

Red Hat Linux 9 からパッチが適用されるホストにマッピングで修正を割り当てる場合は、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

**ステップ 9** [保存 (Save) ] をクリックして、修正マップを保存します。

## サードパーティの脆弱性のマッピング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

サードパーティからの脆弱性情報を VDB に追加するには、インポートしたそれぞれの脆弱性のサードパーティ識別文字列を、既存の SVID、Bugtraq、または SID にマッピングする必要があります。脆弱性のマッピングを作成したら、マッピングはネットワークマップのホストにインポートされたすべての脆弱性に対して機能し、それらの脆弱性に対する影響の関連付けを可能にします。

サードパーティの脆弱性に対する影響の関連付けを有効にし、関連付けの実行を可能にする必要があります。バージョンレスまたはベンダーレスのアプリケーションの場合、Firepower Management Center の設定でアプリケーションタイプの脆弱性をマッピングする必要もあります。

多くのクライアントには関連付けられた脆弱性があり、クライアントが影響評価に使用されますが、サードパーティのクライアントの脆弱性は影響評価に使用できません。



### ヒント

すでに別の Firepower Management Center にサードパーティのマッピングを作成している場合、そのマッピングをエクスポートして、この Management Center にインポートすることができます。その後、必要に応じてインポートしたマッピングを編集できます。

## 手順

**ステップ 1** [ポリシー (Policies)] > [アプリケーション デテクタ (Application Detectors)] を選択します。

**ステップ 2** [ユーザ サードパーティ マッピング (User Third-Party Mappings)] をクリックします。

**ステップ 3** 次の 2 つの選択肢があります。

- **作成** : 新しい脆弱性セットを作成するには、[脆弱性マップセットの作成 (Create Vulnerability Map Set)] をクリックします。
- **編集** : 既存の脆弱性セットを編集するには、脆弱性セットの横にある編集アイコン (✎) をクリックします。代わりに表示アイコン (👁) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 4** [脆弱性マップの追加 (Add Vulnerability Map)] をクリックします。

**ステップ 5** [脆弱性 ID (Vulnerability ID)] フィールドに脆弱性のサードパーティ ID を入力します。

**ステップ 6** [脆弱性の説明 (Vulnerability Description)] を入力します。

**ステップ 7** 必要に応じて、次の操作を実行します。

- [Snort 脆弱性 ID マッピング (Snort Vulnerability ID Mappings)] フィールドに Snort ID を入力します。
- [SVID マッピング (SVID Mappings)] フィールドに、レガシー脆弱性 ID を入力します。
- [Bugtraq 脆弱性 ID マッピング (Bugtraq Vulnerability ID Mappings)] フィールドに、Bugtraq ID 番号を入力します。

**ステップ 8** [追加 (Add)] をクリックします。

## 関連トピック

[ネットワーク検出の脆弱性影響評価の有効化 \(2167 ページ\)](#)

[サーバの脆弱性のマッピング \(988 ページ\)](#)

# カスタム製品マッピング

製品マッピングを使用して、サードパーティによるサーバ入力が適切なシスコ定義に関連付けられていることを確認できます。製品マッピングを定義し有効化した後、マッピングされたベンダー文字列を持つモニタ対象ホスト上のすべてのサーバまたはクライアントが、カスタム製品マッピングを使用します。したがって、サーバのベンダー、製品、バージョンを明示的に設定する代わりに、特定のベンダー文字列でネットワーク マップのすべてのサーバの脆弱性をマップすることをお勧めします。



## カスタム製品マッピングの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

システムが VDB のベンダーおよび製品にサーバをマッピングできない場合は、手動でマッピングを作成できます。カスタム製品マッピングをアクティブにすると、システムは指定されたベンダーおよび製品の脆弱性を、そのベンダー文字列が発生するネットワークマップのすべてのサーバにマッピングします。



- (注) カスタム製品マッピングは、アプリケーションデータのソース (Nmap、ホスト入力機能、Firepower システム自体など) に関係なく、アプリケーションプロトコルのすべての発生に適用されます。ただし、ホスト入力機能を使用してインポートしたデータのサードパーティの脆弱性マッピングが、カスタム製品マッピングを介して設定したマッピングと競合する場合、サードパーティの脆弱性マッピングはカスタム製品マッピングをオーバーライドし、入力が発生したときにサードパーティの脆弱性マッピング設定を使用します。

製品マッピングリストを作成し、各リストをアクティブ化/非アクティブ化することによって、複数のマッピングの同時使用を有効にするか、無効にします。マッピングするベンダーを指定すると、そのベンダーによって作成された製品のみを含むように製品リストが更新されます。

カスタム製品マッピングを作成した後で、カスタム製品マッピングリストをアクティブにする必要があります。カスタム製品マッピングリストをアクティブにすると、指定されたベンダー文字列が発生するすべてのサーバが更新されます。ホスト入力機能を介してインポートされるデータでは、このサーバの製品マッピングをすでに明示的に設定していない限り、脆弱性が更新されます。

たとえば、組織が Apache Tomcat Web サーバのバナーの文字列を Internal Web Server に変更した場合、ベンダー文字列 Internal Web Server をベンダー **Apache** および製品 **Tomcat** にマッピングできます。その後、そのマッピングを含むリストをアクティブにすると、Internal Web Server とラベル付けされたサーバが存在するすべてのホストのデータベースに Apache Tomcat の脆弱性が想定されます。



- ヒント この機能を使用して、もう1つの脆弱性にルール SID をマッピングすることによって、ローカルの侵入ルールに脆弱性をマッピングすることができます。

### 手順

- ステップ 1 [ポリシー (Policies)] > [アプリケーションディテクタ (Application Detectors)] を選択します。

- ステップ 2** [カスタム製品マッピング (Custom Product Mappings) ] をクリックします。
- ステップ 3** [カスタム製品マッピングリストの作成 (Create Custom Product Mapping List) ] をクリックします。
- ステップ 4** [カスタム製品マッピングリスト名 (Custom Product Mapping List Name) ] を入力します。
- ステップ 5** [ベンダー文字列の追加 (Add Vendor String) ] をクリックします。
- ステップ 6** [ベンダー文字列 (Vendor String) ] フィールドに、選択したベンダーおよび製品値にマッピングする必要があるアプリケーションを識別するベンダー文字列を入力します。
- ステップ 7** [ベンダー (Vendor) ] ドロップダウンリストから、マッピングするベンダーを選択します。
- ステップ 8** [製品 (Product) ] ドロップダウンリストから、マッピングする製品を選択します。
- ステップ 9** [追加 (Add) ] をクリックして、マッピングしたベンダー文字列をリストに追加します。
- ステップ 10** オプションで、さらにベンダー文字列のマッピングをリストに追加するには、必要に応じて手順 4 ~ 8 を繰り返します。
- ステップ 11** [保存 (Save) ] をクリックします。

#### 次のタスク

- カスタム製品マッピングリストをアクティブにします。詳細については、[カスタム製品マッピングのアクティブおよび非アクティブの設定 \(2061 ページ\)](#) を参照してください。

## カスタム製品マッピングリストの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ベンダー文字列を追加または削除したり、リスト名を変更したりして、既存のカスタム製品マッピングリストを変更できます。

#### 手順

- ステップ 1** [ポリシー (Policies) ] > [アプリケーションディテクタ (Application Detectors) ] を選択します。
- ステップ 2** [カスタム製品マッピング (Custom Product Mappings) ] をクリックします。
- ステップ 3** 編集する製品マッピングリストの横にある編集アイコン (✎) をクリックします。
- 代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 4** [カスタム製品マッピングの作成 \(2059 ページ\)](#) の説明に従って、リストを変更します。

ステップ5 終了したら、[保存 (Save)] をクリックします。

## カスタム製品マッピングのアクティブおよび非アクティブの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

カスタム製品マッピングリスト全体の使用を一度に有効または無効にすることができます。カスタム製品マッピングリストをアクティブにすると、そのリストの各マッピングが、管理対象デバイスによって検出されたか、またはホスト入力機能を介してインポートされたかに関わらず、指定したベンダー文字列を持つすべてのアプリケーションに適用されます。

### 手順

- ステップ1 [ポリシー (Policies)] > [アプリケーション デテクタ (Application Detectors)] を選択します。
- ステップ2 [カスタム製品のマッピング (Custom Product Mappings)] をクリックします。
- ステップ3 アクティブまたは非アクティブにするカスタム製品のマッピングリストの横にあるスライダをクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

## eStreamer サーバストリーミング

Event Streamer (eStreamer) を使用すると、Firepower Management Center または 7000 または 8000 シリーズ デバイスからの数種類のイベント データを、カスタム開発されたクライアント アプリケーションにストリーム配信できます。詳細については、*Firepower eStreamer Integration Guide* を参照してください。

eStreamer サーバとして使用するアプライアンスで eStreamer イベントの外部クライアントへのストリームを開始するには、その前に、イベントをクライアントに送信するように eStreamer サーバを設定し、クライアントに関する情報を指定して、通信を確立するときに使用する認証クレデンシャルを生成する必要があります。アプライアンスのユーザインターフェイスからこれらすべてのタスクを実行できます。設定が保存されると、選択したイベントが、要求時に、eStreamer クライアントに転送されます。

要求したクライアントに eStreamer サーバが送信できるイベント タイプを制御できます。

表 216: eStreamer サーバで送信可能なイベントタイプ

イベントタイプ (Event Type)	説明	Management Center で使用可能	7000 & 8000 シリーズ デバイスで 使用可能
侵入イベント	管理対象デバイスによって生成される侵入イベント	Yes	Yes
侵入イベント パケットデータ	侵入イベントに関連付けられたパケット	Yes	Yes
侵入イベント追加データ	HTTP プロキシまたはロードバランサ経由で Web サーバに接続しているクライアントの発信元 IP アドレスのような侵入イベントに関連付けられた追加データ	Yes	Yes
検出イベント	検出イベント	Yes	No
相関およびホワイトリストイベント	相関およびホワイトリストイベント	Yes	No
インパクトフラグアラート	Management Center によって生成されたインパクトアラート	Yes	No
ユーザ イベント	ユーザ イベント	Yes	No
マルウェア イベント	マルウェア イベント	Yes	No
ファイル イベント	ファイル イベント	Yes	No
接続イベント	モニタ対象のホストとその他のすべてのホスト間のセッショントラフィックに関する情報	Yes	Yes

## eStreamer イベントタイプの選択

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	Management Center 7000 & 8000 シリーズ	任意 (Any)	Admin

eStreamer サーバで送信可能なイベントの [eStreamer イベント設定 (eStreamer Event Configuration)] チェックボックス管理。クライアントは、eStreamer サーバに送信する要求メッセージで受信するイベントタイプを具体的に要求する必要があります。詳細については、*Firepower eStreamer Integration Guide*を参照してください。

マルチドメイン展開では、どのドメインのレベルでも eStreamer のイベント構成を設定できます。ただし、先祖ドメインで特定のイベントタイプが有効になっている場合は、子孫ドメインのそのイベントタイプを無効にすることはできません。

#### 手順

- ステップ 1 [システム (System)] > [統合 (Integration)] を選択します。
- ステップ 2 [eStreamer] タブをクリックします。
- ステップ 3 [eStreamer イベント設定 (eStreamer Event Configuration)] の下で、[eStreamer サーバストリーミング \(2061 ページ\)](#) の説明に従って要求元のクライアントに転送するイベントタイプの横にあるチェックボックスをオンまたはオフにします。
- ステップ 4 [保存 (Save)] をクリックします。

## eStreamer クライアント通信の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	Management Center 7000 & 8000 シリーズ	任意 (Any)	Admin/Discovery Admin

eStreamer がクライアントに eStreamer イベントを送信するには、その前に、eStreamer ページから eStreamer サーバのピア データベースにクライアントを追加しておく必要があります。また、eStreamer サーバによって生成された認証証明書をクライアントにコピーする必要があります。この手順を完了した後、クライアントが eStreamer サーバに接続できるように eStreamer サービスを再起動する必要はありません。

マルチドメイン展開では、任意のドメインで eStreamer クライアントを作成できます。認証証明書では、クライアントはクライアント証明書のドメインと子孫ドメインからのみイベントを要求することが許可されます。eStreamer 設定ページには、現在のドメインに関連付けられているクライアントのみが表示されるため、証明書をダウンロードまたは取り消す場合は、クライアントが作成されたドメインに切り替えます。

#### 手順

- ステップ 1 [システム (System)] > [統合 (Integration)] を選択します。

- ステップ 2** [eStreamer] タブをクリックします。
- ステップ 3** [クライアントの作成 (Create Client)] をクリックします。
- ステップ 4** [ホスト名 (Hostname)] フィールドに、eStreamer クライアントを実行しているホストのホスト名または IP アドレスを入力します。
- (注) DNS 解決を設定していない場合は、IP アドレスを使用します。
- ステップ 5** 証明書ファイルを暗号化するには、[パスワード (Password)] フィールドにパスワードを入力します。
- ステップ 6** [保存 (Save)] をクリックします。  
これで、eStreamer サーバは、ホストが eStreamer サーバ上のポート 8302 にアクセスすることを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。
- ステップ 7** クライアントのホスト名の横にあるファイルのダウンロードアイコン (📄) をクリックして、証明書ファイルをダウンロードします。
- ステップ 8** SSL 認証のためにクライアントが使用する適切なディレクトリに証明書ファイルを保存します。
- ステップ 9** クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン (🗑️) をクリックします。
- eStreamer サービスを再起動する必要はありません。アクセスはただちに取り消されます。

## ホスト入力クライアントの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	Management Center	任意 (Any)	Admin/Discovery Admin

ホスト入力機能を使用すると、別のアプライアンスで実行されているクライアントプログラムから Firepower Management Center のネットワーク マップを更新できます。たとえば、ネットワーク マップからホストを追加または削除したり、ホスト OS およびサービス情報を更新したりできます。詳細については、*Firepower System Host Input API Guide* を参照してください。



リモートクライアントを実行するには、その前に、[ホスト入力クライアント (Host Input Client)] ページから Firepower Management Center のピアデータベースにクライアントを追加する必要があります。また、Management Center によって生成された認証証明書をクライアントにコピーする必要があります。この手順を完了すると、クライアントは Management Center に接続できます。

マルチドメイン展開では、すべてのドメインにクライアントを作成できます。認証証明書を使用すると、クライアントは、クライアント証明書のドメインに関連付けられているリーフドメインにネットワーク マップ アップデートを送信できます。先祖ドメインの証明書を作成した

場合（または後で証明書ドメインが子孫ドメインの追加後に先祖ドメインになった場合）、その証明書を使用するクライアントは、*Firepower System Host Input API Guide*で説明するように、すべてのトランザクションのターゲット リーフ ドメインを指定する必要があります。

[ホスト入力クライアント (Host Input Client) ] タブには、現在のドメインに関連付けられているクライアントのみが表示されるため、証明書をダウンロードまたは失効させるには、クライアントが作成されたドメインに切り替えます。

## 手順

- 
- ステップ 1 [システム (System) ] > [統合 (Integration) ] を選択します。
  - ステップ 2 [ホスト入力クライアント (Host Input Client) ] タブをクリックします。
  - ステップ 3 [クライアントの作成 (Create Client) ] をクリックします。
  - ステップ 4 [ホスト名 (Hostname) ] フィールドに、ホスト入力クライアントを実行しているホストのホスト名または IP アドレスを入力します。  
  
(注) DNS 解決を設定していない場合は、IP アドレスを使用します。
  - ステップ 5 証明書ファイルを暗号化するには、[パスワード (Password) ] フィールドにパスワードを入力します。
  - ステップ 6 [保存 (Save) ] をクリックします。  
ホスト入力サービスは、ホストが Firepower Management Center 上のポート 8307 にアクセスすることを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。
  - ステップ 7 証明書ファイルの横にあるファイル ダウンロード アイコン (  ) をクリックします。
  - ステップ 8 SSL 認証のためにクライアントが使用するディレクトリに証明書ファイルを保存します。
  - ステップ 9 クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン (  ) をクリックします。
- 

## Nmap スキャン

Firepower システムは、ネットワークのトラフィックをパッシブ分析してネットワーク マップを構築します。このパッシブ分析によって取得される情報は、システムの状態によっては不完全なことがよくあります。ただし、ホストをアクティブにスキャンすることで、完全な情報を取得できます。たとえば、オープンポート上で実行中のサーバがホストにあり、システムによるネットワークのモニタリング中にそのサーバがトラフィックを送受信しなかった場合、システムではそのサーバに関する情報をネットワークマップに追加しません。しかし、アクティブ スキャナを使用して直接そのホストをスキャンすると、サーバの存在を検出できます。

Firepower システムには、Nmap™ という、ネットワーク調査およびセキュリティ監査を目的としたオープン ソースのアクティブ スキャナが統合されています。

Nmap を使用してホストをスキャンすると、システムは以下のように動作します。

- 前に検出されていないオープンポート上のサーバを、該当するホストのホストプロファイルの [サーバ (Servers) ] リストに追加します。ホストプロファイルの [スキャン結果 (Scan Results) ] セクションには、フィルタ処理されていたり閉じていたりしている TCP ポートやUDPポート上で検出されたサーバがリストされます。デフォルトでは、Nmap は 1660 を超える TCP ポートをスキャンします。

Nmap スキャンで識別されたサーバがシステムで認識され、対応するサーバ定義がシステムにある場合、システムは Nmap がそのサーバに使用する名前を、対応する Cisco サーバ定義にマップします。

- スキャン結果と 1500 を超える既知のオペレーティングシステムのフィンガープリントを比較して、オペレーティングシステムを判別し、それぞれにスコアを割り当てます。最高スコアのオペレーティングシステムのフィンガープリントが、ホストに割り当てられるオペレーティングシステムになります。

システムは Nmap のオペレーティングシステム名を Cisco のオペレーティングシステム定義にマップします。

- 追加されたサーバおよびオペレーティングシステムのホストに脆弱性を割り当てます。

(注)

- ホストがネットワークマップ内になければ、Nmap は結果をホストプロファイルに追加することはできません。
- ホストがネットワークマップから削除されると、そのホストに関する Nmap スキャン結果が破棄されます。



#### ヒント

スキャンオプションによっては (ポートスキャンなど) 低帯域幅のネットワークに非常に負荷をかけることがあります。ネットワーク使用率が低い時間帯にこのようなタスクを実行するよう、スケジュールしてください。

スキャンに使用される基礎的な Nmap テクノロジーの詳細については、<http://insecure.org/> にある Nmap のマニュアルを参照してください。

#### 関連トピック

[Nmap スキャンの自動化](#) (225 ページ)

## Nmap 修復オプション

Nmap 修復を作成して、Nmap スキャンの設定を定義します。Nmap 修復は、関連ポリシー内で応答として使用したり、オンデマンドで実行したり、特定の時間に実行するようにスケジュールしたりできます。

Nmap により提供されるサーバやオペレーティングシステムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままであることを注意してください。Nmap を使用してホスト内でオペレーティングシステムやサーバのデータをスキャンすることを計画している場合



は、定期的なスキャンのスケジュールをセットアップして、Nmapによって提供されるオペレーティングシステムやサーバのデータを最新に保つこともできます。

次の表に、Firepower システム上で設定できる Nmap 修復オプションを示します。

表 217: Nmap 修復オプション

オプション	説明	対応する Nmap オプション
[スキャンの開始元イベント (Scan Which Address(es) From Event?) ]	<p>Nmap スキャンを相関ルールに対する応答として使用する場合、イベント内の送信元ホスト、宛先ホスト、またはその両方のどのアドレスをスキャンするか制御する次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> <li>• [送信元アドレスと宛先アドレスのスキャン (Scan Source and Destination Addresses) ] は、イベントの送信元 IP アドレスと宛先 IP アドレスによって表されるホストをスキャンします。</li> <li>• [送信元アドレスのみのスキャン (Scan Source Address Only) ] は、イベントの送信元 IP アドレスによって表されるホストをスキャンします。</li> <li>• [宛先アドレスのみのスキャン (Scan Destination Address Only) ] は、イベントの宛先 IP アドレスによって表されるホストをスキャンします。</li> </ul>	該当なし

オプション	説明	対応する Nmap オプション
[スキャンタイプ (Scan Types) ]		<b>TCP Syn</b> : -sS <b>TCP Connect</b> : -sT <b>TCP ACK</b> : -sA <b>TCP Window</b> : -sW <b>TCP Maimon</b> : -sM

オプション	説明	対応する Nmap オプション
	<p>Nmap がポートをスキャンする方法を選択します。</p> <ul style="list-style-type: none"> <li>• [TCP 同期 (TCP Syn) ] スキャンは、完全な TCP ハンドシェイクを使用せずに数千のポートにただちに接続します。このオプションを使用すると、TCP 接続が開始されますが完了はしていない状態で、admin アカウントが raw パケットアクセス権を持つホストや IPv6 が実行されていないホスト上でステルス モードでクイック スキャンできます。ホストが TCP Syn スキャンで送信される Syn パケットを確認応答すると、Nmap は接続をリセットします。</li> <li>• [TCP 接続 (TCP Connect) ] スキャンは、connect() システム コールを使用して、ホスト上のオペレーティングシステムを介して接続を開きます。TCP Connect スキャンは、Firepower Management Center 上の admin ユーザや管理対象デバイスがホストに対する raw パケット特権を持っていない場合や、IPv6 ネットワークをスキャンしている場合に使用できます。つまり、このオプションは TCP Syn スキャンを使用できない状況で使用します。</li> <li>• [TCP ACK] スキャンは、ACK パケットを送信して、ポートがフィルタ処理されているかいないかを検査します。</li> <li>• [TCP ウィンドウ (TCP Window) ] スキャンは、TCP ACK スキャンと同じ機能に加えて、ポートが開いているか閉じているかも判別します。</li> <li>• [TCP Maimon] スキャンは、FIN/ACK プローブを使用して BSD</li> </ul>	

オプション	説明	対応する Nmap オプション
	派生システムを識別します。	
[UDP ポートのスキャン (Scan for UDP ports) ]	TCP ポートに加えて UDP ポートのスキャンも有効にします。UDP ポートのスキャンには時間がかかることがあるので、クイックスキャンする場合はこのオプションを使用しないように注意してください。	-sU
[イベントからのポートの使用 (Use Port From Event) ]	<p>関連ポリシー内で応答として修復を使用する計画の場合に、修復によるスキャンの対象として、関連応答をトリガーするイベントで指定されたポートのみを有効にします。</p> <ul style="list-style-type: none"> <li>• 関連イベント内のポートをスキャンし、Nmap 修復構成中に指定するポートをスキャンしない場合は、[オン (On) ]を選択します。関連イベント内のポートをスキャンする場合は、Nmap 修復構成中に指定する IP アドレス上のポートが修復によりスキャンされることに注意してください。これらのポートも修復の動的スキャンのターゲットに追加されます。</li> <li>• Nmap 修復構成中に指定するポートのみスキャンするには、[オフ (Off) ]を選択します。</li> </ul> <p>Nmap がオペレーティングシステムやサーバに関する情報を収集するかどうかも制御できます。新しいサーバに関連付けられたポートをスキャンするには、[イベントからのポートの使用 (Use Port From Event) ] オプションを有効にします。</p>	該当なし

オプション	説明	対応する Nmap オプション
[レポート検出エンジンからのスキャン (Scan from reporting detection engine) ]	<p>ホストを報告した検出エンジンがあるアプライアンスからホストへのスキャンを有効にします。</p> <ul style="list-style-type: none"> <li>レポート検出エンジンを実行しているアプライアンスからスキャンするには、[オン (On) ]を選択します。</li> <li>修復内で設定されているアプライアンスからスキャンするには、[オフ (Off) ]を選択します。</li> </ul>	該当なし
[高速ポートスキャン (Fast Port Scan) ]	<p>スキャン元デバイス上の <code>/var/sf/nmap/share/nmap/nmap-services</code> ディレクトリ内にある <code>nmap-services</code> ファイルにリストされている TCP ポートのみに対するスキャンを有効にし、その他のポート設定を無視できるようにします。このオプションと [ポート範囲とスキャンの順序 (Port Ranges and Scan Order) ] オプションを併用できないことに注意してください。</p> <ul style="list-style-type: none"> <li>スキャン元デバイス上の <code>/var/sf/nmap/share/nmap/nmap-services</code> ディレクトリ内の <code>nmap-services</code> ファイルにリストされているポートのみスキャンし、その他のポート設定を無視するには、[オン (On) ]を選択します。</li> <li>すべての TCP ポートをスキャンするには、[オフ (Off) ]を選択します。</li> </ul>	-F
[ポート範囲とスキャンの順序 (Port Ranges and Scan Order) ]	<p>Nmap ポート仕様シンタックスを使用して、スキャンする特定のポートを設定し、スキャンする順序も設定します。このオプションと [高速ポートスキャン (Fast Port Scan) ] オプションを併用できないことに注意してください。</p>	-p

オプション	説明	対応する Nmap オプション
[オープンポートでベンダーとベンダー情報を調査 (Probe open ports for vendor and version information) ]	<p>サーバベンダーとバージョン情報の検出を有効にします。オープンポートでサーバベンダーとバージョン情報を調査する場合、Nmap はサーバの識別に使用するサーバデータを取得します。次に、シスコのサーバデータをそのサーバに置き換えます。</p> <ul style="list-style-type: none"> <li>• ホスト上のオープンポートでサーバ情報をスキャンして、サーバベンダーとバージョンを識別するには、[オン (On) ]を選択します。</li> <li>• ホストのシスコのサーバ情報を使用して続行するには、[オフ (Off) ]を選択します。</li> </ul>	-sV
[サービスバージョンの強度 (Service Version Intensity) ]	<p>サービスバージョンに対する Nmap プロブの強度を選択します。</p> <ul style="list-style-type: none"> <li>• 選択する数値が大きいほど使用するプロブの数が増えるので、スキャンは長時間になり精度が上がります。</li> <li>• 選択する数値が小さいほど、使用するプロブの数が減るので、スキャンは高速になり精度が下がります。</li> </ul>	--version-intensity <intensity>

オプション	説明	対応する Nmap オプション
[オペレーティングシステムの検出 (Detect Operating System) ]	<p>ホストのオペレーティングシステム情報の検出を有効にします。</p> <p>ホストでのオペレーティングシステムの検出を設定した場合、Nmap はホストをスキャンし、その結果を使用してオペレーティングシステムごとに評価を作成します。この評価は、ホスト上でそのオペレーティングシステムが実行されている可能性を反映します。</p> <ul style="list-style-type: none"> <li>• ホストに対してオペレーティングシステムを識別する情報をスキャンするには、[オン (On) ]を選択します。</li> <li>• ホストに関するシスコのオペレーティングシステム情報を使い続ける場合は、[オフ (Off) ]を選択します。</li> </ul>	-o
[すべてのホストをオンラインとして処理 (Treat All Hosts As Online) ]	<p>ホストディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポートスキャンを有効にします。このオプションを有効にすると、Nmap は [ホストディスカバリ方式 (Host Discovery Method) ] と [ホストディスカバリポートリスト (Host Discovery Port List) ] の設定を無視するので注意してください。</p> <ul style="list-style-type: none"> <li>• ホストディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポートスキャンを実行するには、[オン (On) ]を選択します。</li> <li>• [ホストディスカバリ方式 (Host Discovery Method) ] と [ホストディスカバリポートリスト (Host Discovery Port List) ] の設定を使用してホストディスカバリを実行し、使用不能なホスト上でのポートスキャンを省略するには、[オフ (Off) ]を選択します。</li> </ul>	-PN

## Nmap 修復オプション

オプション	説明	対応する Nmap オプション
[ホスト ディスカバリ方式 (Host Discovery Method) ]		<b>TCP SYN</b> : -PS <b>TCP ACK</b> : -PA <b>UDP</b> : -PU



オプション	説明	対応する Nmap オプション
	<p>ホストディスカバリを、ターゲット範囲内のすべてのホストに対して実行するか、[ホストディスカバリポートリスト (Host Discovery Port List)] にリストされているポートを経由して実行するか、または、ポートがリストされていない場合にそのホストディスカバリ方式のデフォルトポートを経由するかを選択します。</p> <p>ここで、[すべてのホストをオンラインとして処理 (Treat All Hosts As Online)] も有効にすると、[ホストディスカバリ方式 (Host Discovery Method)] オプションは無効になり、ホストディスカバリが実行されないことに注意してください。</p> <p>ホストが存在していて利用可能であるかどうかを Nmap がテストする際に使用する方式を以下から選択します。</p> <ul style="list-style-type: none"> <li>• [TCP SYN] オプションは、SYN フラグが設定された空の TCP パケットを送信し、応答を受信するとホストが利用可能であると認識します。デフォルトでは TCP SYN はポート 80 をスキャンします。TCP SYN スキャンは、ステートフルファイアウォールルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。</li> <li>• [TCP ACK] オプションは、ACK フラグが設定された空の TCP パケットを送信し、応答を受信するとホストが利用可能であると認識します。デフォルトでは TCP ACK もポート 80 をスキャンします。TCP ACK スキャンは、ステートレスファイアウォールルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。</li> </ul>	

オプション	説明	対応する Nmap オプション
	<ul style="list-style-type: none"> <li>• [UDP] オプションは、UDP パケットを送信し、クローズポートからポート到達不能応答が戻されるとホストが利用可能であると想定します。デフォルトではUDPはポート 40125 をスキャンします。</li> </ul>	
[ホスト ディスカバリ ポート リスト (Host Discovery Port List) ]	ホスト ディスカバリの実行時にスキャンするポートを、カスタマイズしたカンマ区切りリストで指定します。	ホスト ディスカバリ 方式に応じたポート リスト
[デフォルト NSE スクリプト (Default NSE Scripts) ]	<p>ホスト ディスカバリを行い、サーバ、オペレーティングシステム、脆弱性を検出する Nmap スクリプトのデフォルトセットを実行できるようにします。デフォルトスクリプトのリストについては、<a href="https://nmap.org/nse/doc/categories/default.html">https://nmap.org/nse/doc/categories/default.html</a> を参照してください。</p> <ul style="list-style-type: none"> <li>• Nmap スクリプトのデフォルトセットを実行するには、[オン (On) ] を選択します。</li> <li>• Nmap スクリプトのデフォルトセットを省略するには、[オフ (Off) ] を選択します。</li> </ul>	-sC
[タイミング テンプレート (Timing Template) ]	スキャンプロセスのタイミングを選択します。選択する数値が大きいほど、スキャンは高速になり包括的ではありません。	<b>0</b> : T0 (paranoid) <b>1</b> : T1 (sneaky) <b>2</b> : T2 (polite) <b>3</b> : T3 (normal) <b>4</b> : T4 (aggressive) <b>5</b> : T5 (insane)

## Nmap スキャンのガイドライン

アクティブスキャンにより重要な情報が得られることがありますが、Nmapなどのツールを多用すると、ネットワークリソースに負荷がかかり、重要なホストがクラッシュすることさえあります。アクティブスキャナを使用する際には、以下のガイドラインに従ってスキャン戦略を作成し、スキャンする必要があるホストとポートのみスキャンするようにしてください。

## 適切なスキャンターゲットの選択

Nmap を設定する際に、スキャン対象のホストを識別するスキャンターゲットを作成できます。スキャンターゲットには1つの IP アドレス、IP アドレスの CIDR ブロックまたはオクテット範囲、IP アドレス範囲、スキャンする IP アドレスまたは範囲のリスト、および1つ以上のホスト上のポートが含まれます。

次の方法でターゲットを指定できます。

- IPv6 ホストの場合：
  - 厳密な IP アドレス (192.168.1.101 など)
- IPv4 ホストの場合：
  - 厳密な IP アドレス (192.168.1.101 など) またはカンマスペースで区切った IP アドレスのリスト
  - CIDR 表記を使用した IP アドレスブロック (たとえば、192.168.1.0/24 は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストをスキャンします)
  - オクテットの範囲アドレッシングを使用した IP アドレス範囲 (たとえば、192.168.0-255.1-254 は、192.168.x.x の範囲内の末尾が .0 と .255 以外のすべてのアドレスをスキャンします)
  - ハイフンを使用した IP アドレス範囲 (たとえば、192.168.1.1 - 192.168.1.5 は、両端を含めて 192.168.1.1 から 192.168.1.5 の間の 6 つのホストをスキャンします)
  - カンマスペースで区切ったアドレスか範囲のリスト (たとえば、192.168.1.0/24, 194.168.1.0/24 は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストと、両端を含めて 194.168.1.1 から 194.168.1.254 の間の 254 個のホストをスキャンします)

理想的な Nmap スキャンのスキャンターゲットには、システムで識別できないオペレーティングシステムがあるホスト、識別されていないサーバがあるホスト、最近ネットワーク上で検出されたホストが含まれます。ネットワークマップ内にはないホストに関する Nmap 結果は、ネットワーク マップに追加できないことに注意してください。



### 注意

- Nmap によって提供されるサーバやオペレーティングシステムのデータは、もう1度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、定期的にスキャンをスケジュールします。
- ホストがネットワーク マップから削除されると、Nmap スキャン結果が破棄されます。
- ターゲットをスキャンする権限を持っていることを確認してください。Nmap を使用して自分や自社に属さないホストをスキャンすると違法になる場合があります。

### スキャン対象にする適切なポートの選択

設定するスキャンターゲットごとに、スキャン対象のポートを選択できます。各ターゲット上でスキャンする必要があるポートのセットを正確に識別するため、個々のポート番号、ポート範囲、または一連のポート番号やポート範囲を指定できます。

デフォルトでは、Nmap は 1 から 1024 までの TCP ポートをスキャンします。関連ポリシー内で応答として修復を使用する計画の場合は、関連応答をトリガーするイベントで指定されたポートのみを修復でスキャンできます。オンデマンドまたはスケジュール済みタスクとして修復を実行する場合、または Use Port From Event を使用しない場合は、その他のポート オプションを使用して、スキャンするポートを決定できます。nmap-services ファイルにリストされている TCP ポートのみスキャンし、その他のポート設定を無視するよう選択できます。TCP ポートの他に UDP ポートもスキャンできます。UDP ポートに対するスキャンには時間がかかることがあるので、すばやくスキャンする場合はこのオプションを使用しないように注意してください。スキャン対象として特定のポートかポート範囲を選択するには、Nmap ポート仕様シンタックスを使用してポートを識別します。

### ホスト ディスカバリ オプションの設定

ホストに対してポート スキャンを始める前にホスト ディスカバリを実行するかどうかを決めるか、またはスキャンを計画しているすべてのホストがオンラインであると想定できます。すべてのホストをオンラインとして扱わないことを選択した場合、使用するホスト ディスカバリ方式を選択でき、必要に応じて、ホスト ディスカバリ時のスキャン対象ポートのリストをカスタマイズできます。ホスト ディスカバリ時には、リストされているポートでオペレーティング システムやサーバの情報は調査されません。特定のポートを経由する応答を使用して、ホストがアクティブで使用可能かどうかのみを判別します。ホスト ディスカバリを実行して、ホストが利用可能でなかった場合には、そのホスト上のポートは Nmap でスキャンされません。

### 関連トピック

[Firepower システムの IP アドレス表記法](#) (14 ページ)

[Nmap スキャンの自動化](#) (225 ページ)

## 例：Nmap を使用した不明なオペレーティング システムの解決

この例では、不明なオペレーティング システムを解決するように設計された、Nmap 設定について説明します。Nmap 設定の詳細については、[Nmap スキャンの管理](#) (2081 ページ) を参照してください。

システムでネットワーク上のホストのオペレーティング システムを判別できない場合、Nmap を使用してホストをアクティブ スキャンできます。Nmap は、スキャンから得られた情報を利用して、使用されている可能性のあるオペレーティング システムを評価します。次に、最高の評価のオペレーティング システムを、ホストのオペレーティング システムを識別したものと使用します。

Nmap を使用して新しいホストにオペレーティング システムやサーバの情報を要求すると、スキャン対象のホストに対するシステムによるそのデータのモニタリングは非アクティブになります。Nmap を使用してホスト検出を実行し、システムにより不明なオペレーティング システムがあるとマークが付けられたホストのサーバ オペレーティング システムを検出すると、同

種のホストのグループを識別できる場合があります。その場合、それらのホストのうちの1つに基づいたカスタムフィンガープリントを作成し、システムでそのフィンガープリントを、Nmap スキャンに基づいてそのホスト上で実行されていると判明したオペレーティング システムと関連付けるようにすることができます。可能な限り、Nmap などのサードパーティ製の静的データを入力するよりも、カスタムフィンガープリントを作成してください。カスタムフィンガープリントを使用すると、システムはホストのオペレーティング システムを継続してモニタし、必要に応じて更新できるからです。

この例では、次のことを実行します。

1. **Nmap スキャンインスタンスの追加 (2082 ページ)** の説明に従って、スキャンインスタンスを設定します。
2. 次の設定を使用して Nmap 修復を作成します。
  - [イベントからのポートの使用 (Use Port From Event)] を有効にして、新しいサーバに関連付けられたポートをスキャンします。
  - [オペレーティング システムの検出 (Detect Operating System)] を有効にして、ホストのオペレーティング システムの情報を検出します。
  - [ベンダーおよびバージョン情報のためのポートのプロブ オープン (Probe open ports for vendor and version information)] を有効にして、サーバベンダーとバージョン情報を検出します。
  - ホストが既存であることが判明しているため、[すべてのホストをオンラインとして扱う (Treat All Hosts as Online)] を有効にします。
3. システムで不明なオペレーティング システムがあるホストが検出されたときにトリガーされる相関ルールを作成します。このルールは、**検出イベントが発生し、ホストの OS 情報が変更されており、OS 名が不明**という条件が満たされている場合にトリガーされる必要があります。
4. 相関ルールを組み込む相関ポリシーを作成します。
5. 相関ポリシー内で、ステップ 2 で応答として作成した Nmap 修復をステップ 3 で作成したルールに追加します。
6. 相関ポリシーをアクティブにします。
7. ネットワークマップ上のホストを消去し、強制的にネットワーク検出が再起動されてネットワーク マップが再構築されるようにします。
8. 1日後か2日後に、相関ポリシーによって生成されたイベントを検索します。Nmap 結果から、ホスト上で検出されたオペレーティング システムを分析し、システムで認識されない特定のホスト設定がネットワーク上にあるかどうか調べます。
9. 不明なオペレーティング システムがあるホストが複数検出され、Nmap 結果が同一の場合は、それらのホストの1つに対してカスタムフィンガープリントを作成し、将来類似のホストを識別する際に使用します。

## 関連トピック

- [Nmap 修復の作成 \(2087 ページ\)](#)
- [相関ルールの設定 \(2227 ページ\)](#)
- [Nmap スキャンの結果 \(2092 ページ\)](#)
- [クライアント用のカスタム フィンガープリントの作成 \(2046 ページ\)](#)
- [相関ポリシーの設定 \(2225 ページ\)](#)

## 例：Nmap を使用した新しいホストへの応答

この例では、新しいホストに応答するように設計された、Nmap 設定について説明します。Nmap 設定の詳細については、[Nmap スキャンの管理 \(2081 ページ\)](#) を参照してください。

システムにより、侵入の可能性があるサブネット内で新しいホストが検出された場合、そのホストをスキャンして、そのホストの脆弱性に関する正確な情報を入手できます。

そのためには、このサブネット内に新しいホストが出現した時点で検出し、そのホスト上で Nmap スキャンを実行する修復を起動する相関ポリシーを作成してアクティブにします。

そのためには、次のことを実行します。

1. [Nmap スキャンインスタンスの追加 \(2082 ページ\)](#) の説明に従って、スキャンインスタンスを設定します。
2. 次の設定を使用して Nmap 修復を作成します。
  - [イベントからのポートの使用 (Use Port From Event) ] を有効にして、新しいサーバに関連付けられたポートをスキャンします。
  - [オペレーティングシステムの検出 (Detect Operating System) ] を有効にして、ホストのオペレーティング システムの情報を検出します。
  - [ベンダーおよびバージョン情報のためのポートのプロープオープン (Probe open ports for vendor and version information) ] を有効にして、サーバベンダーとバージョン情報を検出します。
  - ホストが既存であることが判明しているため、[すべてのホストをオンラインとして扱う (Treat All Hosts as Online) ] を有効にします。
3. システムが特定のサブネット上で新しいホストを検出したときにトリガーされる相関ルールを作成します。このルールは、**検出イベントが発生し、新しいホストが検出されたとき** にトリガーされる必要があります。
4. 相関ルールを組み込む相関ポリシーを作成します。
5. 相関ポリシー内で、ステップ 2 で応答として作成した Nmap 修復をステップ 3 で作成したルールに追加します。
6. 相関ポリシーをアクティブにします。
7. 新しいホストが通知されたら、ホストプロファイルを調べて Nmap スキャンの結果を確認し、ホストに適用されている脆弱性に対処します。

このポリシーをアクティブにした後で、修復状態の表示 ([分析 (Analysis)] > [相関 (Correlation)] > [ステータス (Status)]) を定期的に検査して、修復が起動された時点を調べることができます。修復の動的なスキャンターゲットには、サーバ検出の結果としてスキャンされたホストの IP アドレスを含める必要があります。これらのホストのホストプロファイルを調べて、Nmap によって検出されたオペレーティングシステムとサーバに基づいて、対処する必要がある脆弱性がホストにあるかどうか確認します。



#### 注意

大規模なネットワークや動的なネットワークがある場合、新しいホストの検出は頻繁に発生するので、スキャンを使用して応答するには不向きな場合があります。リソースの過負荷を避けるために、頻繁に発生するイベントへの応答として Nmap スキャンを使用しないでください。また、Nmap を使用して新しいホストのオペレーティングシステムやサーバの情報を要求すると、スキャン対象のホストに対するによるそのデータのシスコモニタリングが非アクティブになることに注意してください。

#### 関連トピック

- [Nmap 修復の作成 \(2087 ページ\)](#)
- [相関ルールの設定 \(2227 ページ\)](#)
- [相関ポリシーの設定 \(2225 ページ\)](#)

## Nmap スキャンの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

Nmap スキャンを使用するには、少なくとも 1 つの Nmap スキャンインスタンスと 1 つの Nmap 修復を設定する必要があります。Nmap スキャンターゲットの設定はオプションです。

#### 手順

##### ステップ 1 Nmap スキャンを設定します。

- Nmap スキャン インスタンスを追加します。詳細については、[Nmap スキャン インスタンスの追加 \(2082 ページ\)](#) を参照してください。
- Nmap 修復を作成します。詳細については、[Nmap 修復の作成 \(2087 ページ\)](#) を参照してください。
- 必要に応じて、Nmap スキャン ターゲットを追加します。詳細については、[Nmap スキャン ターゲットの追加 \(2085 ページ\)](#) を参照してください。

##### ステップ 2 Nmap スキャンを実行します。

- オンデマンド Nmap スキャンを実行します。詳細については、[オンデマンド Nmap スキャンの実行 \(2091 ページ\)](#) を参照してください。
- 自動 Nmap スキャンを設定します。詳細については、[Nmap スキャンの自動化 \(225 ページ\)](#) を参照してください。
- 自動 Nmap スキャンをスケジュールします。詳細については、[Nmap スキャンのスケジュール \(226 ページ\)](#) を参照してください。

### 次のタスク

- 関連タスクを表示することで、進行中の Nmap スキャンをモニタします。[タスクメッセージの表示 \(330 ページ\)](#) を参照してください。
- 必要に応じて、次に示すようにスキャンを調整します。
  - Nmap スキャン インスタンスを編集します。詳細については、[Nmap スキャンインスタンスの編集 \(2084 ページ\)](#) を参照してください。
  - Nmap スキャン ターゲットを編集します。詳細については、[Nmap スキャン ターゲットの編集 \(2086 ページ\)](#) を参照してください。
  - Nmap 修復を編集します。詳細については、[Nmap 修復の編集 \(2090 ページ\)](#) を参照してください。

## Nmap スキャン インスタンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

脆弱性についてネットワークをスキャンするのに使用する Nmap モジュールごとに別々のスキャンインスタンスをセットアップできます。Firepower Management Center 上のローカル Nmap モジュールか、リモートでスキャンを実行するために使用するデバイスに対してスキャンインスタンスをセットアップできます。各スキャンの結果は常に Firepower Management Center に保存されます。リモートデバイスからスキャンを実行する場合でも、この場所でスキャンを設定できます。ミッションクリティカルなホストへの不慮のスキャンや悪意のあるスキャンを防ぐには、インスタンスのブラックリストを作成し、そのインスタンスで決してスキャンしてはならないホストを指示できます。

既存のスキャン インスタンスと同じ名前のスキャン インスタンスは追加できません。

マルチドメイン展開では、現在のドメインで作成されたスキャン インスタンスが表示されます。これは編集できます。先祖ドメインで作成されたスキャン インスタンスも表示されますが、これは編集できません。下位のドメインのスキャンインスタンスを表示および編集するには、そのドメインに切り替えます。



## 手順

- ステップ 1** 次のいずれかの方法を使用して Nmap スキャン インスタンスのリストにアクセスします。
- [ポリシー (Policies)] > [アクション (Actions)] > [インスタンス (Instances)] を選択します。
  - [ポリシー (Policies)] > [アクション (Actions)] > [スキャナ (Scanners)] を選択します。
- ステップ 2** 以下の場合、修復を追加します。
- 上記の最初の方法でリストにアクセスした場合は、[新しいインスタンスの追加 (Add a New Instance)] セクションを探し、ドロップダウンリストから Nmap 修復モジュールを選択し、[追加 (Add)] をクリックします。
  - 上記の 2 番目の方法でリストにアクセスした場合は、[Nmap インスタンスの追加 (Add Nmap Instance)] をクリックします。
- ステップ 3** [インスタンス名 (Instance Name)] を入力します。
- ステップ 4** [説明 (Description)] を入力します。
- ステップ 5** オプションで、[ブラックリスト化されたスキャン ホスト (Black Listed Scan hosts)] フィールドで、このスキャンインスタンスがスキャンしないホストまたはネットワークを指定します。
- IPv6 ホストの場合、厳密な IP アドレス (2001:DB8::fedd:eef など)
  - IPv4 ホストの場合、厳密な IP アドレス (192.168.1.101 など) または CIDR 表記を使用した IP アドレス ブロック (たとえば、192.168.1.0/24 は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストをスキャンします)
  - 感嘆符 (!) を使用してアドレス値の否定はできないことに注意してください。
- (注) ブラックリストに含まれるネットワーク内のホストをスキャン対象として特定すると、スキャンは実行されません。
- ステップ 6** オプションで、Firepower Management Center の代わりにリモートデバイスからスキャンを実行するには、そのデバイスの IP アドレスか名前を指定します。この情報は、Management Center Web インターフェイス内のそのデバイスに関する [Information] ページの [Remote Device Name] フィールドに表示されます。
- ステップ 7** [作成 (Create)] をクリックします。  
システムがインスタンスの作成を終えると、編集モードでこのインスタンスが表示されます。
- ステップ 8** 必要に応じて、インスタンスに Nmap の修復を追加します。そのためには、インスタンスの [設定されている修復 (Configured Remediations)] を探し、[追加 (Add)] をクリックし、[Nmap 修復の作成 \(2087 ページ\)](#) の説明に従って修復を作成します。
- ステップ 9** インスタンスのリストに戻るには、[キャンセル (Cancel)] をクリックします。

- (注) [スキャナ (Scanners) ]オプションにより Nmap スキャンインスタンスのリストにアクセスした場合は、インスタンスの修復も併せて追加しないと追加したインスタンスは表示されません。修復が追加されていないインスタンスをすべて表示するには、[インスタンス (Instances) ]メニュー オプションを使ってリストにアクセスします。

## Nmap スキャンインスタンスの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin


スキャンインスタンスを編集する場合、インスタンスに関連付けられている修復を表示、追加、および削除できます。インスタンス内でプロファイルが作成された Nmap モジュールを使用しなくなった場合には、Nmap スキャンインスタンスを削除します。スキャンインスタンスを削除すると、そのインスタンスを使用する修復も削除されることに注意してください。

マルチドメイン展開では、現在のドメインで作成されたスキャンインスタンスが表示されます。これは編集できます。先祖ドメインで作成されたスキャンインスタンスも表示されますが、これは編集できません。下位のドメインのスキャンインスタンスを表示および編集するには、そのドメインに切り替えます。

### 手順

**ステップ 1** 次のいずれかの方法を使用して Nmap スキャンインスタンスのリストにアクセスします。

- [ポリシー (Policies) ] > [アクション (Actions) ] > [インスタンス (Instances) ] を選択します。
- [ポリシー (Policies) ] > [アクション (Actions) ] > [スキャナ (Scanners) ] を選択します。

**ステップ 2** 編集するインスタンスの横にある表示アイコン () をクリックします。

**ステップ 3** [Nmap スキャンインスタンスの追加 \(2082 ページ\)](#) の説明に従って、スキャンインスタンスの設定を変更します。

**ステップ 4** [保存 (Save) ] をクリックします。

**ステップ 5** [完了 (Done) ] をクリックします。

### 次のタスク

- 必要に応じて、スキャンインスタンスに新しい修復を追加します。次を参照してください。 [Nmap 修復の作成 \(2087 ページ\)](#)

- 必要に応じて、インスタンスに関連付けられている修復を編集します。[Nmap 修復の編集 \(2090 ページ\)](#) を参照してください。
- 必要に応じて、インスタンスに関連付けられる修復を削除します。[オンデマンド Nmap スキャンの実行 \(2091 ページ\)](#) を参照してください。
- 必要に応じて、その横にある削除アイコン (🗑️) をクリックして、スキャンインスタンスを削除します。

## Nmap スキャンターゲットの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

Nmap モジュールを設定する際にスキャンターゲットを作成して保存できます。スキャンターゲットは、オンデマンドまたはスケジュール済みのスキャンの実行時にターゲットにするホストとポートを識別します。これにより、毎回新しいスキャンターゲットを作成する必要がなくなります。スキャンターゲットには、スキャンする 1 つの IP アドレスか IP アドレスのブロック、および 1 つ以上のホスト上のポートが含まれます。Nmap ターゲットの場合、オクテット範囲による Nmap のアドレッシングや IP アドレスの範囲も使用できます。Nmap のオクテット範囲によるアドレッシングの詳細については、<http://insecure.org> にある Nmap のマニュアルを参照してください。

(注)

- スキャンターゲットに多数のホストが含まれている場合、スキャンに要する時間が延びる場合があります。回避策として、一度にスキャンするホストを減らしてください。
- Nmap によって提供されるサーバやオペレーティングシステムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、定期的にスキャンをスケジュールします。ホストがネットワーク マップから削除されると、Nmap スキャン結果はすべて破棄されます。
- マルチドメイン展開では、現在のドメインで作成されたスキャンターゲットが表示されます。これは編集できます。先祖ドメインで作成されたスキャンターゲットも表示されますが、これは編集できません。下位のドメインのスキャンターゲットを表示および編集するには、そのドメインに切り替えます。

### 手順

- ステップ 1** [ポリシー (Policies)] > [アクション (Actions)] > [スキャナ (Scanners)] を選択します。
- ステップ 2** ツールバーで、[ターゲット (Targets)] をクリックします。
- ステップ 3** [スキャンターゲットの作成 (Create Scan Target)] をクリックします。

**ステップ 4** [名前 (Name) ]フィールドに、このスキャンターゲットに使用する名前を入力します。

**ステップ 5** [IP 範囲 (IP Range) ]テキストボックスで、[Nmap スキャンのガイドライン \(2076 ページ\)](#) で説明しているシンタックスを使用して、スキャンする 1 つ以上のホストを指定します。

(注) スキャンターゲット内の IP アドレスか範囲のリストでカンマを使用した場合、ターゲットを保存する際にカンマはスペースに変換されます。

**ステップ 6** [ポート (Ports) ]フィールドで、スキャンするポートを指定します。

1 から 65535 までの値を使用して、次のいずれかを入力できます。

- ポート番号
- カンマで区切ったポートのリスト
- ハイフンで区切ったポート番号の範囲
- ハイフンで区切ったポート番号の複数の範囲をカンマで区切ったもの

**ステップ 7** [保存 (Save) ]をクリックします。

#### 関連トピック

[Nmap スキャンの自動化 \(225 ページ\)](#)

## Nmap スキャンターゲットの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin



**ヒント** 修復を使用して特定の IP アドレスをスキャンするつもりがないのに、修復を起動した相関ポリシー違反にホストが関係していたためにその IP アドレスがターゲットに追加された場合は、修復の動的スキャンターゲットを編集できます。

スキャンターゲットにリストされているホストをスキャンする必要がなくなった場合は、そのスキャンターゲットを削除します。

マルチドメイン展開では、現在のドメインで作成されたスキャンターゲットが表示されます。これは編集できます。先祖ドメインで作成されたスキャンターゲットも表示されますが、これは編集できません。下位のドメインのスキャンターゲットを表示および編集するには、そのドメインに切り替えます。

## 手順

- ステップ 1** [ポリシー (Policies)] > [アクション (Actions)] > [スキャナ (Scanners)] を選択します。
- ステップ 2** ツールバーで、[ターゲット (Targets)] をクリックします。
- ステップ 3** 編集するスキャンターゲットの横にある編集アイコン (✎) をクリックします。
- 代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 4** 必要に応じて変更を加えます。詳細については、[Nmap スキャンターゲットの追加 \(2085 ページ\)](#) を参照してください。
- ステップ 5** [Save] をクリックします。
- ステップ 6** 必要に応じて、その横にある削除アイコン (🗑) をクリックして、スキャンターゲットを削除します。

## Nmap 修復の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

Nmap 修復は、既存の Nmap スキャン インスタンスに修復を追加することによってのみ作成できます。修復では、スキャンの設定を定義します。これは関連ポリシーで応答として使用したり、オンデマンドで実行したり、スケジュールタスクとして特定の時刻に実行したりできます。

Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、定期的にスキャンをスケジュールします。ホストがネットワークマップから削除されると、Nmap スキャン結果が破棄されます。

Nmap の機能に関する一般情報については、<http://insecure.org> にある Nmap のマニュアルを参照してください。

マルチドメイン導入では、現在のドメインで作成された Nmap 修復が表示されます。これは編集できます。先祖ドメインで作成された Nmap 修復も表示されますが、これは編集できません。下位ドメインの Nmap 修復を表示および編集するには、そのドメインに切り替えます。

## 始める前に

- [Nmap スキャンインスタンスの追加 \(2082 ページ\)](#) の説明に従って、Nmap スキャンインスタンスを追加します。

## 手順

- 
- ステップ 1** [ポリシー (Policies)] > [アクション (Actions)] > [インスタンス (Instances)] を選択します。
- ステップ 2** 修復を追加するインスタンスの横にある表示アイコン (🔍) をクリックします。
- ステップ 3** [設定済みの修復 (Configured Remediations)] セクションで、[追加 (Add)] をクリックします。
- ステップ 4** [修復名 (Remediation Name)] を入力します。
- ステップ 5** [説明 (Description)] を入力します。
- ステップ 6** 侵入イベント、接続イベント、ユーザイベントをトリガーする関連ルールに応じてこの修復を使用する場合は、[スキャンするイベントのアドレス (Scan Which Address(es) From Event?)] オプションを設定します。
- ヒント** ディスカバリイベントまたはホスト入力イベントに対してトリガーする関連ルールへの応答としてこの修復を使用する計画の場合は、デフォルトでそのイベントに関連するホストの IP アドレスが修復によってスキャンされます。このオプションを設定する必要はありません。
- (注) トラフィック プロファイルの変更に対してトリガーする関連ルールへの応答として Nmap 修復を割り当てないでください。
- ステップ 7** [スキャンタイプ (Scan Type)] オプションを設定します。
- ステップ 8** オプションで、TCP ポートに加えて UDP ポートをスキャンするには、[UDP ポートのスキャン (Scan for UDP ports)] オプションで [オン (On)] を選択します。
- ヒント** UDP ポートスキャンは TCP ポートスキャンよりも時間がかかります。スキャン時間を短縮するには、このオプションを無効のままにします。
- ステップ 9** 関連ポリシー違反への応答としてこの修復を使用する計画の場合は、[イベントからポートを使用 (Use Port From Event)] オプションを設定します。
- ステップ 10** 関連ポリシー違反への応答としてこの修復を使用する計画で、イベントを検出した検出エンジンを実行しているアプライアンスを使用してスキャンを実行するには、[レポート検出エンジンからスキャン (Scan from reporting detection engine)] オプションを設定します。
- ステップ 11** [高速ポート スキャン (Fast Port Scan)] オプションを設定します。
- ステップ 12** [ポート範囲およびスキャン順序 (Port Ranges and Scan Order)] フィールドに、デフォルトでスキャンするポートを入力します。Nmap ポート指定シンタックスを使用し、ポートをスキャンする順序で入力します。
- 次の形式を使用します。
- 1 から 65535 までの値を指定します。
  - ポートを区切るには、カンマスペースを使用します。
  - ポート範囲を示すには、ハイフンを使用します。

- TCP ポートと UDP ポートの両方ともスキャンする場合は、スキャン対象の TCP ポートのリストの先頭に T を挿入し、UDP ポートのリストの先頭に U を挿入します。

(注) 手順8で説明されているように、相関ポリシー違反への応答として修復が起動する場合には、[イベントからポートを使用 (Use Port From Event)] オプションによりこの設定が上書きされます。

例：

UDP トラフィックのポート 53 と 111 をスキャンしてから、TCP トラフィックのポート 21 から 25 までスキャンするには、`u:53,111,t:21-25` と入力します。

- ステップ 13** 開いているポートでサーバベンダーおよびバージョン情報をプローブするには、[ベンダーおよびバージョン情報に関するオープンポートのプローブ (Probe open ports for vendor and version information)] を設定します。
- ステップ 14** 開いているポートをプローブすることにした場合、[サービスバージョンの強さ (Service Version Intensity)] ドロップダウンリストから数値を選択することにより、使用されるプローブの数を設定します。
- ステップ 15** オペレーティングシステム情報をスキャンするには、[オペレーティングシステムの検出 (Detect Operating System)] 設定を行います。
- ステップ 16** ホストディスカバリが行われるかどうか、およびポートのスキャンが使用可能なホストのみに対して実行されるかどうかを決めるには、[すべてのホストをオンラインとして扱う (Treat All Hosts As Online)] を設定します。
- ステップ 17** Nmap でホストの使用可能性をテストする際に使用する方法を設定するには、[ホストディスカバリ方式 (Host Discovery Method)] ドロップダウンリストから方式を選択します。
- ステップ 18** ホストディスカバリ時にポートのカスタムリストをスキャンする場合は、選択したホストディスカバリ方式に適したポートのリストを、[ホストディスカバリポートリスト (Host Discovery Port List)] フィールドにカンマで区切って入力します。
- ステップ 19** [デフォルトNSEスクリプト (Default NSE Scripts)] オプションを設定して、ホストディスカバリおよび、サーバ、オペレーティングシステム、脆弱性のディスカバリにNmapスクリプトのデフォルトセットを使用するかどうかを制御します。
- ヒント デフォルトスクリプトのリストについては、<http://nmap.org/nsedoc/categories/default.html> を参照してください。
- ステップ 20** スキャンプロセスのタイミングを設定するには、[タイミングテンプレート (Timing Template)] ドロップダウンリストからタイミングテンプレート番号を選択します。
- より高速だが、包括的でないスキャンを実行する場合は大きい番号を選択し、低速で、より包括的なスキャンを実行する場合は小さい番号を選択します。
- ステップ 21** [作成 (Create)] をクリックします。  
修復の作成が完了すると、修復が編集モードで表示されます。
- ステップ 22** [完了 (Done)] をクリックして、関連インスタンスに戻ります。
- ステップ 23** [キャンセル (Cancel)] をクリックすると、インスタンスリストに戻ります。

## 関連トピック

[Nmap スキャンの自動化](#) (225 ページ)

[Nmap 修復オプション](#) (2066 ページ)

## Nmap 修復の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

Nmap 修復に加えた変更は、進行中のスキャンには影響しません。新しい設定は、次回スキャンが開始されたときに有効になります。Nmap 修復が不要になったら削除します。

マルチドメイン導入では、現在のドメインで作成された Nmap 修復が表示されます。これは編集できます。先祖ドメインで作成された Nmap 修復も表示されますが、これは編集できません。下位ドメインの Nmap 修復を表示および編集するには、そのドメインに切り替えます。

## 手順

**ステップ 1** 以下のいずれかの方法を使用して、Nmap スキャンインスタンスのリストにアクセスします。

- [ポリシー (Policies)] > [アクション (Actions)] > [インスタンス (Instances)] を選択します。
- [ポリシー (Policies)] > [アクション (Actions)] > [スキャナ (Scanners)] を選択します。

**ステップ 2** 編集する修復にアクセスします。

- 上記の最初の方法でリストにアクセスした場合は、関連するインスタンスの横にある表示アイコン (🔍) をクリックし、次に、[設定済み修復 (Configured Remediations)] セクションで、編集する修復の横にある表示アイコンを再度クリックします。
- 上記の 2 番目の方法でリストにアクセスした場合は、編集する修復の横にある表示アイコン (🔍) をクリックします。

**ステップ 3** [Nmap 修復の作成](#) (2087 ページ) の説明に従って、必要に応じて変更を加えます。

**ステップ 4** 変更を保存する場合は [保存 (Save)] をクリックし、保存せずに終了する場合は [完了 (Done)] をクリックします。

**ステップ 5** 必要に応じて、その横にある削除アイコン (🗑️) をクリックして修復を削除します。



## オンデマンド Nmap スキャンの実行

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

オンデマンド Nmap スキャンは、いつでも必要なときに起動できます。スキャンする IP アドレスとポートを入力するか、既存のスキャン ターゲットを選択することで、オンデマンド スキャンのターゲットを指定できます。

Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、定期的にスキャンをスケジュールします。ホストがネットワークマップから削除されると、Nmap スキャンの結果は破棄されます。

### 始める前に

- 必要に応じて、Nmap スキャン ターゲットを追加します。[Nmap スキャン ターゲットの追加 \(2085 ページ\)](#) を参照してください。

### 手順

- 
- ステップ 1** [ポリシー (Policies)] > [アクション (Actions)] > [スキャナ (Scanners)] を選択します。
- ステップ 2** スキャンの実行時に使用する Nmap 修復の横にあるスキャンアイコン (🔍) をクリックします。
- ステップ 3** 必要に応じて、保存済みのスキャン ターゲットを使用してスキャンする場合は、[保存済ターゲット (Saved Targets)] ドロップダウンリストからターゲットを選択して、[ロード (Load)] をクリックします。
- (注) スキャン ターゲットを追加するには、ダイアログの上部にある編集アイコン (✎) をクリックします。
- ステップ 4** [IP 範囲 (IP Range(s))] フィールドで、スキャンするホストの IP アドレスを指定するかロードされたリストを変更します。
- (注)
- IPv4 アドレスのホストの場合は、複数の IP アドレスをカンマで区切って指定するか、CIDR 表記を使用できます。感嘆符 (!) を前に挿入して IP アドレスを否定することもできます。
  - IPv6 アドレスのホストの場合は、厳密な IP アドレスを使用します。範囲はサポートされていません。

**ステップ 5** [ポート (Ports) ]フィールドで、スキャンするポートを指定するか、ロードされたリストを変更します。

ポート番号、カンマで区切ったポートのリスト、ハイフンで区切ったポート番号の範囲を入力できます。

**ステップ 6** マルチドメイン展開では、[ドメイン (Domain) ]フィールドを使用して、スキャンを実行するリーフドメインを指定します。

**ステップ 7** [今すぐスキャン (Scan Now) ]をクリックします。

### 次のタスク

- 必要に応じて、タスクのステータスをモニタします ([タスクメッセージの表示 \(330 ページ\)](#) を参照)。

### 関連トピック

[Nmap スキャンの自動化 \(225 ページ\)](#)

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

[検索でのポート \(2472 ページ\)](#)

## Nmap スキャンの結果

進行中の Nmap スキャンをモニタし、Firepower システムによって実行されたスキャンの結果あるいは Firepower システム外部で行われたスキャンの結果をインポートして、スキャン結果を表示および分析することができます。

ローカル Nmap モジュールを使用して作成したスキャン結果を、レンダリングされたページとしてポップアップ ウィンドウで表示できます。Nmap 結果ファイルを raw XML 形式でダウンロードすることもできます。

Nmapによって検出されたオペレーティングシステムやサーバの情報を、ホストプロファイルやネットワークマップ内で参照することもできます。ホストのスキャンが生成するサーバ情報がフィルタ除去されているかクローズ状態のポートのサーバに関する情報の場合、または、スキャンが収集した情報がオペレーティングシステム情報やサーバのセクションに含めることができない情報の場合、それらの結果は、ホストプロファイルの [Nmap スキャン結果 (Nmap Scan Results) ]セクションに含めることができます。

### Nmap スキャン結果の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

Nmap スキャンが完了したら、スキャン結果のテーブルを表示できます。

ユーザは検索する情報に応じて結果のビューを操作することができます。スキャン結果にアクセスすると表示されるページは、使用するワークフローに応じて異なります。定義済みのワークフローを使用できます。このワークフローにはスキャン結果のテーブルビューが含まれます。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

<http://insecure.org> で使用可能な Nmap バージョン 1.01 DTD を使用して Nmap の結果をダウンロードして表示することができます。

スキャン結果をクリアすることもできます。

## 手順

**ステップ 1** [ポリシー (Policies)] > [アクション (Actions)] > [スキャナ (Scanners)] を選択します。

**ステップ 2** ツールバーで、[スキャン結果 (Scan Results)] をクリックします。

**ステップ 3** 次の選択肢があります。

- [イベント時間の制約 \(2451 ページ\)](#) の説明に従って、時間範囲を調整します。
- カスタムワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [ (ワークフローの切り替え) ((switch workflow)) ] をクリックします。
- スキャン結果をレンダリングされたページとしてポップアップ ウィンドウで表示するには、スキャン ジョブの横にある [表示 (View)] をクリックします。
- テキスト エディタで raw XML コードを表示できるようにスキャン結果ファイルのコピーを保存するには、スキャンジョブの横の [ダウンロード (Download)] をクリックします。
- スキャン結果をソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- 表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン (✕) をクリックします。表示されるポップアップ ウィンドウで、[適用 (Apply)] をクリックします。

**ヒント** 他のカラムを表示または非表示にするには、[適用 (Apply)] をクリックする前に、該当するチェックボックスをオンまたはオフにします。無効にしたカラムをビューに戻すには、展開の矢印をクリックして検索制約を展開し、[無効にされたカラム (Disabled Columns)] の下のカラム名をクリックします。

- ワークフローの次のページにドリルダウンするには、[ドリルダウン ページの使用 \(2439 ページ\)](#) を参照してください。
- スキャンインスタンスや修復を設定するには、ツールバーの [スキャナ (Scanners)] をクリックしてください ([Nmap スキャンの管理 \(2081 ページ\)](#) を参照)。
- ワークフロー ページ内およびワークフロー ページ間で移動するには、[ワークフロー ページのナビゲーション ツール \(2436 ページ\)](#) を参照してください。

- その他のイベント ビューに移動して関連するイベントを表示するには、[ジャンプ (Jump to)] ドロップダウン リストから、表示するイベント ビューの名前を選択します。
- スキャン結果を検索するには、該当するフィールドに検索条件を入力します。

### 関連トピック

[Nmap スキャン結果のフィールド](#) (2094 ページ)

## Nmap スキャン結果のフィールド

Nmap スキャンを実行すると、Firepower Management Center でデータベース内のスキャン結果が収集されます。次の表に、表示および検索できるスキャン結果テーブルのフィールドを示します。

表 218: スキャン結果のフィールド

フィールド	説明
開始時間 (Start Time)	この結果を作成したスキャンの開始日時。
終了時間 (End Time)	この結果を作成したスキャンの終了日時。
ターゲット (Target)	この結果を作成したスキャンのスキャン ターゲットの IP アドレス (DNS 解決が有効になっている場合はホスト名)。
Scan Type	この結果を作成したスキャンのタイプを示す、Nmap またはサードパーティのスキナ名。
スキャン モード (Scan Mode)	この結果を作成したスキャンのモード： <ul style="list-style-type: none"> <li>• [オンデマンド (On Demand)] : オン デマンドで実行されたスキャンからの結果。</li> <li>• [インポート済み (Imported)] : 別のシステムでスキャンされて Firepower Management Center にインポートされた結果。</li> <li>• [スケジュール済み (Scheduled)] : スケジュール済みタスクとして実行されたスキャンからの結果。</li> </ul>
結果	スキャンの結果。
ドメイン	スキャン ターゲットのドメイン。このフィールドは、マルチドメイン展開の場合にのみ存在します。

### 関連トピック

[イベントの検索](#) (2467 ページ)

## Nmap スキャン結果のインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

Firepower システムの外部で実行した Nmap スキャンによって作成された XML 結果ファイルをインポートできます。以前に Firepower システムからダウンロードした XML 結果ファイルもインポートできます。Nmap スキャン結果をインポートする場合、結果ファイルは XML 形式で、Nmap バージョン 1.01 DTD に準拠している必要があります。Nmap 結果の作成と Nmap DTD の詳細については、<http://insecure.org> にある Nmap のマニュアルを参照してください。

Nmap がホストプロファイルに結果を追加できるようにするには、その前にホストがネットワーク マップ内に存在している必要があります。

### 手順

- 
- ステップ 1 [ポリシー (Policies)] > [アクション (Actions)] > [スキャナ (Scanners)] を選択します。
  - ステップ 2 ツールバーで、[結果のインポート (Import Results)] をクリックします。
  - ステップ 3 マルチドメイン展開では、インポートされた結果の保存場所を指定するために、[ドメイン (Domain)] ドロップダウンリストからリーフ ドメインを選択します。
  - ステップ 4 [参照 (Browse)] をクリックして、結果ファイルに移動します。
  - ステップ 5 [インポートの結果 (Import Results)] ページに戻ったら、[インポート (Import)] をクリックして結果をインポートします。
-





## 第 86 章

# アプリケーションの検出

次のトピックでは、Firepower システム アプリケーション検出について説明します。

- [概要：アプリケーション検出 \(2097 ページ\)](#)
- [カスタム アプリケーションディテクタ \(2104 ページ\)](#)
- [ディテクタ詳細の表示またはダウンロード \(2114 ページ\)](#)
- [ディテクタリストのソート \(2115 ページ\)](#)
- [検出機能リストのフィルタリング \(2115 ページ\)](#)
- [別のディテクタ ページへの移動 \(2117 ページ\)](#)
- [ディテクタのアクティブおよび非アクティブの設定 \(2118 ページ\)](#)
- [カスタム アプリケーションディテクタの編集 \(2119 ページ\)](#)
- [ディテクタの削除 \(2120 ページ\)](#)

## 概要：アプリケーション検出

Firepower システムは IP トラフィックを分析するときに、ネットワーク上でよく使用されているアプリケーションを特定しようとします。アプリケーション認識は、アプリケーションを制御するために不可欠です。

システムによって検出されるアプリケーションには以下の 3 種類があります。

- HTTP や SSH などのホスト間の通信を表すアプリケーション プロトコル
- Web ブラウザや電子メールクライアントなどのホスト上で動作しているソフトウェアを表すクライアント
- HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの *Web* アプリケーション

システムは、ディテクタに指定されている特性に従って、ネットワークトラフィック内のアプリケーションを識別します。たとえば、システムはパケットヘッダーに含まれる ASCII パターンによってアプリケーションを確認できます。加えて、Secure Socket Layer (SSL) プロトコルディテクタは、セキュアなセッションからの情報を使用して、セッションからアプリケーションを識別します。

Firepower システムのアプリケーションディテクタには以下の2つのソースがあります。

- システム提供ディテクタ。Webアプリケーション、クライアント、およびアプリケーションプロトコルを検出します。

アプリケーション（およびオペレーティングシステム）に対して使用できるシステム提供ディテクタは、インストールされている Firepower システムのバージョンと VDB のバージョンによって異なります。リリースノートとアドバイザリに、新しいディテクタと更新されたディテクタに関する情報が記載されています。また、プロフェッショナルサービスが作成した個別のディテクタをインポートすることもできます。検出されるアプリケーションの完全なリストについては、サポートサイトを参照してください。

- カスタムアプリケーションプロトコルディテクタ。Webアプリケーション、クライアント、アプリケーションプロトコルを検出するためにユーザが作成するディテクタです。

また、暗黙的アプリケーションプロトコル検出を通してアプリケーションプロトコルを検出することもできます。これは、クライアントの検出に基づいてアプリケーションプロトコルの存在を推測するものです。

ネットワーク検出ポリシーで定義されているように、システムはモニタ対象ネットワーク内のホスト上で動作しているアプリケーションプロトコルだけを識別します。たとえば、モニタされていないリモートサイト上のFTPサーバに内部ホストがアクセスする場合、システムはアプリケーションプロトコルをFTPとして識別しません。一方、モニタされているホスト上のFTPサーバにリモートまたは内部ホストがアクセスする場合、システムはアプリケーションプロトコルを肯定的に識別できます。

モニタ対象ホストが非モニタ対象サーバに接続するために使用するクライアントをシステムで識別できる場合、システムはクライアントの対応するアプリケーションプロトコルを識別することができますが、そのプロトコルをネットワークマップに追加することはありません。アプリケーション検出が発生するためには、クライアントセッションにサーバからの応答が含まれている必要があることに注意してください。

システムは、検出した各アプリケーションの特徴を把握します（[アプリケーションの特性（390ページ）](#)を参照）。システムはこれらの特徴を使用して、アプリケーションフィルタと呼ばれるアプリケーションのグループを作成します。アプリケーションフィルタは、アクセス制御するため、およびレポートとダッシュボードウィジェットで使用する検索結果とデータを制限するために使用されます。

また、エクスポートしたNetFlowレコード、Nmapのアクティブスキャン、ホスト入力機能を使用してアプリケーションディテクタデータを補完することもできます。

#### 関連トピック

[アプリケーションディテクタの基本](#)（2098ページ）

## アプリケーションディテクタの基本

Firepower システムは、アプリケーションディテクタを使用して、ネットワーク上で一般的に使用されるアプリケーションを識別します。[ディテクタ (Detectors)] ページ ([[ポリシー](#)



(Policies) ] > [アプリケーションディテクタ (Application Detectors) ] を使用してディテクタリストを表示し、検出機能をカスタマイズします。

ディテクタまたはその状態 (アクティブ/非アクティブ) を変更できるかどうかは、そのタイプによって異なります。システムは、アクティブなディテクタのみを使用して、アプリケーショントラフィックを分析します。



(注) シスコが提供するディテクタは、Firepower システムおよび VDB のアップデートによって変更される可能性があります。更新されたディテクタに関する情報については、リリースノートおよびアドバイザリを参照してください。

### シスコが提供する内部ディテクタ

内部ディテクタは、クライアント、Web アプリケーション、およびアプリケーションプロトコルのトラフィック用の特別なディテクタカテゴリです。内部ディテクタはシステムアップデートによって配信され、常にオンになっています。

### シスコが提供するクライアントディテクタ

クライアントディテクタは、クライアントトラフィックを検出し、VDB またはシステムアップデートを介して配信されるか、または Cisco Professional サービスによってインポート用に提供されます。クライアントディテクタを有効または無効にすることができます。インポートしたクライアントディテクタのみエクスポートできます。

### シスコが提供する Web アプリケーションディテクタ

Web アプリケーションディテクタは、HTTP トラフィックペイロード内の Web アプリケーションを検出し、VDB またはシステムアップデートを介して配信されます。Web アプリケーションディテクタは常にオンになっています。

### シスコが提供するアプリケーションプロトコル (ポート) ディテクタ

ポートベースのアプリケーションプロトコルディテクタは、ウェルノウンポートを使用してネットワークトラフィックを識別します。これらは VDB またはシステムアップデートを介して配信されるか、または Cisco Professional サービスによってインポート用に提供されます。アプリケーションプロトコルディテクタを有効または無効にしたり、カスタムディテクタの基礎として使用するためにディテクタ定義を表示することができます。

### シスコが提供するアプリケーションプロトコル (Firepower) ディテクタ

Firepower ベースのアプリケーションプロトコルディテクタは、Firepower アプリケーションフィンガープリントを使用してネットワークトラフィックを分析し、VDB またはシステムアップデートを介して配信されます。アプリケーションプロトコルディテクタを有効または無効にすることができます。

### カスタム アプリケーション デテクタ

カスタム アプリケーション デテクタはパターンベースです。クライアント、Web アプリケーション、またはアプリケーション プロトコルのトラフィックからのパケット内のパターンを検出します。インポートされたカスタム デテクタを完全に制御できます。

## Web インターフェイスでのアプリケーション プロトコルの識別

次の表に、Firepower システムが検出されたアプリケーション プロトコルを識別する方法について概略を示します。

表 219: Firepower システムのアプリケーション プロトコルの識別

ID	説明
アプリケーション プロトコル名	<p>Firepower Management Center は、次のアプリケーション プロトコルの場合に、名前でアプリケーション プロトコルを識別します。</p> <ul style="list-style-type: none"> <li>• システムによって肯定的に識別された</li> <li>• NetFlow データを使用して識別され、/etc/sf/services にポートとアプリケーション プロトコルの関連付けが存在する</li> <li>• ホスト入力機能を使用して手動で識別された</li> <li>• Nmap または別のアクティブな発生源によって識別された</li> </ul>
pending	<p>Firepower Management Center は、システムが肯定的と否定的のどちらでもアプリケーションを識別できない場合に、アプリケーション プロトコルを pending として識別します。</p> <p>多くの場合、システムが保留中のアプリケーションを識別するには、より多くの接続データを収集して分析する必要があります。</p> <p>[アプリケーションの詳細 (Application Details)] および [サーバ (Servers)] テーブルやホスト プロファイルで pending ステータスが表示されるのは、特定のアプリケーション プロトコルトラフィック (検出されたクライアントまたは Web アプリケーショントラフィックから推論されたトラフィック以外) が検出されたアプリケーション プロトコルだけです。</p>

ID	説明
不明	<p>Firepower Management Center は、以下の場合にアプリケーション プロトコルを <code>unknown</code> として識別します。</p> <ul style="list-style-type: none"> <li>• アプリケーションがシステムのディテクタのどれとも一致しない</li> <li>• アプリケーション プロトコルが NetFlow データを使用して識別されたものの、<code>/etc/sf/services</code> にポートとアプリケーション プロトコルの関連付けが存在しない</li> </ul>
空白	<p>使用可能なすべての検出データが検証されましたが、アプリケーション プロトコルが識別されませんでした。[アプリケーションの詳細 (Application Details)] および [サーバ (Servers)] テーブルとホストプロファイルでは、アプリケーション プロトコルが検出されなかった非 HTTP 汎用クライアントトラフィックに対して、アプリケーション プロトコルが空白として表示されます。</p>

## クライアント検出からの暗黙的アプリケーション プロトコル検出

非監視対象サーバにアクセスするために監視対象ホストが使用しているクライアントをシステムが識別できる場合、Firepower Management Center はその接続でクライアントに対応するアプリケーション プロトコルが使用されていると推測します (システムは監視対象ネットワーク上のアプリケーションだけを追跡するため、通常、接続ログには監視対象ホストが非監視対象サーバにアクセスしている接続に関するアプリケーション プロトコル情報が含まれていません)。

暗黙的アプリケーション プロトコル検出と呼ばれるこのプロセスの結果は次のようになります。

- システムはこれらのサーバの New TCP Port イベントまたは New UDP Port イベントを生成しないため、サーバが [サーバ (Servers)] テーブルに表示されません。加えて、これらのアプリケーション プロトコルの検出を基準にして、検出イベントアラートまたは相関ルールをトリガーすることはできません。
- アプリケーション プロトコルはホストに関連付けられないため、ホスト プロファイルの詳細を表示したり、サーバ ID を設定したり、トラフィック プロファイルまたは相関ルールに関するホストプロファイル資格内の情報を使用したりできません。加えて、システムはこの種の検出に基づいて脆弱性とホストを関連付けません。

ただし、アプリケーション プロトコル情報が接続内に存在するかどうかに対する相関イベントをトリガーできます。また、接続ログ内のアプリケーション プロトコル情報を使用して、接続トラッカーとトラフィック プロファイルを作成できます。

## ホスト制限と検出イベント ロギング

システムがクライアント、サーバ、または Web アプリケーションを検出すると、関連するホストがすでにクライアント、サーバ、または Web アプリケーションの最大数に達していなければ、検出イベントが生成されます。

ホストプロファイルには、ホストごとに最大 16 のクライアント、100 のサーバ、および 100 の Web アプリケーションが表示されます。

クライアント、サーバ、または Web アプリケーションの検出によって異なるアクションはこの制限の影響を受けないことに注意してください。たとえば、サーバ上でトリガーするように設定されたアクセスコントロールルールでは、引き続き、接続イベントが記録されます。

## アプリケーション検出に関する特殊な考慮事項

### Squid

システムは、次のいずれかの場合に Squid サーバトラフィックを肯定的に識別します。

- モニタ対象ネットワーク上のホストからプロキシ認証が有効になっている Squid サーバへの接続をシステムが検出した場合
- モニタ対象ネットワーク上の Squid プロキシサーバからターゲットシステム（つまり、クライアントが情報または別のリソースを要求する宛先サーバ）への接続をシステムが検出した場合

ただし、システムは次の場合に Squid サービストラフィックを識別できません。

- モニタ対象ネットワーク上のホストが、プロキシ認証が無効になっている Squid サーバに接続している場合
- Squid プロキシサーバが HTTP 応答から **Via:** ヘッダーフィールドを除去するように設定されている場合

### SSL アプリケーション検出

システムは、Secure Socket Layer (SSL) セッションからのセッション情報を使用してセッション内のアプリケーションプロトコル、クライアントアプリケーション、または Web アプリケーションを識別するアプリケーションディテクタを備えています。

システムは暗号化された接続を検出すると、その接続を汎用 HTTPS 接続として、または、該当する場合には SMTPS などのより特殊なセキュアプロトコルとしてマークします。システムは SSL セッションを検出すると、そのセッションに対する接続イベント内の [クライアント (Client)] フィールドに `ssl client` を追加します。セッションの Web アプリケーションが識別されると、システムでトラフィックの検出イベントが生成されます。

SSL アプリケーショントラフィックの場合は、管理対象デバイスも、サーバ証明書から一般名を検出して SSL ホストパターンからのクライアントまたは Web アプリケーションと照合でき

ます。システムが特定のクライアントを識別すると、SSL client をそのクライアントの名前に置き換えます。

SSL アプリケーショントラフィックは暗号化されるため、システムは暗号化されたストリーム内のアプリケーションデータではなく、証明書内の情報しか識別に使用できません。そのため、SSL ホストパターンではアプリケーションを制作した会社しか識別できない場合があり、同じ会社が作成した SSL アプリケーションは識別情報が同じ可能性があります。

HTTPS セッションが HTTP セッション内から起動される場合などは、管理対象デバイスがクライアント側のパケット内のクライアント証明書からサーバ名を検出します。

SSL アプリケーション識別を有効にするには、応答側のトラフィックをモニタするアクセスコントロールルールを作成する必要があります。このようなルールには、SSL アプリケーションに関するアプリケーション条件または SSL 証明書からの URL を使用した URL 条件を含める必要があります。ネットワーク検出では、応答側の IP アドレスがネットワーク上に存在しなくても、ネットワーク検出ポリシーでモニタできます。アクセスコントロールポリシーの設定によって、トラフィックが識別されるかどうかが決まります。SSL アプリケーションの検出を識別するには、アプリケーションディテクタリストで、または、アプリケーション条件をアクセスコントロールルールに追加するときに、SSL protocol タグでフィルタ処理します。

### 参照先 Web アプリケーション

Web サーバがトラフィックを他の Web サイト（通常は、アドバタイズメントサーバ）に参照する場合があります。ネットワーク上で発生するトラフィック参照のコンテキストをわかりやすくするために、システムは、参照セッションに対するイベント内の [Web アプリケーション (Web Application)] フィールドにトラフィックを参照した Web アプリケーションを列挙します。VDB に既知の参照先サイトのリストが含まれています。システムがこのようなサイトのいずれかからのトラフィックを検出すると、参照元サイトがそのトラフィックに対するイベントと一緒に保存されます。たとえば、Facebook 経由でアクセスされるアドバタイズメントが実際は Advertising.com 上でホストされている場合は、検出された Advertising.com トラフィックが Facebook Web アプリケーションに関連付けられます。また、システムは、Web サイトで他のサイトへの単リンクが提供されている場合などは、HTTP トラフィック内の参照元 URL を検出することもできます。この場合、参照元 URL は [HTTP 参照元 (HTTP Referrer)] イベントフィールドに表示されます。

イベントでは、参照元アプリケーションが存在する場合に、それがトラフィックの Web アプリケーションとして列挙されますが、URL は参照先サイトの URL です。上の例では、トラフィックに対する接続イベントの Web アプリケーションは Facebook ですが、URL は Advertising.com です。参照元 Web アプリケーションが検出されない場合、ホストが自身を参照している場合、または参照がチェインしている場合は、参照先アプリケーションが Web アプリケーションとして表示される場合もあります。ダッシュボードでは、Web アプリケーションの接続カウントとバイトカウントに、Web アプリケーションが参照先のトラフィックに関連付けられたセッションが含まれます。

参照先トラフィックに対して明示的に機能するルールを作成する場合は、参照元アプリケーションではなく、参照先アプリケーションに関する条件を追加する必要があることに注意してください。Facebook から参照される Advertising.com トラフィックをブロックするには、

Advertising.com アプリケーションのアクセス コントロール ルールにアプリケーション条件を追加します。

## カスタム アプリケーション ディテクタ

ネットワーク上でカスタムアプリケーションを使用する場合、アプリケーションの識別に必要な情報をシステムに提供するカスタム Web アプリケーション、クライアント、またはアプリケーションプロトコルディテクタを作成します。アプリケーションディテクタの種類は、[プロトコル (Protocol) ]、[タイプ (Type) ]、および [検出方向 (Direction) ] フィールドで選択した内容によって決まります。

システムがサーバトラフィックでアプリケーションプロトコルの検出および識別を開始するように、クライアントセッションにサーバからの応答パケットを含める必要があります。UDP トラフィックの場合、応答パケットの送信元がサーバとして指定されることに注意してください。

すでに別の Firepower Management Center にディテクタを作成している場合、そのディテクタをエクスポートして、この Firepower Management Center にインポートすることができます。その後、必要に応じてインポートしたディテクタを編集できます。カスタムディテクタおよび Cisco Professional サービスが提供するディテクタをエクスポートおよびインポートすることができます。ただし、シスコが提供するその他の種類のディテクタをエクスポートおよびインポートすることはできません。

## カスタム アプリケーション ディテクタおよびユーザ定義アプリケーション フィールド

次のフィールドを使用して、カスタム アプリケーション ディテクタおよびユーザ定義アプリケーションを設定できます。

### カスタム アプリケーション ディテクタ フィールド：概要

基本および高度なカスタム アプリケーション ディテクタを設定するには、次のフィールドを使用します。

#### アプリケーション プロトコル (Application Protocol)

検出するアプリケーションプロトコル。これには、システムが提供するアプリケーションまたはユーザ定義のアプリケーションを指定できます。

アプリケーションを (アイデンティティルールで設定された) アクティブな認証から除外できるようにする場合は、**User-Agent Exclusion** タグを使用してアプリケーションプロトコルを選択するか、作成する必要があります。

#### 説明

アプリケーション ディテクタの説明。

### [名前 (Name) ]

アプリケーションディテクタの名前。

### ディテクタタイプ (Detector Type)

ディテクタのタイプ ([基本 (Basic) ]または[高度 (Advanced) ])。基本的なアプリケーションディテクタは、一連のフィールドとして Web インターフェイスで作成されます。高度なアプリケーションディテクタは、外部で作成され、カスタム .lua ファイルとしてアップロードされます。

### カスタムアプリケーションディテクタ (Custom Application Detector) フィールド：検出パターン

基本的なカスタムアプリケーションディテクタの検出パターンを設定するには、次のフィールドを使用します。

#### 方向 (Direction)

ディテクタが検出するトラフィックの送信元。[クライアント (Client) ]または[サーバ (Server) ]。

#### オフセット (Offset)

システムがパターンの検索を開始する必要がある、パケットペイロードの先頭からのパケットの場所 (バイト単位)。

パケットペイロードは0バイトから始まるため、パケットペイロードの先頭から数えたバイト数から1を減算することでオフセットを計算します。たとえば、パケットの5桁目のビットパターンを検索するには、[オフセット (Offset) ]フィールドに「4」と入力します。

#### パターン

パターン文字列は、選択した [タイプ (Type) ]に関連付けられます。

#### ポート

ディテクタが検出するトラフィックのポート。

#### プロトコル

検出するプロトコル。選択するプロトコルによって、[タイプ (Type) ]フィールドが表示されるか [URL (URL) ]フィールドが表示されるかが決まります。

プロトコル (および、場合によっては、[タイプ (Type) ]フィールドと [方向 (Direction) ]フィールドの後続の選択) によって、作成するアプリケーションディテクタのタイプ (Web アプリケーション、クライアント、またはアプリケーションプロトコル) が決まります。

ディテクタタイプ (Detector Type)	プロトコル	タイプ (Type) または 方向 (Direction)
Web アプリケーション (Web Application)	HTTP	[タイプ (Type)] は [コンテンツ タイプ (Content Type)] または [URL (URL)] です。
	RTMP	任意 (Any)
	SSL	任意 (Any)
クライアント (Client)	HTTP	[タイプ (Type)] は [ユーザ エージェント (User Agent)] です。
	SIP	任意 (Any)
	TCP または UDP	[方向 (Direction)] は [クライアント (Client)] です。
アプリケーションプロトコル (Application Protocol)	TCP または UDP	[方向 (Direction)] は [サーバ (Server)] です。

### タイプ (Type)

入力したパターン文字列のタイプ。表示されるオプションは、選択した [プロトコル (Protocol)] によって決まります。プロトコルとして [RTMP (RTMP)] を選択すると、[タイプ (Type)] フィールドの代わりに [URL (URL)] フィールドが表示されます。



(注) [タイプ (Type)] として [ユーザ エージェント (User Agent)] を選択すると、システムはアプリケーションの [タグ (Tag)] を **User-Agent Exclusion** に自動的に設定します。

タイプの選択	文字列特性
<b>Ascii</b>	文字列は ASCII でエンコードされます。
<b>Common Name</b>	文字列は、サーバ応答メッセージ内の commonName フィールドの値です。
<b>コンテンツ タイプ (Content Type)</b>	文字列は、サーバ応答ヘッダー内のコンテンツ タイプ フィールドの値です。
<b>16 進数</b>	文字列は、16 進表記です。
<b>組織</b>	文字列は、サーバ応答メッセージ内の organizationName フィールドの値です。



タイプの選択	文字列特性
SIP サーバ	文字列は、メッセージヘッダー内の From フィールドの値です。
SSL ホスト (SSL Host)	文字列は、ClientHello メッセージ内の server_name フィールドの値です。
URL	文字列は URL です。  (注) ディテクタは、ユーザが入力する文字列が URL の完全なセクションであると想定します。たとえば、 <b>cisco.com</b> と入力した場合、 <b>www.cisco.com/support</b> や <b>www.cisco.com</b> と一致しますが、 <b>www.wearecisco.com</b> とは一致しません。
ユーザ エージェント (User Agent)	文字列は、GET リクエストヘッダー内の user-agent フィールドの値です。これは SIP プロトコルにも使用可能であり、文字列が SIP メッセージヘッダー内の User-Agent フィールドの値であることを示します。

## URL

RTMP パケットの C2 メッセージ内の swfURL フィールドの完全な URL または URL のセクション。[プロトコル (Protocol) ] として [RTMP (RTMP) ] を選択すると、[タイプ (Type) ] フィールドの代わりにこのフィールドが表示されます。



- (注) ディテクタは、ユーザが入力する文字列が URL の完全なセクションであると想定します。たとえば、**cisco.com** と入力した場合、**www.cisco.com/support** や **www.cisco.com** と一致しますが、**www.wearecisco.com** とは一致しません。

## ユーザ定義のアプリケーションフィールド

基本および高度なカスタムアプリケーションディテクタでユーザ定義のアプリケーションを設定するには、次のフィールドを使用します。

### ビジネスとの関連性 (Business Relevance)

アプリケーションが娯楽ではなく組織のビジネス活動のコンテキストで使用される可能性。[非常に高い (Very High) ]、[高 (High) ]、[中 (Medium) ]、[低 (Low) ]、または [非常に低い (Very Low) ]。アプリケーションを最も的確に説明するオプションを選択します。

### カテゴリ (Categories)

アプリケーションの最も重要な機能を説明する一般分類。

**説明**

アプリケーションの説明。

**[名前 (Name) ]**

アプリケーションの名前。

**リスク (Risk)**

アプリケーションが組織のセキュリティポリシーに対抗する目的で使用される可能性。  
[非常に高い (Very High) ]、[高 (High) ]、[中 (Medium) ]、[低 (Low) ]または[非常に低い (Very Low) ]。アプリケーションを最も的確に説明するオプションを選択します。

**タグ (Tags)**

アプリケーションに関する追加情報を提供する 1 つ以上の事前定義されたタグ。アプリケーションを (アイデンティティルールで設定された) アクティブな認証から除外できるようにする場合は、**User-Agent Exclusion** タグをアプリケーションに追加する必要があります。

## カスタムアプリケーションディテクタの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

基本または高度なカスタムアプリケーションディテクタを設定できます。

**手順**

- ステップ 1** [ポリシー (Policies) ] > [アプリケーションディテクタ (Application Detectors) ] を選択します。
- ステップ 2** [カスタムディテクタの作成 (Create Custom Detector) ] をクリックします。
- ステップ 3** [名前 (Name) ] と [説明 (Description) ] を入力します。
- ステップ 4** [アプリケーションプロトコル (Application Protocol) ] を選択します。次の選択肢があります。
  - 既存のアプリケーションプロトコルのディテクタを作成する場合 (たとえば、非標準ポートで特定のアプリケーションプロトコルを検出する場合)、ドロップダウンリストからアプリケーションプロトコルを選択します。
  - ユーザ定義アプリケーションのディテクタを作成する場合は、[ユーザ定義のアプリケーションの作成 \(2109 ページ\)](#) に示されている手順に従います。
- ステップ 5** [ディテクタタイプ (Detector Type) ] を選択します。
- ステップ 6** [OK] をクリックします。

**ステップ7** [検出パターン (Detection Patterns) ]または[検出基準 (Detection Criteria) ]を設定します。

- 基本ディテクタを設定する場合は、[基本ディテクタでの検出パターンの指定 \(2111ページ\)](#)の説明に従って、プリセットした[検出パターン (Detection Patterns) ]を指定します。
- 高度なディテクタを設定する場合は、[高度なディテクタでの検出条件の指定 \(2112ページ\)](#)の説明に従って、カスタム[検出基準 (Detection Criteria) ]を指定します。

**注意** 高度なカスタムディテクタは複雑で、有効な.luaファイルを作成すること以外の知識も必要になります。ディテクタを誤って設定すると、パフォーマンスや検出機能にマイナスの影響を与える可能性があります。

**ステップ8** 必要に応じて、[カスタムアプリケーションプロトコルディテクタのテスト \(2113ページ\)](#)の説明に従って、[パケット キャプチャ (Packet Captures) ]を使用して新しいディテクタをテストします。

**ステップ9** [保存 (Save) ]をクリックします。

(注) アクセス コントロールルールにアプリケーションを含めると、ディテクタは自動的にアクティブにされ、使用中は非アクティブにできません。

#### 次のタスク

- [ディテクタのアクティブおよび非アクティブの設定 \(2118ページ\)](#)の説明に従ってディテクタをアクティブにします。

#### 関連トピック

[カスタムアプリケーションディテクタおよびユーザ定義アプリケーションフィールド \(2104ページ\)](#)

## ユーザ定義のアプリケーションの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

ここで作成するアプリケーション、カテゴリ、およびタグは、アクセス コントロールルールやアプリケーションフィルタ オブジェクト マネージャで使用できます。



**注意** ユーザ定義アプリケーションを作成すると、展開プロセスを経由することなく、ただちに Snort プロセスが再起動します。Snort プロセスが再起動すると、すべての管理対象デバイスでトラフィックインスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### 始める前に

- [カスタムアプリケーションディテクタの設定 \(2108 ページ\)](#) の説明に従って、カスタムアプリケーションプロトコルディテクタの設定を開始します。

### 手順

- ステップ 1** [ディテクタの作成 (Create Detector) ] ページで、[追加 (Add) ] をクリックします。
- ステップ 2** [名前 (Name) ] を入力します。
- ステップ 3** [説明 (Description) ] を入力します。
- ステップ 4** [ビジネスとの関連性 (Business Relevance) ] を選択します。
- ステップ 5** [リスク (Risk) ] を選択します。
- ステップ 6** [カテゴリ (Categories) ] の横にある [追加 (Add) ] をクリックしてカテゴリを追加し、新しいカテゴリの名前を入力するか、または [カテゴリ (Categories) ] ドロップダウンリストから既存のカテゴリを選択します。
- ステップ 7** オプションで、[タグ (Tags) ] の横にある [追加 (Add) ] をクリックしてタグを追加し、新しいタグの名前を入力するか、または [タグ (Tags) ] ドロップダウンリストから既存のタグを選択します。
- ステップ 8** [OK] をクリックします。

### 次のタスク

- [カスタムアプリケーションディテクタの設定 \(2108 ページ\)](#) の説明に従って、カスタムアプリケーションプロトコルディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

### 関連トピック

[カスタムアプリケーションディテクタおよびユーザ定義アプリケーションフィールド \(2104 ページ\)](#)

## 基本ディテクタでの検出パターンの指定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

アプリケーションプロトコルのパケットヘッダーで特定のパターン文字列を検索するよう、カスタムアプリケーションプロトコルディテクタを設定できます。また、複数のパターンを検索するようにディテクタを設定することもできます。この場合は、アプリケーションプロトコルのトラフィックは、アプリケーションプロトコルを確実に識別するため、ディテクタのすべてのパターンとマッチングさせる必要があります。

アプリケーションプロトコルディテクタは、オフセットを使用してASCIIまたは16進数のパターンを検索できます。

### 始める前に

- [カスタムアプリケーションディテクタの設定 \(2108 ページ\)](#) の説明に従って、カスタムアプリケーションプロトコルディテクタの設定を開始します。

### 手順

- ステップ 1** [ディテクタの作成 (Create Detector)] ページの [検出パターン (Detection Patterns)] セクションで、[追加 (Add)] をクリックします。
- ステップ 2** ディテクタの検査対象とするトラフィックの [プロトコル (Protocol)] を選択します。
- ステップ 3** ユーザが検出するパターン [タイプ (Type)] を指定します。
- ステップ 4** 指定した [タイプ (Type)] に一致する [パターン文字列 (Pattern String)] を入力します。
- ステップ 5** オプションで、[オフセット (Offset)] を入力します (バイト単位)。
- ステップ 6** オプションで、使用するポートに基づいてアプリケーションプロトコルのトラフィックを指定するには、1 から 65535 までのポートを [ポート (Port(s))] フィールドに入力します。複数のポートを使用する場合は、カンマで区切ります。
- ステップ 7** オプションで、[クライアント (Client)] または [サーバ (Server)] のいずれかの [方向 (Direction)] を選択します。
- ステップ 8** [OK] をクリックします。

**ヒント** パターンを削除する場合、削除するパターンの横の削除アイコン (🗑️) をクリックします。

## 次のタスク

- [カスタムアプリケーションディテクタの設定 \(2108 ページ\)](#) の説明に従って、カスタムアプリケーションプロトコルディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

## 関連トピック

[高度なディテクタでの検出条件の指定 \(2112 ページ\)](#)

## 高度なディテクタでの検出条件の指定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin



**注意** 高度なカスタムディテクタは複雑で、有効な .lua ファイルを作成すること以外の知識も必要になります。ディテクタを誤って設定すると、パフォーマンスや検出機能にマイナスの影響を与える可能性があります。



**注意** 信頼できないソースから .lua ファイルをアップロードしないでください。

カスタム .lua ファイルには、カスタムアプリケーションのディテクタ設定を含めます。カスタム .lua ファイルを作成するには、lua プログラミング言語に関する高度な知識とシスコの C-lua API に関する経験が求められます。以下を使用して、.lua ファイルを準備することを強くお勧めします。

- lua プログラミング言語に関するサードパーティの説明書と参考資料
- オープンソースディテクタ開発者ガイド：<https://www.snort.org/downloads>
- OpenAppID Snort コミュニティリソース：<http://blog.snort.org/search/label/openappid>



(注) システムは、システムコールまたはファイル I/O を参照する .lua ファイルをサポートしていません。

## 始める前に

- [カスタムアプリケーションディテクタの設定 \(2108 ページ\)](#) の説明に従って、カスタムアプリケーションプロトコルディテクタの設定を開始します。

- 該当する .lua ファイルをダウンロードし、内容を調べることによって、有効な .lua ファイルを作成する準備を進めます。ディテクタファイルのダウンロードの詳細については、[ディテクタ詳細の表示またはダウンロード \(2114 ページ\)](#) を参照してください。
- カスタムアプリケーションのディテクタ設定を含む有効な .lua ファイルを作成します。

## 手順

- ステップ 1** 高度なカスタムアプリケーションディテクタの [ディテクタの作成 (Create Detector)] ページにある [検出条件 (Detection Criteria)] セクションで、[追加 (Add)] をクリックします。
- ステップ 2** [参照... (Browse...)] をクリックして、.lua ファイルに移動し、アップロードします。
- ステップ 3** [OK] をクリックします。

## 次のタスク

- [カスタムアプリケーションディテクタの設定 \(2108 ページ\)](#) の説明に従って、カスタムアプリケーションプロトコルディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

## 関連トピック

[基本ディテクタでの検出パターンの指定 \(2111 ページ\)](#)

## カスタムアプリケーションプロトコルディテクタのテスト

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

検出するアプリケーションプロトコルからのトラフィックを持つパケットが格納されたパケットキャプチャ (pcap) ファイルが存在する場合、その pcap ファイルに対してカスタムアプリケーションプロトコルディテクタをテストできます。シスコでは、不要なトラフィックのない単純でクリーンな pcap ファイルを使用することをお勧めします。

pcap ファイルは 256 KB 以下でなければなりません。それより大きい pcap ファイルに対してディテクタのテストを試行すると、Firepower Management Center は自動的にファイルを切り捨て、不完全なファイルをテストします。ディテクタをテストするためにファイルを使用する前に、pcap の未解決のチェックサムを修正する必要があります。

## 始める前に

- [カスタムアプリケーションディテクタの設定 \(2108 ページ\)](#) の説明に従って、カスタムアプリケーションプロトコルディテクタを設定します。

## 手順

- 
- ステップ 1** [ディテクタの作成 (Create Detector)] ページの [パケットキャプチャ (Packet Captures)] セクションで、[追加 (Add)] をクリックします。
- ステップ 2** ポップアップ ウィンドウで pcap ファイルを参照し、[OK] をクリックします。
- ステップ 3** pcap ファイルの内容に対してディテクタをテストするには、pcap ファイルの横にある評価アイコンをクリックします。メッセージに、テストが成功したかどうかを示されます。
- ステップ 4** 必要に応じて手順 1 ~ 3 を繰り返し、その他の pcap ファイルに対してディテクタをテストします。

**ヒント** pcap ファイルを削除するには、削除するファイルの横の削除アイコン (🗑️) をクリックします。

---

## 次のタスク

- [カスタムアプリケーションディテクタの設定 \(2108 ページ\)](#) の説明に従って、カスタムアプリケーションプロトコルディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

## ディテクタ詳細の表示またはダウンロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

ディテクタ リストを使用して、アプリケーションディテクタの詳細を表示 (すべてのディテクタ) したり、ディテクタの詳細をダウンロード (カスタムアプリケーションディテクタのみ) したりできます。

## 手順

- 
- ステップ 1** [ポリシー (Policies)] > [アプリケーションディテクタ (Application Detectors)] を選択します。
- ステップ 2** ディテクタの詳細を表示するには、情報アイコン (i) をクリックして、[概要: アプリケーション検出 \(2097 ページ\)](#) で説明されているリスク、ビジネスとの関連性、タグ、カテゴリを表示します。



- ステップ3** カスタムアプリケーションディテクタのディテクタ詳細をダウンロードするには、ダウンロードアイコン (📄) をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

## ディテクタ リストのソート

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

[ディテクタ (Detectors)] ページには、デフォルトで名前のアルファベット順にディテクタがリストされます。列見出しの横にある上または下矢印は、ページがその列でその方向にソートされていることを示します。

### 手順

- ステップ1** [ポリシー (Policies)] > [アプリケーション ディテクタ (Application Detectors)] を選択します。
- ステップ2** 該当する列見出しをクリックします。

## 検出機能リストのフィルタリング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

### 手順

- ステップ1** [ポリシー (Policies)] > [アプリケーション ディテクタ (Application Detectors)] を選択します。
- ステップ2** [ディテクタリストのフィルタグループ \(2116ページ\)](#) に記載されているフィルタグループの1つを展開し、フィルタの横にあるチェックボックスを選択します。グループ内のすべてのフィルタを選択するには、グループ名を右クリックし、[すべて選択 (Check All)] を選択します。

- ステップ 3** あるフィルタを削除するには、[フィルタ (Filters)] フィールドにあるフィルタの名前の削除アイコン (✖) をクリックするか、フィルタ リストでフィルタを無効にします。グループ内のすべてのフィルタを削除するには、グループ名を右クリックし、[すべて選択解除 (Uncheck All)] を選択します。
- ステップ 4** すべてのフィルタを削除するには、検出機能に適用されるフィルタ リストの横の [すべてクリア (Clear all)] をクリックします。

## ディテクタ リストのフィルタ グループ

複数のフィルタ グループを別個にまたは組み合わせて使用し、ディテクタのリストをフィルタリングすることができます。

### [名前 (Name)]

ユーザが入力した文字列を含む名前または説明でディテクタを検索します。文字列には任意の英数字または特殊文字を含めることができます。

### カスタム フィルタ (Custom Filter)

オブジェクト管理ページで作成したカスタム アプリケーション フィルタに一致するディテクタを検索します。

### 作成者 (Author)

ディテクタを作成したユーザに照らしてディテクタを検索します。次によってディテクタをフィルタリングできます。

- カスタム ディテクタを作成またはインポートした個々のユーザ
- シスコ。これは、個別にインポートされたアドオンディテクタを除く、シスコが提供するすべてのディテクタを表します (ディテクタをインポートした場合、そのユーザはそのディテクタの作成者になります)。
- 任意のユーザ (Any User)。これは、によって提供されたのではないすべてのディテクタを表します。

### 状態 (State)

状態 (つまり、アクティブまたは非アクティブ) に照らしてディテクタを検索します。

### タイプ (Type)

[アプリケーションディテクタの基本 \(2098ページ\)](#) に示すように、ディテクタタイプに従ってディテクタを検索します。

### プロトコル

ディテクタが検査するトラフィック プロトコルに照らしてディテクタを検索します。

### カテゴリ (Category)

検出するアプリケーションに割り当てられたカテゴリに照らしてディテクタを検索します。

### タグ

検出するアプリケーションに割り当てられたタグに照らしてディテクタを検索します。

### リスク

検出するアプリケーションに割り当てられたリスク ([非常に高い (Very High) ]、[高 (High) ]、[中 (Medium) ]、[低 (Low) ]、[非常に低い (Very Low) ]) に照らしてディテクタを検索します。

### ビジネスとの関連性 (Business Relevance)

検出するアプリケーションに割り当てられたビジネスとの関連性 ([非常に高い (Very High) ]、[高 (High) ]、[中 (Medium) ]、[低 (Low) ]、[非常に低い (Very Low) ]) に照らしてディテクタを検索します。

## 別のディテクタ ページへの移動

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

### 手順

- ステップ 1 [ポリシー (Policies) ] > [アプリケーション ディテクタ (Application Detectors) ] を選択します。
- ステップ 2 次のページを表示するには、右下矢印アイコン (➤) をクリックします。
- ステップ 3 前のページを表示するには、左矢印のアイコン (➤) をクリックします。
- ステップ 4 別のページを表示するには、ページ番号を入力して、Enter キーを押します。
- ステップ 5 最後のページに移動するには、右矢印アイコン (➤) をクリックします。
- ステップ 6 最初のページに移動するには、左矢印アイコン (➤) をクリックします。

## ディテクタのアクティブおよび非アクティブの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

ネットワークトラフィックを分析するためにディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブにされています。

システムの検出機能を補完するために、ポートごとに複数のアプリケーションディテクタをアクティブにすることができます。

ポリシーのアクセスコントロールルールにアプリケーションを含め、そのポリシーを導入するときに、そのアプリケーションに対してアクティブなディテクタがない場合、1つ以上のディテクタが自動的にアクティブになります。同様に、導入されているポリシーのアプリケーションが使用されているときに、そのアプリケーションのアクティブなディテクタをすべて非アクティブにしようとしても、ディテクタを非アクティブにすることはできません。



**ヒント** パフォーマンスを向上させるために、使用する予定のないアプリケーションプロトコル、クライアント、または Web アプリケーションのディテクタはすべて非アクティブにします。



**注意** システムまたはカスタムのアプリケーションディテクタをアクティブ化/非アクティブ化すると、展開プロセスを経由することなく、ただちに Snort プロセスが再起動します。Snort プロセスが再起動すると、すべての管理対象デバイスでトラフィックインスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### 手順

- ステップ 1** [ポリシー (Policies)] > [アプリケーションディテクタ (Application Detectors)] を選択します。
- ステップ 2** アクティブまたは非アクティブにするディテクタの横にあるスライダをクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

(注) 一部のアプリケーションディテクタはその他のディテクタによって必要とされることに注意してください。そのようなディテクタのいずれかを非アクティブにすると、それに依存するディテクタも無効となることを示す警告が表示されます。

## カスタムアプリケーションディテクタの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

カスタムアプリケーションディテクタを変更するには、次の手順を使用します。

### 手順

- ステップ 1** [ポリシー (Policies)] > [アプリケーションディテクタ (Application Detectors)] を選択します。
- ステップ 2** 変更するディテクタの横にある編集アイコン (✎) をクリックします。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3** [カスタムアプリケーションディテクタの設定 \(2108 ページ\)](#) の説明に従って、ディテクタを変更します。
- ステップ 4** ディテクタの状態に応じて、次の保存オプションがあります。
  - 非アクティブなディテクタを保存するには、[保存 (Save)] をクリックします。
  - 非アクティブなディテクタを新規の非アクティブなディテクタとして保存するには、[新規保存 (Save as New)] をクリックします。
  - アクティブなディテクタを保存してすぐに使用を開始するには、[保存して再アクティブ化 (Save and Reactivate)] をクリックします。

**注意** カスタムアプリケーションディテクタを保存して再びアクティブ化すると、展開プロセスを経由することなく、ただちに Snort プロセスが再起動します。Snort プロセスが再起動すると、すべての管理対象デバイスでトラフィックインスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

- アクティブなディテクタを新規の非アクティブなディテクタとして保存するには、[新規保存 (Save as New)] をクリックします。

## ディテクタの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

カスタムディテクタおよび Cisco Professional サービスが提供する個別にインポートされたアドオンディテクタを削除することができます。その他の Cisco が提供するディテクタを削除することはできませんが、その多くを非アクティブにすることはできます。



(注) ディテクタが展開されたポリシーで使用されている間は、そのディテクタを削除できません。



**注意** アクティブ化されたカスタム アプリケーションディテクタを削除すると、展開プロセスを経由することなく、ただちに Snort プロセスが再起動します。Snort プロセスが再起動すると、すべての管理対象デバイスでトラフィックインスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### 手順

- ステップ 1** [ポリシー (Policies)] > [アプリケーションディテクタ (Application Detectors)] を選択します。
- ステップ 2** 削除するディテクタの横にある削除アイコン (🗑️) をクリックします。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3** [OK] をクリックします。



## 第 87 章

# ユーザ アイデンティティ ソース

以下のトピックでは、ユーザ認識のソースである、Firepower システム ユーザのアイデンティティ ソースについて説明しています。これらのユーザは、アイデンティティおよびアクセスコントロール ポリシーで制御できます。

- [ユーザ アイデンティティ ソースについて \(2121 ページ\)](#)
- [ユーザ エージェントのアイデンティティ ソース \(2123 ページ\)](#)
- [ISE アイデンティティ ソース \(2126 ページ\)](#)
- [ターミナル サービス \(TS\) エージェントのアイデンティティ ソース \(2131 ページ\)](#)
- [キャプティブ ポータルのアイデンティティ ソース \(2133 ページ\)](#)
- [トラフィック ベース検出のアイデンティティ ソース \(2143 ページ\)](#)

## ユーザ アイデンティティ ソースについて

次の表に、Firepower システムでサポートされているユーザ アイデンティティ ソースの概要を示します。各アイデンティティ ソースは、ユーザ認識のためのユーザの記憶域を提供します。これらのユーザは、アイデンティティおよびアクセスコントロールポリシーで制御できます。

ユーザ アイデンティティ ソース	ポリシー	サーバ要件	タイプ (Type)	認証タイプ (Authentication Type)	ユーザ認識	ユーザ制御	詳細
ユーザ エージェント	アイデンティティ	Microsoft Active Directory	権限のあるログイン	パッシブ	○	○	<a href="#">ユーザ エージェントのアイデンティティ ソース (2123 ページ)</a>

ユーザアイデンティティソース	ポリシー	サーバ要件	タイプ (Type)	認証タイプ (Authentication Type)	ユーザ認識	ユーザ制御	詳細
ISE	アイデンティティ	Microsoft Active Directory	権限のあるログイン	パッシブ	○	○	<a href="#">ISE アイデンティティソース (2126 ページ)</a>
TS エージェント	アイデンティティ	Microsoft Windows Terminal Server	権限のあるログイン	パッシブ	○	○	<a href="#">ターミナルサービス (TS) エージェントのアイデンティティソース (2131 ページ)</a>
キャプティブポータル	アイデンティティ	LDAP または Microsoft Active Directory	権限のあるログイン	Active	○	○	<a href="#">キャプティブポータルのアイデンティティソース (2133 ページ)</a>
トラフィックベースの検出	ネットワーク検出	適用対象外	権限のないログイン	適用対象外	[はい (Yes) ]	[いいえ (No) ]	<a href="#">トラフィックベース検出のアイデンティティソース (2143 ページ)</a>

展開するアイデンティティソースを選択する際には、以下を検討してください。

- 非 LDAP ユーザログインにはトラフィックベースの検出を使用する必要があります。たとえば、ユーザエージェントのみを使用してユーザアクティビティを検出している場合は、非 LDAP ログインを制限しても効果はありません。
- 失敗したログインまたは認証アクティビティを記録するには、トラフィックベースの検出またはキャプティブポータルを使用する必要があります。失敗したログインまたは認証試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。



- キャプティブ ポータルのアイデンティティ ソースには、ルーテッドインターフェイスを備えた管理対象デバイスが必要です。キャプティブ ポータルでインライン（タップ モードとも呼ばれます）インターフェイスを使用することはできません。

これらのアイデンティティ ソースからのデータは、Firepower Management Center のユーザデータベースとユーザアクティビティ データベースに格納されます。Firepower Management Center サーバユーザダウンロードを設定して、新しいユーザ データがデータベースに自動的かつ定期的にダウンロードされるようにできます。

必要なアイデンティティ ソースを使用してアイデンティティ ルールを設定したら、各ルールにアクセス コントロール ポリシーを関連付け、ポリシーを有効にするために管理対象デバイスに展開する必要があります。アクセスコントロールポリシーおよび展開の詳細については、[ユーザ条件、レルム条件、およびISE 属性条件（ユーザ制御）](#)（401 ページ）を参照してください。

Firepower システムでのユーザ検出の一般情報については、[ユーザ アイデンティティについて](#)（2031 ページ）を参照してください。

## ユーザ エージェントのアイデンティティ ソース

ユーザエージェントは、パッシブ認証方法で、信頼できるアイデンティティ ソース（つまり、信頼された Active Directory サーバでユーザ情報が提供されます）でもあります。ユーザ エージェントは、Firepower システムと統合されると、ユーザが Active Directory クレデンシャルでホストにログインする、またはホストからログアウトするときに、そのユーザをモニタします。ユーザエージェントから取得されたデータは、ユーザ認識とユーザ制御に使用できます。

ユーザ エージェントは、各ユーザを IP アドレスと関連付けます。これにより、ユーザ条件を使用するアクセスコントロールルールをトリガーすることができます。1つのユーザ エージェントを使用して、最大5つの Active Directory サーバでユーザ アクティビティをモニタでき、最大5つの Firepower Management Center に暗号化データを送信できます。

ユーザ エージェントは失敗したログイン試行を報告しません。

## ユーザ エージェントのガイドライン

ユーザ エージェントは、以下を含む段階的な設定が必要です。

- ユーザ エージェントがインストールされている少なくとも1台のコンピュータ。
- ユーザ エージェントがインストールされたコンピュータまたは Active Directory サーバと Firepower Management Center との間の接続。
- ユーザ エージェントからユーザ データを受け取る各 Firepower Management Center で設定されたアイデンティティ レルム。

段階的なユーザ エージェントの設定とサーバの要件の詳細については、『Firepower ユーザ エージェント構成ガイド』を参照してください。



- (注) コンピュータまたは Active Directory サーバの時間が Firepower Management Center の時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。

Firepower Management Center 接続は、ログインとログオフがユーザエージェントによって検出されたユーザのメタデータを取得可能にするだけでなく、アクセスコントロールルール内で使用するユーザとグループを指定するためにも使用されます。ユーザエージェントが特定のユーザ名を除外するように設定されている場合は、そのようなユーザ名のログインデータは Firepower Management Center に報告されません。ユーザエージェントのデータは、Firepower Management Center のユーザデータベースとユーザアクティビティデータベースに保存されます。



- (注) ユーザエージェントは \$ 記号で終わる Active Directory ユーザ名を Firepower Management Center に送信できません。これらのユーザをモニタする場合は、最後の \$ の文字を削除する必要があります。

複数のユーザがリモートセッションを使用してホストにログインしている場合は、エージェントがそのホストからのログインを正確に検出しない場合があります。これを防ぐ方法の詳細については、『Firepower ユーザエージェント構成ガイド』を参照してください。

## ユーザ制御のためのユーザエージェントの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin/Access Admin/Network Admin

ユーザエージェントの詳細については、[ユーザエージェントのアイデンティティソース \(2123 ページ\)](#) を参照してください。

### 始める前に

- [レールの作成 \(2185 ページ\)](#) の説明に従って、ユーザエージェント接続用の Active Directory レールを設定し、有効にします。

### 手順

**ステップ 1** Firepower Management Center にログインします。

**ステップ 2** [システム (System)] > [統合 (Integration)] をクリックします。

**ステップ 3** [アイデンティティの送信元 (Identity Sources)] タブをクリックします。

**ステップ 4** [サービスタイプ (Service Type)] に [ユーザ エージェント (User Agent)] をクリックし、ユーザ エージェント接続を有効にします。

(注) 接続を無効にするには、[なし (None)] をクリックします。

**ステップ 5** [新規エージェント (New Agent)] をクリックして新しいエージェントを追加します。

**ステップ 6** エージェントをインストールするコンピュータの [ホスト名 (Hostname)] または [アドレス (Address)] を入力します。IPv4 アドレスを使用する必要があります。IPv6 アドレスを使用してユーザ エージェントに接続するように Firepower Management Center を設定することはできません。

**ステップ 7** [追加 (Add)] をクリックします。

**ステップ 8** 接続を削除するには、削除アイコン (🗑️) をクリックして、その削除を確認します。

#### 次のタスク

- *Firepower* ユーザ エージェント構成ガイドの説明に従って、ユーザ エージェントの設定を続けます。
- [アイデンティティルールの作成 \(2193 ページ\)](#) の説明に従ってアイデンティティルールを設定します。
- アイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けます ([アクセス制御への他のポリシーの関連付け \(1340 ページ\)](#) を参照)。
- [設定変更の導入 \(350 ページ\)](#) の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。

## ユーザ エージェント アイデンティティ ソースのトラブルシューティング

ユーザ エージェント接続に問題が起きた場合は、*Firepower* ユーザ エージェント構成ガイドを確認してください。

このガイドの関連するトラブルシューティング情報については、[レルムとユーザのダウンロードのトラブルシューティング \(2182 ページ\)](#) と [ユーザ制御のトラブルシューティング \(405 ページ\)](#) を参照してください。

ユーザ エージェントによって報告されるユーザ データに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにないユーザ エージェントユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。ユーザのアクティビティは、システムがユーザのダウンロードでユーザに関する情報の取得に成功するまでルールで処理されず、Web インターフェイスに表示されません。

- Firepower Management Center のハイ アベイラビリティが設定されており、プライマリが失敗した場合、たとえ以前ユーザを確認できており、Firepower Management Center にダウンロード済みであっても、フェールオーバーダウンタイム中にユーザエージェントが報告したすべてのログインが特定不能となります。未確認のユーザは Firepower Management Center には不明なユーザとして記録されます。ダウンタイム後、[不明 (Unknown) ]ユーザはアイデンティティ ポリシーのルールに従って再び識別され、処理されます。

## ISE アイデンティティ ソース

Cisco Identity Services Engine (ISE) の展開を Firepower システムと統合して、ISE をパッシブ認証に使用できます。

ISE は、信頼できるアイデンティティ ソースで、Active Directory (AD)、LDAP、RADIUS、または RSA を使用して認証するユーザに関するユーザ認識データを提供します。さらに、Active Directory ユーザのユーザ制御を行えます。ISE は、ISE ゲスト サービス ユーザの失敗したログイン試行またはアクティビティは報告しません。



- (注) Firepower は、マシンの認証をユーザと関連付けないため、AD 認証と同時に 802.1x マシン認証を使用することはできません。802.1x アクティブ ログインを使用する場合は、802.1x アクティブ ログイン (マシンとユーザの両方) だけを報告するように ISE を設定します。このように設定すれば、マシン ログインはシステムに 1 回だけ報告されます。

Cisco ISE の詳細については、*Cisco Identity Services Engine Administrator Guide*を参照してください。

## ISE ガイドライン

Firepower システムで ISE を構成する際に、このセクションで説明されているガイドラインを使用してください。

### ISE バージョンと設定の互換性

ご使用の ISE バージョンと設定は、次のように Firepower との統合や相互作用に影響を与えます。

- ISE サーバと Firepower Management Center の時刻を同期します。そうしないと、システムが予期しない間隔でユーザのタイムアウトを実行する可能性があります。
- ISE データを使用してユーザ制御を実装するには、[レールの作成 \(2185 ページ\)](#) の説明に従って、pxGrid のペルソナを想定して ISE サーバのレールを設定し有効にします。
- 多数のユーザグループをモニタするように ISE を設定した場合、システムはメモリ制限のためにグループに基づいてユーザマッピングをドロップすることがあります。その結果、

レールまたはユーザ条件を使用するルールが想定どおりに実行されない可能性があります。

- ISE のバージョン 1.3 には、IPv6 対応エンドポイントのサポートが含まれていません。ISE のこのバージョンを実行している場合、ユーザアイデンティティデータを収集したり、IPv6 対応エンドポイント上で修正を実行したりすることはできません。
- ISE のバージョン 2.0 パッチ 4 以降には、IPv6 対応エンドポイントのサポートが含まれています。
- ISE の展開で ISE Endpoint Protection Service (EPS) が有効で設定されている場合は、ISE 接続を使用して、関連ポリシー違反に関与している送信元または宛先ホストに対する ISE EPS 修復を実行できます。
- ユーザの EPSStatus が変更された後でユーザの SGT を更新するように ISE の展開を設定した場合は、ISE EPS 修復により、Firepower Management Center 上の SGT も更新されます。

システムのこのバージョンと互換性がある特定のバージョンの ISE については、『Cisco Firepower Compatibility Guide』を参照してください。

## ISE 属性

ISE 接続を設定すると、ISE 属性データが Firepower Management Center データベースに入力されます。ユーザ認識とユーザ制御に使用できる ISE 属性は、次のとおりです。

### セキュリティ グループ タグ (SGT) (Security Group Tag (SGT))

セキュリティ グループ タグ (SGT) は、信頼ネットワーク内のトラフィックの送信元の権限を指定します。Cisco ISE および Cisco TrustSec は、ネットワークに入るときに、セキュリティ グループ アクセス (SGA) と呼ばれる機能を使用して、パケットに SGT 属性を適用します。これらの SGT は、ISE または TrustSec 内のユーザの割り当てられたセキュリティ グループに対応します。ID ソースとして ISE を設定すると、Firepower システムは、これらの SGT を使用してトラフィックをフィルタリングできます。



- (注) 一部のルールでは、カスタム SGT 条件が ISE によって割り当てられなかった SGT 属性にタグ付けされたトラフィックを照合できます。これはユーザ制御とみなされず、アイデンティティ ソースとして ISE を使用しない場合にのみ機能します。[カスタム SGT 条件 \(406 ページ\)](#) を参照してください。

### エンドポイント ロケーション (Endpoint Location) (またはロケーション IP (Location IP))

[エンドポイント ロケーション (Endpoint Location)] 属性は、ISE によって識別される、ユーザの認証に ISE を使用したネットワーク デバイスの IP アドレスです。

### エンドポイント プロファイル (Endpoint Profile) (またはデバイス タイプ (Device Type))

[エンドポイント プロファイル (Endpoint Profile)] 属性は、ISE によって識別されるユーザのエンドポイント デバイス タイプです。

## ユーザ制御用 ISE の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin/Access Admin/Network Admin

### 始める前に

- [レールの作成 \(2185ページ\)](#) の説明に従い、pxGrid ペルソナを想定して ISE サーバのレールを設定し、有効にします。
- 暗号化接続を使用して ISE サーバで Firepower Management Center を認証するには、Firepower Management Center のアクセス元となるマシンで証明書データとキーを利用可能にするか、[PKI オブジェクト](#) します。

### 手順

**ステップ 1** Firepower Management Center にログインします。

**ステップ 2** [システム (System)] > [統合 (Integration)] をクリックします。

**ステップ 3** [アイデンティティの送信元 (Identity Sources)] タブをクリックします。

**ステップ 4** [サービスタイプ (Service Type)] で [Identity Services Engine] をクリックし、ISE 接続を有効にします。

(注) 接続を無効にするには、[なし (None)] をクリックします。

**ステップ 5** [プライマリ ホスト名/IP アドレス (Primary Host Name/IP Address)]、およびオプションで [セカンダリ ホスト名/IP アドレス (Secondary Host Name/IP Address)] を入力します。

**ステップ 6** [pxGrid サーバ CA (pxGrid Server CA)] および [MNT サーバ CA (MNT Server CA)] リストから該当する認証局を、[FMC サーバ証明書 (FMC Server Certificate)] リストから適切な証明書をそれぞれクリックします。また、追加アイコン (+) をクリックして証明書を追加することもできます。

(注) [FMC サーバ証明書 (FMC Server Certificate)] には、**clientAuth** 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていません。

**ステップ 7** (オプション) CIDR ブロック表記を使用して [ISE ネットワーク フィルタ (ISE Network Filter)] を入力します。

**ステップ 8** 接続をテストするには、[テスト (Test)] をクリックします。

テストが失敗した場合、接続障害に関する詳細については、[その他のログ (Additional Logs)] をクリックします。

### 次のタスク

- [アイデンティティポリシーの作成 \(2192 ページ\)](#) の説明に従って、制御するユーザおよび他のオプションを、アイデンティティ ポリシーを使って指定します。
- [アクセス制御への他のポリシーの関連付け \(1340 ページ\)](#) の説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックのフィルタリングと、必要に応じて検査を実行します。
- [設定変更の導入 \(350 ページ\)](#) の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- [ワークフローの使用 \(2429 ページ\)](#) の説明に従って、ユーザアクティビティをモニタします。

## ISE 設定フィールド

次のフィールドを使用して ISE への接続を設定します。

### プライマリおよびセカンダリ ホスト名/IP アドレス (Primary and Secondary Host Name/IP Address)

プライマリ (およびオプションでセカンダリ) ISE サーバのホスト名または IP アドレス。

### pxGrid サーバ CA (pxGrid Server CA)

pxGrid フレームワークの認証局。展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

### MNT サーバ CA (MNT Server CA)

一括ダウンロード実行時の ISE 証明書の認証局。展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

### FMC サーバ証明書 (FMC Server Certificate)

ISE への接続時、または一括ダウンロードの実行時に Firepower Management Center が ISE に提供する必要がある証明書およびキー。



(注) [FMC サーバ証明書 (FMC Server Certificate)] には、**clientAuth** 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれてはなりません。

### ISE ネットワーク フィルタ (ISE Network Filter)

オプションのフィルタで、ISE が Firepower Management Center にレポートするデータを制限するために設定できます。ネットワークフィルタを指定する場合、ISEはそのフィルタ内のネットワークからデータをレポートします。次の方法でフィルタを指定できます。

- 任意 (**Any**) のフィルタを指定する場合はフィールドを空白のままにします。
- CIDR 表記を使用して単一の IPv4 アドレス ブロックを入力します。
- CIDR 表記を使用して IPv4 アドレス ブロックのリストをカンマで区切って入力します。



(注) このバージョンの FirePOWER システムは、ISE のバージョンに関係なく、IPv6 アドレスを使用したフィルタリングをサポートしません。

## ISE アイデンティティ ソースのトラブルシューティング

関連の他のトラブルシューティングについては、[レルムとユーザのダウンロードのトラブルシューティング \(2182 ページ\)](#) および [ユーザ制御のトラブルシューティング \(405 ページ\)](#) を参照してください。

ISE 接続に問題が起こった場合は、次のことを確認してください。

- ISE と Firepower システムを正常に統合するには、ISE 内の pxGrid アイデンティティ マッピング機能を有効にする必要があります。
- [FMC サーバ証明書 (FMC Server Certificate) ] には、[clientAuth] 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれてはなりません。
- ISE サーバの時刻は、Firepower Management Center の時刻と同期している必要があります。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。
- 展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。
- 展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。
- バージョン 6.0.x からバージョン 6.1.x に更新した後に ISE 接続の問題が発生する場合は、pxGrid サーバの証明書を確認します。バージョン 6.1 が準拠する RFC6125-6.4.4 では、SAN 値が指定されている場合、証明書 CN を無視する必要があります。ISE 展開における pxGrid サーバの証明書に CN 値と 1 つ以上の SAN 値が設定されている場合は、CN 値を削除し、それをさらなる SAN 値として追加します。

ISE によって報告されるユーザデータに関する問題が発生した場合は、次の点に注意してください。



- システムはデータがまだデータベースにない ISE ユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。ISE ユーザから見えるアクティビティは、システムがユーザのダウンロードで情報の取得に成功するまでアクセスコントロールルールで処理されず、Web インターフェイスに表示されません。
- LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE ユーザに対するユーザ制御は実行できません。
- Firepower Management Center は、ISE ゲスト サービス ユーザのユーザデータを受信できません。
- ISE が TS エージェントと同じユーザをモニタした場合、Firepower Management Center は TS エージェントのデータを優先します。TS エージェントと ISE が同じ IP アドレスによる同一のアクティビティを報告した場合は、TS エージェントのデータのみが Firepower Management Center に記録されます。
- 使用する ISE バージョンと構成は、Firepower システムでの ISE の使用方法に影響を与えます。詳細については、[ISE アイデンティティ ソース \(2126 ページ\)](#) を参照してください。

サポートされている機能に問題がある場合は、[ISE アイデンティティ ソース \(2126 ページ\)](#) で詳細を参照してバージョンの互換性を確認してください。

## ターミナルサービス (TS) エージェントのアイデンティティ ソース

TS エージェントはパッシブ認証方式で、Firepower システムでサポートされる権限のあるアイデンティティ ソースの 1 つです。Windows Terminal Server が認証を実行し、TS エージェントがスタンドアロンまたはハイアベイラビリティの Firepower Management Center にその認証の実行を報告します。

TS エージェントは、Windows Terminal Server にインストールされると、個々のユーザがモニタ対象ネットワークにログインまたはログアウトする際にそのユーザに固有のポート範囲を割り当てます。Firepower Management Center では、この固有のポートを使用して Firepower システムの個々のユーザを識別します。1 つの TS エージェントを使用して、1 つの Windows Terminal Server 上のユーザ アクティビティをモニタし、暗号化データを Firepower Management Center に送信できます。

TS エージェントは失敗したログイン試行を報告しません。TS エージェントから取得されたデータは、ユーザ認識とユーザ制御に使用できます。

### TS エージェントのガイドライン

TS エージェントには段階的な設定が必要で、次のものがあります。

1. TS エージェントがインストールおよび設定された Windows Terminal Server。
2. サーバがモニタするユーザを対象とする 1 つ以上のアイデンティティ レルム。

TS エージェントは、Microsoft Windows Terminal Server にインストールします。段階的な TS エージェントのインストールと設定、およびサーバと Firepower システムの要件の詳細については、『Cisco Terminal Services (TS) Agent Guide』を参照してください。

TS エージェントのデータは [ユーザ (Users) ] テーブル、[ユーザ アクティビティ (User Activity) ] テーブル、および [接続イベント (Connection Event) ] テーブルに表示され、ユーザ認識とユーザ制御に使用できます。



- (注) TS エージェントが別のパッシブ認証のアイデンティティ ソース (ユーザ エージェントまたは ISE) と同じユーザをモニタする場合、Firepower Management Center では TS エージェントのデータを優先します。TS エージェントと別のパッシブのアイデンティティ ソースが同じ IP アドレスでアクティビティを報告した場合、TS エージェントのデータだけが Firepower Management Center に記録されます。

## TS エージェントのユーザ制御の構成

TS エージェントをユーザ認識およびユーザ制御のアイデンティティ ソースとして使用するには、『Cisco Terminal Services (TS) Agent Guide』の説明に従って TS エージェント ソフトウェアをインストールして構成してください。

次に行う作業：

- [アイデンティティ ポリシーの作成 \(2192 ページ\)](#) の説明に従い、アイデンティティ ポリシーを使用して、制御するユーザおよびその他のオプションを指定します。
- [アクセス制御への他のポリシーの関連付け \(1340 ページ\)](#) の説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックをフィルタし、オプションで検査します。
- [設定変更の導入 \(350 ページ\)](#) の説明に従って、管理対象デバイスにアイデンティティ ポリシーおよびアクセス コントロール ポリシーを展開します。
- [ワークフローの使用 \(2429 ページ\)](#) の説明に従って、ユーザ アクティビティをモニタします。

## TS エージェント アイデンティティ ソースのトラブルシューティング

関連の他のトラブルシューティングについては、[レルムとユーザのダウンロードのトラブルシューティング \(2182 ページ\)](#) および [ユーザ制御のトラブルシューティング \(405 ページ\)](#) を参照してください。

TS エージェントと Firepower システムの統合に問題が起こった場合は、次のことを確認してください。

- TS エージェントサーバと Firepower Management Center の時計を同期させる必要があります。

- TS エージェントが別のパッシブ認証 ID ソース（ユーザエージェントまたは ISE）と同じユーザをモニタしている場合、Firepower Management Center は TS エージェントのデータを優先します。TS エージェントとパッシブ ID ソースが同じ IP アドレスによるアクティビティを報告した場合は、TS エージェントのデータのみが Firepower Management Center に記録されます。

トラブルシューティングのすべての情報は、『*Cisco Terminal Services (TS) Agent Configuration Guide*』を参照してください。

## キャプティブポータルのアイデンティティソース

キャプティブポータルは、Firepower システムでサポートされる権限のあるアイデンティティソースの 1 つです。これは Firepower システムでサポートされる唯一のアクティブな認証方式であり、ユーザは管理対象デバイスを使用してネットワークに対する認証を行うことができます。

通常、キャプティブポータルを使用して、インターネットにアクセスするため、または制限されている内部リソースにアクセスするための認証を要求します。必要に応じて、リソースへのゲストアクセスを設定することができます。システムはキャプティブポータルユーザを認証した後、それらのユーザのトラフィックをアクセス制御ルールに従って処理します。キャプティブポータルは、HTTP および HTTPS のトラフィックのみで認証を行います。



- (注) キャプティブポータルが認証を実行する前に、HTTPS トラフィックを復号化する必要があります。

キャプティブポータルはまた、失敗した認証の試行を記録します。失敗した試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。キャプティブポータルで報告される失敗した認証アクティビティのユーザアクティビティタイプは [認証失敗ユーザ (Failed Auth User) ] です。

キャプティブポータルから取得された認証データはユーザ認識とユーザ制御に使用できます。

## キャプティブポータルのガイドライン

アイデンティティポリシーでキャプティブポータルを設定して展開すると、指定されたレールのユーザは以下のデバイスを介して認証を行ってからネットワークにアクセスします。

- 7000 および 8000 シリーズ デバイス上の仮想ルータ
- バージョン 9.5(2) 以降で稼働するルーテッドモードの ASA FirePOWER デバイス
- ルーテッドモードの Firepower Threat Defense デバイス

## 必要なルーテッドインターフェイス

キャプティブポータルアクティブ認証を実行できるのは、ルーテッドインターフェイスが設定されているデバイスのみです。キャプティブポータルにルールを設定していて、キャプティブポータルデバイスにインラインインターフェイスとルーテッドインターフェイスが含まれている場合は、デバイス上のルーテッドインターフェイスのみを対象とする[インターフェイス条件](#)を設定する必要があります。

アクセスコントロールポリシーで参照されているアイデンティティポリシーに1つ以上のキャプティブポータルのアイデンティティルールが含まれ、以下を管理する Firepower Management Center にポリシーを展開する場合、次のようになります。

- ルーテッドインターフェイスが設定されている1つ以上のデバイスの場合、ポリシー導入は成功し、ルーテッドインターフェイスがアクティブ認証を実行します。

システムは ASA with FirePOWER デバイスでインターフェイスタイプを検証しません。ASA with FirePOWER デバイス上でインライン（タップモード）インターフェイスにキャプティブポータルポリシーを適用すると、ポリシーは正常に展開されますが、これらのルールに一致するトラフィック内のユーザは「不明」と識別されます。

- 1つ以上の NGIPSv デバイスの場合、ポリシー導入は失敗します。

## キャプティブポータルとポリシー

アイデンティティポリシーのキャプティブポータルを設定し、アイデンティティルールのアクティブ認証を呼び出します。アイデンティティポリシーはアクセスコントロールポリシーで呼び出されます。

キャプティブポータルのいくつかのアイデンティティポリシー設定はアクセスコントロールポリシーの [アクティブ認証 (Active Authentication)] タブページで行い、残りの設定はアクセスコントロールポリシーに関連付けられたアイデンティティルールで行います。

アクティブ認証ルールには [アクティブ認証 (Active Authentication)] ルールアクションが含まれているか、または [パッシブ認証でユーザを識別できない場合はアクティブ認証を使用する (Use active authentication if passive authentication cannot identify user)] が選択された [パッシブ認証 (Passive Authentication)] ルールアクションが含まれています。それぞれのケースで、システムは SSL 復号を透過的に有効化/無効化し、これにより Snort プロセスが再起動します。



**注意** SSL 復号が無効の場合（つまりアクセスコントロールポリシーに SSL ポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

## キャプティブ ポータルの要件と制約事項

以下の要件と制約事項に注意してください。

- システムがサポートするキャプティブ ポータル ログインの数は 1 秒あたり最大 20 です。
- (ルーテッドモードで ASA バージョン 9.5(2) 以降を実行する) ASA FirePOWER デバイスをキャプティブ ポータルに使用するには、**captive-portal** ASA CLI コマンドを使用してキャプティブ ポータルでのアクティブ認証を有効にし、『ASA ファイアウォール設定ガイド (バージョン 9.5(2) 以降)』  
(<http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html> [英語]) の説明に従ってポートを定義します。
- キャプティブ ポータルに使用する予定のデバイスの IP アドレスおよびポートを宛先とするトラフィックを許可する必要があります。アクセス制御で宛先が許可されない場合、キャプティブ ポータルを使用してトラフィックを認証することはできません。
- キャプティブ ポータルアクティブ認証を HTTPS トラフィックで行う場合、SSL ポリシーを使用して、認証対象のユーザからのトラフィックを復号する必要があります。キャプティブ ポータルユーザの Web ブラウザと管理対象デバイス上のキャプティブ ポータルデーモンとの間の接続では、トラフィックを復号できません。この接続は、キャプティブ ポータルユーザの認証に使用されます。

## ユーザ制御のためのキャプティブ ポータルの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意 (Any)	Control	任意 (NGIPSv を除く)	任意 (Any)	Administrator/Access Admin/Network Admin

キャプティブ ポータルの詳細については、[キャプティブ ポータルのガイドライン \(2133 ページ\)](#) および[キャプティブ ポータルフィールド \(2139 ページ\)](#) を参照してください。

### 始める前に

- ルーテッドインターフェイスが設定された 1 つ以上のデバイスが、Firepower Management Center によって管理されていることを確認します。  
Firepower Management Center で ASA with FirePOWER デバイスを管理している場合には、[キャプティブ ポータルのガイドライン \(2133 ページ\)](#) を参照してください。
- [レルムの作成 \(2185 ページ\)](#) の説明に従って Active Directory のレルムを設定し、有効化します。
- キャプティブ ポータルで暗号化認証を使用するには、Firepower Management Center のアクセス元となるマシンで証明書データとキーを利用可能にするか、PKI オブジェクトを作成

します。PKI オブジェクトの作成方法については、[PKI オブジェクト \(487 ページ\)](#) を参照してください。

## 手順

**ステップ 1** まだ Firepower Management Center にログインしていない場合は、ログインします。

**ステップ 2** キャプティブポータル用のアクティブな認証アイデンティティルールを作成します。

- a) [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [アイデンティティ (Identity)] の順にクリックして、アイデンティティポリシーを作成または編集します。
- b) (オプション) [カテゴリの追加 (Add Category)] をクリックし、そのキャプティブポータルアイデンティティルール用にカテゴリを追加して、カテゴリの [名前 (Name)] を入力します。
- c) [アクティブ認証 (Active Authentication)] タブをクリックします。
- d) リストから適切な [サーバ証明書 (Server Certificate)] を選択するか、追加アイコン (+) をクリックして証明書を追加します。
- e) [ポート (Port)] を入力して、[最大ログイン試行回数 (Maximum login attempts)] を指定します。(デフォルトで、キャプティブポータルはポート 885 を使用します。)
- f) (オプション) [キャプティブポータルフィールド \(2139 ページ\)](#) の説明に従って、[アクティブ認証応答ページ (Active Authentication Response Page)] を選択します。
- g) [保存 (Save)] をクリックします。
- h) [ルール (Rules)] タブをクリックします。
- i) [ルールの追加 (Add Rule)] をクリックして新しいキャプティブポータルアイデンティティポリシールールを追加するか、編集アイコン (✎) をクリックして既存のルールを編集します。
- j) ルールの [名前 (Name)] を入力します。
- k) [アクション (Action)] 一覧から [アクティブ認証 (Active Authentication)] をクリックします。

システムは、非 TCP トラフィックでキャプティブポータルアクティブ認証を実施できません。アイデンティティルールの [アクション (Action)] が [アクティブ認証 (Active Authentication)] である (つまりキャプティブポータルを使用している) 場合、またはパッシブ認証を使用しており、[レルムおよび設定 (Realms & Settings)] タブページのオプションで [パッシブ認証でユーザを識別できない場合にアクティブ認証を使用 (Use active authentication if passive authentication cannot identify user)] がオンに設定されている場合、TCP ポート制約のみを使用します。

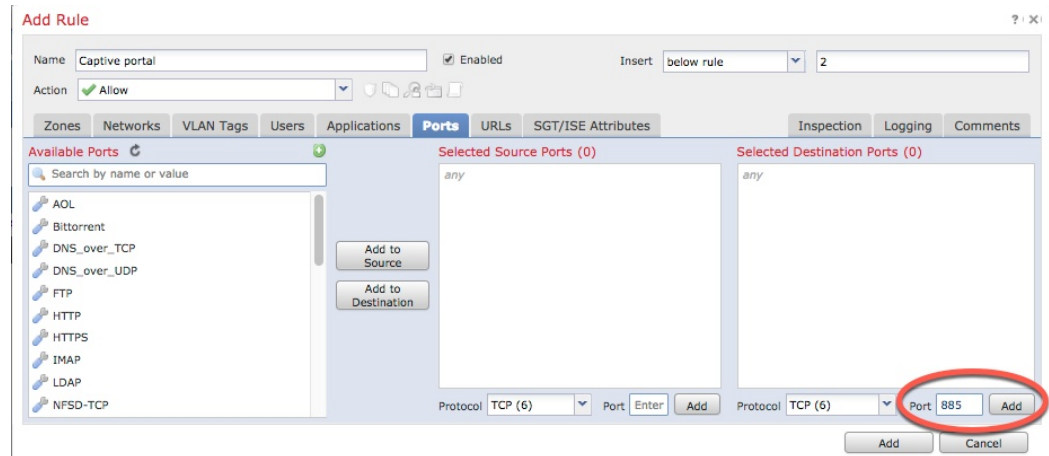
アイデンティティルールの [アクション (Action)] が [パッシブ認証 (Passive Authentication)] または [認証なし (No Authentication)] である場合、非 TCP トラフィックに基づいてポート条件を作成できます。

- l) [レルムおよび設定 (Realm & Settings)] タブをクリックします。
- m) [レルム (Realms)] 一覧から、ユーザ認証に使用するレルムを選択します。

- n) (オプション) [認証でユーザを識別できない場合はゲストとして識別する (Identify as Guest if authentication cannot identify user)] をオンにします。詳細については、[キャプティブポータルフィールド \(2139 ページ\)](#) を参照してください。
- o) リストから [認証タイプ (Authentication Type)] を 1 つクリックします。
- p) (オプション) キャプティブポータルから特定のアプリケーショントラフィックを除外する方法については、[キャプティブポータルからのアプリケーションの除外 \(2140 ページ\)](#) を参照してください。
- q) [ルール条件タイプ \(371 ページ\)](#) の説明に従って、ルールに条件を追加します (ポートやネットワークなど)。
- r) [追加 (Add)] をクリックします。
- s) ページの上部にある [保存 (Save)] をクリックします。

**ステップ 3** キャプティブポータルポート (デフォルトでは TCP 885) 上のトラフィックを許可するキャプティブポータルに関するアクセスコントロールポリシーを設定します。


- a) アクセスコントロールポリシーエディタで、[ルールの追加 (Add Rule)] をクリックします。
- b) ルールの [名前 (Name)] を入力します。
- c) [アクション (Action)] 一覧から、[許可 (Allow)] を選択します。
- d) [ポート (Ports)] タブをクリックします。
- e) [選択した宛先ポート (Selected Destination Ports)] フィールドの [プロトコル (Protocol)] 一覧から、[TCP] を選択します。
- f) [ポート (Port)] フィールドに、「885」と入力します。
- g) [ポート (Port)] フィールドの横にある [追加 (Add)] をクリックします。  
次の図は例を示しています。




- h) ページ下部の [追加 (Add)] をクリックします。

**ステップ 4** レルム内のユーザがキャプティブポータルを使用してリソースにアクセスできるようにするには、同じアクセスコントロールポリシーに別のルールを追加します。

- a) ルールエディタで、[ルールの追加 (Add Rule)] をクリックします。
- b) ルールの [名前 (Name)] を入力します。
- c) [アクション (Action)] 一覧から、[許可 (Allow)] を選択します。

- d) [ユーザ (Users) ] タブをクリックします。
- e) [使用可能なレルム (Available Realms) ] 一覧で、許可するレルムをクリックします。
- f) レルムが表示されない場合は、 (更新) をクリックします。
- g) [使用可能なユーザ (Available Users) ] 一覧で、ルールに追加するユーザを選択し、[ルールに追加 (Add to Rule) ] をクリックします。
- h) (オプション) [ルール条件タイプ \(371 ページ\)](#) の説明に従って、アクセスコントロールポリシーに条件を追加します。
- i) [追加 (Add) ] をクリックします。
- j) [アクセス制御ルール (access control rule) ] ページで、[保存 (Save) ] をクリックします。
- k) ポリシーエディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリックメニューを使用してカットアンドペーストを実行します。ルールには 1 から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワークトラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

**ステップ 5** キャプティブポータルユーザが HTTPS プロトコルを使用して Web ページにアクセスできるように、[不明 (Unknown) ] なユーザ用の SSL 復号化ルールを設定します。

- a) [PKI オブジェクト \(487 ページ\)](#) の説明に従って、SSL トラフィックを複合化するための証明書オブジェクトを作成します (まだ作成していない場合)。
- b) [ポリシー (Policies) ] > [アクセスコントロール (Access Control) ] > [SSL] の順にクリックします。
- c) [新しいポリシー (New Policy) ] をクリックします。
- d) ポリシーの [名前 (Name) ] を入力し、[デフォルトのアクション (Default Action) ] を選択します。デフォルトのアクションについては、[SSL ポリシーのデフォルトアクション \(1458 ページ\)](#) を参照してください。
- e) [保存 (Save) ] をクリックします。
- f) [ルールの追加 (Add Rule) ] をクリックします。
- g) ルールの [名前 (Name) ] を入力します。
- h) [アクション (Action) ] 一覧から、[復号-再署名 (Decrypt - Resign) ] を選択します。
- i) [with] 一覧から、使用する PKI オブジェクトを選択します。
- j) [ユーザ (Users) ] タブをクリックします。
- k) [使用可能なレルム (Available Realms) ] 一覧の上にある  (更新) をクリックします。
- l) [使用可能なレルム (Available Realms) ] 一覧で、[特殊なアイデンティティ (Special Identities) ] をクリックします。
- m) [使用可能なユーザ (Available Users) ] 一覧で、[不明 (Unknown) ] をクリックします。
- n) [ルールに追加 (Add to Rule) ] をクリックします。
- o) (オプション) [SSL ルールの条件 \(1474 ページ\)](#) の説明に従って、他のオプションを設定します。
- p) [追加 (Add) ] をクリックします。
- q) ページの上部にある [保存 (Save) ] をクリックします。



- ステップ 6** アイデンティティポリシーと SSL ポリシーをアクセスコントロールポリシーに関連付けます。（アクセスコントロールポリシーを新規に作成することも、既存のものを使用することもできます）。
- [**ポリシー (Policies)**] > [**アクセスコントロール (Access Control)**] > [**アクセスコントロール (Access Control)**] の順にクリックして、アクセスコントロールポリシーを作成または編集します。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
  - 新しいアクセスコントロールポリシーを作成するか、既存のポリシーを編集します。
  - ページ上部の [**アイデンティティポリシー (Identity Policy)**] の横にあるリンクをクリックします。
  - 一覧から、使用するアイデンティティポリシーの名前を選択し、ページ上部にある [**保存 (Save)**] をクリックします。
  - 上記の手順を繰り返して、使用するキャプティブポータル SSL ポリシーをアクセスコントロールポリシーに関連付けます。
  - [アクセスコントロールポリシーのターゲットデバイスの設定 \(1337ページ\)](#) の説明に従って、管理対象デバイスでそのポリシーをターゲットにします（この手順をまだ行っていない場合）。

#### 次のタスク

- [設定変更の導入 \(350ページ\)](#) の説明に従って、使用するアイデンティティポリシーとアクセスコントロールポリシーを管理対象デバイスに展開します。
- [ワークフローの使用 \(2429ページ\)](#) の説明に従って、ユーザアクティビティをモニタします。

## キャプティブポータルフィールド

次のフィールドを使用して、アイデンティティポリシーの [**アクティブ認証 (Active Authentication)**] タブでキャプティブポータルを設定します。[アイデンティティルールフィールド \(2194ページ\)](#) も参照してください。

#### サーバ証明書 (Server Certificate)

キャプティブポータルデーモンが示すサーバ証明書。

#### [ポート (Port)]

キャプティブポータル接続のために使用するポート番号。ASA FirePOWER デバイスをキャプティブポータルに使用しようとする場合は、このフィールドのポート番号が、**captive-portal** CLI コマンドを使用して ASA FirePOWER デバイスで設定したポート番号と一致していなければなりません。

#### 最大ログイン試行回数 (Maximum login attempts)

ユーザのログイン要求がシステムによって拒否されるまでに許容されるログイン試行失敗の最大数。

### アクティブ認証回答ページ (Active Authentication Response Page)

キャプティブポータルユーザに対して表示される、システム提供またはカスタムの HTTP 応答ページ。アイデンティティポリシーのアクティブ認証設定で [アクティブ認証回答ページ (Active Authentication Response Page)] を選択したら、[HTTP 応答ページ (TTP Response Page)] で 1 つ以上のアイデンティティルールを [認証タイプ (Authentication Type)] [[認証プロトコル (Authentication Protocol)] ] として設定する必要があります。

システム提供の HTTP 応答ページには、[ユーザ名 (Username)] と [パスワード (Password)] フィールドに加え、[ゲストとしてログイン (Login as guest)] ボタンがあり、ユーザはゲストとしてネットワークにアクセスできます。単一のログイン方法を表示するには、カスタム HTTP 応答ページを設定します。

次のオプションから選択します。

- 汎用的な応答を使用する場合は、[システム提供 (System-provided)] をクリックします。表示アイコン (🔍) をクリックすると、このページの HTML コードが表示されます。
- カスタム応答を作成する場合は、[カスタム (Custom)] をクリックします。システム提供コードを示すウィンドウが表示され、これを置換または変更できます。完了したら、変更を保存します。カスタム ページは、編集アイコン (✎) をクリックすると編集できます。

## キャプティブポータルからのアプリケーションの除外

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意、ただし NGIPsv を除く	任意 (Any)	Administrator/Access Admin/Network Admin

アプリケーション (HTTP ユーザエージェント文字列によって指定される) を選択し、キャプティブポータルのアクティブ認証から除外することができます。これにより、選択されたアプリケーションからのトラフィックが認証を受けずにアイデンティティポリシーを通過できるようになります。



(注) このリストに表示されるのは、**User-Agent Exclusion** タグが付けられたアプリケーションのみです。

## 手順

- ステップ 1** アイデンティティ ルール エディタ ページの [レルムおよび設定 (Realm & Settings)] タブで、[アプリケーションフィルタ (Application Filters)] リストのシスコ提供のフィルタを使用して、フィルタに追加するアプリケーションのリストを絞り込みます。
- リストを展開および縮小するには、各フィルタタイプの横にある矢印をクリックします。
  - フィルタ タイプを右クリックし、[すべて選択 (Check All)] または [すべて選択解除 (Uncheck All)] をクリックします。このリストには、各タイプで選択したフィルタ数が示されることに注意してください。
  - 表示されるフィルタを絞り込むには、[名前を検索 (Search by name)] フィールドに検索文字列を入力します。これは、カテゴリとタグの場合に特に有効です。検索をクリアするには、クリアアイコン (✕) をクリックします。
  - フィルタのリストを更新し、選択したフィルタをすべてクリアするには、リロードアイコン (🔄) をクリックします。
  - すべてのフィルタと検索フィールドをクリアするには、[すべてのフィルタをクリア (Clear All Filters)] をクリックします。
- (注) リストには一度に 100 のアプリケーションが表示されます。
- ステップ 2** [使用可能なアプリケーション (Available Applications)] リストから、フィルタに追加するアプリケーションを選択します。
- 前の手順で指定した制約を満たすすべてのアプリケーションを追加するには、[フィルタに一致するすべてのアプリケーション (All apps matching the filter)] を選択します。
  - 表示される個別のアプリケーションを絞り込むには、[名前を検索 (Search by name)] フィールドに検索文字列を入力します。検索をクリアするには、クリアアイコン (✕) をクリックします。
  - 使用可能な個別のアプリケーションのリストを参照するには、リストの下部にあるページングアイコンを使用します。
  - アプリケーションのリストを更新し、選択したアプリケーションをすべてクリアするには、リロードアイコン (🔄) をクリックします。
- ステップ 3** 外部認証から除外する、選択したアプリケーションを追加します。クリックしてドラッグするか、[ルールに追加 (Add to Rule)] をクリックできます。結果は次のもので構成されています。
- 選択したアプリケーション フィルタ

- 選択した個別の使用可能なアプリケーション、または [フィルタに一致するすべてのアプリケーション (All apps matching the filter) ]

#### 次のタスク

- [アイデンティティルールの作成 \(2193 ページ\)](#) の説明に従ってアイデンティティルールの設定を続けます。

## キャプティブポータルのアイデンティティソースのトラブルシューティング

関連の他のトラブルシューティングについては、[レルムとユーザのダウンロードのトラブルシューティング \(2182 ページ\)](#) および [ユーザ制御のトラブルシューティング \(405 ページ\)](#) を参照してください。

キャプティブポータルに関する問題が発生した場合は、次の点を確認してください。

- キャプティブポータルサーバの時刻は、Firepower Management Center の時刻と同期している必要があります。
- 設定済みの DNS 解決があり、**Kerberos** (または Kerberos をオプションとする場合は **HTTP ネゴシエート**) キャプティブポータルを実行するアイデンティティルールを作成する場合は、キャプティブポータルデバイスの完全修飾ドメイン名 (FQDN) を解決するように DNS サーバを設定する必要があります。FQDN は、DNS 設定時に指定したホスト名と一致する必要があります。

ASA with FirePOWER Services および Firepower Threat Defense デバイスの場合、FQDN は、キャプティブポータルに使用されるルーテッドインターフェイスの IP アドレスに解決される必要があります。

- **Kerberos** (または Kerberos をオプションとする場合に **HTTP ネゴシエート**) を、アイデンティティルールの [認証タイプ (Authentication Type) ] として選択する場合、選択する [レルム (Realm) ] は、Kerberos キャプティブポータルアクティブ認証を実行できるように、[アクティブディレクトリ参加ユーザ名 (AD Join Username) ] と [アクティブディレクトリ参加パスワード (AD Join Password) ] を使用して設定する必要があります。
- アイデンティティルールの [認証タイプ (Authentication Type) ] として [HTTP 基本 (HTTP Basic) ] を選択した場合、ネットワーク上のユーザはセッションがタイムアウトしたことを認識しない場合があります。ほとんどの Web ブラウザは、**HTTP 基本** ログインからクレンジナルをキャッシュし、古いセッションがタイムアウトした後にシームレスに新しいセッションを開始するためにそのクレンジナルを使用します。
- Firepower Management Center と管理対象デバイスとの間の接続に障害が発生した場合、ユーザが以前に認識され Firepower Management Center にダウンロードされた場合を除き、デバイスによって報告されたすべてのキャプティブポータルログインはダウンタイム中に特

定できません。識別されていないユーザは、Firepower Management Center で [不明 (Unknown) ] のユーザとして記録されます。ダウンタイム後、不明のユーザはアイデンティティ ポリシーのルールに従って再確認され、処理されます。

- キャプティブ ポータルに使用する予定のデバイスにインライン インターフェイスとルーテッドインターフェイスの両方が含まれる場合、キャプティブポータルデバイス上でルーテッドインターフェイスだけを対象とするようにキャプティブポータルアイデンティティルールでゾーン条件を設定する必要があります。
- システムは ASA with FirePOWER デバイスでインターフェイス タイプを検証しません。ASA with FirePOWER デバイス上でインライン (タップ モード) インターフェイスにキャプティブポータルポリシーを適用すると、ポリシーは正常に展開されますが、これらのルールに一致するトラフィック内のユーザは「不明」と識別されます。

## トラフィック ベース検出のアイデンティティ ソース

トラフィック ベース検出は、Firepower システムでサポートされている唯一の権限のないアイデンティティ ソースです。トラフィック ベース検出を設定すると、管理対象デバイスは、指定したネットワークでの LDAP、AIM、POP3、IMAP、Oracle、SIP (VoIP)、FTP、HTTP、MDNS、SMTP のログインを検出します。トラフィック ベースの検出から取得されたデータは、ユーザ認識にのみ使用できます。権威のあるアイデンティティ ソースとは異なり、トラフィック ベースの検出はネットワーク検出ポリシーで設定します。[トラフィック ベースのユーザ検出の設定 \(2161 ページ\)](#) を参照してください。

次の制限事項に注意してください。

- トラフィック ベースの検出では、LDAP 接続に対する Kerberos ログインのみを LDAP 認証として解釈します。また、管理対象デバイスは、SSL や TLS などのプロトコルを使用して暗号化された LDAP 認証を検出できません。
- トラフィック ベースの検出では OSCAR プロトコルを使用した AIM ログインだけを検出します。TOC2 を使用する AIM ログインは検出できません。
- トラフィック ベースの検出では SMTP ログインを制限することができません。これは、ユーザが SMTP ログインに基づいてデータベースに追加されていないためです。システムが SMTP ログインを検出しても、一致する電子メールアドレスのユーザがデータベース内に存在しなければ、そのログインは記録されません。

トラフィック ベースの検出は、失敗したログイン試行も記録します。失敗ログイン試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。トラフィック ベースの検出により検出された失敗ログイン アクティビティのユーザ アクティビティ タイプは [失敗したユーザ ログイン (Failed User Login) ] です。



- (注) システムは失敗した HTTP ログインと成功した HTTP ログインを区別できません。HTTP ユーザ情報を表示するには、トラフィック ベースの検出設定で [失敗したログイン試行の取得 (Capture Failed Login Attempts) ] を有効にする必要があります。



- 注意** ネットワーク検出ポリシーを使用して、HTTP、FTP、MDNS プロトコルを介した非権限、トラフィック ベースのユーザ検出を有効/無効にすると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### トラフィック ベースの検出データ

デバイスがトラフィック ベースの検出を使用してログインを検出すると、次の情報をユーザ アクティビティとして記録するために Firepower Management Center に送信します。

- ログインで識別されたユーザ名
- ログインの時刻
- ログインに関係する IP アドレス。このアドレスは、ユーザのホスト (LDAP、POP3、IMAP、および AIM ログインの場合)、サーバ (HTTP、MDNS、FTP、SMTP および Oracle ログインの場合)、またはセッション発信元 (SIP ログインの場合) の IP アドレスになります。
- ユーザの電子メールアドレス (POP3、IMAP、および SMTP ログインの場合)
- ログインを検出したデバイスの名前

ユーザがすでに検出されている場合、Firepower Management Center はそのユーザのログイン履歴を更新します。Firepower Management Center は POP3 および IMAP ログイン内の電子メールアドレスを使用して LDAP ユーザに関連付ける場合があることに注意してください。これは、Firepower Management Center が新しい IMAP ログインを検出して、その IMAP ログイン内の電子メールアドレスが既存の LDAP ユーザのアドレスと一致した場合は、IMAP ログインで新しいユーザが作成されるのではなく、LDAP ユーザの履歴が更新されることを意味します。

ユーザが以前に検出されなかった場合、Firepower Management Center はユーザ データベースにユーザを追加します。AIM、SIP、Oracle ログインでは、常に新しいユーザ レコードが作成されます。これは、それらのログインイベントには Firepower Management Center が他のログインタイプに関連付けることができるデータが含まれていないためです。

Firepower Management Center は、次の場合に、ユーザ アイデンティティまたはユーザ ID を記録しません。

- そのログインタイプを無視するようにネットワーク検出ポリシーを設定した場合

- 管理対象デバイスが SMTP ログインを検出したものの、ユーザ データベースに電子メールアドレスが一致する、検出済みの LDAP、POP3、または IMAP ユーザが含まれていない場合

ユーザ データはユーザ テーブルに追加されます。

### トラフィック ベースの検出戦略

ユーザ アクティビティを検出するプロトコルを制限して、検出するユーザの総数を削減することにより、ほぼ完全なユーザ情報を提供していると思われるユーザに焦点を絞ることができます。プロトコルの検出を制限すると、ユーザ名の散乱を最小限に抑え、Firepower Management Center 上の記憶域を節約することができます。

トラフィック ベースの検出プロトコルを選択する際には、以下を検討してください。

- AIM、POP3、IMAP などのプロトコル経由でユーザ名を取得すると、契約業者、訪問者、およびその他のゲストからのネットワーク アクセスによって組織に無関係なユーザ名が収集される可能性があります。
- AIM、Oracle、および SIP ログインは、無関係なユーザ レコードを作成する可能性があります。この現象は、このようなログイン タイプが、システムが LDAP サーバから取得するユーザ メタデータのいずれにも関連付けられていないうえ、管理対象デバイスが検出するその他のログイン タイプに含まれている情報のいずれにも関連付けられていないために発生します。そのため、Firepower Management Center は、これらのユーザとその他のユーザ タイプを関連付けることができません。







## 第 88 章

# ネットワーク検出ポリシー

以下のトピックでは、ネットワーク検出ポリシーを作成、設定、管理する方法について説明します。

- [概要：ネットワーク検出ポリシー](#) (2147 ページ)
- [ネットワーク検出のカスタマイズ](#) (2148 ページ)
- [ネットワーク検出ルール](#) (2150 ページ)
- [高度なネットワーク検出オプションの設定](#) (2162 ページ)
- [ネットワーク検出戦略のトラブルシューティング](#) (2174 ページ)

## 概要：ネットワーク検出ポリシー

Firepower Management Center 上のネットワーク検出ポリシーは、システムが組織のネットワーク アセットに関するデータを収集する方法と、どのネットワーク セグメントとポートをモニタ対象とするかを制御します。

マルチドメイン展開では、各リーフドメインがそれぞれ独立したネットワーク検出ポリシーを使用します。ネットワーク検出ポリシーのルールやその他の設定をドメイン間で共有、継承、コピーすることはできません。新しいドメインを作成するたびに、システムにより、その新しいドメインに対してデフォルト設定を使用したネットワーク検出ポリシーが作成されます。カスタマイズが必要な場合は、新しいポリシーに明示的に適用する必要があります。

Firepower システムがモニタしてトラフィック内のネットワーク データに基づいて検出データを生成するネットワークおよびポート、ポリシーを適用するゾーンは、ポリシー内の検出ルールで指定します。ルール内では、ホスト、アプリケーション、権限のないユーザを検出するかどうかを設定できます。検出からネットワークとゾーンを除外するルールを作成できます。

NetFlow エクスポートからのデータの検出を設定して、ネットワーク上でユーザデータが検出されるトラフィックのプロトコルを制限できます。

ネットワーク検出ポリシーに用意されている単一のデフォルトルールは、すべてのモニタ対象トラフィックからアプリケーションを検出するように設定されています。このルールが除外するネットワーク、ゾーン、ポートはなく、ホストとユーザの検出も設定されていません。また、このルールは NetFlow エクスポートをモニタするように設定されてはいません。このポリシーは、管理対象デバイスが Firepower Management Center に登録されると、デフォルトでその

デバイスに導入されます。ホストまたはユーザデータの収集を開始するには、検出ルールを追加または変更して、ポリシーをデバイスに再展開する必要があります。

ネットワーク検出の範囲を調整する場合は、追加の検出ルールを作成して、デフォルトルールを変更または削除できます。

管理対象デバイスごとのアクセスコントロールポリシーは、そのデバイスに許可されたトラフィック、つまり、ネットワーク検出を使用してモニタ可能なトラフィックを定義することに注意してください。アクセスコントロールを使用して特定のトラフィックをブロックすると、システムでホスト、ユーザ、またはアプリケーションのアクティビティに関するトラフィックを検査できなくなります。たとえば、アクセスコントロールポリシーでソーシャルネットワーキングアプリケーションへのアクセスをブロックすると、システムはそれらのアプリケーションに関する検出データを一切提供できなくなります。

検出ルールでトラフィックベースのユーザ検出を有効にすると、一連のアプリケーションプロトコル全体のトラフィック内のユーザログインアクティビティを通して権限のないユーザを検出できます。必要に応じて、すべてのルールにわたって特定のプロトコル内の検出を無効にできます。一部のプロトコルを無効にすると、Firepower Management Center モデルに関連付けられたユーザ制限に達するのを防ぐのに役立ち、他のプロトコルからのユーザに使用可能なユーザカウントを確保できます。

詳細ネットワーク検出設定を使用すれば、記録するデータの種類、検出データの保存方法、アクティブにする侵害の兆候 (IOC) ルール、影響評価に使用する脆弱性マッピング、送信元からの検出データが競合していた場合の対処を管理できます。また、ホスト入力の送信元や NetFlow エクスポートをモニタ対象として追加することもできます。

## ネットワーク検出のカスタマイズ

Firepower システムによって収集されるネットワークトラフィックに関する情報は、この情報に関連付けて最も脆弱で最も重要なネットワークのホストを識別することができる場合に、最もその価値を発揮します。

たとえば、ネットワーク上に SuSE Linux のカスタマイズバージョンを実行している複数のデバイスがある場合、システムはそのオペレーティングシステムを識別することができません。そのため、脆弱性をそれらのホストにマッピングすることはできません。しかし、システムに SuSE Linux に関する脆弱性のリストがあるならば、同じオペレーティングシステムを実行する他のホストを識別するために使用できるカスタムフィンガープリントを、ホストのいずれか 1 台に対して作成することができます。フィンガープリントに SuSE Linux の脆弱性リストのマッピングを含め、フィンガープリントに一致する各ホストとそのリストに関連付けることができます。

また、ホストの入力機能を使用して、ホストデータをサードパーティシステムからネットワークマップに直接入力することもできます。ただし、サードパーティのオペレーティングシステムやアプリケーションデータは、脆弱性情報に自動的にマッピングされません。脆弱性を確認し、サードパーティのオペレーティングシステム、サーバ、アプリケーションプロトコルデータを使用してホストの影響の関連付けを実行する場合、サードパーティシステムからのベンダーとバージョンの情報を、脆弱性データベース (VDB) にリストされているベンダーと

バージョンにマッピングする必要があります。また、ホストの入力データを継続的に維持する必要がある場合もあります。アプリケーションデータを Firepower システムのベンダーおよびバージョン定義にマッピングしたとしても、インポートされたサードパーティの脆弱性はクライアントまたは Web アプリケーションの影響評価に使用されないことに注意してください。

システムがネットワーク上のホストで実行されているアプリケーションプロトコルを識別できない場合は、システムがポートまたはパターンに基づいてアプリケーションを識別できるようにする、ユーザ定義のアプリケーションプロトコルディテクタを作成できます。また、特定のアプリケーションディテクタをインポートしたり、アクティブ/非アクティブにしたりすることによって、Firepower システムのアプリケーション検出機能をカスタマイズすることができます。

さらに、Nmap アクティブスキャナのスキャン結果を使用してオペレーティングシステムやアプリケーションデータの検出を置き換えたり、サードパーティの脆弱性で脆弱性リストを拡張したりすることもできます。システムは複数のソースからのデータを照合して、アプリケーションの ID を判別できます。

## ネットワーク検出ポリシーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

マルチドメイン展開では、各ドメインに個別のネットワーク検出ポリシーがあります。ユーザアカウントで複数のドメインを管理できる場合は、ポリシーを設定するリーフドメインに切り替えます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** ポリシーの次のコンポーネントを設定します。

- 検出ルール： [ネットワーク検出ルールの設定 \(2151 ページ\)](#) を参照してください。
- ユーザのトラフィックベースの検出： [トラフィックベースのユーザ検出の設定 \(2161 ページ\)](#) を参照してください。
- 高度なネットワーク検出オプション： [高度なネットワーク検出オプションの設定 \(2162 ページ\)](#) を参照してください。

- カスタム オペレーティング システム定義 (フィンガープリント) : [クライアント用のカスタムフィンガープリントの作成 \(2046ページ\)](#) および [サーバ用のカスタムフィンガープリントの作成 \(2049ページ\)](#) を参照してください。

## ネットワーク検出ルール

ネットワーク検出ルールを使用すれば、ネットワーク マップに対して検出される情報を調整し、必要な特定のデータだけを含めるようにすることができます。ネットワーク検出ポリシー内のルールは順番に評価されます。モニタリング基準が重複したルールを作成できますが、その場合はシステム パフォーマンスに影響する可能性があります。

モニタリングからホストまたはネットワークを除外すると、そのホストまたはネットワークがネットワーク マップに表示されず、それに対するイベントが報告されません。Cisco では、モニタリングからロードバランサ (またはロードバランサ上の特定のポート) と NAT デバイスを除外することを推奨しています。これらのデバイスは紛らわしいイベントを過剰に生成するため、データベースがいっぱいになったり、Firepower Management Center が過負荷になったりする可能性があります。たとえば、モニタ対象 NAT デバイスが短期間にオペレーティング システムの複数の更新を表示する場合があります。ロードバランサと NAT デバイスの IP アドレスがわかっている場合は、モニタリングからそれらを除外できます。



**ヒント** システムは、ネットワーク トラフィックを検査することにより、複数のロードバランサと NAT デバイスを識別できます。

加えて、カスタム サーバフィンガープリントを作成する必要がある場合は、フィンガープリントを行っているホストとの通信に使用されている IP アドレスをモニタリングから一時的に除外する必要があります。そうしないと、ネットワーク マップおよびディスカバリ イベントビューに、その IP アドレスによって表されるホストに関する不正確な情報が混在することになります。フィンガープリントを作成したら、その IP アドレスをモニタするようにポリシーを設定し直すことができます。

Cisco では、NetFlow エクスポートと Firepower システム管理対象デバイスを使用して、同じネットワークセグメントをモニタしないことも推奨しています。重複しないルールを使用してネットワーク検出ポリシーを設定するのが理想です。管理対象デバイスによって生成された重複接続ログはシステムによって破棄されます。ただし、管理対象デバイスと NetFlow エクスポートの両方で検出された接続に関する重複接続ログを破棄することはできません。

## ネットワーク検出ルールの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

検出ルールを設定し、ニーズに合わせてホスト データとアプリケーション データの検出を調整できます。

### 始める前に

- ネットワーク データを検出するトラフィックの接続を記録していることを確認します。[接続ロギングストラテジー \(2504 ページ\)](#) を参照してください。
- エクスポートされた NetFlow レコードを収集する場合は、[NetFlow エクスポートのネットワーク検出ポリシーへの追加 \(2169 ページ\)](#) の説明に従って NetFlow エクスポートを追加します。

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [ルールの追加 (Add Rule)] をクリックします。

**ステップ 3** [アクションと検出されるアセット \(2152 ページ\)](#) の説明に従って、ルールの [アクション (Action)] を設定します。

**ステップ 4** オプションの検出パラメータを設定します。

- ルールアクションを特定のネットワークに制限します。[監視対象ネットワークの制限 \(2153 ページ\)](#) を参照してください。
- ルールアクションを特定のゾーン内のトラフィックに制限します。[ネットワーク検出ルールでのゾーンの設定 \(2158 ページ\)](#) を参照してください。
- ポートをモニタリングから除外します。[ネットワーク検出ルールでのポートの除外 \(2156 ページ\)](#) を参照してください。
- NetFlow データ検出のルールを設定します。[NetFlow データ検出のルールの設定 \(2154 ページ\)](#) を参照してください。

**ステップ 5** [保存 (Save)] をクリックします。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## アクションと検出されるアセット

検出ルールを設定する場合は、ルールのアクションを選択する必要があります。アクションの効果は、管理対象デバイスと NetFlow エクスポートのどちらからデータを検出するルールを使用しているかによって異なります。

次の表に、これら2つのシナリオで指定されたアクション設定を使用したルールで検出されるアセットの説明を示します。

表 220: 検出ルールのアクション

	管理対象デバイス (Managed Device)	NetFlow エクスポート
除外 (Exclude)	指定されたネットワークをモニタリング対象から除外します。接続の発信元ホストまたは宛先ホストを検出から除外すると、接続は記録されますが、除外したホストの検出イベントは作成されません。	指定されたネットワークをモニタリング対象から除外します。接続の発信元ホストまたは宛先ホストを検出から除外すると、接続は記録されますが、除外したホストの検出イベントは作成されません。
検出: ホスト (Discover: Hosts)	検出イベントに基づいて、ネットワークマップにホストを追加します。(任意。ユーザ検出が有効になっていない場合は必須)。	NetFlow レコードに基づいて、ネットワークマップにホストを追加し、接続をログに記録します。(必須)
検出: アプリケーション (Discover: Applications)	アプリケーション検出に基づいて、ネットワークマップにアプリケーションを追加します。アプリケーションも検出しないルールでは、ホストまたはユーザを検出できないことに注意してください。(必須)	NetFlow レコードと /etc/sf/services 内のポートとアプリケーションプロトコルの関連付けに基づいて、ネットワークマップにアプリケーションプロトコルを追加します。(オプション)
検出: ユーザ (Discover: Users)	ネットワーク検出ポリシーで設定されたユーザプロトコルに関するトラフィックベースの検出に基づいてユーザをユーザテーブルに追加し、ユーザアクティビティをログに記録します。(オプション)	適用対象外
NetFlow 接続のロギング (Log NetFlow Connections)	適用対象外	NetFlow 接続のみをログに記録します。ホストまたはアプリケーションは検出しません。

ルールを使用して管理対象デバイスのトラフィックをモニタする場合は、アプリケーションロギングが必要です。ルールを使用してユーザをモニタする場合は、ホストロギングが必要です。ルールを使用して、エクスポートされたNetFlowレコードをモニタする場合は、ユーザをログに記録するように設定することはできず、アプリケーションロギングは任意です。



(注) ネットワーク検出ポリシーの[アクション (Action)]の設定に基づいて、エクスポートされたNetFlowレコードで接続が検出されます。アクセスコントロールポリシーの設定に基づいて、管理対象デバイスラフィックで接続が検出されます。

## モニタ対象ネットワーク

検出ルールは、モニタ対象アセットの検出を、指定されたネットワーク上のホストとの間のトラフィックだけを対象に行います。検出ルールでは、指定されたネットワーク内の1つ以上のIPアドレスが割り当てられた接続に対して検出が行われ、モニタ対象ネットワーク内のIPアドレスに対してのみイベントが生成されます。デフォルトの検出ルールでは、モニタされているすべてのトラフィックのアプリケーションを検出します (すべてのIPv4トラフィックについては0.0.0.0/0、すべてのIPv6トラフィックについては::/0)。

NetFlow検出を処理し、接続データだけを記録するルールを設定すると、システムは、指定のネットワークの接続元と接続先のIPアドレスを記録します。ネットワーク検出ルールがNetFlowネットワーク接続を記録する唯一の方法を提供することに注意してください。

また、ネットワークオブジェクトまたはオブジェクトグループを使用してモニタ対象ネットワークを指定することもできます。

### 監視対象ネットワークの制限

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

すべての検出ルールに1つ以上のネットワークを含める必要があります。

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [ルールの追加 (Add Rule)] をクリックします。

**ステップ 3** [ネットワーク (Networks)] タブが表示されていない場合は、そのタブをクリックします。

## NetFlow データ検出のルールの設定

**ステップ 4** 必要に応じて、[使用可能なネットワーク (Available Networks)] リストにネットワーク オブジェクトを追加します。詳細については、[検出ルール設定時のネットワーク オブジェクトの作成 \(2155 ページ\)](#) を参照してください。

(注) ネットワーク検出ポリシーで使用されるネットワーク オブジェクトを変更した場合、その変更は設定の変更を展開するまで反映されません。

**ステップ 5** ネットワークを指定します。

- [使用可能なネットワーク (Available Networks)] リストからネットワークを選択します。

**ヒント** ネットワークがすぐにリストに表示されない場合は、リロードアイコン (🔄) をクリックします。

- [使用可能なネットワーク (Available Networks)] ラベルの下にあるテキスト ボックスに IP アドレスを入力します。

**ステップ 6** [追加 (Add)] をクリックします。

**ステップ 7** 必要に応じて、別のネットワークを追加するために、前の 2 つの手順を繰り返します。

**ステップ 8** [保存 (Save)] をクリックして、変更を保存します。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## NetFlow データ検出のルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

Firepower システムでは、NetFlow エクスポートからのデータを使用して、接続および検出イベントを生成したり、ネットワーク マップにホストとアプリケーションのデータを追加したりできます。

検出ルール内で NetFlow エクスポートを選択する場合、ルールは指定されたネットワークの NetFlow データの検出に制限されます。NetFlow デバイスを選択すると使用可能なルールアクションが変更されるため、モニタする NetFlow デバイスを選択してからルール動作の他の側面を設定します。NetFlow エクスポートをモニタするためのポートの除外を設定することはできません。

## 始める前に

- NetFlow-enabled デバイスをネットワーク検出ポリシーに追加します。[NetFlow エクスポートのネットワーク検出ポリシーへの追加 \(2169 ページ\)](#) を参照してください。



## 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [ルールの追加 (Add Rule)] をクリックします。

**ステップ 3** [NetFlow デバイス (NetFlow Device)] タブを選択します。

**ステップ 4** [NetFlow デバイス (NetFlow Device)] ドロップダウンリストから、モニタする NetFlow エクスポートの IP アドレスを選択します。

**ステップ 5** Firepower システムの管理対象デバイスで収集する NetFlow データのタイプを指定します。

- 接続のみ: [アクション (Action)] ドロップダウンリストから Log NetFlow Connections を選択します。
- ホスト、アプリケーション、および接続: [アクション (Action)] ドロップダウンリストから Discover を選択します。[ホスト (Hosts)] チェックボックスが自動的にオンになり、接続データの収集が有効になります。オプションで、[アプリケーション] チェックボックスをオンにして、アプリケーションデータを収集できます。

**ステップ 6** [保存 (Save)] をクリックします。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 検出ルール設定時のネットワーク オブジェクトの作成


スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

新規ネットワーク オブジェクトを再使用可能なネットワーク オブジェクトおよびグループのリストに追加することで、検出ルールに表示される使用可能なネットワークのリストにそれらのオブジェクトを追加できます。

## 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

- ステップ2** [ネットワーク (Networks) ] タブで、[ルール追加 (Add Rule) ] をクリックします。
- ステップ3** [利用可能なネットワーク (Available Networks) ] の隣にある追加アイコン (  ) をクリックします。
- ステップ4** [ネットワークオブジェクトの作成 \(434ページ\)](#) の説明に従って、ネットワークオブジェクトを作成します。
- ステップ5** [ネットワーク検出ルールを設定 \(2151ページ\)](#) の説明に従って、ネットワーク検出ルールの追加を完了します。

## ポート除外

モニタリングからホストを除外できるのと同様に、モニタリングから特定のポートを除外できます。次に例を示します。

- ロードバランサは短期間に同じポート上の複数のアプリケーションを報告する可能性があります。モニタリングからそのポートを除外する (Web ファームを処理するロードバランサ上のポート 80 を除外するなど) ようにネットワーク検出ルールを設定できます。
- 組織で特定の範囲のポートを使用するカスタムクライアントを使用しているとします。このクライアントからのトラフィックが紛らわしいイベントを過剰に生成する場合は、モニタリングからそれらのポートを除外できます。同様に、DNS トラフィックをモニタしないように設定することもできます。この場合は、検出ポリシーがポート 53 をモニタしないように、ルールを設定します。

除外するポートを追加するときには、[利用可能なポート (Available Ports) ] リストから再利用可能なポートオブジェクトを選択するのか、送信元または宛先除外リストにポートを直接追加するのか、新しい再利用可能なポートを作成してからそれを除外リストに移動するのかを決定できます。



(注) NetFlow データの検出を処理するルールでポートを除外することはできません。

### ネットワーク検出ルールでのポートの除外

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

NetFlow データ検出を処理するルールにあるポートを除外することはできません。

### 手順

- ステップ1** [ポリシー (Policies) ] > [ネットワーク検出 (Network Discovery) ] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [ルール of 追加 (Add Rule)] をクリックします。

**ステップ 3** [ポート of 除外 (Port Exclusions)] タブ をクリックします。

**ステップ 4** 必要に応じて、[検出ルール設定時のポートオブジェクトの作成 \(2157ページ\)](#) で説明されているように、使用可能なポートリストにポートオブジェクトを追加します。

**ステップ 5** 次のいずれかの方法を使用して、モニタリング対象から特定の送信元ポートを除外します。

- [使用可能なポート (Available Ports)] リストから1つまたは複数のポートを選択して、[送信元に追加 (Add to Source)] をクリックします。
- ポートオブジェクトを追加せずに特定の送信元ポートからのトラフィックを除外するには、[選択済の送信元ポートリスト (Selected Source Ports)] で、[プロトコル (Protocol)] を選択し、[ポート (Port)] 番号 (1 から 65535 の数値) を入力して、[追加 (Add)] をクリックします。

**ステップ 6** 次のいずれかの方法を使用して、モニタリング対象から特定の宛先ポートを除外します。

- [使用可能なポート (Available Ports)] リストから1つまたは複数のポートを選択して、[宛先に追加 (Add to Destination)] をクリックします。
- ポートオブジェクトを追加せずに特定の宛先ポートからのトラフィックを除外するには、[選択済の宛先ポートリスト (Selected Destination Ports)] で、[プロトコル (Protocol)] を選択し、[ポート (Port)] 番号を入力して、[追加 (Add)] をクリックします。

**ステップ 7** [保存 (Save)] をクリックして、変更内容を保存します。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 検出ルール設定時のポートオブジェクトの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

新規ポートオブジェクトを、Firepower システム内の任意の場所で使用できる再使用可能なポートオブジェクトおよびグループのリストに追加することで、検出ルールに表示される使用可能なポートのリストにそれらのオブジェクトを追加できます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [ネットワーク (Networks)] タブで、[ルールの追加 (Add Rule)] をクリックします。

**ステップ 3** [ポートの除外 (Port Exclusions)] をクリックします。

**ステップ 4** [利用可能なポート (Available Ports)] リストにポートを追加するには、オブジェクトの追加アイコン (+) をクリックします。

**ステップ 5** [名前 (Name)] を入力します。

**ステップ 6** [プロトコル (Protocol)] フィールドで、除外するトラフィックのプロトコルを指定します。

**ステップ 7** [ポート (Port)] フィールドに、モニタリングから除外するポートを入力します。

単一のポート、ダッシュ (-) を使用したポートの範囲、またはポートとポート範囲のカンマ区切りのリストを指定できます。許容されるポート値は 1 ~ 65535 です。

**ステップ 8** [保存 (Save)] をクリックします。

**ステップ 9** ポートがすぐにリストに表示されない場合は、更新アイコン (↻) をクリックします。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ネットワーク検出ルールのゾーン

パフォーマンスを向上させるために、ルール内の監視対象ネットワークに物理的に接続されている管理対象デバイス上のセンシング インターフェイスがルール内のゾーンに含まれるように、検出ルールを設定することができます。

残念ながら、ネットワーク設定の変更は通知されないことがあります。ネットワーク管理者が通知せずにルーティングやホストの変更によりネットワーク設定を変更した場合、正しいネットワーク検出ポリシー設定を完全に把握するのが難しくなります。管理対象デバイス上のセンシングインターフェイスがどのようにネットワークに物理的に接続されているかが不明な場合は、ゾーンの設定はデフォルト値のままにしておいてください。このデフォルト値によって、システムは展開環境内のすべてのゾーンに検出ルールを展開します (ゾーンが除外されない場合、システムではすべてのゾーンに検出ポリシーを展開します)。

#### ネットワーク検出ルールでのゾーンの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

## 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [ルールの追加 (Add Rule)] をクリックします。

**ステップ 3** [ゾーン (Zones)] タブをクリックします。

**ステップ 4** [使用可能なゾーン (Available Zones)] リストでゾーンを選択します。

**ステップ 5** [保存 (Save)] をクリックして、加えた変更を保存します。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## トラフィック ベース検出のアイデンティティ ソース

トラフィック ベース検出は、Firepower システムでサポートされている唯一の権限のないアイデンティティ ソースです。トラフィック ベース検出を設定すると、管理対象デバイスは、指定したネットワークでの LDAP、AIM、POP3、IMAP、Oracle、SIP (VoIP)、FTP、HTTP、MDNS、SMTP のログインを検出します。トラフィック ベースの検出から取得されたデータは、ユーザ認識にのみ使用できます。権威のあるアイデンティティ ソースとは異なり、トラフィック ベースの検出はネットワーク検出ポリシーで設定します。[トラフィック ベースのユーザ検出の設定 \(2161 ページ\)](#) を参照してください。

次の制限事項に注意してください。

- トラフィック ベースの検出では、LDAP 接続に対する Kerberos ログインのみを LDAP 認証として解釈します。また、管理対象デバイスは、SSL や TLS などのプロトコルを使用して暗号化された LDAP 認証を検出できません。
- トラフィック ベースの検出では OSCAR プロトコルを使用した AIM ログインだけを検出します。TOC2 を使用する AIM ログインは検出できません。
- トラフィック ベースの検出では SMTP ログインを制限することができません。これは、ユーザが SMTP ログインに基づいてデータベースに追加されていないためです。システムが SMTP ログインを検出しても、一致する電子メールアドレスのユーザがデータベース内に存在しなければ、そのログインは記録されません。

トラフィック ベースの検出は、失敗したログイン試行も記録します。失敗ログイン試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。トラフィック ベースの検出により検出された失敗ログイン アクティビティのユーザ アクティビティ タイプは [失敗したユーザ ログイン (Failed User Login)] です。



- (注) システムは失敗した HTTP ログインと成功した HTTP ログインを区別できません。HTTP ユーザ情報を表示するには、トラフィック ベースの検出設定で [失敗したログイン試行の取得 (Capture Failed Login Attempts) ] を有効にする必要があります。



- 注意** ネットワーク検出ポリシーを使用して、HTTP、FTP、MDNS プロトコルを介した非権限、トラフィック ベースのユーザ検出を有効/無効にすると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

### トラフィック ベースの検出データ

デバイスがトラフィック ベースの検出を使用してログインを検出すると、次の情報をユーザ アクティビティとして記録するために Firepower Management Center に送信します。

- ログインで識別されたユーザ名
- ログインの時刻
- ログインに関係する IP アドレス。このアドレスは、ユーザのホスト (LDAP、POP3、IMAP、および AIM ログインの場合)、サーバ (HTTP、MDNS、FTP、SMTP および Oracle ログインの場合)、またはセッション発信元 (SIP ログインの場合) の IP アドレスになります。
- ユーザの電子メール アドレス (POP3、IMAP、および SMTP ログインの場合)
- ログインを検出したデバイスの名前

ユーザがすでに検出されている場合、Firepower Management Center はそのユーザのログイン履歴を更新します。Firepower Management Center は POP3 および IMAP ログイン内の電子メールアドレスを使用して LDAP ユーザに関連付ける場合があることに注意してください。これは、Firepower Management Center が新しい IMAP ログインを検出して、その IMAP ログイン内の電子メールアドレスが既存の LDAP ユーザのアドレスと一致した場合は、IMAP ログインで新しいユーザが作成されるのではなく、LDAP ユーザの履歴が更新されることを意味します。

ユーザが以前に検出されなかった場合、Firepower Management Center はユーザ データベースにユーザを追加します。AIM、SIP、Oracle ログインでは、常に新しいユーザ レコードが作成されます。これは、それらのログインイベントには Firepower Management Center が他のログインタイプに関連付けることができるデータが含まれていないためです。

Firepower Management Center は、次の場合に、ユーザ アイデンティティまたはユーザ ID を記録しません。

- そのログインタイプを無視するようにネットワーク検出ポリシーを設定した場合

- 管理対象デバイスが SMTP ログインを検出したものの、ユーザ データベースに電子メールアドレスが一致する、検出済みの LDAP、POP3、または IMAP ユーザが含まれていない場合

ユーザ データはユーザ テーブルに追加されます。

### トラフィック ベースの検出戦略

ユーザ アクティビティを検出するプロトコルを制限して、検出するユーザの総数を削減することにより、ほぼ完全なユーザ情報を提供していると思われるユーザに焦点を絞ることができます。プロトコルの検出を制限すると、ユーザ名の散乱を最小限に抑え、Firepower Management Center 上の記憶域を節約することができます。

トラフィック ベースの検出プロトコルを選択する際には、以下を検討してください。

- AIM、POP3、IMAP などのプロトコル経由でユーザ名を取得すると、契約業者、訪問者、およびその他のゲストからのネットワーク アクセスによって組織に無関係なユーザ名が収集される可能性があります。
- AIM、Oracle、および SIP ログインは、無関係なユーザ レコードを作成する可能性があります。この現象は、このようなログイン タイプが、システムが LDAP サーバから取得するユーザ メタデータのいずれにも関連付けられていないうえ、管理対象デバイスが検出するその他のログイン タイプに含まれている情報のいずれにも関連付けられていないために発生します。そのため、Firepower Management Center は、これらのユーザ とその他のユーザ タイプを関連付けることができません。

### トラフィック ベースのユーザ検出の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

ネットワーク検出ルールでトラフィック ベースのユーザ検出を有効にすると、ホスト検出が自動で有効になります。トラフィック ベースの検出の詳細については、[トラフィック ベース検出のアイデンティティ ソース \(2143 ページ\)](#) を参照してください。

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [ユーザ (Users)] をクリックします。

**ステップ 3** 編集アイコン (✎) をクリックします。

- ステップ 4** ログインを検出するプロトコルのチェックボックスをオンにするか、ログインを検出しないプロトコルのチェックボックスをオフにします。
- ステップ 5** オプションで、LDAP、POP3、FTP、IMAP トラフィックで検出されたログイン試行の失敗を記録したり、HTTP ログインのユーザ情報を取得するには、[失敗したログイン試行のキャプチャ (Capture Failed Login Attempts) ] を有効にします。
- ステップ 6** [保存 (Save) ] をクリックします。

### 次のタスク



#### 注意

ネットワーク検出ポリシーを使用して、HTTP、FTP、MDNS プロトコルを介した非権限、トラフィック ベースのユーザ検出を有効/無効にすると 設定の変更を展開すると **Snort** プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

- [ネットワーク検出ルールの設定 \(2151 ページ\)](#) の説明に従って、ユーザを検出するようにネットワーク検出ルールを設定します。
- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## 高度なネットワーク検出オプションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

ネットワーク検出ポリシーの [詳細 (Advanced) ] タブを使用すれば、検出するイベント、検出データの保存期間と更新頻度、影響相関に使用する脆弱性マッピング、およびオペレーティング システム ID とサーバ ID の競合の解決方法に関するポリシー全体の設定を構成できます。加えて、ホスト入力ソースと NetFlow エクスポートを追加して、他のソースからのデータのインポートを許可できます。



- (注) 検出イベントとユーザ活動イベントのデータベースイベント制限はシステム構成で設定されます。



## 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [詳細設定 (Advanced)] をクリックします。

**ステップ 3** 変更する設定の横にある編集アイコン (✎) または追加アイコン (+) をクリックします。

- [データストレージ設定 (Data Storage Settings)] : [ネットワーク検出データストレージの設定 \(2172 ページ\)](#) の説明に従って、設定を更新します。
- [イベントロギング設定 (Event Logging Settings)] : [ネットワーク検出イベントロギングの設定 \(2172 ページ\)](#) の説明に従って、設定を更新します。
- [全般設定 (General Settings)] : [ネットワーク検出全般設定 \(2164 ページ\)](#) の説明に従って、設定を更新します。
- [ID 競合設定 (Identity Conflict Settings)] : [ネットワーク検出アイデンティティ競合の解決の設定 \(2165 ページ\)](#) の説明に従って、設定を更新します。
- [侵害の兆候設定 (General Settings)] : [侵害の兆候ルールの有効化 \(2168 ページ\)](#) の説明に従って、設定を更新します。
- [NetFlow エクスポート (NetFlow Exporters)] : [NetFlow エクスポートのネットワーク検出ポリシーへの追加 \(2169 ページ\)](#) の説明に従って、設定を更新します。
- [OS およびサーバの ID ソース (OS and Server Identity Sources)] : [ネットワーク検出 OS およびサーバアイデンティティソースの追加 \(2173 ページ\)](#) の説明に従って、設定を更新します。
- [影響評価に使用する脆弱性 (Vulnerabilities to use for Impact Assessment)] : [ネットワーク検出の脆弱性影響評価の有効化 \(2167 ページ\)](#) の説明に従って、設定を更新します。

**ステップ 4** [保存 (Save)] をクリックします。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 関連トピック

[データベース イベント数の制限 \(930 ページ\)](#)

# ネットワーク検出の一般設定

一般設定は、システムがネットワークマップを更新する頻度と、検出中にサーババナーをキャプチャするかどうかを制御します。

**[バナーのキャプチャ (Capture Banners)]**

サーバベンダーとバージョン（「バナー」）をアドバタイズするネットワークトラフィックからの見出し情報をシステムで保存させる場合、このチェックボックスをオンにします。この情報は、収集された情報に追加のコンテキストを提供できます。サーバ詳細にアクセスすることによって、ホストに関して収集されたサーババナーにアクセスできます。

**[アップデート間隔 (Update Interval)]**

システムが情報を更新する時間間隔（ホストの IP アドレスのいずれかが最後に検出された時点、アプリケーションが使用された時点、アプリケーションのヒット数など）。デフォルト設定は 3600 秒（1 時間）です。

更新タイムアウトの時間間隔を短く設定すると、より正確な情報がホスト画面に表示されますが、より多くのネットワークイベントが生成されることに注意してください。

**ネットワーク検出全般設定**

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

**手順**

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [詳細設定 (Advanced)] をクリックします。

**ステップ 3** [全般設定 (General Settings)] の横にある編集アイコン (✎) をクリックします。

**ステップ 4** [ネットワーク検出の一般設定 \(2163 ページ\)](#) の説明に従って設定を更新します。

**ステップ 5** [保存 (Save)] をクリックして、全般設定を保存します。

**次のタスク**

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

**ネットワーク検出アイデンティティ競合の設定**

システムは、オペレーティングシステムとサーバのフィンガープリントをトラフィック内のパターンに照合することで、どのオペレーティングシステムおよびアプリケーションがホストで

実行されているかを判別します。最も信頼できるオペレーティングシステムとサーバの ID 情報を提供するために、システムは複数のソースからのフィンガープリント情報を照合します。

システムは、すべてのパッシブデータを使用して、オペレーティングシステム ID を抽出し、信頼値を割り当てます。

デフォルトでは、ID 競合が存在しなければ、スキャナまたはサードパーティアプリケーションによって追加された ID データで、Firepower System によって検出された ID データが上書きされます。[アイデンティティ ソース (Identity Sources)] 設定を使用して、スキャナとサードパーティアプリケーションのフィンガープリント ソースをプライオリティでランク付けできます。システムはソースごとに1つずつの ID を保持しますが、プライオリティが最も高いサードパーティアプリケーションまたはスキャナソースからのデータのみが最新の ID として使用されます。ただし、プライオリティに関係なく、ユーザ入力データによって、スキャナまたはサードパーティアプリケーションのデータが上書きされることに注意してください。

ID 競合は、[アイデンティティ ソース (Identity Sources)] 設定に列挙されたアクティブ スキャナ ソースまたはサードパーティアプリケーション ソースと Firepower システム ユーザのどちらかから取得された既存の ID と競合する ID をシステムが検出した場合に発生します。デフォルトでは、ID 競合は自動的に解決されないため、ホストプロファイルを通して、または、ホストをスキャンし直すか新しい ID データを追加し直してパッシブ ID を上書きすることにより、解決する必要があります。ただし、パッシブ ID またはアクティブな ID のいずれかを維持することで、競合を自動的に解決するようにシステムを設定できます。

#### [ID 競合イベントを生成する (Generate Identity Conflict Event)]

ID 競合が発生したときにシステムがイベントを生成するかどうかを指定します。

#### [自動的に競合を解決する (Automatically Resolve Conflicts)]

[自動的に競合を解決する (Automatically Resolve Conflicts)] ドロップダウンリストから、次のいずれかを選択します。

- ID 競合の手動での競合解決を強制する場合は、[無効 (Disabled)]
- ID 競合が発生したときにシステムがパッシブ フィンガープリントを使用するようにする場合は、[アイデンティティ (Identity)]
- ID 競合が発生したときにシステムが優先度が最も高いアクティブなソースの現在の ID を使用するようにする場合は、[キープアクティブ (Keep Active)]

## ネットワーク検出アイデンティティ競合の解決の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

## 手順

- ステップ1 [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。  
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ2 [詳細設定 (Advanced)] をクリックします。
- ステップ3 [ID 競合設定 (Identity Conflict Settings)] の横にある編集アイコン (✎) をクリックします。
- ステップ4 [ネットワーク検出アイデンティティ競合の設定 \(2164ページ\)](#) の説明に従って、[ID競合設定の編集 (Edit Identity Conflict Settings)] ポップアップウィンドウの設定を更新します。
- ステップ5 [保存 (Save)] をクリックして、ID 競合設定を保存します。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

# ネットワーク検出の脆弱性の影響の評価オプション

Firepower システムで侵入イベントとの影響相関を実行する方法を設定できます。有効な選択肢は次のとおりです。

- システム ベースの脆弱性情報を使用して影響相関を実行する場合は、[ネットワーク検出の脆弱性マッピングを使用 (Use Network Discovery Vulnerability Mappings)] チェックボックスをオンにします。
- サードパーティの脆弱性参照を使用して影響相関を実行する場合は、[サードパーティの脆弱性マッピングを使用 (Use Third-Party Vulnerability Mappings)] チェックボックスをオンにします。詳細については、*Firepower System Host Input API Guide* を参照してください。

チェックボックスのどちらかまたは両方を選択できます。システムが侵入イベントを生成し、選択された脆弱性マッピングセット内の脆弱性のあるサーバまたはオペレーティングシステムがそのイベントに関係するホストに含まれている場合、侵入イベントは脆弱 (レベル1: 赤) 影響アイコンでマークされます。ベンダーまたはバージョン情報のないサーバの場合は、Firepower Management Center 構成で脆弱性マッピングを有効にする必要があることに注意してください。

両方のチェックボックスをオフにした場合は、侵入イベントが脆弱 (レベル1: 赤) 影響アイコンでマークされません。

## 関連トピック

- [サードパーティの脆弱性のマッピング \(2057 ページ\)](#)
- [サーバの脆弱性のマッピング \(988 ページ\)](#)

## ネットワーク検出の脆弱性影響評価の有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [詳細設定 (Advanced)] をクリックします。

**ステップ 3** [影響評価に使用する脆弱性 (Vulnerabilities to use for Impact Assessment)] の横にある編集アイコン (✎) をクリックします。

**ステップ 4** [ネットワーク検出の脆弱性の影響の評価オプション \(2166 ページ\)](#) 説明に従って、[脆弱性設定の編集 (Edit Vulnerability Settings)] ポップアップ ウィンドウで設定を更新します。

**ステップ 5** [保存 (Save)] をクリックして、脆弱性設定を保存します。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 侵害の兆候

Firepower システムでは、ネットワーク検出ポリシー内の IOC ルールを使用して悪意のある手段によって侵害されている可能性があるホストを特定します。ホストがこれらのシステム提供のルールで指定されている条件を満たしている場合、そのホストはシステムによって侵害の兆候 (IOC) でタグ付けされます。関連のルールは *IOC* ルールと呼ばれます。各 IOC ルールは 1 種類の IOC タグに対応しています。*IOC* タグは可能性のある侵害の性質を指定します。

次のうちいずれかの事態が発生すると、関与しているホストに Firepower Management Center がタグを付けます。

- システムは、侵入、接続、セキュリティ インテリジェンス、およびファイルまたはマルウェア イベントを使用してモニタ対象のネットワークとそのトラフィックについて集められたデータを関連付け、潜在的な IOC が発生したと判断します。
- Firepower Management Center は AMP クラウドを経由してエンドポイント向け AMP の展開から IOC データをインポートすることができます。このデータがホスト自体の活動 (個別のプログラムによってまたはプログラム上で実行されるアクションなど) を検査するた

め、ネットワーク専用データでは理解するのが難しい可能性がある脅威に対する理解が促されます。便宜上、Firepower Management Center はシスコが開発した新しい IOC タグを AMP クラウドから自動的に取得します。

この機能を設定するには、[侵害の兆候ルールの有効化 \(2168 ページ\)](#) を参照してください。

また、ホストの IOC データに対する関連ルールと、IOC でタグ付けされたホストから成るコンプライアンス ホワイトリストも記述することができます。

タグ付けされた IOC の調査や操作を行うには、[侵害の兆候データ \(2717 ページ\)](#) とそのサブトピック参照してください。

## 侵害の兆候ルールの有効化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

システムで侵害の兆候 (IOC) を検出してタグを付けるには、まず、ネットワーク検出ポリシーで 1 つ以上の IOC ルールを有効化する必要があります。IOC ルールのそれぞれが IOC タグの 1 つのタイプに対応します。すべての IOC ルールはシスコが事前定義しています。オリジナルルールを作成することはできません。ネットワークや組織のニーズに合わせて、一部またはすべてのルールを有効にすることができます。たとえば、Microsoft Excel などのソフトウェアを使用しているホストが絶対に監視対象ネットワーク上に出現しない場合は、Excel ベースの脅威に関係する IOC タグを有効にしないようにできます。



### ヒント

個別のホストの IOC ルールを無効にするには、[単一ホストにおける侵害の兆候のルール状態の編集 \(2721 ページ\)](#) を参照してください。

### 始める前に

IOC ルールは Firepower システムの他のコンポーネントと、AMP for Endpoints によって提供されるデータに基づいてトリガーされるため、これらのコンポーネントが正しくライセンス付与され、IOC タグを設定できるように設定されている必要があります。侵入検知および防御 (IPS) および Advanced Malware Protection (AMP) など、有効にする予定の IOC ルールに関連付けられている Firepower システムの機能を有効にします。IOC ルールの関連機能が有効になっていないと、関連データが収集されず、ルールをトリガーできません。

### 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

- ステップ 2** [詳細設定 (Advanced) ] をクリックします。
- ステップ 3** [侵害の兆候設定 (Indications of Compromise Settings) ] の横にある編集アイコン (✎) をクリックします。
- ステップ 4** IOC 機能全体のオンとオフを切り替えるには、[IOC の有効化 (Enable IOC) ] の横にあるスライダをクリックします。
- ステップ 5** 個別の IOC ルールをグローバルに有効または無効にするには、ルールの [有効 (Enabled) ] 列のスライダをクリックします。
- ステップ 6** [保存 (Save) ] をクリックして IOC ルール設定を保存します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## NetFlow エクスポートのネットワーク検出ポリシーへの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

#### 始める前に

- [Firepower システムの NetFlow データ \(2027 ページ\)](#) の説明に従い、使用する NetFlow エクスポートを設定します。
- NetFlow の他の要件については、[NetFlow データを使用するための要件 \(2027 ページ\)](#) の説明を参照してください。

#### 手順

- ステップ 1** [ポリシー (Policies) ] > [ネットワーク検出 (Network Discovery) ] を選択します。
- マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 2** [詳細設定 (Advanced) ] をクリックします。
- ステップ 3** [NetFlow デバイス (NetFlow Devices) ] の横にある追加アイコン (+) をクリックします。
- ステップ 4** [IP アドレス (IP Address) ] フィールドに、NetFlow データを収集する対象デバイスの管理を行うネットワークデバイスの IP アドレスを入力します。
- ステップ 5** 必要に応じて、以下を行います。

- NetFlow エクスポートをさらに追加するには、上記の2つのステップを繰り返します。
- 削除アイコン (🗑️) をクリックして、NetFlow エクスポートを削除します。検出ルールで NetFlow エクスポートを使用する場合は、先にルールを削除しないと、[詳細 (Advanced)] ページからデバイスを削除できないことに注意してください。

**ステップ 6** [保存 (Save) ] をクリックします。

---

### 次のタスク

- [ネットワーク検出ルールの設定 \(2151 ページ\)](#) の説明に従い、NetFlow トラフィックをモニタリングするネットワーク検出ルールを設定します。
- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## ネットワーク検出のデータ ストレージ設定

ディスクバリのデータストレージ設定では、ホスト制限とタイムアウトの設定が行われます。

### ホスト制限の到達時 (When Host Limit Reached)

Firepower Management Center がモニタでき、ネットワーク マップに保存できるホストの数。モデルによって異なります。ホスト制限に到達した後に新しいホストを検出すると、[ホスト制限の到達時 (When Host Limit Reached) ] オプションが制御を行います。次の操作を実行できます。

### ホストをドロップ (Drop hosts)

システムは、長期間非アクティブになっているホストをドロップして、新しいホストを追加します。これがデフォルトの設定です。

### 新しいホストを挿入しない (Don't insert new hosts)

システムは、新たに検出されたホストを追跡しません。システムが新しいホストを追跡するのは、管理者がドメインのホスト制限を増加させた後などに、ホストカウントが制限を下回る場合、ネットワークマップからホストを手動で削除する場合、またはホストが非アクティブであることからタイムアウトと見なされる場合のみです。

マルチドメイン展開では、リーフドメインは使用可能なモニタされたホストのプールを共有します。各リーフドメインがネットワークマップに値を入力できるように、ホスト制限をサブドメインレベルのドメインプロパティで設定できます。各リーフドメインには独自のネットワーク検出ポリシーがあるため、次の表で説明するように各リーフドメインは、システムが新しいホストを検出すると、独自の動作を制御します。



表 221: マルチテナンシーによるホスト制限への到達

設定	ドメインのホスト制限の有無	ドメインのホスト制限に到達した場合	先祖ドメインのホスト制限に到達した場合
ホストをドロップ	Yes	制限付きドメインの最も古いホストをドロップします。	ホストをドロップするように設定されているすべての子孫リーフ ドメインで最も古いホストをドロップします。  ドロップされるホストがなければ、ホストの追加は行われません。
	No	適用対象外	ホストをドロップし、一般プールを共有するように設定されているすべての子孫リーフ ドメインで最も古いホストをドロップします。
新しいホストを挿入しない	「Yes」または「No」で教えてください。	ホストの追加は行われません。	ホストの追加は行われません。

#### ホスト タイムアウト (Host Timeout)

システムが、非アクティブであるという理由でネットワーク マップからホストを除外するまでの分単位の時間。デフォルト設定は 10080 分 (1 週間) です。ホスト IP アドレスと MAC アドレスは個別にタイムアウトすることができますが、関連するアドレスのすべてがタイムアウトするまで、ホストはネットワーク マップから削除されません。

ホストの早期タイムアウトを避けるために、ホストのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

#### サーバタイムアウト (Server timeout)

システムが、非アクティブであるという理由でネットワーク マップからサーバを除外するまでの分単位の時間。デフォルト設定は 10080 分 (1 週間) です。

サーバの早期タイムアウトを避けるために、サービスのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

#### クライアントアプリケーションのタイムアウト (Client Application Timeout)

システムが、非アクティブであるという理由でネットワーク マップからクライアントを除外するまでの分単位の時間。デフォルト設定は 10080 分 (1 週間) です。

クライアントのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

## 関連トピック

[Firepower システムのホスト制限](#) (2035 ページ)

[ドメインのプロパティ](#) (341 ページ)

## ネットワーク検出データストレージの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

## 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [詳細設定 (Advanced)] をクリックします。

**ステップ 3** [データストレージ設定 (Data Storage Settings)] の横にある編集アイコン (✎) をクリックします。

**ステップ 4** [ネットワーク検出のデータストレージ設定 \(2170 ページ\)](#) の説明に従って、[データストレージ設定 (Data Storage Settings)] ダイアログの設定を更新します。

**ステップ 5** [保存 (Save)] をクリックして、データストレージ設定を保存します。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ネットワーク検出イベントロギングの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

イベントロギング設定は、検出イベントとホスト入力イベントを記録するかどうかを制御します。イベントを記録しない場合は、イベントビューで検索することも、関連ルールをトリガーするために使用することもできません。

## 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [詳細設定 (Advanced)] をクリックします。

**ステップ 3** [イベント ログGING設定 (Event Logging Settings)] の横にある編集アイコン (✎) をクリックします。

**ステップ 4** [ディスカバリ イベントタイプ \(2698 ページ\)](#) および [ホスト入力 イベントタイプ \(2703 ページ\)](#) の説明に従って、データベースに記録する検出イベントタイプとホスト入力 イベントタイプの横にあるチェックボックスをオンまたはオフにします。

**ステップ 5** [保存 (Save)] をクリックして、イベント ログGING設定を保存します。

## 次のタスク

- ・設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ネットワーク検出 OS およびサーバアイデンティティ ソースの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

ネットワーク検出ポリシーの[詳細 (Advanced)] タブで、新しいアクティブソースを追加し、また、既存の送信元の優先度やタイムアウトの設定を変更できます。

このページにスキャナを追加しても、Nmap スキャナ用の完全な統合機能は追加されませんが、インポートされたサードパーティアプリケーションまたはスキャン結果の統合が可能になります。

サードパーティアプリケーションまたはスキャナからデータをインポートする場合は、ソースからの脆弱性がネットワークで検出された脆弱性にマップされていることを確認してください。

## 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [詳細設定 (Advanced)] をクリックします。

**ステップ 3** [OS とサーバ ID ソース (OS and Server Identity Sources)] の横にある編集アイコン (✎) をクリックします。

**ステップ 4** 新しいソースを追加するには、[ソースの追加 (Add Sources)] をクリックします。

**ステップ 5** 名前を入力します。

**ステップ 6** ドロップダウン リストからインプット ソースの [タイプ (Type)] を選択します。

- AddScanResult 機能を使用してスキャン結果をインポートする場合は、[スキャナ (Scanner)] を選択します。
- スキャン結果をインポートしない場合は、[アプリケーション (Application)] を選択します。

**ステップ 7** このソースによるネットワーク マップへの ID の追加からその ID の削除までの期間を指定するには、[タイムアウト (Timeout)] ドロップダウンリストから、[時間 (Hours)]、[日 (Days)]、または [週 (Weeks)] を選択し、該当する期間を入力します。

**ステップ 8** 必要に応じて、以下を行います。

- ソースを昇格させて、オペレーティング システム ID とアプリケーション ID よりもリストでは下にあるソースを優先的に使用するには、そのソースを選択して上矢印をクリックします。
- ソースを降格させて、リストで上にあるソースから提供される ID が存在しない場合にのみオペレーティング システム ID とアプリケーション ID を使用するには、そのソースを選択して下矢印をクリックします。
- ソースを削除するには、ソースの横にある削除アイコン (🗑️) をクリックします。

**ステップ 9** [保存 (Save)] をクリックして、ID ソース設定を保存します。

---

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

#### 関連トピック

[サードパーティの脆弱性のマッピング \(2057 ページ\)](#)

## ネットワーク検出戦略のトラブルシューティング

システムのデフォルトの検出機能に変更を加える前に、実装すべきソリューションを決定できるように、どのホストが正しく識別されていないかと、その原因を分析してください。

#### 管理対象デバイスは正しく配置されていますか

ロードバランサ、プロキシサーバ、NAT デバイスなどのネットワーク デバイスが、識別されないホストまたは誤って識別されたホストと管理対象デバイスとの間に存在する場合は、カスタムフィンガープリントを使用するのではなく、誤って識別されたホストのより近くに管理対

象デバイスを配置します。このシナリオでは、カスタムフィンガープリントの使用は推奨しません。

#### 識別されないオペレーティングシステムに一意の TCP スタックがありますか

システムがホストを誤って識別した場合、カスタムフィンガープリントを作成してアクティブにするか、検出（ディスカバリ）データの代わりに Nmap またはホストの入力データを使用するかを決定するために、ホストが誤って識別された理由を調べる必要があります。



#### 注意

ホストの誤認が発生した場合は、カスタムフィンガープリントを作成する前にサポート担当者にお問い合わせください。

ホストがデフォルトではシステムに検出されないオペレーティングシステムを実行していて、識別用の TCP スタックの特性を既存の検出されているオペレーティングシステムと共有していない場合、カスタムフィンガープリントを作成する必要があります。

たとえば、システムで識別できない一意の TCP スタックを保持する Linux のカスタマイズバージョンが存在する場合、継続的に自分でデータを更新する必要があるスキャン結果またはサードパーティのデータを使用するのではなく、システムがそのホストを識別してそのホストを監視し続けることができるカスタムフィンガープリントを作成する方が便利です。

オープンソースの Linux ディストリビューションの多くで同じカーネルを使用しているため、システムでは Linux のカーネル名を使用してそれらを識別することに注意してください。Red Hat Linux システム用のカスタムフィンガープリントを作成する場合、同じフィンガープリントが複数の Linux ディストリビューションに一致するために、その他のオペレーティングシステム（Debian Linux、Mandrake Linux、Knoppix など）が Red Hat Linux として識別されることがあります。

フィンガープリントをあらゆる状況で使用することは避けてください。たとえば、ホストの TCP スタックが別のオペレーティングシステムと類似するか、または同一になるように、すでに変更済みの場合があります。たとえば、Apple Mac OS X ホストのフィンガープリントが Linux 2.4 ホストと同じフィンガープリントになるように変更されると、システムはそのホストを Mac OS X ではなく Linux 2.4 として識別します。その Mac OS X ホストにカスタムフィンガープリントを作成すると、すべての正規の Linux 2.4 ホストが誤って Mac OS X ホストとして識別される場合があります。この場合、Nmap が正しくホストを識別するならば、そのホストに対して定期的な Nmap スキャンをスケジュールできます。

ホスト入力を使用して、サードパーティ製のシステムからデータをインポートする場合、サーバおよびアプリケーションプロトコルを説明するためにサードパーティが使用するベンダー、製品、およびバージョンの文字列を、それらの製品の Cisco の定義にマッピングする必要があります。アプリケーションデータを Firepower システムのベンダーとバージョンの定義にマッピングした場合でも、インポートされたサードパーティ製の脆弱性はクライアントまたは Web アプリケーションの影響評価には使用されないことに注意してください。

システムは複数のソースからのデータを照合して、オペレーティングシステムまたはアプリケーションの現在の ID を判別することがあります。

Nmap データの場合、定期的な Nmap スキャンをスケジュールできます。ホスト入力データの場合、インポート用の Perl スクリプト、またはコマンドラインユーティリティを定期的に行うことができます。ただし、アクティブのスキャンデータとホスト入力データは、検出（ディスカバリ）データの頻度で更新されないことがあるので注意してください。

### Firepower システムがすべてのアプリケーションを識別できますか

ホストがシステムによって正しく識別されるものの、識別されないアプリケーションがホストにある場合、ユーザ定義のディテクタを作成して、アプリケーションを識別するために役立つポートおよびパターン マッチング情報をシステムに提供することができます。

### 脆弱性を修正するパッチを適用しましたか

システムがホストを正しく識別するものの、適用した修正が反映されない場合、ホスト入力機能を使用してパッチ情報をインポートすることができます。パッチ情報をインポートする場合、修正名をデータベース内の修正にマッピングする必要があります。

### サードパーティ製の脆弱性を追跡しますか

影響の関連付け（相関）に使用したいサードパーティ製システムからの脆弱性情報がある場合、サーバおよびアプリケーションプロトコル用のサードパーティの脆弱性 ID を Cisco のデータベース内の脆弱性 ID にマッピングしてから、ホスト入力機能を使用してそれらの脆弱性をインポートすることができます。ホスト入力機能の使用の詳細については、『*Firepower System Host Input API Guide*』を参照してください。アプリケーションデータを Firepower システムのベンダーとバージョンの定義にマッピングした場合でも、インポートされたサードパーティ製の脆弱性はクライアントまたは Web アプリケーションの影響評価には使用されないことに注意してください。



## 第 89 章

# レルムとアイデンティティ ポリシー

次のトピックでは、レルムとアイデンティティ ポリシーについて説明します。

- [レルムとアイデンティティ ポリシーについて \(2177 ページ\)](#)
- [レルムの作成 \(2185 ページ\)](#)
- [アイデンティティ ポリシーの作成 \(2192 ページ\)](#)
- [アイデンティティ ルールの作成 \(2193 ページ\)](#)
- [レルムの管理 \(2197 ページ\)](#)
- [アイデンティティ ポリシーの管理 \(2199 ページ\)](#)
- [アイデンティティ ルールの管理 \(2199 ページ\)](#)

## レルムとアイデンティティ ポリシーについて

レルムは、同じディレクトリ クレデンシャルを共有する 1 つ以上の LDAP または Microsoft Active Directory サーバで構成されます。ユーザおよびユーザ グループ クエリやユーザ制御を実行したり、権限のあるアイデンティティ ソースを設定したりするには、レルムを設定する必要があります。1 つ以上のレルムを設定すると、アイデンティティ ポリシーを設定できます。

アイデンティティ ポリシーは、ネットワーク上のトラフィックを権限のあるアイデンティティ ソースおよびレルムと関連付けます。1 つ以上のアイデンティティ ポリシーを設定した後、1 つをアクセス コントロール ポリシーに関連付け、そのアクセス コントロール ポリシーを管理対象デバイスに展開できます。

## レルムについて

レルムとは、Firepower Management Center とモニタリング対象のサーバ上にあるユーザ アカウントの間の接続です。レルムでは、サーバの接続設定と認証フィルタの設定を指定します。レルムでは次のことを実行できます。

- アクティビティをモニタするユーザとユーザ グループを指定する。
- 権限のあるユーザ、および権限のあるユーザ以外の一部のユーザ（トラフィック ベースの検出で検出された POP3 および IMAP ユーザ、およびトラフィック ベースの検出、ユーザ

エージェント、TS エージェント、ISE によって検出されたユーザ) のユーザ メタデータについてユーザ リポジトリに照会する。

レルム内のディレクトリとして複数のドメインコントローラを追加できますが、同じ基本レルム情報を共有する必要があります。レルム内のディレクトリは、LDAP サーバのみ、または Active Directory (AD) サーバのみである必要があります。レルムを有効にすると、保存された変更は次回 Firepower Management Centerがサーバに照会するときに適用されます。

ユーザ認識を行うには、[レルムがサポートされているサーバ](#)のレルムを設定する必要があります。システムは、これらの接続を使用して、POP3 および IMAP ユーザに関連するデータについてサーバにクエリし、トラフィック ベースの検出で検出された LDAP ユーザに関するデータを収集します。

システムは、POP3 および IMAP ログイン内の電子メールアドレスを使用して、Active Directory、OpenLDAP、または Oracle Directory Server Enterprise Edition サーバ上の LDAP ユーザに関連付けます。たとえば、LDAP ユーザと電子メールアドレスが同じユーザの POP3 ログインを管理対象デバイスが検出すると、システムはLDAP ユーザのメタデータをそのユーザに関連付けます。

ユーザ制御を実行するために以下のいずれかを設定できます。

- ユーザ エージェントまたは ISE 用の AD サーバのレルム
- TS エージェント用の AD サーバのレルム
- キャプティブ ポータル用の AD、Oracle Directory、OpenLDAP サーバのレルム

### ユーザ ダウンロードについて

特定の検出されたユーザの、次のユーザとユーザ グループのメタデータを取得するために、Firepower Management Center と LDAP サーバまたは AD サーバとの間の接続を確立するためのレルムを設定することができます。

- キャプティブ ポータルで認証された、あるいはユーザ エージェントまたは ISE で報告された LDAP および AD ユーザ。このメタデータは、ユーザ認識とユーザ制御に使用できます。
- トラフィック ベースの検出で検出された POP3 と IMAP ユーザ ログイン (ユーザが LDAP または AD ユーザと同じ電子メールアドレスを持つ場合)。このメタデータは、ユーザ認識に使用できます。

レルム内の1つのディレクトリとして、個々のサーバ接続を設定します。ユーザ認識とユーザ制御のためにレルムのユーザおよびユーザ グループデータをダウンロードするには、[アクセスコントロールのためのユーザおよびユーザ グループのダウンロード (Download users and user groups for access control)] をオンにする必要があります。

Firepower Management Centerは、ユーザごとに次の情報とメタデータを取得します。

- LDAP ユーザ名



- 姓と名
- 電子メール アドレス (Email address)
- 部署名 (Department)
- 電話番号 (Telephone number)

#### ユーザ アクティビティ データについて

ユーザ アクティビティ データはユーザ アクティビティ データベースに保存され、ユーザのアイデンティティ データはユーザ データベースに保存されます。アクセス制御で保存できる使用可能なユーザの最大数は Firepower Management Center モデルによって異なります。含めるユーザとグループを選択するときは、ユーザの総数がモデルの上限より少ないことを確認してください。アクセス制御パラメータの範囲が広すぎる場合、Firepower Management Center はできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザの数をメッセージセンターの [タスク (Tasks) ] タブ ページで報告します。



- (注) ユーザリポジトリからシステムによって検出されたユーザを削除しても、Firepower Management Center はユーザ データベースからそのユーザを削除しません。そのため、手動で削除する必要があります。ただし、LDAP に対する変更は、Firepower Management Center が次に権限のあるユーザのリストを更新したときにアクセス コントロール ルールに反映されます。

## レールムおよび信頼できるドメイン

Firepower Management Center でレールムを設定すると、そのレールムは Active Directory または LDAP ドメインに関連付けられます。

互いに信頼する Microsoft Active Directory (AD) ドメインのグループ化は、一般的にフォレストと呼ばれます。この信頼関係により、ドメインは異なる方法で互いのリソースにアクセスできます。たとえば、ドメイン A で定義されたユーザ アカウントに、ドメイン B で定義されたグループのメンバーとしてマークを付けることができます。

Firepower システムは、信頼できる AD ドメインをサポートしていません。つまり、Firepower システムは、どのドメインが互いに信頼しているかを追跡せず、どのドメインが互いの親ドメインまたは子ドメインかを認識しません。また、Firepower システムでは、信頼関係が Firepower システム外で実施される場合でも、クロスドメイン信頼を使用する環境のサポートを保証するテストがまだ行われていません。

詳細については、[レールムとユーザのダウンロードのトラブルシューティング \(2182 ページ\)](#) を参照してください。

## レールムがサポートされているサーバ

レールムを設定して次のサーバタイプに接続すると、Firepower Management Center からの TCP/IP アクセスを提供できます。

サーバタイプ (Server Type)	ユーザ認識によるデータ取得のサポート	ユーザエージェントによるデータ取得のサポート	ISEによるデータ取得のサポート	TS エージェントによるデータ取得のサポート	キャプティブポータルによるデータ取得のサポート
Windows Server 2008 と Windows Server 2012 上の Microsoft Active Directory	○	○	○	○	○
Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0	[はい (Yes) ]	[いいえ (No) ]	[はい (Yes) ]	[いいえ (No) ]	○
Linux 上の OpenLDAP	[はい (Yes) ]	[いいえ (No) ]	[いいえ (No) ]	[いいえ (No) ]	○

(注) TS エージェントが別のパッシブ認証 ID ソース (ユーザ エージェントまたは ISE) と共有されている Windows サーバ上の Microsoft Active Directory にインストールされている場合、Firepower Management Center は TS エージェントのデータを優先します。TS エージェントとパッシブ ID ソースが同じ IP アドレスによるアクティビティを報告した場合は、TS エージェントのデータのみが Firepower Management Center に記録されます。

サーバグループの設定に関して次の点に注意してください。

- ユーザグループまたはグループ内のユーザに対してユーザ制御を実行するには、LDAP または Active Directory サーバでユーザグループを設定する必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、Firepower Management Center はユーザグループ制御を実行できません。
- グループ名は LDAP で内部的に使用されているため、**s-** で開始することはできません。グループ名または組織単位名には、アスタリスク (\*)、イコール (=)、バックスラッシュ (\) などの特殊文字は使用できません。使用すると、それらのグループまたは組織単位内のユーザはダウンロードされず、アイデンティティポリシーでは使用できません。
- サーバのサブグループのメンバーであるユーザを含める (または除外する) Active Directory レールムを設定する場合には、Active Directory サーバがレポートするユーザ数が、Windows

Server 2008 または 2012 の Microsoft Active Directory のグループ 1 つにつき 5000 ユーザに制限される点にご注意ください。

必要に応じて、より多くのユーザをサポートするため、このデフォルトの制限を引き上げるよう Active Directory サーバの設定を変更できます。

- ターミナル サービス環境でサーバにより報告されるユーザを一意に識別するには、Cisco Terminal Services (TS) エージェントを設定する必要があります。TS エージェントをインストールし、設定すると、このエージェントは各ユーザに別個のポートを割り当て、Firepower System はこれらのユーザを一意に識別できるようになります。

TS エージェントの詳細については、『Cisco Terminal Services (TS) Agent Guide』を参照してください。

## サポートされるサーバフィールド名

Firepower Management Center がサーバからユーザ メタデータを取得できるようにするには、レーム内のサーバが、次の表に記載されているフィールド名を使用する必要があります。サーバ上のフィールド名が正しくない場合、Firepower Management Centerはそのフィールドの情報を使ってデータベースに入力できなくなります。

表 222: Firepower Management Center フィールドへのサーバフィールドのマッピング

メタデータ	Management Center のフィールド	Active Directory フィールド	Oracle Directory Server フィールド	OpenLDAP フィールド
LDAP ユーザ名	[ユーザ名 (Username) ]	samaccountname	cn uid	cn uid
first name	名	givenname	givenname	givenname
last name	姓	sn	sn	sn
メールアドレス	E メール	メールアドレス userprincipalname (mail に値が設定されていない場合)	メールアドレス	メールアドレス
部署	部署名 (Department)	部署 distinguishedname (department に値が設定されていない場合)	部署	ou
電話番号	電話	telephonenumber	適用対象外	telephonenumber

## レلمとユーザのダウンロードのトラブルシューティング

予期しないサーバ接続の動作に気付いたら、レلم設定、デバイス設定、またはサーバ設定の調整を検討してください。関連の他のトラブルシューティングについては、次を参照してください。

- [ユーザエージェントアイデンティティソースのトラブルシューティング \(2125 ページ\)](#)
- [ISE アイデンティティソースのトラブルシューティング \(2130 ページ\)](#)
- [TS エージェントアイデンティティソースのトラブルシューティング \(2132 ページ\)](#)
- [キャプティブポータルアイデンティティソースのトラブルシューティング \(2142 ページ\)](#)
- [ユーザ制御のトラブルシューティング \(405 ページ\)](#)

### 症状：アクセスコントロールポリシーがグループのメンバーシップと一致しない

この解決策は、他の AD ドメインとの信頼関係にある AD ドメインに適用されます。以下の説明で、外部ドメインドメインは、ユーザがログインするドメイン以外のドメインを指します。

ユーザが信頼されている外部ドメインで定義されたグループに属している場合、Firepower は外部ドメインのメンバーシップを追跡しません。たとえば、次のシナリオを考えてください。

- ドメイン コントローラ 1 と 2 は相互に信頼している
- グループ A はドメイン コントローラ 2 で定義されている
- コントローラ 1 のユーザ mparvinder はグループ A のメンバーである

ユーザ mparvinder はグループ A に属しているが、メンバーシップグループ A を指定する Firepower のアクセスコントロールポリシールールが一致しません。

**解決策：**グループ A に属する、すべてのドメイン 1 のアカウントを含むドメイン コントローラ 1 に同様のグループを作成します。グループ A またはグループ B のすべてのメンバーに一致するように、アクセスコントロールポリシールールを変更します。

### 症状：アクセスコントロールポリシーが子ドメインのメンバーシップと一致しない

ユーザが親ドメインの子であるドメインに属している場合、Firepower はドメイン間の親/子関係を追跡しません。たとえば、次のシナリオを考えてください。

- ドメイン child.parent.com はドメイン parent.com の子である
- ユーザ mparvinder は child.parent.com で定義されている

ユーザ mparvinder が子ドメインに属しているが、parent.com と一致する Firepower アクセスコントロールポリシーが child.parent.com ドメインの mparvinder と一致しません。

**解決策：** parent.com または child.parent.com のいずれかのメンバーシップに一致するようにアクセス コントロール ポリシー ルールを変更します。

#### 予期しない時間にユーザ タイムアウトが発生する

予期しない間隔でユーザ タイムアウトが実行されていることに気付いたら、ユーザ エージェント、ISE、TS エージェント サーバの時間が Firepower Management Centerの時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。

#### レーム設定で指定したようにユーザが含まれない、または除外されない

サーバのサブグループのメンバーであるユーザを選別できる Active Directory レームを設定する際は、Microsoft Windows サーバが報告するユーザの数を以下に制限することに注意します。

- Windows サーバ 2008 または 2012 では、グループごとに 5000 ユーザまで。Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0

必要に応じて、より多くのユーザをサポートするため、このデフォルトの制限を引き上げるようサーバの設定を変更できます。

#### ユーザがダウンロードされない

グループ名または組織単位名に特殊文字が使用されている Active Directory グループのユーザは、アイデンティティ ポリシー ルールで使用できない可能性があります。たとえば、グループ名または組織単位名にアスタリスク (\*)、イコール (=)、バックスラッシュ (\) などの特殊文字が含まれている場合、これらのグループ内のユーザはダウンロードされず、アイデンティティ ポリシーで使用できません。

**解決策：** グループ名または組織単位名から特殊文字を削除します。

#### 未知の ISE とユーザエージェントのユーザのユーザデータが Web インターフェイスで表示されない

システムはデータがまだデータベースにない ISE、ユーザエージェントまたは TS エージェントユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。状況によっては、システムが Microsoft Windows サーバからこの情報を正常に取得するためにさらに時間がかかることもあります。データ取得が成功するまで、ISE、ユーザエージェント、TS エージェントユーザから見えるアクティビティは Web インターフェイスに表示されません。

これにより、アクセス制御ルールを使ったユーザトラフィックの処理も妨げられることがある点に注意します。

#### イベントのユーザデータが想定外の内容になる

ユーザやユーザアクティビティイベントに想定外の IP アドレスが含まれる場合は、レームを確認します。複数のレームに同一の [AD プライマリ ドメイン (AD Primary Domain)] の値を設定することはできません。

ターミナルサーバでのログインによるユーザが **Web インターフェイス** で一意に特定されない導入されている構成にターミナルサーバが含まれ、これに接続されている 1 つまたは複数のサーバにレルムが設定されている場合は、ターミナルサーバ環境でのユーザログインを正確に報告するため **Cisco Terminal Services (TS) エージェント** を設定する必要があります。TS エージェントをインストールし、設定すると、このエージェントは各ユーザに別個のポートを割り当て、Firepower System はこれらのユーザを Web インターフェイスで一意に識別できるようになります。

TS エージェントの詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。

## アイデンティティポリシーについて

アイデンティティポリシーには、アイデンティティルールが含まれます。アイデンティティルールでは、トラフィックのセットを、レルムおよび認証方式（パッシブ認証、アクティブ認証、または認証なし）と関連付けます。

アイデンティティルールで呼び出す前に、使用するレルムおよび認証方式を完全に設定しておく必要があります。

- [システム (System) ] > [統合 (Integration) ] > [レルム (Realms) ] でアイデンティティポリシー外のレルムを設定します。詳細については、[レルムの作成 \(2185 ページ\)](#) を参照してください。
- パッシブ認証のアイデンティティソースであるユーザエージェントと ISE は、[システム (System) ] > [統合 (Integration) ] > [アイデンティティソース (Identity Sources) ] で設定します。詳細については、[ユーザ制御のためのユーザエージェントの設定 \(2124 ページ\)](#) および [ユーザ制御用 ISE の設定 \(2128 ページ\)](#) を参照してください。
- パッシブ認証のアイデンティティソースである TS エージェントについては、Firepower システムの外で設定します。詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。
- アクティブ認証のアイデンティティソースであるキャプティブポータルについては、アイデンティティポリシー内で設定します。詳細については、[ユーザ制御のためのキャプティブポータルの設定 \(2135 ページ\)](#) を参照してください。

単一のアイデンティティポリシーに複数のアイデンティティルールを追加した後、ルールの順番を決めます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールがそのトラフィックを処理するルールです。

1 つ以上のアイデンティティポリシーを設定した後、アクセスコントロールポリシーの 1 つのアイデンティティポリシーを呼び出す必要があります。ネットワークのトラフィックがアイデンティティルールの条件と一致する場合、システムはトラフィックを指定されたレルムと関連付け、指定されたアイデンティティソースを使用してトラフィックのユーザを認証します。

アイデンティティポリシーを設定しない場合、システムはユーザ認証を実行しません。

## 関連トピック

[ユーザアイデンティティソース](#) (2121 ページ)

## レルムの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator、 Access Admin、 Network Admin

レルム設定フィールドの詳細については、[レルムフィールド](#) (2186 ページ) を参照してください。

## 手順

- 
- ステップ 1** Firepower Management Center にログインします。
- ステップ 2** [システム (System)] > [統合 (Integration)] をクリックします。
- ステップ 3** [レルム (Realms)] をクリックします。
- ステップ 4** 新しいレルムを作成するには、[新規レルム (New Realm)] をクリックします。
- ステップ 5** その他のタスク (レルムの有効化、無効化、削除など) を実行する場合は、[レルムの管理](#) (2197 ページ) を参照してください。
- ステップ 6** [レルムフィールド](#) (2186 ページ) で説明したように、レルム情報を入力します。
- ステップ 7** (オプション) レルムへの接続をテストするには、[テスト (Test)] をクリックします。
- (注) レルムテストが成功するには、[AD 結合ユーザ名 (AD Join Username)] と [AD 結合パスワード (AD Join Password)] の両方のフィールドに値を入力する必要があります。
- ステップ 8** [OK] をクリック
- ステップ 9** [レルムディレクトリの設定](#) (2189 ページ) で説明したように、少なくとも1つのディレクトリを設定します。
- ステップ 10** [ユーザとグループのダウンロード](#) (2190 ページ) の説明に従って、(アクセスコントロールに必要な) ユーザとユーザグループのダウンロードを設定します。
- ステップ 11** [レルム設定 (Realm Configuration)] タブをクリックします。
- ステップ 12** [認証済みユーザ (Authenticated Users)]、[認証に失敗したユーザ (Failed Authentication Users)]、および [ゲストユーザ (Guest Users)] にユーザセッションタイムアウト値 (分単位) を入力します。
-

### 次のタスク

- [レルム ディレクトリの設定 \(2189 ページ\)](#)
- レルムの編集、削除、有効化、または無効化を行います。 [レルムの管理 \(2197 ページ\)](#) を参照してください
- [レルムの比較 \(2198 ページ\)](#)。
- 必要に応じて、タスクのステータスをモニタします ([タスク メッセージの表示 \(330 ページ\)](#) を参照)。

## レルム フィールド

次のフィールドを使用してレルムを設定します。

### レルムの設定 (Realm Configuration) フィールド

これらの設定は、レルム内のすべてのサーバまたはコントローラ (別名ディレクトリ) に適用されます。

#### [名前 (Name) ]

レルムの一意の名前。英数字や特殊文字に対応しています。

#### 説明

(オプション) レルムの説明を入力します。

#### AD プライマリ ドメイン (AD Primary Domain)

Active Directory レルム専用です。ユーザ認証が必要となる Active Directory サーバのドメインです。



(注) [AD プライマリ ドメイン (AD Primary Domain) ] 値のすべてのレルムが一意である必要があります。

#### AD 参加ユーザ名 (AD Join Username) 、AD 参加パスワード (AD Join Password)

Kerberos のキャプティブ ポータルのアクティブ認証を目的とした AD レルムでは、クライアントをドメインに参加させる適切な権利を有するユーザのユーザ名とパスワードとが区別されています。

アイデンティティ ルールの [認証タイプ (Authentication Type) ] に **Kerberos** を選択する場合 (または **Kerberos** をオプションとして **HTTP Negotiate** を選択する場合) 、Kerberos キャプティブ ポータル アクティブ認証を実行するには、[アクティブディレクトリ参加ユーザ名 (AD Join Username) ] と [アクティブディレクトリ参加パスワード (AD Join Password) ] を使用して、選択した [レルム (Realm) ] を設定する必要があります。



### [ディレクトリ ユーザ名 (Directory Username) ] と [ディレクトリ パスワード (Directory Password) ]

取得するユーザ情報に適切な権限を持っているユーザの識別用のユーザ名とパスワード。

### ベース DN (Base DN)

Firepower Management Center がユーザ データの検索を開始するサーバのディレクトリ ツリー。

通常、ベース識別名 (DN) には企業ドメイン名および部門を示す基本構造があります。たとえば、Example 社のセキュリティ部門のベース DN は、`ou=security,dc=example,dc=com` となります。

### グループ DN (Group DN)

Firepower Management Center がグループ属性を持つユーザを検索するサーバのディレクトリ ツリー。



- 
- (注) グループ名または組織単位名には、アスタリスク (\*)、イコール (=)、バックスラッシュ (\) などの特殊文字は使用できません。使用した場合、それらのグループのユーザはダウンロードされず、アイデンティティ ポリシーで使用できないためです。
- 

### グループ属性 (Group Attribute)

(オプション) サーバのグループ属性：メンバー、または一意のメンバー。

### タイプ (Type)

レルム、AD、LDAP のタイプ。



- 
- (注) キャプティブ ポータルのみ、LDAP レルムをサポートします。
- 

## レルムの設定 (Realm Configuration) フィールド

### Active Directory 情報

Active Directory 情報のフィールドについては、このセクションの前半で説明しました。

### [ユーザ セッション タイムアウト (User Session Timeout) ]

ユーザセッションがタイムアウトするまでの分数を入力します。デフォルトは1440分 (24時間) です。



- 
- (注) ユーザセッションタイムアウト値は、アクティブ認証 (キャプティブ ポータル) とパッシブ認証 (TS エージェント、ユーザエージェント、ISE) の両方に適用されます。大きな値を設定すると、ユーザセッションが終了しない可能性があり、他のユーザによってこれらのセッションが要求される場合があります。
-

## レルムのディレクトリ フィールド (Realm Directory Fields)

これらの設定は、レルム内の個々のサーバ (ディレクトリ) に適用されます。

### 暗号化 (Encryption)

Firepower Management Center サーバ接続に使用する暗号化方式。

- **STARTTLS** : 暗号化 LDAP 接続
- **LDAPS** : 暗号化 LDAP 接続
- なし : 非暗号化 LDAP 接続 (保護されていないトラフィック)

### ホスト名/IP アドレス (Hostname/IP Address)

サーバのホスト名または IP アドレス。[暗号化 (Encryption)] 方式を指定する場合は、このフィールドでホスト名を指定します。

### [ポート (Port)]

Firepower Management Center サーバ接続に使用するポート。

### SSL 証明書 (SSL Certificate)

サーバへの認証に使用する SSL 証明書。SSL 証明書を使用するために、STARTTLS または LDAPS を [暗号化 (Encryption)] タイプとして設定できます。

認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IP アドレス (Hostname/IP Address)] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で **computer1.example.com** を使用している場合は、接続が失敗します。

### ユーザのダウンロード (User Download) フィールド

[使用可能なグループ (Available Groups)]、[含むに追加する (Add to Include)]、[除外するに追加する (Add to Exclude)]

ダウンロードしてユーザ認識やユーザ制御に使用できるようにするグループを特定します。

- [使用可能グループ ボックス (Available Groups)] にグループが残っている場合、グループのダウンロードは行われません。
- グループを [含むに追加する (Add to Include)] ボックスに移動させた場合、そのグループはダウンロードされ、ユーザデータはユーザ認識やユーザ制御に利用できません。
- [除外に追加する (Add to Exclude)] ボックスにグループを移動させると、グループがダウンロードされ、ユーザデータはユーザ認識に利用できますが、ユーザ制御には利用できません。
- 含まれないグループのユーザを含めるには、[含めるグループ (Groups to Include)] の下のフィールドにそのユーザ名を入力し、[追加 (Add)] をクリックします。

- 除外されないグループのユーザを除外するには、[除外するグループ (Groups to Exclude)] の下のフィールドにそのユーザ名を入力し、[追加 (Add)] をクリックします。

#### 自動ダウンロードの開始、繰り返し設定 (Begin automatic download at, Repeat every)

自動ダウンロードの回数を指定します。

#### ユーザおよびグループのダウンロード (ユーザアクセス制御に必須)

ユーザ認識用およびユーザ制御用にユーザとグループをダウンロードできるようになります。

## レルム ディレクトリの設定

この手順では、ドメイン コントローラなどのサーバに対応するレルム ディレクトリを作成できます。それぞれ異なるユーザやグループを認証する複数のドメイン コントローラを1つのユーザリポジトリ (Active Directory など) に設定することができます。

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator/Access Admin/Network Admin

レルムディレクトリの設定フィールドに関する詳細については、[レルムフィールド \(2186ページ\)](#) を参照してください。

#### 始める前に

オプションでSSL証明書を使用してディレクトリで認証するには、Firepower Management Centerのアクセス元となるマシンでPKIオブジェクトするか、証明書データとキーを利用可能にします。

#### 手順

- ステップ 1** まだ実行していない場合は、Firepower Management Center にログインし、[統合 (Integration)] > [レルム (Realms)] をクリックします。
- ステップ 2** [レルム (Realms)] タブ ページで、ディレクトリの設定対象となるレルムの名前をクリックします。
- ステップ 3** [ディレクトリ (Directory)] タブ ページで、[ディレクトリの追加 (Add Directory)] をクリックします。
- ステップ 4** [サーバのホスト名/IP アドレス (Hostname / IP Address)] と [ポート (Port)] を入力します。
- ステップ 5** [暗号化モード (Encryption Mode)] を選択します。

- ステップ 6** (オプション) リストから [SSL 証明書 (SSL Certificate)] を 1 つ選択するか、追加アイコン (🟢) をクリックして証明書を追加します。
- ステップ 7** 接続をテストするには、[テスト (Test)] をクリックします。
- ステップ 8** [OK] をクリックします。
- ステップ 9** [保存 (Save)] をクリックします。[レルム (Realms)] タブ ページに戻ります。
- ステップ 10** レルムをまだ有効にしていない場合は、[レルム (Realms)] タブ ページで、[状態 (State)] を有効にします。

### 次のタスク

- [ユーザとグループのダウンロード \(2190 ページ\)](#) .

## ユーザとグループのダウンロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator/Access Admin/Network Admin

このセクションでは、Active Directory サーバから Firepower Management Center にユーザとグループをダウンロードする方法について説明します。含めるグループを指定しなかった場合、システムは指定されたパラメータと一致するすべてのグループのユーザデータを取得します。パフォーマンス上の理由から、アクセスコントロールに使用するユーザを表すグループだけを明示的に含めることをお勧めします。

Firepower Management Center がサーバから取得可能なユーザの最大数は Firepower Management Center モデルによって異なります。レルムのダウンロードパラメータの範囲が広すぎる場合、Firepower Management Center はできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数を Message Center の [タスク (Task)] タブで報告します。




- (注) Firepower Management Center では、Unicode 文字を含むユーザ名は表示されません。ユーザやグループをダウンロードする前に、Unicode 文字を英数字に置き換えてください。


レルム設定フィールドの詳細については、[レルムフィールド \(2186 ページ\)](#) を参照してください。

### 手順

- ステップ 1** Firepower Management Center にログインします。

**ステップ2** [統合 (Integration) ]>[レルム (Realms) ]をクリックします。

**ステップ3** ユーザとグループを手動でダウンロードするには、ユーザやユーザグループをダウンロードするレルムの横にあるダウンロードアイコン (  ) をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。残りの手順をスキップできます。

**ステップ4** 自動でユーザとグループをダウンロードするようにレルムを設定するには、自動でユーザやグループをダウンロードするように設定するレルムの横にある編集アイコン (  ) をクリックします。

**ステップ5** [ユーザアクセス制御 (User Access Control) ] タブ ページで、[ (ユーザアクセス制御に必要な) ユーザとグループをダウンロードする (Download users and groups (required for user access control)) ] をオンにします。

**ステップ6** 一覧から [自動ダウンロードの開始時間 (Begin automatic download at) ] の時間を選択します。

**ステップ7** [繰り返し設定 (Repeat Every) ] 一覧からダウンロード間隔を選択します。

**ステップ8** ダウンロードにユーザグループを含めるか除外するには、[選択可能なグループ (Available Groups) ] 列からユーザグループを選択し、[含めるに追加 (Add to Include) ] または [除外に追加 (Add to Exclude) ] をクリックします。

複数のユーザはカンマで区切ります。このフィールドでは、アスタリスク (\*) をワイルドカード文字として使用できます。

(注) そのグループのユーザに対してユーザ制御を実行する場合は、[含めるに追加 (Add to Include) ] をクリックする必要があります。

次の注意事項に従ってください。

- [使用可能グループボックス (Available Groups) ] にグループが残っている場合、グループのダウンロードは行われません。
- グループを [含むに追加する (Add to Include) ] ボックスに移動させた場合、そのグループはダウンロードされ、ユーザデータはユーザ認識やユーザ制御に利用できます。
- [除外に追加する (Add to Exclude) ] ボックスにグループを移動させると、グループがダウンロードされ、ユーザデータはユーザ認識に利用できますが、ユーザ制御には利用できません。
- 含まれないグループのユーザを含めるには、[含めるグループ (Groups to Include) ] の下のフィールドにそのユーザ名を入力し、[追加 (Add) ] をクリックします。
- 除外されないグループのユーザを除外するには、[除外するグループ (Groups to Exclude) ] の下のフィールドにそのユーザ名を入力し、[追加 (Add) ] をクリックします。

## アイデンティティポリシーの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator/Access Admin/Network Admin

### 始める前に

- [レールの作成 \(2185ページ\)](#) の説明に従って1つ以上のレールを作成し、有効にします。

### 手順

- ステップ1 Firepower Management Center にログインします。
- ステップ2 [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [ID (Identity)] をクリックし、[新しいポリシー (New Policy)] をクリックします。
- ステップ3 [名前 (Name)] を入力し、必要に応じて [説明 (Description)] を入力します。
- ステップ4 [保存 (Save)] をクリックします。
- ステップ5 ポリシーにルールを追加するには、[アイデンティティルールの作成 \(2193ページ\)](#) で説明されているように、[ルールの追加 (Add Rule)] をクリックします。
- ステップ6 ルールカテゴリを作成するには、[カテゴリの追加 (Add Category)] をクリックします。
- ステップ7 キャプティブポータルアクティブ認証を設定するには、[ユーザ制御のためのキャプティブポータルの設定 \(2135ページ\)](#) で説明されているように、[アクティブ認証 (Active Authentication)] タブをクリックします。
- ステップ8 [保存 (Save)] をクリックして、アイデンティティポリシーを保存します。

### 次のタスク

- 照合するユーザおよび他のオプションを指定するルールを、アイデンティティポリシーに追加します ([アイデンティティルールの作成 \(2193ページ\)](#) を参照)。
- 指定したリソースへのアクセスを特定のユーザに許可またはブロックするには、このアイデンティティポリシーをアクセスコントロールポリシーに関連付けます ([アクセス制御への他のポリシーの関連付け \(1340ページ\)](#) を参照)。
- 設定変更を管理対象デバイスに展開します ([設定変更の導入 \(350ページ\)](#) を参照)。

## アイデンティティ ルールの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator/Access Admin/Network Admin

アイデンティティ ルールの設定オプションに関する詳細については、[アイデンティティ ルール フィールド \(2194 ページ\)](#) を参照してください。

### 手順

- ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。
- ステップ 2 [ポリシー (Policies) ]>[アクセス コントロール (Access Control) ]>[ID (Identity) ]をクリックします。
- ステップ 3 アイデンティティ ルールの追加先となるアイデンティティ ポリシーの横にある [編集 (edit) ] (✎) をクリックします。  
  
代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 4 [ルールの追加 (Add Rule) ] をクリックします。
- ステップ 5 名前を入力します。
- ステップ 6 ルールを有効にするかどうかを指定します。
- ステップ 7 既存のカテゴリにルールを追加するには、ルールを [挿入 (Insert) ] する場所を指定します。新しいカテゴリを追加するには、[カテゴリの追加 (Add Category) ] をクリックします。
- ステップ 8 一覧からルール [アクション (Action) ] を選択します。
- ステップ 9 [レルムおよび設定 (Realms & Settings) ] タブをクリックします。
- ステップ 10 [レルム (Realms) ] 一覧から、アイデンティティ ルールのレルムを選択します。各アイデンティティ ルールにレルムを関連付ける必要があります。  
  
レルム要件の唯一の例外は、ISE SGT 属性タグのみを使用してユーザ制御を実装する場合があります。この場合は、ISE サーバのレルムを設定する必要はありません。ISE SGT 属性条件は、関連するアイデンティティ ポリシーの有無にかかわらずポリシーで設定できます。
- ステップ 11 キャプティブ ポータルを設定する場合は、[ユーザ制御のためのキャプティブ ポータルの設定 \(2135 ページ\)](#) を参照してください。
- ステップ 12 (オプション) アイデンティティ ルールに条件を追加するには、[ルール条件タイプ \(371 ページ\)](#) を参照してください。
- ステップ 13 [追加 (Add) ] をクリックします。

- ステップ 14** ポリシーエディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリックメニューを使用してカットアンドペーストを実行します。ルールには1から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワークトラフィックの処理に必要なリソースが削減され、ルールのプリエンブションを回避できます。
- ステップ 15** [保存 (Save) ] をクリックします。

---

#### 関連トピック

[Snort® の再起動シナリオ \(354 ページ\)](#)

## アイデンティティ ルール フィールド

次のフィールドを使用して、アイデンティティ ルールを設定します。

#### [有効 (Enabled) ]

このオプションを選択すると、アイデンティティ ポリシーのアイデンティティ ルールが有効になります。このオプションの選択を解除すると、アイデンティティ ルールが無効になります。

#### アクション (Action)

指定したレムでユーザに対して実行する認証のタイプを指定します。これには、[パッシブ認証 (Passive Authentication) ] (デフォルト)、[アクティブ認証 (Active Authentication) ]、または[認証なし (No Authentication) ]があります。アイデンティティ ルールのアクションとして選択する前に、認証方式、またはアイデンティティ ソースを完全に設定する必要があります。



**注意** SSL 復号が無効の場合 (つまりアクセス コントロール ポリシーに SSL ポリシーが含まれない場合) に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort® の再起動によるトラフィックの動作 \(356 ページ\)](#) を参照してください。

アクティブ認証ルールには [アクティブ認証 (Active Authentication) ] ルールアクションが含まれているか、または [パッシブ認証でユーザを識別できない場合はアクティブ認証を使用する (Use active authentication if passive authentication cannot identify user) ] が選択された [パッシブ認証 (Passive Authentication) ] ルールアクションが含まれています。

---

Firepower システムのバージョンでサポートされるパッシブおよびアクティブ認証方式の詳細については、[ユーザアイデンティティ ソースについて \(2121 ページ\)](#) を参照してください。



## レルム

指定されたアクションを実行するユーザが含まれるレルム。アイデンティティルールのレルムとして選択する前に、レルムを完全に設定する必要があります。



(注) [Kerberos] (または [Kerberos] をオプションとする場合は [HTTP ネゴシエート (HTTP Negotiate)]) を、アイデンティティルールの [認証タイプ (Authentication Type)] として選択する場合、選択する [レルム (Realm)] は、Kerberos キャプティブポータルアクティブ認証を実行できるように、[AD 参加ユーザ名 (AD Join Username)] と [AD 参加パスワード (AD Join Password)] を使用して設定する必要があります。

パッシブ認証がユーザを識別できない場合は、アクティブ認証を使用します。

このオプションを選択すると、パッシブまたは VPN 認証でユーザを識別できない場合にキャプティブポータルアクティブ認証を使用してユーザが認証されます。このオプションを選択するには、アイデンティティポリシーでキャプティブポータルアクティブ認証を設定する必要があります。

このオプションを無効にすると、VPN ID を持たないユーザまたはパッシブ認証では識別できないユーザは、「不明 (Unknown)」と識別されます。

認証でユーザを識別できない場合は特別 ID/ゲストとして識別する (Identify as Special Identities/Guest if authentication cannot identify user)

ルールアクションとして [アクティブ認証 (Active Authentication)] (つまり、キャプティブポータル認証) を設定している場合にのみ、このフィールドが表示されます。

## 認証タイプ

キャプティブポータルアクティブ認証を実行するために使用する方法です。選択は、レルム、LDAP、または AD のタイプによって異なります。

- 暗号化されていない HTTP 基本認証 (BA) 接続を使用してユーザを認証するには、[HTTP 基本 (HTTP Basic)] を選択します。ユーザはブラウザのデフォルトの認証ポップアップウィンドウを使用してネットワークにログインします。  
ほとんどの Web ブラウザは、**HTTP 基本** ログインからクレデンシャルをキャッシュし、古いセッションがタイムアウトした後にシームレスに新しいセッションを開始するためにそのクレデンシャルを使用します。
- NT LAN Manager (NTLM) 接続を使用してユーザを認証するには **NTLM** を選択します。この選択は AD レルムを選択するときのみ使用できます。透過的な認証がユーザのブラウザで設定されている場合、ユーザは自動的にログインします。透過的な認証が設定されていない場合、ユーザは各自のブラウザでデフォルトの認証ポップアップウィンドウを使用してネットワークにログインします。
- Kerberos 接続を使用してユーザを認証する場合は、[Kerberos] を選択します。この選択は、セキュア LDAP (LDAPS) が有効になっているサーバに対して AD レルムを選択する場合にのみ可能です。透過的な認証がユーザのブラウザで設定されている場

合、ユーザは自動的にログインします。透過的な認証が設定されていない場合、ユーザは各自のブラウザでデフォルトの認証ポップアップウィンドウを使用してネットワークにログインします。



---

(注) 選択する [レルム (Realm) ] は、Kerberos キャプティブ ポータル アクティブ認証を実行するために、[AD 参加ユーザ名 (AD Join Username) ] および [AD 参加パスワード (AD Join Password) ] を使用して設定する必要があります。

---



---

(注) Kerberos キャプティブ ポータルを実行するアイデンティティルールを作成しようとしており、DNS 解決は設定済みである場合は、キャプティブポータルデバイスの完全修飾ドメイン名 (FQDN) を解決する DNS サーバを設定する必要があります。FQDN は、DNS の設定時に指定したホスト名と一致する必要があります。

ASA with FirePOWER Services および Firepower Threat Defense デバイスの場合、FQDN は、キャプティブポータルに使用されるルーテッドインターフェイスの IP アドレスに解決される必要があります。

---

- キャプティブポータルサーバが認証接続に HTTP 基本認証、Kerberos、または NTLM を選択できるようにするには、[HTTP ネゴシエート (HTTP Negotiate) ] を選択します。このタイプは AD レルムを選択するときのみ使用できます。



---

(注) 選択する [レルム (Realm) ] は、[HTTP ネゴシエート (HTTP Negotiate) ] で Kerberos キャプティブポータルアクティブ認証を選択するために、[AD 参加ユーザ名 (AD Join Username) ] および [AD 参加パスワード (AD Join Password) ] を使用して設定する必要があります。

---



(注) [HTTP ネゴシエート (HTTP Negotiate)] キャプティブ ポータルを実行するアイデンティティ ルールを作成しようとしており、DNS 解決は設定済みである場合は、キャプティブ ポータル デバイスの完全修飾ドメイン名 (FQDN) を解決する DNS サーバを設定する必要があります。キャプティブポータルに使用するデバイスの FQDN は、DNS の設定時に入力したホスト名と一致している必要があります。

ASA with FirePOWER Services デバイスの場合、FQDN は ASA FirePOWER モジュールの FQDN です。

## レルムの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator/Access Admin/Network Admin

このセクションでは、[レルム (Realms)] ページ上のコントロールを使用して、レルムに関するさまざまなメンテナンスタスクを実行する方法について説明します。次の点に注意してください。

- コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 代わりに表示アイコン (🔗) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

### 手順

- ステップ 1** Firepower Management Center にログインします。
- ステップ 2** [システム (System)] > [統合 (Integration)] をクリックします。
- ステップ 3** [レルム (Realms)] をクリックします。
- ステップ 4** レルムを削除するには、削除アイコン (🗑️) をクリックします。
- ステップ 5** レルムを編集するには、レルムの横にある編集アイコン (✏️) をクリックし、[レルムの作成 \(2185 ページ\)](#) の説明に従って変更を行います。
- ステップ 6** レルムを有効にするには、[状態 (State)] を右にスライドします。レルムを無効にするには、左にスライドします。

**ステップ 7** ユーザおよびユーザグループをダウンロードするには、ダウンロードアイコン (↓) をクリックします。

**ステップ 8** レルムをコピーするには、コピーアイコン (📄) をクリックします。

**ステップ 9** レルムを比較する方法については、[レルムの比較 \(2198 ページ\)](#) を参照してください。

## レルムの比較

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator、 Security Approver、 Access Admin、 Network Admin

### 手順

**ステップ 1** Firepower Management Center にログインします。

**ステップ 2** [システム (System)] > [統合 (Integration)] をクリックします。

**ステップ 3** [レルム (Realms)] をクリックします。

**ステップ 4** [システム (System)] > [統合 (Integration)] をクリックします。

**ステップ 5** [レルム (Realms)] をクリックします。

**ステップ 6** [レルムの比較 (Compare Realms)] をクリックします。

**ステップ 7** [比較対象 (Compare Against)] リストから [レルムの比較 (Compare Realm)] を選択します。

**ステップ 8** [レルム A (Realm A)] および [レルム B (Realm B)] リストから比較するレルムを選択します。

**ステップ 9** [OK] をクリック

**ステップ 10** 個々の変更を選択するには、タイトルバーの上の [前へ (Previous)] または [次へ (Next)] をクリックします。

**ステップ 11** (オプション) [比較レポート (Comparison Report)] をクリックして、レルム比較レポートを生成します。

**ステップ 12** (オプション) [新しい比較 (New Comparison)] をクリックして、新しいレルム比較ビューを生成します。

## アイデンティティ ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator/Access Admin/Network Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

### 手順

- ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。
- ステップ 2 [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [ID (Identity)] をクリックします。
- ステップ 3 ポリシーを削除するには、削除 (🗑️) をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 4 ポリシーを編集するには、ポリシーの横にある編集 (✏️) をクリックし、[アイデンティティ ポリシーの作成 \(2192 ページ\)](#) の説明に従って変更を行います。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 5 ポリシーをコピーするには、コピー アイコン (📄) をクリックします。
- ステップ 6 ポリシーのレポートを生成するには、[現在のポリシー レポートの生成 \(363 ページ\)](#) の説明に従ってレポート アイコン (📄) をクリックします。
- ステップ 7 ポリシーを比較する方法については、[ポリシーの比較 \(361 ページ\)](#) を参照してください。

## アイデンティティ ルールの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator/Access Admin/Network Admin

## 手順

---

- ステップ1** まだ Firepower Management Center にログインしていない場合は、ログインします。
- ステップ2** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [ID (Identity)] をクリックします。
- ステップ3** 編集するポリシーの横にある編集アイコン (✎) をクリックします。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ4** アイデンティティルールを編集するには、編集アイコン (✎) をクリックし、[アイデンティティポリシーの作成 \(2192 ページ\)](#) の説明に従って変更を行います。
- ステップ5** アイデンティティルールを削除するには、削除アイコン (🗑) をクリックします。
- ステップ6** ルールカテゴリを作成するには、[カテゴリの追加 (Add Category)] をクリックし、位置とルールを選択します。
- ステップ7** [保存 (Save)] をクリックします。
- 

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。



## 第 **XXI** 部

### 相関とコンプライアンス

- [コンプライアンス ホワイトリスト \(2203 ページ\)](#)
- [相関ポリシー \(2223 ページ\)](#)
- [トラフィック プロファイル \(2269 ページ\)](#)
- [修復 \(2285 ページ\)](#)







## 第 90 章

# コンプライアンス ホワイトリスト

次のトピックでは、関連ポリシーに追加する前にコンプライアンス ホワイトリストを設定する方法について説明します。

- [コンプライアンス ホワイトリストの概要 \(2203 ページ\)](#)
- [コンプライアンス ホワイト リストの作成 \(2209 ページ\)](#)
- [コンプライアンス ホワイト リストの管理 \(2218 ページ\)](#)
- [共有ホスト プロファイルの管理 \(2220 ページ\)](#)

## コンプライアンス ホワイトリストの概要

コンプライアンス ホワイトリスト (ホワイトリストと省略されることもある) は、どのオペレーティングシステム、アプリケーション (Web とクライアント)、およびプロトコルがネットワーク上のホストで許可されるかを指定する一連の条件です。システムはホストがホワイトリストに違反するとイベントを生成します。

コンプライアンス ホワイトリストには 2 つの主要な構成要素があります。

- ターゲットは、ホワイトリスト評価の対象として選択するホストです。サブネット、VLAN、およびホスト属性で制約して、全部または一部のモニタ対象ホストを評価できません。マルチドメイン展開では、ドメインと、ドメイン内またはドメインをまたいだサブネットを対象にすることができます。
- ホスト プロファイルは、ターゲットのコンプライアンス基準を指定します。グローバルホスト プロファイルはオペレーティングシステムに依存しません。1 つのホワイトリスト固有として、またはホワイト リスト間で共有される、オペレーティング システム固有のホスト プロファイルを設定することもできます。

Cisco Talos Security Intelligence and Research Group (Talos) は、推奨設定が指定されたデフォルトのホワイトリストを提供しています。カスタムホワイトリストを作成することも可能です。単純なカスタム ホワイトリストでは、特定のオペレーティング システムを実行するホストのみを許可できます。より複雑なホワイトリストでは、すべてのオペレーティングシステムを許可するとともに、特定のポートで特定のアプリケーションプロトコルを実行する際にホストが使用する必要のあるオペレーティング システムを指定できます。



- (注) システムは、ホストをエクスポートされた NetFlow レコードからネットワーク マップに追加できますが、これらのホストに使用できる情報は限られます ([NetFlow データと管理対象デバイスデータの違い \(2028 ページ\)](#) を参照)。この制限は、コンプライアンス ホワイトリストの作成方法に影響する場合があります。

### コンプライアンス ホワイトリストの実装

ホワイトリストを実装するには、アクティブな相関ポリシーにホワイトリストを追加します。システムはターゲットを評価し、対応する属性を各ホストに割り当てます。

- 準拠 (Compliant) : ホストはホワイトリストに違反していません。
- 非準拠 (Non-Compliant) : ホストはホワイトリストに違反しています。
- 評価されていない (Not Evaluated) : ホストがホワイトリストのターゲットではないか、現在評価中であるか、またはシステムに十分な情報がないためホストが準拠しているかどうかを判断できません。



- (注) ホスト属性を削除するには、対応するホワイトリストを削除します。1つのホワイトリストを非アクティブ化、削除、または相関ポリシーから削除しても、各ホストのホスト属性は削除されず、属性の値が変更されることもありません。

最初の評価後、モニタ対象ホストがアクティブなホワイトリストに違反するたびにホワイトリスト イベントが生成されます。また、ホワイトリスト違反が記録されます。

ワークフロー、ダッシュボード、およびネットワーク マップを使用して、システム全体のコンプライアンス アクティビティをモニタし、個々のホストがホワイトリストにいつどのように違反したのかを判断できます。修復およびアラートでホワイトリスト違反に自動的に応答することもできます。

#### 例 : Web サーバへの HTTP の制限

セキュリティ ポリシーは、Web サーバのみが HTTP を実行できることを指定しています。HTTP を実行しているホストを特定するために Web ファーム以外のネットワーク全体を評価するホワイトリストを作成します。

ネットワーク マップとダッシュボードを使用して、ネットワークのコンプライアンスの概要を一目で把握できます。数秒で、ポリシーに違反して HTTP を実行している組織内のホストを正確に特定して適切に対処できます。

その後で、相関機能を使用して、Web ファーム内に存在しないホストが HTTP の実行を開始するたびに警告するようにシステムを設定できます。

## 関連トピック

[相関ポリシーの設定](#) (2225 ページ)

# コンプライアンス ホワイトリストのターゲット ネットワーク

ターゲット ネットワークは、ホワイトリスト コンプライアンス評価の対象となるホストを指定します。ホワイトリストには、複数のターゲット ネットワークを含めることができ、いずれかのターゲットの基準を満たすホストが評価されます。

最初、ターゲット ネットワークは IP アドレスまたはアドレス範囲で制約されています。マルチドメイン展開では、初期の制約にドメインも含まれます。

システム提供のデフォルトのホワイトリストでは、すべての監視対象ホスト 0.0.0.0/0 および ::/0 がターゲット設定されています。マルチドメイン展開では、デフォルトのホワイトリストはグローバルドメインに制約されています (グローバルドメインでのみ使用可能です)。

ホストがホワイトリストに対して有効ではなくなるようにターゲット ネットワークまたはホストを変更すると、ホストはホワイトリストで評価されなくなり、準拠と非準拠のいずれとしてもみなされなくなります。

## ターゲット ネットワークの調査と改善

ホワイトリストにターゲット ネットワークを追加すると、システムにより、準拠ホストの特徴を確認できるようにネットワーク マップを調査するよう求められます。調査により、ターゲットは、調査済みのホストを表すホワイトリストに追加されます。

サブネットまたは個別のホストを調査できます。マルチドメイン展開では、ドメイン全体を調査することも、ドメインをまたいで調査することもできます。先祖ドメインを調査すると、システムによってこのドメインの子孫が調査されます。

追加されたターゲットに加えて、調査では、調査で検出されたオペレーティングシステムごとに1つのホストプロファイルがホワイトリストに入力されます。デフォルトで、これらのホストプロファイルは、システムが該当するオペレーティングシステム上で検出したクライアント、アプリケーションプロトコル、Web アプリケーション、およびプロトコルのすべてを許可します。

ターゲット ネットワークを調査 (または調査をスキップ) した後、対象を絞り込みます。IP アドレスを使用してホストを除外するか、ホスト属性または VLAN によりターゲット ネットワークを制約します。

## コンプライアンス ホワイトリストを使用したドメインの対象化

マルチドメイン展開では、ドメインとターゲット ネットワークは密接にリンクされています。

- リーフドメインの管理者は、自分のリーフドメイン内のホストを評価するホワイトリストを作成できます。
- 上位ドメインの管理者は、ドメインをまたいでホストを評価するホワイトリストを作成できます。同じホワイトリストで、ドメインの異なるさまざまなサブネットを対象にすることができます。

グローバル ドメインの管理者であり、展開全体の Web サーバに同じコンプライアンス基準を導入する必要があるというシナリオを考えてみます。コンプライアンス基準を定義するグローバル ドメインに 1 つのホワイトリストを作成できます。次に、各リーフ ドメイン内の Web サーバの IP スペース（または個別の IP アドレス）を指定するターゲット ネットワークを使用して、ホワイトリストを制約します。



- (注) リーフ ドメインの IP アドレスと範囲を対象にすることに加えて、上位のドメインを使用してターゲット ネットワークを制約することもできます。より高いレベルのドメインのサブネットをターゲットにすると、各子孫リーフ ドメイン内の同じサブネットがターゲットになります。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

## コンプライアンス ホワイトリストのホスト プロファイル

コンプライアンス ホワイトリストにおいて、ホスト プロファイルは、ターゲット ホスト上で実行を許可するオペレーティング システム、クライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを指定します。コンプライアンス ホワイトリストで使用できるホスト プロファイルは 3 種類あります。3 種類のホスト プロファイルはそれぞれ、エディタ上での表示が異なります。

表 223:コンプライアンス ホワイトリストのホスト プロファイルタイプ

ホスト プロファイル タイプ	表示	説明
グローバル	すべてのオペレーティング システム	オペレーティング システムに関係なく、ターゲット ホスト上で実行が許可されている内容を指定します。
オペレーティング システム別	プレーン テキストで表示	特定のオペレーティング システムを使用するターゲット ホスト上で実行が許可されている内容を指定します。
共有	イタリックで表示	複数のホワイト リストで使用可能なオペレーティング システム条件を指定します。

### オペレーティング システム固有のホスト プロファイル

コンプライアンス ホワイトリストでは、オペレーティング システム固有のホスト プロファイルで、ネットワーク上での実行を許可するオペレーティング システムだけでなく、それらのオ

オペレーティングシステム上での実行を許可するアプリケーションプロトコル、クライアント、Web アプリケーション、およびプロトコルも指定します。

たとえば、準拠ホストでは Microsoft Windows の特定のバージョンを実行することを要件にすることができます。別の例として、SSH の実行を Linux ホストのポート 22 で許可した上で、SSH クライアントのベンダーとバージョンをさらに制限することもできます。

ネットワーク上での実行を許可するオペレーティング システムごとに 1 つのホスト プロファイルを作成します。ネットワーク上でオペレーティングシステムを禁止する場合は、そのオペレーティング システム用のホスト プロファイルを作成しないでください。たとえば、ネットワーク上のすべてのホストで Windows が実行されるようにするには、そのオペレーティング システム用のホスト プロファイルのみを含めるようにホワイト リストを設定します。



- (注) 未確認ホストは、確認されるまで、すべてのホワイトリストに準拠していると見なされます。ただし、不明ホストのホワイト リスト ホスト プロファイルを作成することはできません。未確認ホストとは、オペレーティングシステムを識別するために十分な情報が収集されていないホストのことです。不明ホストとは、既知のフィンガープリントと一致しないオペレーティング システムを使用しているホストのことです。

## 共有ホスト プロファイル

コンプライアンス ホワイトリストでは、共有ホスト プロファイルが特定のオペレーティング システムに関連付けられますが、それぞれの共有ホスト プロファイルを複数のホワイトリスト内で使用できます。

たとえば、世界中にオフィスがあり、拠点ごとに別々のホワイトリストを使用する一方、Apple Mac OS X を実行しているすべてのホストに対しては常に同じプロファイルを使用するとします。その場合、該当するオペレーティングシステム用の共有プロファイルを作成し、そのプロファイルをすべてのホワイトリストで使用するという方法があります。

デフォルト ホワイトリストでは、組み込みホスト プロファイルと呼ばれる特殊なカテゴリの共有ホスト プロファイルが使用されます。これらのプロファイルは、組み込みのアプリケーションプロトコル、Web アプリケーション、プロトコル、クライアントを使用します。コンプライアンス ホワイトリスト エディタでは、システムはこれらのプロファイルを組み込みホスト プロファイルアイコン (📁) で示します。

マルチドメイン展開では、現在のドメインで作成された共有ホスト プロファイルが表示されます。このプロファイルは編集できます。また、先祖ドメインからの共有ホスト プロファイルも表示されますが、これは編集できません。下位のドメインで作成された共有ホスト プロファイルを表示および編集するには、そのドメインに切り替えます。



- (注) 共有ホスト プロファイル (組み込みを含む) を変更した場合や、組み込みアプリケーションプロトコル、プロトコル、またはクライアントを変更した場合、それを使用するすべてのホワイトリストに変更が影響します。意図しない変更を加えた場合や、該当する組み込みの要素を削除した場合は、工場出荷時の初期状態にリセットできます。

## ホワイトリスト違反のトリガー

ホストのホワイトリストコンプライアンスは、システムで次のことが発生すると変化する場合があります。

- ホストのオペレーティングシステムの変更を検出
- ホストのオペレーティングシステムまたはホスト上のアプリケーションプロトコルに関するアイデンティティの競合を検出
- ホスト上でアクティブになっている新しいTCPサーバポート（SMTPまたはWebサーバによって使用されるポートなど）、または、ホスト上で実行中の新しいUDPサーバを検出
- ホスト上で実行中の検出されたTCPサーバまたはUDPサーバで、アップグレードのためのバージョン変更などの変更を検出
- ホスト上で実行中の新しいクライアントアプリケーションまたはWebアプリケーションを検出
- クライアントアプリケーションまたはWebアプリケーションを非アクティブを理由にそのデータベースからドロップ
- ホストが新しいネットワークまたはトランスポートプロトコルと通信していることを検出
- 新しいジェイルブレイクされたモバイルデバイスを検出
- ホスト上でTCPポートまたはUDPポートが閉じられたか、タイムアウトしたことを検出

さらに、ホスト入力機能またはホストプロファイルを使用して次の操作を実行することによって、ホストのコンプライアンスの変化をトリガーできます。

- ホストにクライアント、プロトコル、またはサーバを追加する
- ホストからクライアント、プロトコル、またはサーバを削除する
- ホストにオペレーティングシステム定義を設定する
- ホストが有効なターゲットでなくなるようにホストのホスト属性を変更する



- (注) 非常に多数のイベントが発生しないように、システムでは、その最初の評価に基づいて非準拠のホストにホワイトリストイベントを生成せず、またユーザがアクティブなホワイトリストまたは共有ホストプロファイルを変更した結果としてホストを非準拠にしません。ただし、違反は記録されます。すべての非準拠ターゲットに対してホワイトリストイベントを生成する場合は、検出データを消去してください。ネットワークアセットを再検出すると、ホワイトリストイベントをトリガーすることがあります。

### 例：オペレーティングシステムのコンプライアンス

ホワイトリストで Microsoft Windows ホストのみがネットワーク上で許可されるように指定されている場合、システムでは、Mac OS X を実行中のホストを検出するとホワイトリスト イベントを生成します。さらに、ホワイトリストに関連付けられているホスト属性が、そのホストに関して [準拠 (Compliant)] から [非準拠 (Non-Compliant)] に変更されます。

この例のホストが [準拠 (Compliant)] に復帰するには、次のいずれかが行われる必要があります。

- Mac OS X オペレーティングシステムを許可するようにホワイトリストを編集する
- ホストのオペレーティングシステム定義を手動で Microsoft Windows に変更する
- オペレーティングシステムが変更されて Microsoft Windows に戻ったことをシステムが検出する

### 例：非準拠のアセットをネットワーク マップから削除する

ホワイトリストで FTP の使用が許可されていない場合に、アプリケーション プロトコルのネットワーク マップ、またはイベント ビューから FTP を削除すると、FTP を実行中のホストは準拠になります。ただし、システムがこのアプリケーション プロトコルを再度検出すると、システムによってホワイトリスト イベントが生成され、そのホストは非準拠になります。

### 例：完全な情報に基づいてのみトリガーを実行

ホワイトリストでポート 21 で TCP FTP トラフィックだけを許可していた場合、システムでポート 21/TCP で不明なアクティビティを検出すると、ホワイトリストはトリガーを実行しません。ホワイトリストがトリガーを実行するのは、システムがトラフィックを FTP 以外のトラフィックとして識別するか、またはユーザがホスト入力機能を使用してトラフィックを非 FTP トラフィックとして指定した場合だけです。システムは、部分的な情報のみを使用して違反を記録することはありません。

## コンプライアンス ホワイトリストの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ホワイトリストを作成する際には、ネットワークを調べて最初のターゲットを作成するように求めるプロンプトが表示されます。これは、コンプライアンスに準拠するホストの特徴を指定するのに役立ちます。

## 手順

- ステップ 1** [ポリシー (Policies)] > [相関 (Correlation)] を選択し、[ホワイトリスト (White List)] タブをクリックします。
- ステップ 2** [新規ホワイトリスト (New White List)] をクリックします。
- ステップ 3** 必要に応じて、最初のターゲットネットワークの [IP アドレス (IP Address)] および [ネットマスク (Netmask)] を入力します。マルチドメイン導入では、ターゲットネットワークが存在する [ドメイン (Domain)] を選択します。
- ヒント** モニタリング対象のネットワーク全体を調査するには、デフォルト値の 0.0.0.0/0 と ::/0 を使用します。
- (注) ターゲットネットワークのドメインを選択した後は、ドメインを変更できません。より高いレベルのドメインのサブネットをターゲットにすると、各子孫リーフドメイン内の同じサブネットがターゲットになります。システムは、各リーフドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。
- ステップ 4** ターゲット ネットワークを追加します。
- [追加 (Add)] : 調査せずにターゲット ネットワークを追加する場合は、[追加 (Add)] をクリックします。
  - [ネットワークの追加および調査 (Add and Survey Network)] : ターゲット ネットワークを追加して調査する場合は、[ネットワークの追加および調査 (Add and Survey Network)] をクリックします。
  - [スキップ (Skip)] : ネットワークを調査せずにホワイト リストを作成する場合は、[スキップ (Skip)] をクリックします。
- ステップ 5** 必要に応じて、ホワイト リストの新しい [名前 (Name)] および [説明 (Description)] を入力します。
- ステップ 6** 必要に応じて、[脱獄モバイルデバイスを許可 (Allow Jailbroken Mobile Devices)] を選択して、ネットワークで脱獄モバイルデバイスを許可します。このオプションを無効にすると、ジェイルブレイクされたデバイスによってホワイトリスト違反が生成されます。
- ステップ 7** [コンプライアンス ホワイトリストのターゲット ネットワークの設定 \(2211 ページ\)](#) の説明に従って、1 つ以上の [ターゲット ネットワーク (Target Network)] をホワイト リストに追加します。
- ステップ 8** [許可されるホストプロファイル (Allowed Host Profiles)] を使用して、準拠ホストの特徴を指定します。
- グローバルホストプロファイル : ホワイト リストのグローバルホストプロファイルを編集するには、[任意のオペレーティングシステム (Any Operating System)] をクリックし、[ホワイトリスト ホスト プロファイルの作成 \(2213 ページ\)](#) の説明に従います。



- 調査済みプロファイルの編集：ネットワーク調査によって作成された既存のオペレーティング システム固有のホスト プロファイルを編集するには、その名前をクリックし、[ホワイト リスト ホスト プロファイルの作成 \(2213 ページ\)](#) の説明に従います。
- 新規プロファイルの作成：このホワイト リストに新しいオペレーティング システム固有のホスト プロファイルを作成するには、[許可されるホスト プロファイル (Allowed Host Profiles) ]の隣にある追加アイコン (+) をクリックし、[ホワイト リスト ホスト プロファイルの作成 \(2213 ページ\)](#) の説明に従います。
- 共有ホスト プロファイルの追加：ホワイト リストに既存の共有ホスト プロファイルを追加するには、[共有ホスト プロファイルの追加 (Add Shared Host Profile) ]をクリックし、追加する共有ホスト プロファイルを選択して、[OK] をクリックします。共有ホスト プロファイルは斜体で表示されます。

**ステップ 9** [ホワイト リストの保存 (Save White List) ] をクリックします。

#### 次のタスク

- [相関ポリシーの設定 \(2225 ページ\)](#) の説明に従って、アクティブな相関ポリシーにホワイト リストを追加します。システムはすぐにホワイト リストの評価および違反の生成を開始します。

#### 関連トピック

- [コンプライアンス ホワイト リストのターゲット ネットワーク \(2205 ページ\)](#)
- [選択したホストに基づいたコンプライアンスのホワイト リストの作成 \(2714 ページ\)](#)
- [Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## コンプライアンス ホワイト リストのターゲット ネットワークの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ターゲット ネットワークを追加するときには、ターゲット ネットワークを調査して、準拠しているホストを特定することができます。この調査によって、調査で検出された各オペレーティング システムの 1 つのホスト プロファイルがホワイト リストに追加されます。これらのホスト プロファイルは、システムが該当するオペレーティング システム上で検出したクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルのすべてを許可します。

## 手順

**ステップ1** コンプライアンス ホワイトリスト エディタで、[ターゲット ネットワークの追加 (Add Target Network)] をクリックします。

**ステップ2** ターゲット ネットワークの [IP アドレス (IP Address)] と [ネットマスク (Netmask)] を入力します。

**ステップ3** マルチドメイン展開では、ターゲット ネットワークが存在する [ドメイン (Domain)] を選択します。

(注) ターゲット ネットワークのドメインを選択した後は、ドメインを変更できません。より高いレベルのドメインのサブネットをターゲットにすると、各子孫リーフドメイン内の同じサブネットがターゲットになります。システムは、各リーフドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

**ステップ4** ターゲット ネットワークを追加します。

- 追加 (Add) : 調査なしでターゲット ネットワークを追加するには、[追加 (Add)] をクリックします。
- ネットワークの追加と調査 (Add and Survey Network) : ターゲット ネットワークを追加および調査するには、[ネットワークの追加と調査 (Add and Survey Network)] をクリックします。

**ステップ5** 必要に応じて、新しいターゲットをクリックしてさらに構成します。

- 名前 (Name) : 新しい [名前 (Name)] を入力します。
- ネットワークの追加 (Add Networks) : 追加のホストをターゲットにするには、追加アイコン (+) をクリックして、[IP アドレス (IP Address)] と [ネットマスク (Netmask)] を入力します。ネットワークをホワイト リスト コンプライアンスから除外するには、[除外 (Exclude)] を選択します。
- ホスト属性の追加 (Add Host Attributes) : 特定のホスト属性を持つホストをターゲットにするには、追加アイコン (+) をクリックして、[属性 (Attribute)] とその [値 (Value)] を指定します。
- VLAN の追加 (Add VLANs) : VLAN をターゲットにするには、追加アイコン (+) をクリックして VLAN 番号を入力します (802.1q VLAN の場合)。
- 削除 (Delete) : ターゲット制限を削除するには、削除アイコン (🗑️) をクリックします。

**ステップ6** 最後に保存した後で行ったすべての変更をすぐに実装するには、[ホワイトリストの保存 (Save White List)] をクリックします。

関連トピック

[コンプライアンス ホワイトリストのターゲット ネットワーク](#) (2205 ページ)

[Firepower システムの IP アドレス表記法](#) (14 ページ)

## ホワイト リスト ホスト プロファイルの作成

スマート ライセ ンス	従来のライセンス	サポートされるデ バイス	サポートされるド メイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ホストプロファイルは、ターゲットホスト上での実行を許可するオペレーティングシステム、クライアント、アプリケーションプロトコル、Web アプリケーション、およびプロトコルといった、ホワイトリストの適合基準を指定します。

すべてのホワイトリストには、オペレーティングシステムに依存しないグローバルホストプロファイルがあります。たとえば、Mozilla Firefox を許可するように複数の Microsoft Windows ホストプロファイルと Linux ホストプロファイルを編集する代わりに、検出されたオペレーティングシステムに関係なく、Firefox を許可するようにグローバルホストプロファイルを設定できます。

また、各オペレーティングシステム専用のホストプロファイルを設定できます。これは、単一のホワイトリスト専用としても、複数のホワイトリストの共有プロファイルとしても設定できます。



(注) 共有ホストプロファイル (ビルトインを含む) を変更した場合、またはビルトインアプリケーションプロトコル、プロトコル、クライアントを変更した場合、これらのプロファイルを使用するすべてのホワイトリストに影響します。これらのビルトイン要素に意図しない変更や削除を行った場合は、出荷時のデフォルトにリセットできます。

### 始める前に

- [コンプライアンス ホワイトリストの編集 \(2219 ページ\)](#) の説明に従い、ホワイトリスト内でホストプロファイルを作成または編集します。または、[共有ホストプロファイルの管理 \(2220 ページ\)](#) の説明に従い、共有ホストプロファイルを作成または編集します。

### 手順

**ステップ 1** ホワイトリスト適合ホストプロファイル エディタで、以下のホストプロファイルを設定します。

- 名前 : [名前 (Name) ] を入力します。

- **オペレーティングシステム**：ホストプロファイルを特定のオペレーティングシステム専用にするには、[OSベンダ (OS Vendor) ]、[OS名 (OS Name) ]、[バージョン (Version) ] ドロップダウンリストを使用します。グローバルホストプロファイルはすべてのオペレーティングシステムを実行するホストへ適用されることを目的としたプロファイルであるため、これに制限を設定することはできません。
- **アプリケーションプロトコル**：アプリケーションプロトコルを許可するには、追加アイコン (+) をクリックし、[アプリケーションプロトコルのホワイトリスト \(2214 ページ\)](#) の説明に従います。
- **クライアント**：クライアントを許可するには、追加アイコン (+) をクリックし、[クライアントのホワイトリスト \(2215 ページ\)](#) の説明に従います。
- **Web アプリケーション**：Web アプリケーションを許可するには、追加アイコン (+) をクリックし、[Web アプリケーションのホワイトリスト \(2216 ページ\)](#) の説明に従います。
- **プロトコル**：プロトコルを許可するには、追加アイコン (+) をクリックし、[プロトコルのホワイトリスト \(2217 ページ\)](#) の説明に従います。
- **削除**：一度許可した項目への許可を解除するには、削除アイコン (🗑️) をクリックします。
- **プロパティの編集**：許可されているアプリケーションプロトコルのプロパティ、クライアント、プロトコルを編集するには、その名前をクリックします。変更は、変更した要素を使用する各ホストプロファイルに反映されます。

**ヒント** プロファイルに一致するホストにすべてのアプリケーションプロトコル、クライアント、web アプリケーションを許可するには、該当する [すべて許可 (Allow all...)] チェックボックスを選択します。

**ステップ 2** 最後の保存以降に施した変更をすぐに適用するには、[ホワイトリストを保存 (Save White List)] (または、共有ホストプロファイルを編集している場合は[すべてのプロファイルを保存 (Save All Profiles)] ) をクリックします。

## アプリケーションプロトコルのホワイトリスト

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ホワイトリストホストプロファイルを使用して、グローバルにまたは特定のオペレーティングシステムに対して、アプリケーションプロトコルのホワイトリストを作成できます。オプションで、ポート、ベンダー、バージョンによって、アプリケーションプロトコルを制限できます。たとえば、ポート 22/TCP で、Linux ホスト上で実行する OpenSSH の特定のバージョンを許可することができます。

手順

**ステップ 1** ホワイトリスト ホスト プロファイルを作成または変更しているときに、[許可されるアプリケーション プロトコル (Allowed Application Protocols)] (またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可されるアプリケーション プロトコル (Globally Allowed Application Protocols)] ) の横にある追加アイコン (+) をクリックします。

**ステップ 2** 次の 2 つの対処法があります。

- 許可するアプリケーション プロトコルが表示されたら、これらを選択します。Web インターフェイスには、ホワイトリストによって、過去に許可されたアプリケーション プロトコル、または今許可しようとしているアプリケーション プロトコルが表示されます。
- リストにないアプリケーション プロトコルを許可するには、[<新規アプリケーション プロトコル> (<New Application Protocol>)] を選択し、[OK] をクリックしてアプリケーション プロトコル エディタを表示します。許可するアプリケーション プロトコル [タイプ (Type)] と [プロトコル (Protocol)] を選択します。オプションで、[ポート (port)]、[ベンダー (Vendor)]、[バージョン (Version)] によって、アプリケーション プロトコルを制限します。

(注) アプリケーションのテーブル ビューに表示されているとおり正確にベンダーやバージョンを入力する必要があります。ベンダーまたはバージョンを指定しなかった場合は、タイプとプロトコルが一致している限り、ホワイトリストではすべてのベンダーとバージョンが許可されます。

**ステップ 3** [OK] をクリックします。

**ステップ 4** 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存 (Save White List)] をクリックします。

## クライアントのホワイトリスト

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティングシステムに対して、クライアントのホワイトリストを作成できます。オプションで、クライアントを特定のバージョンに限定することができます。たとえば、Microsoft Windows ホスト上での実行を Microsoft Internet Explorer 10 のみに許可することができます。

手順

**ステップ 1** ホワイトリスト ホスト プロファイルを作成または変更しているときに、[許可されるクライアント (Allowed Clients)] (またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可されるクライアント (Globally Allowed Clients)] ) の横にある追加アイコン (+) をクリックします。

**ステップ 2** 次の 2 つの対処法があります。

- 許可するクライアントが表示されたら、これらを選択します。Web インターフェイスには、ホワイトリストによって、過去に許可されたクライアント、または今許可しようとしているクライアントが表示されます。
- リストにないクライアントを許可するには、[<新規クライアント> (<New Client>)] を選択し、[OK] をクリックしてクライアント エディタを表示します。ドロップダウンリストから許可する [クライアント (Client)] を選択し、オプションで許可するクライアントの [バージョン (Version)] を制限します。

(注) クライアントのテーブルビューに表示されているとおりに正確にバージョンを入力する必要があります。バージョンを指定しない場合、ホワイトリストはすべてのバージョンを許可します。

**ステップ 3** [OK] をクリックします。

**ステップ 4** 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存 (Save White List)] をクリックします。

Web アプリケーションのホワイトリスト

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティング システムに対して、Web アプリケーションのホワイトリストを作成できます。

手順

**ステップ 1** ホワイトリスト ホスト プロファイルを作成または変更しているときに、[許可される Web アプリケーション (Allowed Web Applications)] (またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可される Web アプリケーション (Globally Allowed Web Applications)] ) の横にある追加アイコン (+) をクリックします。

**ステップ 2** 許可する Web アプリケーションを選択します。

**ステップ 3** [OK] をクリックして、

**ステップ 4** 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存 (Save White List)] をクリックします。

## プロトコルのホワイトリスト

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティングシステムに対して、プロトコルのホワイトリストを作成できます。ARP、IP、TCP、UDP は、常にすべてのホスト上での実行が許可されます。これらを禁止することはできません。

### 手順

**ステップ 1** ホワイトリスト ホスト プロファイルを作成または変更しているときに、[許可されるプロトコル (Allowed Protocols)] (またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可されるプロトコル (Globally Allowed Protocols)]) の横にある追加アイコン (+) をクリックします。

**ステップ 2** 次の 2 つの対処法があります。

- 許可するプロトコルが表示されたら、これらを選択します。Web インターフェイスには、ホワイトリストによって、過去に許可されたプロトコル、または今許可しようとしているプロトコルが表示されます。
- リストにないプロトコルを許可するには、[<新規プロトコル> (<New Protocol>)] を選択し、[OK] をクリックしてプロトコルエディタを表示します。[タイプ (Type)] ドロップダウンリストから、プロトコルタイプ ([ネットワーク (Network)] や [トランスポート (Transport)]) を選択し、ドロップダウンリストから [プロトコル (Protocol)] を選択します。

**ヒント** リスト内に存在しないプロトコルを指定するには、[その他 (手動入力) (Other (manual entry))] を選択します。ネットワーク プロトコルの場合は、<http://www.iana.org/assignments/ethernet-numbers/> に記載されている適切な番号を入力します。トランスポート プロトコルの場合は、<http://www.iana.org/assignments/protocol-numbers/> に記載されている適切な番号を入力します。

**ステップ 3** [OK] をクリックします。

**ステップ 4** 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存 (Save White List)] をクリックします。

# コンプライアンス ホワイトリストの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

[ホワイトリスト (White List)] ページは、コンプライアンス ホワイトリストと共有ホストプロファイルの管理に使用できます。デフォルト ホワイトリストは、推奨設定を表すものであり、組み込みホストプロファイルと呼ばれる特殊なカテゴリの共有ホストプロファイルを使用します。

マルチドメイン展開では、現在のドメインで作成されたコンプライアンス ホワイトリストが表示されます。これは、編集が可能なリストです。また、先祖ドメインからの選択したホワイトリストも表示されますが、これは編集できません。下位のドメインで作成されたホワイトリストを表示および編集するには、そのドメインに切り替えます。



(注) 設定に無関係なドメイン (名前、管理対象デバイスなど) に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。デフォルト ホワイトリストは、グローバルドメインでのみ使用できます。

## 手順

**ステップ 1** [ポリシー (Policies)] > [関連 (Correlation)] を選択して、[ホワイトリスト (White List)] タブをクリックします。

**ステップ 2** コンプライアンス ホワイトリストを管理します。

- 作成：新しいホワイトリストを作成するには、[新規ホワイトリスト (New White List)] をクリックして、[コンプライアンス ホワイトリストの作成 \(2209 ページ\)](#) で説明する手順を実行します。
- 削除：使用していないホワイトリストを削除するには、削除アイコン (🗑️) をクリックして、ホワイトリストの削除を確認します。また、ホワイトリストを削除すると、ネットワーク上のすべてのホストから、そのリストに関連付けられたホスト属性も削除されます。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 編集：既存のホワイトリストを変更するには、編集アイコン (✎) をクリックし、[コンプライアンス ホワイトリストの編集 \(2219 ページ\)](#) で説明する手順を実行します。代わりに表示アイコン (👁️) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。



- 共有ホストプロファイル：ホワイトリストの共有ホストプロファイルを管理するには、[共有プロファイルの編集 (Edit Shared Profiles)] をクリックして、[共有ホストプロファイルの管理 \(2220 ページ\)](#) で説明する手順を実行します。

## コンプライアンス ホワイトリストの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

アクティブな相関ポリシーに含まれるコンプライアンス ホワイトリストを修正して保存すると、システムは、ホワイトリストのターゲットネットワークのホストのコンプライアンスを再評価します。この再評価で一部のホストがコンプライアンス準拠または違反とされた場合でも、ホワイトリストイベントは生成されません。

### 手順

**ステップ 1** [ポリシー (Policies)] > [相関 (Correlation)] を選択し、[ホワイトリスト (White List)] タブをクリックします。

**ステップ 2** 変更するホワイトリストの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** コンプライアンス ホワイトリストを編集します。

- 名前と説明：名前または説明を変更するには、左側のパネルでホワイトリストの名前をクリックしてホワイトリストの基本情報を表示し、新しい情報を入力します。
- ジェイルブレイクされたデバイスの許可：ネットワーク上でジェイルブレイクされたモバイルデバイスを許可するには、左側のパネルでホワイトリストの名前をクリックしてホワイトリストの基本情報を表示し、[ジェイルブレイクされたモバイルデバイスを許可 (Allow Jailbroken Mobile Devices)] を有効にします。このオプションを無効にすると、ジェイルブレイクされたデバイスによってホワイトリスト違反が生成されます。
- 許可されるホストプロファイルの追加：このホワイトリストに対してオペレーティングシステム固有のホストプロファイルを作成するには、[許可されているホストプロファイル (Allowed Host Profiles)] の横にある追加アイコン (+) をクリックし、[ホワイトリストホストプロファイルの作成 \(2213 ページ\)](#) の説明に従って続行します。
- 共有ホストプロファイルの追加：ホワイトリストに既存の共有ホストプロファイルを追加するには、[共有ホストプロファイルの追加 (Add Shared Host Profile)] をクリックし、

追加する共有ホスト プロファイルを選択して [OK] をクリックします。共有ホスト プロファイルは斜体で表示されます。

- ターゲット ネットワークの追加：ホストを調査することなく新しいターゲット ネットワークを追加するには、ターゲット ネットワークの横にある追加アイコン (+) をクリックし、[コンプライアンス ホワイトリストのターゲット ネットワークの設定 \(2211 ページ\)](#) の説明に従って続行します。
- ホスト プロファイルの削除：ホワイトリストから共有またはオペレーティング システム固有のホスト プロファイルを削除するには、ホスト プロファイルの横にある削除アイコン (🗑️) をクリックし、選択内容を確認します。共有ホスト プロファイルを削除すると、それがホワイトリストから除外されますが、プロファイルは削除されず、それを使用する他のホワイトリストからも除外されません。ホワイトリストのグローバルホスト プロファイルは削除できません。
- ターゲット ネットワークの削除：ホワイトリストからターゲット ネットワークを削除するには、ネットワークの横にある削除アイコン (🗑️) をクリックし、選択内容を確認します。
- グローバルホスト プロファイルの編集：ホワイトリストのグローバルホスト プロファイルを編集するには、[任意のオペレーティング システム (Any Operating System)] をクリックし、[ホワイトリストホスト プロファイルの作成 \(2213 ページ\)](#) の説明に従って続行します。
- 他のホスト プロファイルの編集：共有またはオペレーティング システム固有のホスト プロファイルを編集するには、ホスト プロファイルの名前をクリックし、[ホワイトリストホスト プロファイルの作成 \(2213 ページ\)](#) の説明に従って続行します。
- ターゲット ネットワークの編集：ターゲット ネットワークを編集するには、ネットワークの名前をクリックし、[コンプライアンス ホワイトリストのターゲット ネットワークの設定 \(2211 ページ\)](#) の指示に従って続行します。

**ステップ 4** 前回の保存以降に行ったすべての変更をすぐに実装するには、[ホワイトリストの保存 (Save White List)] をクリックします。

## 共有ホスト プロファイルの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

コンプライアンス ホワイトリストでは、共有ホスト プロファイルは特定のオペレーティング システムに関連付けられますが、それぞれの共有ホスト プロファイルを複数のホワイト リスト内で使用できます。複数のホワイト リストを作成するが、同じホスト プロファイルを使用

して複数のホワイトリストで特定のオペレーティングシステムを実行するホストを評価する場合は、共有のホストプロファイルを使用します。

マルチドメイン展開では、現在のドメインで作成された共有ホストプロファイルが表示されます。これは、編集が可能なプロファイルです。また、先祖ドメインからの共有ホストプロファイルも表示されますが、これは編集できません。下位のドメインで作成された共有ホストプロファイルを表示および編集するには、そのドメインに切り替えます。



- (注) 共有ホストプロファイル（組み込みを含む）を変更した場合や、組み込みアプリケーションプロトコル、プロトコル、またはクライアントを変更した場合、それを使用するすべてのホワイトリストに変更が影響します。意図しない変更を加えた場合や、該当する組み込みの要素を削除した場合は、工場出荷時の初期状態にリセットできます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [相関 (Correlation)] を選択して、[ホワイトリスト (White List)] タブをクリックします。

**ステップ 2** [共有プロファイルの編集 (Edit Shared Profiles)] をクリックします。

**ステップ 3** 共有ホストプロファイルを管理します。

- 共有ホストプロファイルの作成：ホストの調査なしで新しい共有ホストプロファイルを作成するには、[共有ホストプロファイル (Shared Host Profiles)] の横にある追加アイコン (+) をクリックし、[ホワイトリストホストプロファイルの作成 \(2213 ページ\)](#) で説明する手順を実行します。
- 調査によるホストプロファイルの作成：ネットワークの調査によって複数の新しい共有ホストプロファイルを作成するには、[ターゲットネットワークの追加 (Add Target Network)] をクリックして、[コンプライアンスホワイトリストのターゲットネットワークの設定 \(2211 ページ\)](#) で説明する手順を実行します。
- 削除：共有ホストプロファイルを削除するには、削除アイコン (🗑️) をクリックして、選択内容を確認します。
- 編集：既存の共有ホストプロファイル（組み込み共有ホストプロファイルを含む）を変更するには、そのプロファイルの名前をクリックして、[ホワイトリストホストプロファイルの作成 \(2213 ページ\)](#) で説明する手順を実行します。
- 組み込みのホストプロファイルのリセット：すべての組み込みホストプロファイルを工場出荷時の初期状態にリセットするには、[組み込みホストプロファイル (Built-in Host Profiles)] をクリックして、[工場出荷時の初期状態にリセット (Reset to Factory Defaults)] をクリックしてから、選択内容を確認します。

**ステップ 4** 最後の保存以降に行われたすべての変更をすぐに実装するには、[すべてのプロファイルの保存 (Save All Profiles) ]をクリックします。

---



## 第 91 章

# 相関ポリシー

次のトピックでは、相関ポリシーおよびルールの設定方法について説明します。

- [相関ポリシーとルールの概要 \(2223 ページ\)](#)
- [相関ポリシーの設定 \(2225 ページ\)](#)
- [相関ルールの設定 \(2227 ページ\)](#)
- [相関応答グループの設定 \(2266 ページ\)](#)

## 相関ポリシーとルールの概要

相関機能を使用することで、ネットワークへの脅威に対して相関ポリシーを使用してリアルタイムで応答することができます。

ネットワーク上のアクティビティによって、アクティブな相関ポリシー内の相関ルールまたはコンプライアンスホワイトリストのいずれかがトリガーされると、相関ポリシー違反が発生します。

### 相関ルール

アクティブな相関ポリシー内の相関ルールがトリガーされると、システムによって相関イベントが生成されます。相関ルールは、以下の場合にトリガーされます。

- 特定のタイプのイベント（接続、侵入、マルウェア、ディスクバリエーション、ユーザ アクティビティなど）がシステムによって生成された。
- ネットワーク トラフィックが通常のプロファイルから逸脱している。

以下の方法で相関ルールを制約することもできます。

- ホスト プロファイル限定を追加すると、トリガー イベントに関連するホストのプロファイルからの情報に基づいてルールを制約できます。
- 接続トラッカーを相関ルールに追加すると、ルールの初期基準に一致した場合、システムは特定の接続を追跡し始めます。その後、追跡対象の接続がさらに追加の基準を満たす場合のみ、相関イベントが生成されます。

- ユーザ限定を相関ルールに追加すると、特定のユーザまたはユーザ グループを追跡します。たとえば、特定のユーザのトラフィックや特定の部門からのトラフィックに対してのみトリガーされるように相関ルールを制約することができます。
- スヌーズ期間の追加。相関ルールがトリガーされた後、スヌーズ期間により指定したインターバルの間、そのルールは再びトリガーされません。スヌーズ期間が経過すると、ルールは再びトリガー可能になり、新しいスヌーズ期間が始まります。
- 非アクティブ期間の追加。非アクティブ期間中は、相関ルールはトリガーされません。

展開のライセンスなしでも相関ルールを設定できますが、ライセンス許可のないコンポーネントを使用するルールはトリガーされません。

### コンプライアンス ホワイトリスト

コンプライアンス ホワイト リストは、ネットワーク上のホストでどのオペレーティング システム、アプリケーション（Webおよびクライアント）、プロトコルが許可されるかを指定します。アクティブな相関ポリシーで使用されているホワイトリストにホストが違反した場合、ホワイト リスト イベントがシステムによって生成されます。

### 相関応答

相関ポリシー違反への応答には、シンプルなアラートや、さまざまな修復（ホストのスキャンなど）が含まれます。それぞれの相関ルールまたはホワイトリストを、単一の応答または応答グループに関連付けることができます。

ネットワークトラフィックが複数のルールまたはホワイトリストをトリガーとして使用した場合、システムはそれぞれのルールとホワイトリストに関連付けられているすべての応答を起動します。

### 相関およびマルチテナンシー

マルチドメイン展開では、ドメインレベルで利用可能な任意のルール、ホワイトリスト、応答を使って、任意のドメイン レベルで相関ポリシーを作成できます。高位レベルドメインの管理者はドメイン内、および複数ドメインで関連付けを実行できます。

- ドメインによって相関ルールを制約すると、そのドメインの子孫で報告されるイベントが照合されます。
- 高位レベルドメインの管理者は複数ドメインでホストを評価するコンプライアンス ホワイトリストを作成できます。同じホワイトリストで、異なるドメイン内の異なるサブネットを対象にすることができます。



(注) システムは、各リーフドメインに個別のネットワークマップを作成します。リテラルの設定（IPアドレス、VLANタグ、ユーザ名など）を使用してドメイン間の相関ルールを制約すると、予期しない結果になる可能性があります。

関連トピック

[コンプライアンス ホワイトリストの概要](#) (2203 ページ)

[Firepower Management Center アラート応答](#) (2341 ページ)

[修復の概要](#) (2285 ページ)

## 相関ポリシーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

相関ルール、コンプライアンスのホワイトリスト、アラート応答、および修復を使用して相関ポリシーを作成します。

マルチドメイン展開では、任意のドメインレベルで、そのレベルで使用可能な構成設定を使用して相関ポリシーを作成できます。

各相関ポリシーと、そのポリシーで使用される各ルールとホワイトリストにプライオリティを割り当てることができます。ルールとホワイトリストのプライオリティは、相関ポリシーのプライオリティをオーバーライドします。ネットワークトラフィックが相関ポリシーに違反した場合、違反があったルールまたはホワイトリストに独自のプライオリティがない限り、結果の相関イベントでポリシーのプライオリティ値が表示されます。

### 手順

- ステップ 1 [ポリシー (Policies)] > [相関 (Correlation)] を選択します。
- ステップ 2 [ポリシーの作成 (Create Policy)] をクリックします。
- ステップ 3 [ポリシー名 (Policy Name)] と [ポリシーの説明 (Policy Description)] を入力します。
- ステップ 4 [デフォルト プライオリティ (Default Priority)] ドロップダウン リストから、ポリシーのプライオリティを選択します。ルールのプライオリティのみを使用するには、[なし (None)] を選択します。
- ステップ 5 [ルールの追加 (Add Rules)] をクリックし、ポリシーで使用するルールとホワイトリストを選択して、[追加 (Add)] をクリックします。
- ステップ 6 各ルールまたはホワイトリストの [優先順位 (Priority)] リストから、プライオリティを選択します。
  - 1 ~ 5 のプライオリティ値
  - なし
  - デフォルト (Default) (ポリシーのデフォルト プライオリティを使用)
- ステップ 7 [ルールとホワイトリストに応答を追加する \(2226 ページ\)](#) の説明に従ってルールとホワイトリストに応答を追加します。

ステップ 8 [保存 (Save) ] をクリックします。

次のタスク

- スライダをクリックして、ポリシーをアクティブにします。

## ルールとホワイトリストに応答を追加する

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

それぞれの関連ルールまたはホワイトリストを、単一の応答または応答グループに関連付けることができます。ネットワークトラフィックが複数のルールまたはホワイトリストをトリガーとして使用した場合、システムはそれぞれのルールとホワイトリストに関連付けられているすべての応答を起動します。トラフィック プロファイルの変更への応答として使用された場合は、Nmap 修復が開始されないことに注意してください。

マルチドメイン展開では、現在のドメインまたは先祖ドメインで作成された応答を使用できません。

手順

ステップ 1 関連ポリシーエディタで、応答を追加するルールまたはホワイトリストの横にある応答アイコン (🔗) をクリックします。

ステップ 2 [未割り当ての応答 (Unassigned Responses) ] の下で、ルールまたはホワイトリストがトリガーとして使用された場合に起動する応答を選択して、上矢印 (^) をクリックします。

ステップ 3 [更新 (Update) ] をクリックします。

関連トピック

[Firepower Management Center アラート応答 \(2341 ページ\)](#)

[修復の概要 \(2285 ページ\)](#)

## 関連ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin



アクティブな相関ポリシーへの変更は、即座に反映されます。

相関ポリシーを有効化すると、システムは即座にイベントの処理を開始して、応答をトリガーします。システムは、最初の有効化後の評価時に、非準拠ホストのホワイトリストイベントを生成しない点に注意してください。

マルチドメイン展開では、現在のドメインで作成された相関ポリシーが表示されます。このポリシーは編集可能です。また、先祖ドメインからの選択した相関ポリシーも表示されますが、これは編集できません。下位のドメインで作成された相関ポリシーを表示および編集するには、そのドメインに切り替えます。



(注) 設定に無関係なドメイン（名前、管理対象デバイスなど）に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。

### 手順

**ステップ 1** [ポリシー (Policies)] > [相関 (Correlation)] を選択します。

**ステップ 2** 相関ポリシーを管理します。

- アクティブ化または非アクティブ化：スライダをクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 作成：[ポリシーの作成 (Create Policy)] をクリックします。[相関ポリシーの設定 \(2225 ページ\)](#) を参照してください。
- 編集：編集アイコン (✎) をクリックします。[相関ポリシーの設定 \(2225 ページ\)](#) を参照してください。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 削除：削除アイコン (🗑️) をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

## 相関ルールの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

単純な相関ルールでは、特定のタイプのイベントが発生することのみが必要です。より具体的な条件を指定する必要はありません。たとえば、トラフィックプロファイル変化に基づく相関

ルールでは、条件を指定する必要はありません。また、複数の条件と追加した制約を使用して複雑な関連ルールを作成することもできます。

関連ルールトリガー基準、ホストプロファイル限定、ユーザ限定、または接続トラッカーを作成するときの構文はそれぞれに異なりますが、メカニズムはすべて同じです。



(注) マルチドメイン展開では、関連ルールを先祖ドメインで制約すると、そのドメインの子孫によってレポートされるイベントと一致します。

### 始める前に

- 関連イベントをトリガーするために使用するタイプの情報が展開で収集されていることを確認します。たとえば、個々の接続イベントまたは接続サマリーイベントで使用可能な情報は、検出方法、ロギング方法、イベントタイプなど、いくつかの要因により異なります。システムは、ホストをエクスポートされたNetFlowレコードからネットワークマップに追加できますが、これらのホストに使用できる情報は限られます ([NetFlow データと管理対象デバイス データの違い \(2028 ページ\)](#) を参照)。

### 手順

**ステップ 1** [ポリシー (Policies)] > [関連 (Correlation)] を選択し、[ルール管理 (Rule Management)] タブをクリックします。

**ステップ 2** [Create Rule] をクリックします。

**ステップ 3** [ルール名 (Rule Name)] と [ルールの説明 (Rule Description)] を入力します。

**ステップ 4** 必要に応じて、ルールの [ルールグループ (Rule Group)] を選択します。

**ステップ 5** 基本イベントタイプを選択し、必要に応じて、関連ルールの追加のトリガー条件を指定します。次の基本イベントタイプを選択できます。

- **侵入イベントが発生** : [侵入イベントトリガー条件の構文 \(2230 ページ\)](#) を参照してください。
- **マルウェアイベントが発生** : [マルウェアイベントトリガー条件の構文 \(2232 ページ\)](#) を参照してください。
- **検出イベントが発生** : [ディスカバリイベントトリガー条件の構文 \(2234 ページ\)](#) を参照してください。
- **ユーザ アクティビティが検出された** : [ユーザ アクティビティのイベント トリガー条件の構文 \(2238 ページ\)](#) を参照してください。
- **ホスト入力イベントが発生** : [ホスト入力イベントトリガー条件の構文 \(2239 ページ\)](#) を参照してください。
- **接続イベントが発生** : [接続イベントトリガー条件の構文 \(2240 ページ\)](#) を参照してください。
- **トラフィックプロファイルの変更** : [トラフィックプロファイル変化の構文 \(2244 ページ\)](#) を参照してください。

**ステップ 6** 必要に応じて、次のいずれかまたはすべてを追加することによって相関ルールをさらに制約します。

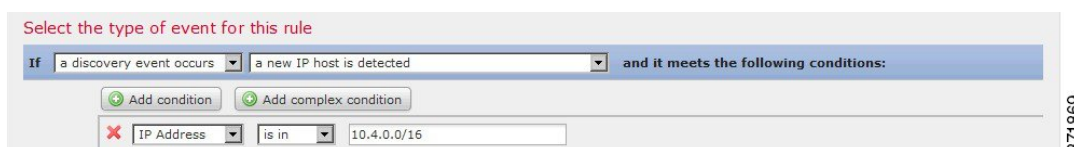
- **ホストプロファイル限定**：[ホストプロファイル限定の追加（Add Host Profile Qualification）] をクリックします。[相関ホストプロファイル限定の構文（2247 ページ）](#) を参照してください。
- **接続トラッカー**：[接続トラッカーの追加（Add Connection Tracker）] をクリックします。[接続トラッカー（2251 ページ）](#) を参照してください。
- **ユーザ限定**：[ユーザ限定の追加（Add User Qualification）] をクリックします。[ユーザ限定の構文（2250 ページ）](#) を参照してください。
- **スヌーズ期間**：ルールオプションで、[スヌーズ（Snooze）] テキストフィールドとドロップダウンリストを使用して、相関ルールのトリガー後、次に相関ルールをトリガーするまで待機する間隔を指定します。
- **非アクティブ期間**：ルールオプションで、[非アクティブ期間の追加（Add Inactive Period）] をクリックします。テキスト フィールドとドロップダウン リストを使用して、相関ルールに基づくネットワークトラフィック評価をシステムに停止させる時点および頻度を指定します。

**ヒント** スヌーズ期間を削除するには、間隔を **0**（秒、分、または時間）に指定します。

**ステップ 7** [Save Rule] をクリックします。

### 相関ルールの単純な例

新しいホストが特定のサブネットで検出されると、次の単純な相関ルールがトリガーされます。カテゴリが IP アドレスを表す場合、演算子として [is in] または [is not in] を選択すると、CIDR などの特殊な表記で表される IP アドレス ブロックにその IP アドレスが含まれるのか、含まれないのかを指定できます。



### 次のタスク

- [相関ポリシーの設定（2225 ページ）](#) の説明に従って、相関ポリシーでルールを使用します。

### 関連トピック

- [相関ルールの管理（2265 ページ）](#)
- [相関ルールの作成メカニズム（2262 ページ）](#)
- [スヌーズ期間および非アクティブ期間（2261 ページ）](#)
- [NetFlow データと管理対象デバイス データの違い（2028 ページ）](#)

## 侵入イベントトリガー条件の構文

侵入イベントを基本イベントとして選択した場合、次の表で説明する方法に従って関連ルールの条件を作成します。

表 224: 侵入イベントの構文

指定する項目	選択する演算子と内容
アクセスコントロールポリシー	侵入イベントを生成した侵入ポリシーを使用するアクセスコントロールポリシーを1つ以上選択します。
アクセスコントロールルール名	侵入イベントを生成した侵入ポリシーを使用するアクセスコントロールルールの名前の全体またはその一部を入力します。
アプリケーションプロトコル	侵入イベントに関連付けられたアプリケーションプロトコルを1つ以上選択します。
アプリケーションプロトコルカテゴリ	アプリケーションプロトコルのカテゴリを1つ以上選択します。
分類	分類を1つ以上を選択します。
クライアント	侵入イベントに関連付けられたクライアントを1つ以上選択します。
クライアントカテゴリ	クライアントのカテゴリを1つ以上選択します。
接続先(国)または送信元(国)	侵入イベントの送信元または宛先IPアドレスに関連付けられた国を1つ以上選択します。
宛先IP、送信元IP、送信元IPと宛先IPの両方、または、送信元IPか宛先IPのいずれか	単一のIPアドレスまたはアドレスブロックを入力します。
宛先ポート/ICMPコードまたは送信元ポート/ICMPタイプ	送信元トラフィックのポート番号またはICMPタイプ、または宛先トラフィックのポート番号またはICMPコードを入力します。
Device	イベントを生成した可能性があるデバイスを1つ以上選択します。
ドメイン	1つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのためにFirepower Management Centerを設定したことがある場合に表示されます。
出力インターフェイスまたは入力インターフェイス	インターフェイスを1つ以上選択します。

指定する項目	選択する演算子と内容
出力セキュリティゾーンまたは入力セキュリティゾーン	1つ以上のセキュリティゾーンまたはトンネルゾーンを選択します。
ジェネレータ ID	プリプロセッサを1つ以上選択します。
影響フラグ	侵入イベントに割り当てられた影響レベルを選択します。  NetFlow データからネットワーク マップに追加されたホストに使用可能なオペレーティングシステムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクトレベル1：赤）インパクトレベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティングシステム ID を手動で設定します。
インライン結果	システムは、侵入ポリシーの結果としてパケットを [ドロップした (dropped) ] か [ドロップしたと想定 (would have dropped) ] したのかを選択します。  システムは、インライン展開、スイッチド展開、またはルーテッド展開のパケットをドロップできます。侵入ポリシーのドロップ動作や侵入ルール状態とは無関係に、パッシブ展開（インラインセットがタップモードである場合を含む）ではシステムがパケットをドロップしません。
侵入ポリシー	侵入イベントを生成した侵入ポリシーを1つ以上選択します。
IOC タグ	侵入イベントの結果として侵害の兆候タグが設定されているかどうかを選択します。
[プライオリティ (Priority) ]	ルールの優先順位を選択します。  ルールベースの侵入イベントの場合、優先順位はpriority キーワードまたは classtype キーワードのいずれかの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。
プロトコル	<a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a> にリストされているトランスポートプロトコルの名前または番号を入力します。
ルール メッセージ	ルール メッセージの全体またはその一部を入力します。
ルール SID	単一の Snort ID (SID) またはカンマ区切りの複数の SID を入力します。  演算子として [に含まれる (is in) ] または [に含まれない (is not in) ] を選択する場合、複数選択ポップアップウィンドウを使用することはできません。SID のカンマ区切りリストを入力する必要があります。
ルール タイプ	ルールをローカルにするかどうかを指定します。  ローカルルールには、カスタマイズされた標準テキスト侵入ルール、ユーザーが変更した標準テキストルール、見出し情報を変更してルールを保存するときに作成される共有オブジェクト ルールの新規インスタンスが含まれます。

指定する項目	選択する演算子と内容
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを選択します。
SSL 証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL 証明書のサブジェクトの共通名 (CN)	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの国 (C)	セッションの暗号化に使用された証明書のサブジェクトの国番号を 1 つ以上選択します。
SSL 証明書のサブジェクトの組織 (O)	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの部門 (OU)	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを 1 つ以上選択します。
[ ユーザ名 (Username) ]	侵入イベントで送信元ホストにログインしたユーザを示すユーザ名を入力します。
VLAN ID (Admin. VLAN ID)	侵入イベントをトリガーとして使用したパケットに関連付けられた最も内側の VLANID を入力します。
Web アプリケーション	侵入イベントに関連付けられた Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

#### 関連トピック

[侵入イベント フィールド \(2557 ページ\)](#)

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## マルウェア イベント トリガー条件の構文

マルウェア イベントで関連ルールをベースとして使用するには、まず、使用するマルウェア イベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次のオプションを選択できます。

- [ エンドポイントベースのマルウェアの検出 (by endpoint-based malware detection) ] (エンドポイント向け AMP)
- [ ネットワークベースのマルウェアの検出 (by network-based malware detection) ] (ネットワーク向け AMP)

- [レトロスペクティブ ネットワークベースのマルウェアの検出 (by retrospective network-based malware detection) ] (ネットワーク向け AMP)

マルウェア イベントを基本イベントとして選択する場合、次の表で説明する方法に従って相関ルールの条件を作成します。

表 225: マルウェア イベントの構文

指定する項目	選択する演算子と内容
アプリケーション プロトコル	マルウェア イベントに関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
クライアント	マルウェア イベントに関連付けられたクライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアントのカテゴリを 1 つ以上選択します。
接続先 (国) または送信元 (国)	マルウェア イベントの送信元または宛先 IP アドレスに関連付けられた国を 1 つ以上選択します。
宛先 IP、ホスト IP、または送信元 IP	単一の IP アドレスまたはアドレスブロックを入力します。
送信先ポート/ICMP コード	宛先トラフィックのポート番号または ICMP コードを入力します。
傾向	[マルウェア (Malware) ] または [カスタム検出 (Custom Detection) ]、あるいはその両方を選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
イベント タイプ (Event Type)	エンドポイントベースのマルウェア イベントに関連付けられたイベント タイプを 1 つ以上選択します。
ファイル名	ファイルの名前を入力します。
ファイル タイプ	ファイル タイプを選択します。
ファイル タイプ カテゴリ	ファイル タイプ カテゴリを 1 つ以上選択します。

指定する項目	選択する演算子と内容
IOC タグ	マルウェア イベントの結果として侵害の兆候タグが設定 [される (is) ]か、設定 [されない (is not) ]かを選択します。
SHA-256	ファイルの SHA-256 ハッシュ値を入力するか貼り付けます。
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを選択します。
SSL 証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL 証明書のサブジェクトの共通名 (CN)	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの国 (C)	セッションの暗号化に使用された証明書のサブジェクトの国番号を 1 つ以上選択します。
SSL 証明書のサブジェクトの組織 (O)	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの部門 (OU)	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを 1 つ以上選択します。
送信元ポート/ICMP タイプ	送信元トラフィックのポート番号または ICMP タイプを入力します。
Web アプリケーション	マルウェア イベントに関連付けられた Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

#### 関連トピック

[ファイルおよびマルウェア イベント フィールド \(2617 ページ\)](#)

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## ディスカバリ イベント トリガー条件の構文

ディスカバリ イベントで相関ルールをベースとして使用するには、まず、使用するディスカバリ イベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次の表は、選択可能なディスカバリ イベントのタイプを示しています。



ホップ変更によって相関ルールをトリガーとして使用したり、ホスト制限到達のためにシステムが新しいホストをドロップした時点で相関ルールをトリガーとして使用したりすることはできません。ただし、[任意のタイプのイベントがある (there is any type of event) ]を選択することで、任意のタイプのディスカバリ イベントの発生時にルールをトリガーできます。

表 226: 相関ルールのトリガー条件とディスカバリ イベント タイプ

選択するオプション	選択内容
クライアントが変更された	クライアント更新
クライアントがタイムアウトになった	クライアント タイムアウト
ホスト IP アドレスが再使用されている	DHCP : IP アドレスの再割り当て
ホスト制限に達したためホストが削除された	ホスト削除 : ホスト制限に到達
ホストがネットワーク デバイスとして識別されている	ネットワーク デバイスへのホスト タイプの変更
ホストがタイムアウトになった	ホスト タイムアウト
ホストの IP アドレスが変更された	DHCP : IP アドレスの変更
NETBIOS 名の変更が検出された	NETBIOS 名の変更
新しいクライアントが検出された	新しいクライアント
新しい IP ホストが検出された	新しいホスト
新しい MAC アドレスが検出された	ホストの追加 MAC の検出
新しい MAC ホストが検出された	新しいホスト
新しいネットワーク プロトコルが検出された	新しいネットワーク プロトコル
新しいトランスポート プロトコルが検出された	新しいトランスポート プロトコル
TCP ポートが閉じた	TCP ポート クローズ
TCP ポートがタイムアウトした	TCP ポート タイムアウト
UDP ポートが閉じた	UDP ポート クローズ
UDP ポートがタイムアウトした	UDP ポート タイムアウト
VLAN タグが更新された	VLAN タグ情報の更新
IOC が設定された	侵害の兆候
オープン TCP ポートが検出された	新しい TCP ポート
オープン UDP ポートが検出された	新しい UDP ポート

ディスカバリ イベントトリガー条件の構文

選択するオプション	選択内容
ホストの OS 情報が変更された	新しい OS
ホストの OS またはサーバ ID でコンフリクトが発生した	アイデンティティ競合
ホストの OS またはサーバ ID がタイムアウトした	アイデンティティ タイムアウト
任意のタイプのイベントがある	任意のイベント タイプ
MAC アドレスに関する新しい情報がある	MAC 情報の変更
TCP サーバに関する新しい情報がある	TCP サーバ情報の更新
UDP サーバに関する新しい情報がある	UDP サーバ情報の更新

次の表では、ディスカバリ イベントを基本イベントとして選択するとき、関連ルールの条件を作成する方法を説明します。

表 227: ディスカバリ イベントの構文

指定する項目	選択する演算子と内容
アプリケーション プロトコル	アプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
アプリケーション ポート	アプリケーション プロトコルのポート番号を入力します。
クライアント	クライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアントのカテゴリを 1 つ以上選択します。
クライアント バージョン	クライアントのバージョン番号を入力します。
Device	ディスカバリ イベントを生成した可能性があるデバイスを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合にのみ表示されます。
ハードウェア	モバイル デバイスのハードウェア モデルを入力します。たとえば、すべての Apple iPhone に一致させるには <b>iPhone</b> と入力します。

指定する項目	選択する演算子と内容
ホストタイプ	ホストタイプを1つ以上選択します。ホスト、またはいずれかのタイプのネットワークデバイスを選択できます。
IP アドレスまたは新しい IP アドレス	単一のIPアドレスまたはアドレスブロックを入力します。
ジェイルブローケン	イベントのホストがジェイルブレイクされたモバイルデバイスであることを示すには [はい (Yes) ] を、そうでない場合は [いいえ (No) ] を選択します。
MAC アドレス	ホストの MAC アドレス全体またはその一部を入力します。  たとえば、特定のハードウェア製造元のデバイスの MAC アドレスが 0A:12:34 で始まることがわかっている場合、演算子として [開始 (begins with) ] を選択し、値として <b>0A:12:34</b> を入力できます。
MAC タイプ	MAC アドレスが [ARP/DHCP で検出 (ARP/DHCP Detected) ] されたかどうかを選択します。  つまり、MAC アドレスがホストに属していることをシステムがポジティブに識別したのか ([ARP/DHCP で検出 (is ARP/DHCP Detected) ])、または、管理対象デバイスとホストの間にルータがあるなどの理由で、その MAC アドレスを持つ多数のホストをシステムが認識しているのか ([ARP/DHCP で検出されない (is not ARP/DHCP Detected) ]) を選択します。
MAC ベンダー	ディスカバリ イベントをトリガーとして使用したネットワークトラフィックで使われている NIC の MAC ハードウェアベンダーの名前全体またはその一部を入力します。
Mobile	イベントのホストがモバイルデバイスであることを示すには [はい (Yes) ] を、そうでない場合は [いいえ (No) ] を選択します。
[NETBIOS 名 (NETBIOS Name) ]	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	<a href="http://www.iana.org/assignments/ethernet-numbers">http://www.iana.org/assignments/ethernet-numbers</a> にリストされているネットワークプロトコル番号を入力します。
OS 名	オペレーティングシステムの名前を1つ以上選択します。
OS ベンダー	オペレーティングシステムのベンダーを1つ以上選択します。
OS バージョン	オペレーティングシステムのバージョンを1つ以上選択します。

指定する項目	選択する演算子と内容
プロトコルまたは トランスポート プロトコル	<a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a> にリストされている トランスポート プロトコルの名前または番号を入力します。
ソース (Source)	ホスト入力データのソースを選択します (オペレーティング システムとサーバのアイデンティティ変更およびタイムアウトの場合)。
ソース タイプ	ホスト入力データのソースのタイプを選択します (オペレーティング システムとサーバのアイデンティティ変更およびタイムアウトの場合)。
VLAN ID (Admin. VLAN ID)	イベントに関連しているホストの VLAN ID を入力します。
Web アプリケーション	Web アプリケーションを選択します。

関連トピック

- [ディスカバリ イベント タイプ \(2698 ページ\)](#)
- [ディスカバリ イベントのフィールド \(2706 ページ\)](#)
- [Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## ユーザアクティビティのイベントトリガー条件の構文

ユーザアクティビティで相関ルールをベースとして使用するには、まず、使用するユーザアクティビティのタイプを選択します。選択肢が使用可能なトリガー条件の設定を決定します。次のオプションを選択できます。

- **a new user identity was detected** (新しいユーザ ID の検出)
- **a user logs into a host** (ユーザがホストにログイン)

ユーザアクティビティを基本イベントとして選択する場合、次の表で説明する方法に従って相関ルールの条件を作成します。

表 228: ユーザアクティビティの構文

指定する項目	選択する演算子と内容
Device	ユーザアクティビティを検出した可能性のあるデバイスを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

指定する項目	選択する演算子と内容
[IPアドレス (IP Address) ]	単一のIPアドレスまたはアドレスブロックを入力します。
[ユーザ名 (Username) ]	ユーザ名を入力します。

関連トピック

- [ユーザアクティビティデータのフィールド](#)
- [Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## ホスト入カイベント トリガー条件の構文

ホスト入カイベントで相関ルールをベースとして使用するには、まず、使用するホスト入カイベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次の表では、選択可能なホスト入カイベントのタイプを示しています。

ユーザ定義によるホスト属性定義を追加/削除/変更するとき、あるいは脆弱性の影響限定を設定するときに、相関ルールをトリガーとして使用することはできません。

表 229: 相関ルールのトリガー条件とホスト入カイベントタイプ

選択するオプション	ルールをトリガーとして使用するイベントタイプ
クライアントが追加された	クライアントの追加 (Add Client)
クライアントが削除された	クライアントの削除 (Delete Client)
ホストが追加された	ホストの追加 (Add Host)
プロトコルが追加された	プロトコルの追加 (Add Protocol)
プロトコルが削除された	プロトコルの削除 (Delete Protocol)
スキャン結果が追加された	スキャン結果の追加 (Add Scan Result)
サーバ定義が設定された	サーバ定義の設定 (Set Server Definition)
サーバが追加された	ポートの追加 (Add Port)
サーバが削除された	ポートの削除 (Delete Port)
脆弱性が無効とマークされた	脆弱性を無効に設定 (Vulnerability Set Invalid)
脆弱性が有効とマークされた	脆弱性を有効に設定 (Vulnerability Set Valid)
アドレスが削除された	ホスト/ネットワークの削除 (Delete Host/Network)
属性値が削除された	ホスト属性値の削除 (Host Attribute Delete Value)
属性値が設定された	ホスト属性値の設定 (Host Attribute Set Value)

選択するオプション	ルールをトリガーとして使用するイベントタイプ
OS 定義が設定された	オペレーティングシステム定義の設定 (Set Operating System Definition)
ホストの重要度が設定された	ホスト重要度の設定 (Set Host Criticality)

次の表では、ホスト入力イベントを基本イベントとして選択するときに、関連ルールの条件を作成する方法を説明します。

表 230: ホスト入力イベントの構文

指定する項目	選択する演算子と内容
ドメイン	1つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
[IPアドレス (IP Address) ]	単一のIPアドレスまたはアドレスブロックを入力します。
ソース (Source)	ホスト入力データのソースを選択します。
ソースタイプ (Source Type)	ホスト入力データのソースのタイプを選択します。

#### 関連トピック

- [ホスト入力イベントタイプ \(2703 ページ\)](#)
- [ディスクバリエーションのフィールド \(2706 ページ\)](#)
- [Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## 接続イベントトリガー条件の構文

接続イベントで関連ルールをベースとして使用するには、まず、使用する接続イベントのタイプを指定します。接続イベントで利用可能な情報は、システムが接続をログに記録した方法、理由、および時によって変わることにご注意ください。次のオプションを選択できます。

- 接続の開始または終了時のいずれか
- 接続の開始時
- 接続の終了時

次の表では、接続イベントを基本イベントとして選択するときに、関連ルールの条件を作成する方法を説明します。

表 231: 接続イベントの構文

指定する項目	選択する演算子と内容
アクセス コントロール ポリシー	接続をログに記録したアクセス コントロール ポリシーを1つ以上選択します。
アクセス コントロール ルールのアクション	接続をログに記録したアクセス コントロール ルールに関連付けられたアクションを1つ以上選択します。 あとで接続を処理するルールまたはデフォルトアクションとは無関係に、ネットワークトラフィックがいずれかのモニタ ルールの条件に一致した場合に相関イベントをトリガーとして使用するには、[モニタ (Monitor) ]を選択します。
アクセス コントロール ルール (	接続をログに記録したアクセス コントロール ルールの名前のすべてまたは一部を入力します。 あとで接続を処理したルールまたはデフォルトアクションとは無関係に、接続と一致した条件を持つモニタ ルールの名前を入力できます。
アプリケーション プロトコル	接続に関連付けられたアプリケーション プロトコルを1つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを1つ以上選択します。
クライアント	クライアントを1つ以上選択します。
クライアント カテゴリ	クライアントのカテゴリを1つ以上選択します。
クライアント バージョン	クライアントのバージョン番号を入力します。
接続時間	接続イベントの時間 (秒数) を入力します。
接続タイプ	接続情報がどのように取得されたかに基づいて、相関ルールをトリガーするかどうかを指定します。  <ul style="list-style-type: none"> <li>• エクスポートされた NetFlow データから生成された接続イベントに、[生成元 (is) ] および [Netflow] を選択します。</li> <li>• Firepower システムの管理対象デバイスによって検出された接続イベントに、[生成元でない (is not) ] および [Netflow] を選択します。</li> </ul>
接続先 (国) または送信元 (国)	接続イベントの送信元または宛先 IP アドレスに関連付けられた国を1つ以上選択します。
Device	接続を検出したデバイスを1つ以上選択します。または (エクスポートされた NetFlow レコードからの接続データの場合) 接続を処理したデバイスを1つ以上選択します。

指定する項目	選択する演算子と内容
ドメイン	1つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
出力インターフェイスまたは入力インターフェイス	インターフェイスを1つ以上選択します。
出力セキュリティゾーンまたは入力セキュリティゾーン	1つ以上のセキュリティゾーンまたはトンネルゾーンを選択します。
イニシエータバイト数、レスポндаバイト数、または合計バイト数	次のいずれかを入力します。 <ul style="list-style-type: none"> <li>送信されたバイト数 ([イニシエータバイト数 (Initiator Bytes)] )。</li> <li>受信されたバイト数 ([レスポндаバイト数 (Responder Bytes)] )。</li> <li>送受信されたバイト数 ([合計バイト数 (Total Bytes)] )。</li> </ul>
イニシエータ IP、レスポнда IP、イニシエータおよびレスポнда IP の両方、あるいはイニシエータ IP またはレスポнда IP	単一の IP アドレスまたはアドレスブロックを指定します。
イニシエータ パケット数、レスポнда パケット数、または合計パケット数	次のいずれかを入力します。 <ul style="list-style-type: none"> <li>送信されたパケット数 ([イニシエータ パケット (Initiator Packets)] )。</li> <li>受信されたパケット数 ([レスポнда パケット数 (Responder Packets)] )。</li> <li>送受信されたパケット数 ([合計パケット数 (Total Packets)] )</li> </ul>
イニシエータ ポート/ICMP タイプまたはレスポнда ポート/ICMP コード	イニシエータ トラフィックのポート番号または ICMP タイプ、あるいはレスポнда トラフィックのポート番号または ICMP コードを入力します。
IOC タグ	接続イベントにより侵害の兆候タグが設定[される (is)] または設定[されない (is not)] かどうかを指定します。
NetBIOS 名	接続におけるモニタ対象ホストの NetBIOS 名を入力します。
NetFlow デバイス	関連ルールをトリガーするために使用する NetFlow エクスポートの IP アドレスを選択します。ネットワーク検出ポリシーに NetFlow エクスポートを追加していない場合、[NetFlow デバイス (NetFlow Device)] ドロップダウン リストは空白になります。
プレフィルタ ポリシー	接続を処理したプレフィルタ ポリシーを1つ以上選択します。



指定する項目	選択する演算子と内容
理由 (Reason)	接続イベントに関連付けられた理由を1つ以上選択します。
セキュリティ インテリジェンス カテゴリ (Security Intelligence Category)	接続イベントに関連付けられたセキュリティインテリジェンスのカテゴリを1つ以上選択します。 接続終了イベントの条件としてセキュリティ インテリジェンス カテゴリを使用するには、アクセス コントロール ポリシーでカテゴリを [ブロック (Block) ] ではなく [モニタ (Monitor) ] に設定します。
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを指定します。
SSL 証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL 証明書ステータス (SSL Certificate Status)	セッションの暗号化に使用された証明書に関連付けられたステータスを1つ以上選択します。
SSL 証明書のサブジェクトの共通名 (CN)	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの国 (C)	セッションの暗号化に使用された証明書のサブジェクトの国番号を1つ以上選択します。
SSL 証明書のサブジェクトの組織 (O)	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの部門 (OU)	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL 暗号スイート (SSL Cipher Suite)	セッションの暗号化に使用された暗号スイートを1つ以上選択します。
SSL 暗号化セッション (SSL Encrypted Session)	[正常に復号 (Successfully Decrypted) ] を選択します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを1つ以上選択します。
SSL ポリシー	暗号化された接続をログに記録した SSL ポリシーを1つ以上選択します。
SSL ルール名	暗号化された接続をログに記録した SSL ルールの名前名のすべてまたは一部を入力します。
SSL サーバ名	クライアントが暗号化された接続を確立したサーバの名前のすべてまたは一部を入力します。
SSL URL カテゴリ	暗号化された接続でアクセスされた URL のカテゴリを1つ以上選択します。

指定する項目	選択する演算子と内容
SSL バージョン	セッションの暗号化に使用された SSL または TLS バージョンを 1 つ以上選択します。
TCP フラグ	関連ルールをトリガーとして使用するために接続イベントに含まれていなければならない TCP フラグを選択します。NetFlow レコードから生成された接続データにのみ TCP フラグが含まれます。
トランスポート プロトコル	接続で使用されたトランスポート プロトコル: <b>TCP</b> または <b>UDP</b> を入力します。
トンネル/プレフィルタ ルール	接続を処理したトンネルまたはプレフィルタ ルールの名前のすべてまたは一部を入力します。
URL	接続でアクセスされた URL 全体またはその一部を入力します。
URL カテゴリ	接続でアクセスされた URL のカテゴリを 1 つ以上選択します。
URLレピュテーション	接続でアクセスされた URL のレピュテーション値を 1 つ以上選択します。
[ユーザ名 (Username) ]	接続でいずれかのホストにログインしたユーザのユーザ名を入力します。
Web アプリケーション	接続に関連付けられた Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

#### 関連トピック

[接続およびセキュリティ インテリジェンス イベント フィールド \(2523 ページ\)](#)

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

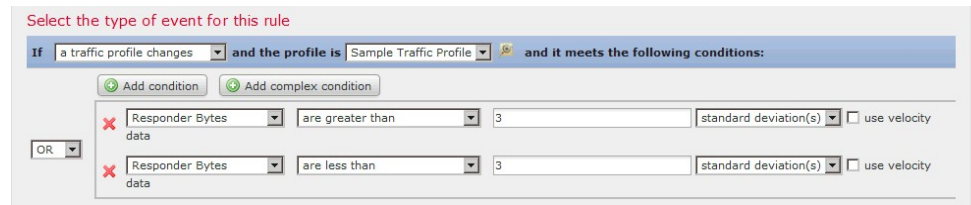
## トラフィック プロファイル変化の構文

トラフィック プロファイル変化で関連ルールをベースとして使用するには、まず、使用するトラフィック プロファイルを選択します。ルールは、選択するプロファイルによって特徴付けられるパターンからネットワーク トラフィックが逸脱するときにトリガーされます。

raw データ、またはデータから計算された統計情報のいずれかに基づいてルールをトリガーできます。たとえば、ネットワーク内を移動するデータ量 (バイト数で測定) が急激に変化した場合、攻撃または他のセキュリティーポリシー違反が発生した可能性があります。そのような変動時にトリガーとして使用されるルールを作成できます。以下のいずれかの場合にトリガーとして使用されるよう、ルールを指定できます。

- ネットワーク内を移動するバイト数が特定のバイト数を上回る場合
- ネットワーク内を移動するバイト数が、平均トラフィック量より上または下の特定数の標準偏差を超えて急激に変化した場合

ネットワーク内を移動するバイト数が、特定数の標準偏差からなる範囲を（上または下に）超えたときにトリガーとして使用されるルールを作成するには、次の図に示すように、上限と下限を指定する必要があります。



移動するバイト数が、平均を基準とした特定数の標準偏差の上側を超えた場合にトリガーとして使用されるルールを作成するには、以下の図に示されている最初の条件だけを使用します。

移動するバイト数が、平均を基準とした特定数の標準偏差の下側を超えた場合にトリガーとして使用されるルールを作成するには、2番目の条件だけを使用します。

[速度データを使用する (use velocity data)] チェックボックスを選択すると、データポイント間の変化率に基づいて相関ルールをトリガーできます。上記の例で仮に速度データを使用する場合は、次のいずれかの時点でルールがトリガーとして使用されるように指定できます。

- ネットワーク内を移動するバイト数の変化が、平均変化率より上または下の特定数の標準偏差を超えた場合
- ネットワーク内を移動するバイト数の変化が、特定のバイト数を上回った場合

トラフィックプロファイル変化を基準イベントとして選択した場合、以下の表で説明する方法に従って相関ルールの条件を作成します。

表 232: トラフィック プロファイル変化の構文

指定する項目	選択する演算子と入力内容	いずれかを選択
接続数	検出された接続の合計数 または 平均より上または下の標準偏差の数（検出された接続数がこれを超えるとルールがトリガーとして使用されます）	接続 standard deviation(s) : 標準偏差の数

指定する項目	選択する演算子と入力内容	いずれかを選択
合計バイト数、イニシエータバイト数、またはレスポндаバイト数	<p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• 送信された合計バイト数 ([合計バイト数 (Total Bytes) ])</li> <li>• 送信されたバイト数 ([イニシエータバイト数 (Initiator Bytes) ])</li> <li>• 受信されたバイト数 ([レスポндаバイト数 (Responder Bytes) ])</li> </ul> <p>または</p> <p>平均より上または下の標準偏差の数 (上の条件のいずれかはルールがトリガーとして使用される必要があります)</p>	<p>bytes</p> <p>standard deviation(s) : 標準偏差の数</p>
合計パケット数、イニシエータパケット数、またはレスポндаパケット数	<p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• 送信された合計パケット数 ([合計パケット数 (Total Packets) ])</li> <li>• 送信されたパケット数 ([イニシエータパケット数 (Initiator Packets) ])</li> <li>• 受信されたパケット数 ([レスポндаパケット数 (Responder Packets) ])</li> </ul> <p>または</p> <p>平均より上または下の標準偏差の数 (上の条件のいずれかはルールがトリガーとして使用される必要があります)</p>	<p>packets</p> <p>standard deviation(s) : 標準偏差の数</p>
一意のイニシエータ	<p>セッションを開始した個別のホストの数</p> <p>または</p> <p>平均より上または下の標準偏差の数 (検出された一意のイニシエータ数はルールがトリガーとして使用される必要があります)</p>	<p>initiators : イニシエータ数</p> <p>standard deviation(s) : 標準偏差の数</p>
一意のレスポнда	<p>セッションに回答した個別のホストの数</p> <p>または</p> <p>平均より上または下の標準偏差の数 (検出された一意のレスポнда数はルールがトリガーとして使用される必要があります)</p>	<p>responders : レスポнда数</p> <p>standard deviation(s) : 標準偏差の数</p>

## 相関ホスト プロファイル限定の構文

イベントに関連するホストのホストプロファイルに基づいて相関ルールを制約するには、[ホストプロファイル限定 (host profile qualification)] を追加します。マルウェア イベント、トラフィック プロファイル変化、または新しい IP ホスト検出によってトリガーとして使用される相関ルールには、ホストプロファイル限定を追加することはできません。

ホストプロファイル限定を作成するときには、まず、相関ルールを制約するために使用するホストを指定します。選択可能なホストは、ルールの基盤となるイベントのタイプによって異なります。

- 接続イベント：[レスポндаホスト (Responder Host)] または [イニシエータホスト (Initiator Host)] を選択します。
- 侵入イベント：[宛先ホスト (Destination Host)] または [送信元ホスト (Source Host)] を選択します。
- ディスカバリ イベント、ホスト入力イベントは、またはユーザ アクティビティ：[ホスト (Host)] を選択します。

次の表では、相関ルールのホスト プロファイル限定を作成する方法について説明します。

表 233: ホスト プロファイル限定の構文

指定する項目	選択する演算子と内容
[アプリケーションプロトコル (Application Protocol)] > [アプリケーションプロトコル (Application Protocol)]	アプリケーションプロトコルを選択します。
[アプリケーションプロトコル (Application Protocol)] > [アプリケーションポート (Application Port)]	アプリケーションプロトコルのポート番号を入力します。
[アプリケーションプロトコル (Application Protocol)] > [プロトコル (Protocol)]	プロトコルを選択します。
[アプリケーションプロトコルカテゴリ (Application Protocol Category)]	カテゴリを選択します。
[クライアント (Client)] > [クライアント (Client)]	クライアントを選択します。
[クライアント (Client)] > [クライアントバージョン (Client Version)]	クライアントバージョンを入力します。
[クライアントカテゴリ (Client Category)]	カテゴリを選択します。

指定する項目	選択する演算子と内容
ドメイン	1つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
ハードウェア	モバイルデバイスのハードウェアモデルを入力します。たとえば、すべての Apple iPhone に一致させるには <b>iPhone</b> と入力します。
[ホストの重要度 (Host Criticality) ]	ホストの重要度を選択します。
ホストタイプ	ホストタイプを1つ以上選択します。通常のホスト、またはいずれかのタイプのネットワークデバイスを選択できます。
[IOC タグ (IOC Tag) ]	侵害の兆候タグを1つ以上選択します。
ジェイルブローケン	イベントのホストがジェイルブレイクされたモバイルデバイスであることを示すには [はい (Yes) ] を、そうでない場合は [いいえ (No) ] を選択します。
[MAC アドレス (MAC Address) ]>[MAC アドレス (MAC Address) ]	ホストの MAC アドレス全体またはその一部を入力します。
[MAC アドレス (MAC Address) ]>[MAC タイプ (MAC Type) ]	<p>MAC タイプが ARP/DHCP で検出されるかどうかを選択します。</p> <ul style="list-style-type: none"> <li>• システムは MAC アドレスがホストに属していることをポジティブに識別した ([ARP/DHCP で検出 (is ARP/DHCP Detected) ])</li> <li>• たとえば、デバイスとホスト間にはルータがあるため、システムはその MAC アドレスを持つ多くのホストを認識している ([ARP/DHCP で検出されない (is not ARP/DHCP Detected) ])</li> <li>• MAC タイプが無関係 ([どれでもない (is any) ])</li> </ul>
[MAC ベンダー (MAC Vendor) ]	ホストが使用するハードウェアの MAC ベンダー全体またはその一部を入力します。
Mobile	イベントのホストがモバイルデバイスであることを示すには [はい (Yes) ] を、そうでない場合は [いいえ (No) ] を選択します。

指定する項目	選択する演算子と内容
[NetBIOS 名 (NetBIOS Name) ]	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	<a href="http://www.iana.org/assignments/ethernet-numbers">http://www.iana.org/assignments/ethernet-numbers</a> にリストされているネットワーク プロトコル番号を入力します。
[オペレーティング システム (Operating System) ]>[OS ベンダー (OS Vendor) ]	オペレーティング システムのベンダー名を 1 つ以上選択します。
[オペレーティング システム (Operating System) ]>[OS 名 (OS Name) ]	オペレーティング システムの名前を 1 つ以上選択します。
[オペレーティング システム (Operating System) ]>[OS バージョン (OS Version) ]	オペレーティング システムのバージョンを 1 つ以上選択します。
[トランスポート プロトコル (Transport Protocol) ]	<a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a> にリストされているトランスポート プロトコルの名前または番号を入力します。
VLAN ID (Admin. VLAN ID)	ホストの VLAN ID 番号を入力します。
Web アプリケーション	Web アプリケーションを選択します。
[Web アプリケーションのカテゴリ (Web Application Category) ]	カテゴリを選択します。
使用可能な任意のホスト属性 (デフォルト コンプライアンス ホワイトリスト ホスト属性を含む)	ホスト属性タイプに応じて適切な値を入力または選択します。

### 暗黙的または汎用のクライアントを使用したホスト プロファイル限定の作成

システムが client が続くアプリケーションプロトコルの名前 (たとえば、HTTPS client) を使用して検出されたクライアントをレポートする場合、このクライアントは暗黙的または汎用のクライアントです。これらの場合、システムは特定のクライアントを検出していませんが、サーバ応答トラフィックに基づいてクライアントの存在を推測しています。

暗黙的または汎用のクライアントを使用してホストプロファイル限定を作成するには、クライアントではなく、レスポンド ホストで実行されているアプリケーションプロトコルを使用して制約します。

### イベントデータを使用したホスト プロファイル限定の作成

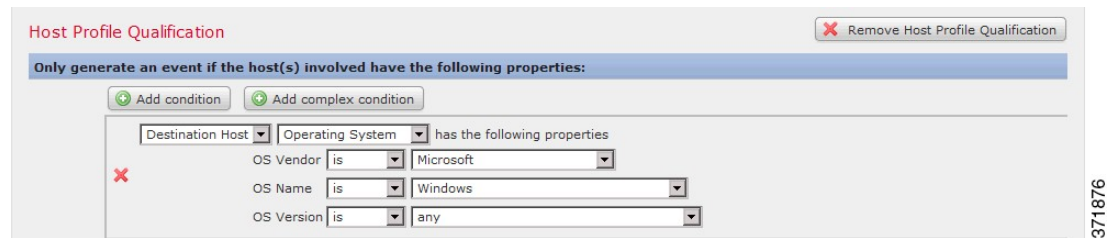
ホストプロファイル限定の制約時に、多くの場合、相関ルールの基本イベントからデータを使用できます。

たとえば、モニタ対象のいずれかのホストで特定のブラウザが使用されていることをシステムが検出した場合に、相関ルールがトリガーとして使用されるとします。さらに、この使用を検出するときに、ブラウザのバージョンが最新でない場合はイベントを生成すると仮定します。

この場合、[クライアント (Client)] は [イベントクライアント (Event Client)] ですが、[クライアントバージョン (Client Version)] が最新のバージョンでない場合にのみルールがトリガーされるように、この関連ルールをホストプロファイル限定に追加できます。

### ホストプロファイル限定の例

次のホストプロファイル限定は、ルールの基礎となるディスカバリイベントに関連するホストが Microsoft Windows のバージョンを実行している場合にのみ、ルールがトリガーとして使用されるように関連ルールを制約します。



### 関連トピック

[ホストデータフィールド \(2708 ページ\)](#)

## ユーザ限定の構文

接続、侵入、ディスカバリ、またはホスト入力の内いずれかのイベントを使用して関連ルールをトリガーとして使用する場合、イベントに関連するユーザのアイデンティティに基づいてルールを制約することができます。この制約は、ユーザ限定と呼ばれます。たとえば、送信元または宛先ユーザのアイデンティティが販売部門所属である場合にのみトリガーとして使用するよう、関連ルールを制約できます。

トラフィックプロファイル変化やユーザアクティビティ検出によってトリガーとして使用される関連ルールに、ユーザ限定を追加することはできません。また、システムは、アイデンティティレームで確立された Firepower Management Center サーバの接続を介してユーザの詳細を取得します。この情報は、データベース内のすべてのユーザに関して入手可能とは限りません。

ユーザ限定を作成するときには、まず、関連ルールを制約するために使用するアイデンティティを指定します。選択可能なアイデンティティは、ルールの基本イベントのタイプによって異なります。

- 接続イベント：[イニシエータのアイデンティティ (Identity on Initiator)] または [レスポンドのアイデンティティ (Identity on Responder)] を選択します。
- 侵入イベント：[宛先のアイデンティティ (Identity on Destination)] または [送信元のアイデンティティ (Identity on Source)] を選択します。
- ディスカバリ イベント：[ホストのアイデンティティ (Identity on Host)] を選択します。
- ホスト入力イベント：[ホストのアイデンティティ (Identity on Host)] を選択します。



次の表では、相関ルールのユーザ限定を作成する方法について説明します。

表 234: ユーザ限定の構文

指定する項目	選択する演算子と内容
認証プロトコル (Authentication Protocol)	ユーザを検出するために使用される認証プロトコル (またはユーザ タイプ) プロトコルを選択します。
部署名 (Department)	部署を入力します。
ドメイン (Domain)	1つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
E メール	電子メール アドレスを入力します。
名	名を入力します。
姓	姓を入力します。
電話	電話番号を入力します。
[ユーザ名 (Username) ]	ユーザ名を入力します。

関連トピック

[ユーザ データのフィールド](#)

## 接続トラッカー

接続トラッカー は、ルールの最初の基準 (ホスト プロファイルおよびユーザ認定を含む) に一致した後にシステムが特定の接続のトラッキングを始めるよう、相関ルールを制約します。追跡される接続が、指定した期間にわたって収集された追加の基準を満たす場合には、システムがルールの相関イベントを生成します。



ヒント

通常、接続トラッカーは特定のトラフィックだけをモニタし、トリガーとして使用された場合には指定された一定期間だけ実行されます。接続トラッカーは、広範なネットワークトラフィックをモニタして持続的に実行されるトラフィック プロファイルとは対照的です。

接続トラッカーがイベントを生成する方法は2つあります。

### 条件に一致するとただちに起動する接続トラッカー

ネットワークトラフィックが接続トラッカーの条件に一致すると即座に相関ルールが起動するよう、接続トラッカーを設定できます。この場合、タイムアウト期間が満了していても、システムはその接続トラッカーインスタンスでの接続のトラッキングを停止します。相関ルールをトリガーとして使用したのと同じタイプのポリシー違反が再び発生した場合、システムは新しい接続トラッカーを作成します。

ただし、ネットワークトラフィックが接続トラッカーの条件に一致する前にタイムアウト期間が満了した場合、システムは相関イベントを生成せず、そのルールインスタンスの接続のトラッキングを停止します。

たとえば、特定のタイプの接続が特定の期間中に特定回数を超えて発生した場合にのみ相関イベントを生成させることで、接続トラッカーをある種のイベントしきい値として機能させることができます。あるいは、初回接続後に過剰なデータ転送量をシステムが検出した場合にのみ、相関イベントを生成させることもできます。

### タイムアウト期間の満了時に起動する接続トラッカー

タイムアウト期間全体にわたって収集されるデータに依存するよう、接続トラッカーを設定できます。この場合、タイムアウト期間が満了するまでは起動しません。

たとえば、特定の期間内に検出された転送量が特定のバイト数を下回った場合に接続トラッカーを起動するよう設定すると、システムはその期間が経過するまで待って、ネットワークトラフィックがその条件に一致した場合はイベントを生成します。

## 接続トラッカーの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

### 始める前に

- 接続、侵入、検出、ユーザID、ホスト入力イベントに基づいて相関ルールを作成します。マルウェア イベントやトラフィック プロファイルの変更に基づいたルールに接続トラッカーを追加することはできません。

### 手順

- ステップ 1** 相関ルールエディタで、[接続トラッカーの追加 (Add Connection Tracker)] をクリックします。
- ステップ 2** 追跡する接続を指定します。 [接続トラッカーの構文 \(2253 ページ\)](#) を参照してください。
- ステップ 3** 追跡する接続に応じて、いつ相関イベントを生成するかを指定します。 [接続トラッカーイベントの構文 \(2256 ページ\)](#) を参照してください。

**ステップ 4** トラッカーの条件が満たされなければならない時間の間隔（秒、分または時）を指定します。

## 接続トラッカーの構文

次の表は、どのような接続を追跡するかを指定する接続トラッカー条件の作成方法を説明しています。

表 235: 接続トラッカーの構文

指定する項目	選択する演算子と内容
アクセス コントロール ポリシー	追跡対象の接続を処理したアクセスコントロールポリシーを1つ以上選択します。
アクセス コントロール ルールのアクション	追跡対象の接続をログに記録したアクセス コントロール ルールに関連付けられたアクセス コントロール ルール アクションを1つ以上選択します。  あとで接続を処理するルールまたはデフォルト アクションとは無関係に、任意のモニター ルールの条件に一致する接続を追跡するには、[モニター (Monitor)] を選択します。
アクセス コントロール ルール名	追跡対象の接続をログに記録したアクセス コントロール ルールの名前のすべてまたはその一部を入力します。  モニター ルールに一致する接続を追跡するには、モニター ルールの名前を入力します。あとで接続を処理するルールまたはデフォルト アクションとは無関係に、システムは該当する接続を追跡します。
アプリケーション プロトコル	アプリケーション プロトコルを1つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコル カテゴリを1つ以上選択します。
クライアント	クライアントを1つ以上選択します。
クライアント カテゴリ	クライアント カテゴリを1つ以上選択します。
クライアント バージョン	クライアントのバージョンを入力します。
接続時間	接続時間（秒数）を入力します。

指定する項目	選択する演算子と内容
接続タイプ	<p>接続情報がどのように取得されたかに基づいて、相関ルールをトリガーするかどうかを指定します。</p> <ul style="list-style-type: none"> <li>• エクスポートされた NetFlow レコードから生成された接続イベントに、[生成元 (is) ]および[Netflow]を選択します。</li> <li>• Firepower システムの管理対象デバイスによって検出された接続イベントに、[生成元でない (is not) ]および [Netflow] を選択します。</li> </ul>
接続先 (国) または送信元 (国)	国を 1 つ以上選択します。
Device	追跡対象の接続を検出したデバイスを 1 つ以上選択します。NetFlow 接続を追跡する場合は、エクスポートされた NetFlow レコードからの接続データを処理するデバイスを選択します。
入力インターフェイスまたは出力インターフェイス	インターフェイスを 1 つ以上選択します。
入力セキュリティゾーンまたは出力セキュリティゾーン	1 つ以上のセキュリティゾーンまたはトンネルゾーンを選択します。
イニシエータ IP、レスポнда IP、またはイニシエータ/レスポнда IP	単一の IP アドレスまたはアドレスブロックを入力します。
イニシエータ バイト数、レスポнда バイト数、または合計バイト数	<p>次のいずれかを入力します。</p> <ul style="list-style-type: none"> <li>• 送信されたバイト数 ([イニシエータバイト数 (Initiator Bytes) ])</li> <li>• 受信されたバイト数 ([レスポндаバイト数 (Responder Bytes) ])</li> <li>• 送受信されたバイト数 ([合計バイト数 (Total Bytes) ])</li> </ul>
イニシエータ パケット数、レスポнда パケット数、または合計パケット数	<p>次のいずれかを入力します。</p> <ul style="list-style-type: none"> <li>• 送信されたパケット数 ([イニシエータ パケット数 (Initiator Packets) ])</li> <li>• 受信されたパケット数 ([レスポнда パケット数 (Responder Packets) ])</li> <li>• 送受信されたパケット数 ([合計パケット数 (Total Packets) ])</li> </ul>

指定する項目	選択する演算子と内容
イニシエータ ポート/ICMP タイプまたはレスポнда ポート/ICMP コード	イニシエータ トラフィックのポート番号または ICMP タイプ、あるいはレスポнда トラフィックのポート番号または ICMP コードを入力します。
IOC タグ	侵害の兆候タグが設定されて [いる (is) ] または設定されて [いない (is not) ] かどうかを選択します。
NETBIOS 名	接続におけるモニタ対象ホストの NetBIOS 名を入力します。
NetFlow デバイス	追跡する NetFlow エクスポートの IP アドレスを選択します。ネットワーク検出ポリシーに NetFlow エクスポートを追加していない場合、[NetFlow デバイス (NetFlow Device) ] ドロップダウン リストは空白になります。
プレフィルタ ポリシー	追跡対象の接続を処理したプレフィルタ ポリシーを 1 つ以上選択します。
理由 (Reason)	追跡対象の接続に関連付けられている理由を 1 つ以上選択します。
セキュリティ インテリジェンス カテゴリ	追跡対象の接続に関連付けられているセキュリティ インテリジェンスのカテゴリを 1 つ以上選択します。
TCP フラグ	接続を追跡するために接続に含まれている必要のある TCP フラグを選択します。TCP フラグ データは、エクスポートされた NetFlow レコードから生成された接続にのみ含まれます。
トランスポート プロトコル	接続に使用されるトランスポート プロトコルを選択します。
URL	追跡対象の接続でアクセスされた URL のすべてまたはその一部を入力します。
URL Category	追跡対象の接続でアクセスされた URL のカテゴリを 1 つ以上選択します。
URLレピュテーション	追跡対象の接続でアクセスされた URL のレピュテーション値を 1 つ以上選択します。
[ユーザ名 (Username) ]	追跡対象の接続でいずれかのホストにログインしたユーザのユーザ名を入力します。
Web アプリケーション	Web アプリケーションを 1 つ以上選択します。

指定する項目	選択する演算子と内容
[Web アプリケーションのカテゴリ (Web Application Category) ]	Web アプリケーションのカテゴリを1つ以上選択します。

### イベント データを使用した接続トラッカーの作成

接続トラッカーを作成するときに、多くの場合、関連ルールの基本イベントからデータを使用できます。

たとえば、システムが新しいクライアントを検出するときに、関連ルールがトリガーされると想定します。接続トラッカーをこのタイプの関連ルールに追加すると、システムは次の基本イベントを参照する制約のあるトラッカーを自動的に入力します。

- [イニシエータ/レスポンド IP (Initiator/Responder IP) ] が [イベント IP アドレス (Event IP Address) ] に設定される。
- [クライアント (Client) ] が [イベント クライアント (Event Client) ] に設定される。



**ヒント** 特定の IP アドレスまたは IP アドレス ブロックに関連する接続を追跡するには、[手動エンタリにスイッチ (switch to manual entry) ] をクリックして、手動で IP を指定します。[イベント フィールドにスイッチ (switch to event fields) ] をクリックすると、イベントの IP アドレスを使用する設定に戻ります。

### 関連トピック

- [接続およびセキュリティ インテリジェンス イベント フィールド \(2523 ページ\)](#)
- [Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## 接続トラッカー イベントの構文

追跡対象の接続に基づいてどのようなときに関連イベントを生成するかを指定する接続トラッカー条件を作成するには、次の表の説明に従います。

表 236: 接続トラッカー イベントの構文

指定する項目	選択する演算子と入力内容
接続数	検出された接続の合計数
SSL 暗号化セッションの数	検出された SSL または TLS 暗号化セッションの合計数

指定する項目	選択する演算子と入力内容
合計バイト数、イニシエータ バイト数、またはレスポнда バイト数	次のいずれかになります。 <ul style="list-style-type: none"> <li>• 送信された合計バイト数 ([合計バイト数 (Total Bytes) ])</li> <li>• 送信されたバイト数 ([イニシエータ バイト数 (Initiator Bytes) ])</li> <li>• 受信されたバイト数 ([レスポнда バイト数 (Responder Bytes) ])</li> </ul>
合計パケット数、イニシエータ パケット数、またはレスポнда パケット数	次のいずれかになります。 <ul style="list-style-type: none"> <li>• 送信された合計パケット数 ([合計パケット数 (Total Packets) ])</li> <li>• 送信されたパケット数 ([イニシエータ パケット数 (Initiator Packets) ])</li> <li>• 受信されたパケット数 ([レスポнда パケット数 (Responder Packets) ])</li> </ul>
一意のイニシエータまたは一意のレスポнда	次のいずれかになります。 <ul style="list-style-type: none"> <li>• 検出されたセッションを開始した個別のホスト数 ([一意のイニシエータ (Unique Initiators) ])</li> <li>• 検出された接続に応答した個別のホスト数 ([一意のレスポнда (Unique Responders) ])</li> </ul>

## 外部ホストからの過剰な接続の設定例

ネットワーク 10.1.0.0/16 のセンシティブ ファイルをアーカイブし、通常、ネットワーク外のホストはネットワーク内のホストへの接続を開始することはないシナリオを考慮します。ネットワーク外から接続が開始される場合もありますが、2分以内に4つ以上の接続が開始されたときに、これが懸念材料であると判断します。

次の図に示すルールでは、接続が10.1.0.0/16 ネットワーク外からネットワーク内に発生したときに、基準に適合するトラッキング接続を開始するように指定します。その後、2分以内に署名に一致する4つの接続（発信側の接続を含む）が検出されても相関イベントを生成します。

**Rule Information** Add User Qualification Add Host Profile Qualification

Rule Name: Archive Connections - Outside

Rule Description: Trigger on 4 outside connections to 10.1.0.0/16 in 2 minutes

Rule Group: Ungrouped

Select the type of event for this rule

If a connection event occurs at either the beginning or the end of the connection and it meets the following conditions:

AND

- Initiator IP is not in 10.1.0.0/16
- Responder IP is in 10.1.0.0/16

**Connection Tracker** Remove Connection Tracker

... start tracking connections that meet the following conditions:

AND

- Initiator IP is not in 10.1.0.0/16 (switch to event fields)
- Responder IP is in 10.1.0.0/16 (switch to event fields)

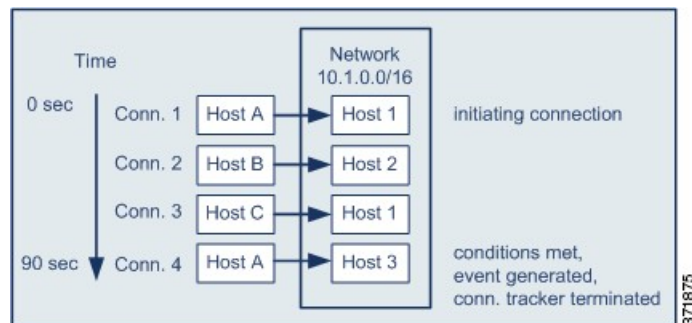
... and generate an event if:

total Number of Connections are greater than or equal to 4

in the next 2 minutes

371879

以下の図は、ネットワークトラフィックが上記の関連ルールをトリガーとして使用できる方法を示します。



371875

この例では、関連ルールの基本的条件に適合する接続が検出されました。つまり、接続が 10.1.0.0/16 ネットワーク外のホストからネットワーク内のホストへの接続が検出されました。これにより、接続トラッカーが生成されました。

接続トラッカーは、次のステージで処理します。

- ネットワーク外のホスト A からネットワーク内のホスト 1 への接続が検出されると、トラッキング接続を開始します。
- 接続トラッカーの署名に一致する 2 つ以上の接続（ホスト B ~ ホスト 2、ホスト C ~ ホスト 1）を検出します。
- 2 分の時間制限内でホスト A がホスト 3 に接続すると、4 つの認定されている接続を検出します。ルール条件が適合します。



- 最後に、相関イベントを生成し、トラッキング接続を停止します。

## BitTorrent の過剰なデータ転送の設定例

最初に監視対象のネットワークのホストに接続後、過剰な BitTorrent データの転送が検出された場合は相関イベントを生成するシナリオを考慮します。

次の図は、監視対象ネットワーク上に BitTorrent アプリケーションプロトコルを検出した場合にトリガーとして使用される相関ルールを示します。このルールには、監視対象ネットワークのホスト（この例では 10.1.0.0/16）が、最初のポリシー違反後の 5 分間に 7 MB を超えるデータ（7340032 バイト）を BitTorrent を介してまとめて転送する場合にのみルールがトリガーとして使用されるように制約する接続トラッカーがあります。

Select the type of event for this rule

If a discovery event occurs there is new information about a TCP server and it meets the following conditions:

AND

- IP Address is in 10.1.0.0/16
- Application Protocol is BitTorrent

Connection Tracker Remove Connection Tracker

... start tracking connections that meet the following conditions:

AND

- Responder IP is Event IP Address ( switch to manual entry )
- Application Protocol is BitTorrent
- Transport Protocol is TCP

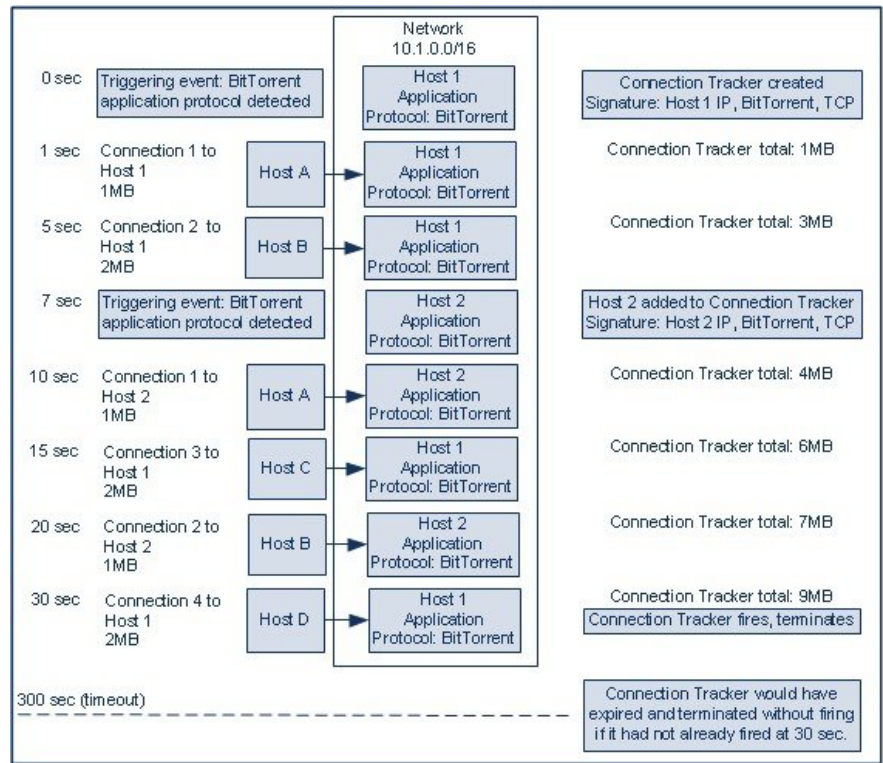
... and generate an event if:

- total Responder Bytes are greater than 7340032

in the next 5 minutes

371872

以下の図は、ネットワークトラフィックが上記の相関ルールをトリガーとして使用できる方法を示します。



この例では、2つのホスト（ホスト1、ホスト2）に BitTorrent TCP アプリケーションプロトコルが検出されました。この2つのホストは、BitTorrent を介して4つの他のホスト（ホストA、ホストB、ホストC、ホストD）にデータを転送しました。

接続トラッカーは、次の工程で処理しました。

- まず、ホスト1で BitTorrent アプリケーションプロトコルが検出されると、0秒マーカーで接続のトラッキングを開始します。次の5分以内に7MBの BitTorrent TCP データの転送が検出されない場合（300秒マーカーにより）、接続トラッカーは無効になる点にご注意ください。
- 5秒で、ホスト1は、署名に一致する3MBデータを転送します。
  - 1秒マーカーでは、ホスト1からホストAへ1MB（供給した接続トラッカーに対して数えた全 BitTorrent トラフィック1MB）
  - 5秒マーカーでホスト1からホストBへ2MB（合計3MB）
- 7秒では、ホスト2で BitTorrent アプリケーションプロトコルを検出し、ホスト2に対しても BitTorrent 接続のトラッキングを開始します。
- 20秒では、ホスト1とホスト2の両方から転送される署名に一致する追加のデータを検出します。
  - 10秒マーカーでホスト2からホストAへ1MB（合計4MB）
  - 15秒マーカーでホスト1からホストCへ2MB（合計6MB）

- 20 秒マーカーでホスト 2 からホスト B へ 1MB (合計 7MB)
- ホスト 1 とホスト 2 では、現在合わせて 7MB の BitTorrent データが転送されていますが、ルールはトリガーとして使用されていません。これは、転送された合計バイト数が 7MB を超えている ([レスポンドのバイトは 7340032 を超えています (Responder Bytes are greater than 7340032)] ) 必要があるためです。この時点で、トラッカーのタイムアウト期間内の残りの 280 秒の間、追加の BitTorrent 転送が検出されない場合に、トラッカーは無効になり、相関イベントは作成されません。
- ただし、30 秒の時点で、別の BitTorrent 転送が検出され、次のルールの条件が満たされません。
  - 30 秒マーカーでは、ホスト 1 からホスト D へ 2 MB (合計 9 MB)
- 最後に、相関イベントが生成されます。また、5 分間が無効にならなくても接続トラッカーインスタンスについてはトラッキング接続を停止します。この時点で BitTorrent TCP アプリケーションプロトコルを用いて新しい接続が検出されると、新しい接続トラッカーが生成されます。ホスト 1 が 2 MB すべてをホスト D に転送した後に相関イベントが生成される点にご注意ください。これは、セッションが終了するまで接続データを計算することはないためです。

## スヌーズ期間および非アクティブ期間

相関ルールでスヌーズ期間を設定することができます。スヌーズ期間を設定すると、相関ルールがトリガーとして使用されたとき、指定した時間間隔内にルール違反が再び発生しても、システムはその期間中はルールのトリガーを停止します。スヌーズ期間が経過すると、ルールは再びトリガー可能になります (新しいスヌーズ期間が始まります)。

たとえば、通常はトラフィックを全く生成しないはずのホストがネットワーク上にあるとします。このホストが関与する接続がシステムで検出されるたびにトリガーとして使用される単純な相関ルールの場合、このホストで送受信されるネットワークトラフィックによっては、短時間に多数の相関イベントが生成される可能性があります。ポリシー違反を示す相関イベントの数を制限するために、スヌーズ期間を追加できます。これにより、(指定した期間内に) システムで検出されたそのホストに関連する最初の接続に対してのみ、システムは相関イベントを生成します。

また、相関ルールで非アクティブ期間を設定することもできます。非アクティブ期間中は、相関ルールはトリガーとして使用されません。非アクティブ期間を毎日、毎週、または毎月繰り返すように設定できます。たとえば、ホストオペレーティングシステム変更を探すために内部ネットワークで夜間に Nmap スキャンを実行するとします。この場合、相関ルールが誤ってトリガーとして使用されないよう、毎日のスキャン時間帯に、該当する相関ルールで非アクティブ期間を設定することができます。

## 相関ルールの作成メカニズム

相関ルールは、ルールがトリガーされる条件を指定して作成します。条件で使用できるシンタックスは、作成しようとしている要素により異なりますが、メカニズムはすべて同じです。

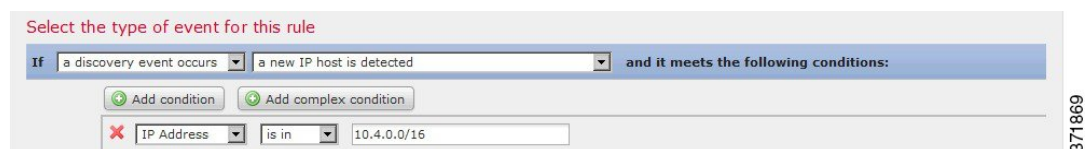
ほとんどの条件は、カテゴリ、演算子、値の3つの部分からなります。

- 相関ルールトリガー、ホストプロファイル認定、接続トラッカー、ユーザ認定のどれを作成しているのかに応じて、選択できるカテゴリが異なります。相関ルールトリガーでは、さらにルールの基本イベントタイプにより選択できるカテゴリが異なります。条件によっては、それぞれ独自の演算子と値を持つ複数のカテゴリが含まれることがあります。
- 条件に使用可能な演算子はカテゴリによって異なります。
- 条件の値を指定するために使用できるシンタックスは、カテゴリと演算子に応じて異なります。場合によっては、テキストフィールドに値を入力する必要があります。それ以外の場合、ドロップダウンリストから値（1つあるいは複数の値）を選択できます。

たとえば、新しいホストが検出されるたびに相関イベントを生成するには、条件を一切含まない単純なルールを作成できます。



ルールをさらに制約して、新しいホストが 10.4.x.x ネットワークで検出された場合にのみイベントを生成するには、1つの条件を追加できます。



構造に複数の条件を含める場合は、それらの条件を **AND** または **OR** 演算子でつなげる必要があります。同じレベルにある複数の条件は、次のように一緒に評価されます。

- **AND** 演算子は、制御対象のレベルにあるすべての条件が満たされなければならないことを示します。
- **OR** 演算子は、制御対象のレベルにある少なくとも1つの条件が満たされなければならないことを示します。

10.4.x.x ネットワークおよび 192.168.x.x ネットワーク上の非標準ポートで SSH アクティビティを検出する以下のルールには、4つの条件が設定されており、下の2つは複合条件を形成しています。



論理的には、ルールは次のように評価されます。

(A and B and (C or D))

表 237: ルールの評価

値	条件で指定する内容
A	アプリケーションプロトコルが SSH である
B	アプリケーションポートが 22 ではない
C	IP アドレスが 10.0.0.0/8 内にある
D	IP アドレスが 192.168.0.0/16 内にある



**注意** 頻繁に発生するイベントによってトリガーされる複雑な相関ルールを評価することにより、システムパフォーマンスが低下する可能性があります。たとえば、ロギングするすべての接続に対して、複数の条件からなるルールをシステムが評価しなければならない場合、リソースが過負荷になる可能性があります。

## 相関ルールへの条件の追加とリンク設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

### 手順

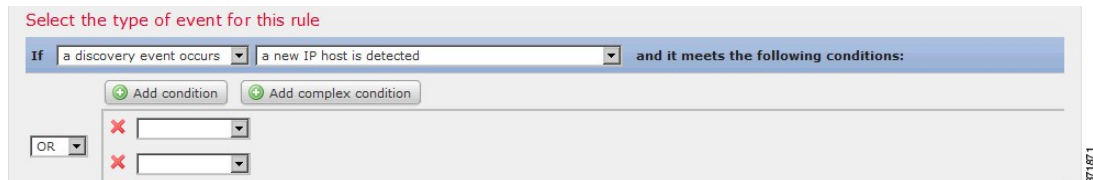
**ステップ 1** 相関ルールエディタで、単純条件または複合条件を追加します。

- 単純: [条件の追加 (Add condition)] をクリックします。
- 複合: [複合条件の追加 (Add complex condition)] をクリックします。

**ステップ 2** 条件の左にあるドロップダウンリストから [AND] または [OR] 演算子を選択して条件を結合します。

**例:単純条件と複合条件の対比**

次の図は、単純条件 2 つを [OR] 演算子で結合した関連ルールを示したものです。



次の図は、単純条件 1 つと、複合条件 1 つを [OR] 演算子で結合した関連ルールを示したものです。複合条件は 2 つの単純条件を [AND] 演算子で結合して構成します。



**関連ルール条件での複数の値の使用**

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

関連条件を作成するときに、条件の構文でドロップダウンリストから値を選択できる場合、通常はリストから複数の値を選択できます。

**手順**

- ステップ 1** 関連ルール エディタで、演算子として [存在する (is in) ] または [存在しない (is not in) ] を選択して 1 つの条件を作成します。
- ステップ 2** テキストフィールド内の任意の場所または [編集 (Edit) ] リンクをクリックします。
- ステップ 3** [使用可能 (Available) ] の下にある複数の値を選択します。また、クリックしてドラッグすることで、隣接する複数の値を選択できます。
- ステップ 4** 右矢印 (>) をクリックして、選択した項目を [Selected] に移動します。

ステップ5 [OK] をクリックします。

## 相関ルールの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

マルチドメイン展開では、現在のドメインで作成された相関ルールとグループが表示されます。これらは編集可能です。また、先祖ドメインからの選択した相関ルールとグループも表示されますが、これらは編集できません。下位のドメインで作成された相関ルールとグループを表示および編集するには、そのドメインに切り替えます。



(注) 設定に無関係なドメイン（名前、管理対象デバイスなど）に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。

アクティブな相関ポリシーのルールへの変更は、即座に反映されます。

### 始める前に

- ルールを削除する場合は、そのルールをすべての相関ポリシーから削除します。詳細については、[相関ポリシーの管理 \(2226 ページ\)](#) を参照してください。

### 手順

**ステップ1** [ポリシー (Policies)] > [相関 (Correlation)] を選択して、[ルール管理 (Rule Management)] タブをクリックします。

**ステップ2** ルールを管理します。

- 作成：[ルールの作成 (Create Rule)] をクリックします。[相関ルールの設定 \(2227 ページ\)](#) を参照してください。
- グループの作成：[グループの作成 (Create Group)] をクリックし、グループの名前を入力して、[保存 (Save)] をクリックします。グループにルールを追加するには、ルールを編集します。
- 編集：編集アイコン (✎) をクリックします。[相関ルールの設定 \(2227 ページ\)](#) を参照してください。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- ルールまたはルールグループの削除：削除アイコン (🗑️) をクリックします。ルールグループを削除すると、ルールのグループ化が解除されます。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

## 関連応答グループの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

アラートおよび修復の関連応答グループを作成し、グループをアクティブにして、アクティブな関連ポリシー内の関連ルールに割り当てることができます。システムは、ネットワークトラフィックが関連ルールに一致すると、すべてグループ化された応答を開始します。

アクティブなグループまたはいずれかのグループ化された応答に対する変更は、アクティブな関連ポリシーで行う場合、ただちに有効になります。

### 手順

- ステップ 1** [ポリシー (Policies)] > [関連 (Correlation)] を選択し、[グループ (Group)] をクリックします。
- ステップ 2** [グループの作成 (Create Group)] をクリックします。
- ステップ 3** 名前を入力します。
- ステップ 4** 作成時にグループをアクティブにする場合は、[アクティブ (Active)] チェックボックスをオンにします。  
非アクティブ化されたグループは応答を開始しません。
- ステップ 5** グループに [使用可能な応答 (Available Responses)] を選択し、右矢印 (>) をクリックして、それらを [グループ内の応答 (Responses in Group)] に移動します。応答を他の方法で移動するには、左矢印 (<) を使用します。
- ステップ 6** [保存 (Save)] をクリックします。

### 次のタスク

- 作成時にグループをアクティブにしなかった場合、アクティブにするには、スライダをクリックします。



関連トピック

[Firepower Management Center アラート応答 \(2341 ページ\)](#)

[修復の概要 \(2285 ページ\)](#)

## 相関応答グループの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

応答グループは、相関ポリシーで使用されていない場合は削除できます。応答グループを削除することで、その応答のグループ化を解除します。また、応答グループを削除せずに、一時的に非アクティブにすることもできます。これにより、グループはシステムに残りますが、ポリシーに違反するときにはグループが開始されなくなります。

マルチドメイン展開では、現在のドメインで作成されたグループが表示されます。これは編集できます。先祖ドメインで作成されたグループも表示されますが、これは編集できません。下位のドメインで作成されたグループを表示および編集するには、そのドメインに切り替えます。

アクティブな使用中の応答グループへの変更は、即座に反映されます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [相関 (Correlation)] を選択して、[グループ (Group)] をクリックします。

**ステップ 2** 応答グループを管理します。

- アクティブ化または非アクティブ化：スライダをクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 作成：[グループの作成 (Create Group)] をクリックします。[相関応答グループの設定 \(2266 ページ\)](#) を参照してください。
- 編集：編集アイコン (✎) をクリックします。[相関応答グループの設定 \(2266 ページ\)](#) を参照してください。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 削除：削除アイコン (🗑️) をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。





## 第 92 章

# トラフィック プロファイル

ここでは、トラフィック プロファイルの設定方法について説明します。

- [トラフィック プロファイルの概要 \(2269 ページ\)](#)
- [トラフィック プロファイルの管理 \(2273 ページ\)](#)
- [トラフィック プロファイルの設定 \(2275 ページ\)](#)

## トラフィック プロファイルの概要

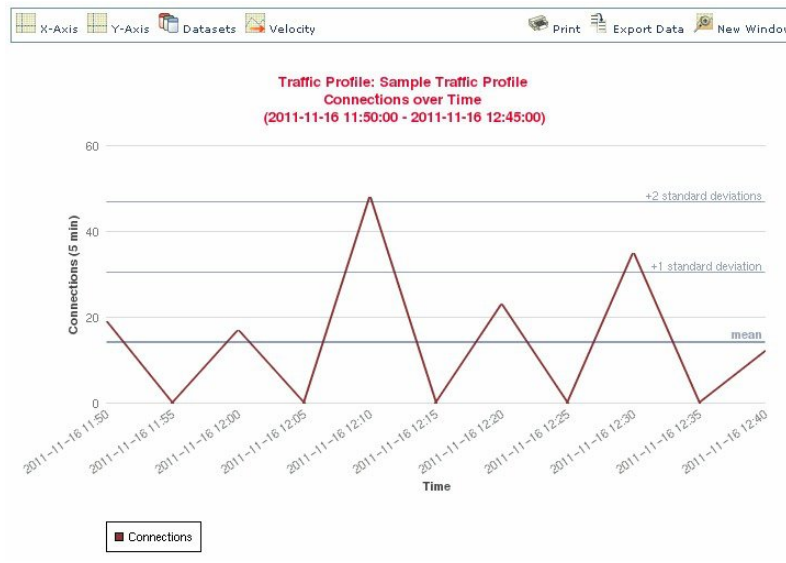
トラフィック プロファイルはプロファイル生成時間枠 (PTW) 内に収集した接続データを基に、ネットワークトラフィックをグラフで表したものです。この測定結果が正常なネットワークトラフィックを表しているものと推定します。学習期間が経過すると、新たなトラフィックをプロファイルに照らして評価することで異常なネットワークトラフィックを検出します。

デフォルト PTW は 1 週間ですが、最短で 1 時間、最長で数週間に変更できます。デフォルトで、トラフィックプロファイルは 5 分間隔でシステム生成の接続イベントに関する統計情報を生成します。ただし、このサンプリング レートは最大 1 時間間隔まで拡大することができます。



**ヒント** シスコは少なくとも 100 のデータ ポイントを含む PTW の設定を推奨します。統計的に意味のある十分なデータがトラフィック プロファイルに含まれるように、PTW とサンプリング レートを設定する必要があります。

次の図は、PTW を 1 日、サンプリング レートを 5 分としたトラフィック プロファイルを示しています。



37249

また、トラフィックプロファイルの非アクティブ期間を設定することもできます。トラフィックプロファイルは非アクティブ期間もデータ収集を行います。収集したデータをプロファイル統計の計算に使用しません。トラフィックプロファイルの時系列グラフでは、非アクティブ期間が網掛け領域として示されます。

たとえば、すべてのワークステーションが毎日深夜 0:00 にバックアップされるネットワークインフラストラクチャがあるとします。バックアップには約 30 分かかり、その間はネットワークトラフィックが急増します。予定されたバックアップ時間に合わせてトラフィックプロファイルの非アクティブ期間を繰り返すよう設定します。



(注) システムは接続の終了データを使って接続グラフとトラフィックプロファイルを作成します。トラフィックプロファイルを使用するには、必ず Firepower Management Center データベースに接続の終了イベントをロギングしてください。

### トラフィック プロファイルの実装

トラフィックプロファイルを有効にすると、システムは設定した学習期間 (PTW) の間接続データを収集し、評価します。システムは学習期間が経過すると、トラフィックプロファイルを対象にした関連ルールを評価します。

たとえば、ネットワークを通過するデータ量 (パケット数、KB 数、または接続数で測定) が、平均トラフィック量に比べて標準偏差の 3 倍も急激に上昇した場合、攻撃または他のセキュリティポリシー違反を示す可能性があるとして判断してトリガーするルールを作成できます。その後、このルールを関連ポリシーに組み込んで、トラフィックの急増に関するアラートを出したり、応答として修復を実行したりできます。

### トラフィック プロファイルの対象設定

トラフィック プロファイルは、プロファイル条件とホスト プロファイル限定による制約を受けます。

プロファイル条件を使って、すべてのネットワーク トラフィックをプロファイリングすることもできます。また、トラフィック プロファイルの対象を絞って、特定のドメイン、特定のドメイン内や複数のドメイン内のサブネット、または個別のホストをモニタすることもできます。マルチドメイン展開では次のプロファイリングが可能です。

- リーフ ドメイン管理者は、リーフ ドメイン内のネットワーク トラフィックをプロファイリングできます。
- 高位レベル ドメインの管理者は、ドメイン内または複数ドメインでトラフィックのプロファイリングができます。

また、プロファイル条件では接続データに基づく基準を設けてトラフィック プロファイルを制約することもできます。たとえば、特定のポート、プロトコル、アプリケーションが使われているセッションのみトラフィック プロファイルでプロファイリングを行うようにプロファイル条件を設定できます。

また、トラッキング対象のホストに関する情報を使用してトラフィック プロファイルを制約することもできます。この制約は、ホストプロファイル限定と呼ばれます。たとえば、重要度の高いホストに限定して接続データを収集できます。



- (注) トラフィック プロファイルを高位レベルのドメインに制約すると、各子孫リーフ ドメインのトラフィックと同じ種類のトラフィックが集約され、プロファイリングされることとなります。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、ドメイン間のトラフィックをプロファイルすると、予期しない結果になる可能性があります。

#### 関連トピック

[相関ポリシーとルールの概要](#) (2223 ページ)

## トラフィック プロファイル条件

単純なトラフィック プロファイル条件とホスト プロファイル限定を作成できます。また、複数の条件の組み合わせとネストによってより複雑な構造を作成することもできます。

条件には、カテゴリ、演算子、および値という 3 つの部分があります。

- 使用できるカテゴリは、トラフィック プロファイル条件を作成しているか、それともホスト プロファイル限定を作成しているかに応じて異なります。
- 使用できる演算子は、選択したカテゴリによって異なります。

- 条件の値を指定するために使用できる構文は、カテゴリと演算子に応じて異なります。場合によっては、テキストフィールドに値を入力する必要があります。それ以外の場合、ドロップダウンリストから1つ以上の値を選択できます。

ホストプロファイル限定の場合、開始側または応答側のホストに関する情報のデータを使用して、トラフィック プロファイルに制約を適用するかどうかを指定する必要があります。

構造に複数の条件を含める場合は、それらの条件を [および (AND)] 演算子または [または (OR)] 演算子で結合する必要があります。同じレベルにある複数の条件は、次のように一緒に評価されます。

- **AND** 演算子は、制御対象のレベルにあるすべての条件が満たされなければならないことを示します。
- [または (OR)] 演算子は、制御対象のレベルにある複数の条件の少なくとも1つが満たされている必要があることを示します。

### 制約が適用されていないトラフィック プロファイル

モニタ対象ネットワークセグメント全体のデータを収集するトラフィック プロファイルを作成する場合、次の図に示すように、条件を含まない非常に単純なプロファイルを作成できます。

### 単純なトラフィック プロファイル

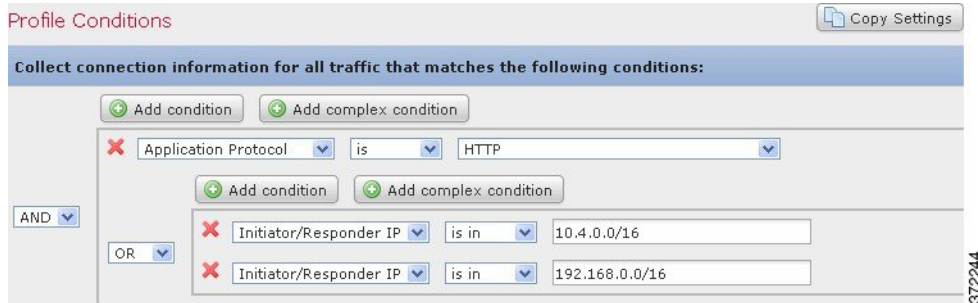
プロファイルに制約を適用して、1つのサブネットのデータのみを収集するには、次の図に示すように1つの条件を追加できます。

### 複雑なトラフィック プロファイル

次のトラフィック プロファイルには、[および (AND)] で結合された 2 つの条件が含まれています。つまり、両方の条件とも満たされる場合に限り、このトラフィック プロファイルは接続データを収集します。この例では、特定のサブネット内の IP アドレスを持つすべてのホストに関する HTTP 接続を収集します。



一方、次のトラフィック プロファイルでは、2 つのサブネットのいずれかの HTTP アクティビティに関する接続データを収集しますが、最後は複合条件を構成しています。



論理的には、上記のトラフィック プロファイルは次のように評価されます。

(A and (B or C))

条件	条件で指定する内容
A	アプリケーションプロトコル名が HTTP である
B	IP アドレスが 10.4.0.0/16 内にある
C	IP アドレスが 192.168.0.0/16 内にある

## トラフィック プロファイルの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

アクティブで完全なトラフィック プロファイルに対して記述されたルールのみが、関連ポリシー違反をトリガーできます。各トラフィック プロファイルの横にあるスライダアイコンは、プロファイルがアクティブでありデータを収集しているかどうかを示します。経過表示バーは、トラフィック プロファイルの学習期間のステータスを示します。

マルチドメイン展開では、現在のドメインで作成されたトラフィック プロファイルが表示されます。これは、編集が可能なプロファイルです。また、先祖ドメインからの選択したトラフィック プロファイルも表示されますが、これは編集できません。下位のドメインで作成されたトラフィック プロファイルを表示および編集するには、そのドメインに切り替えます。



(注) プロファイルの条件が無関係なドメインに関する情報（名前や管理対象デバイスなど）を公開する場合、システムは先祖ドメインからのトラフィック プロファイルを表示しません。

## 手順

**ステップ 1** [ポリシー (Policies)] > [関連 (Correlation)] を選択して、[トラフィック プロファイル (Traffic Profiles)] タブをクリックします。

**ステップ 2** トラフィック プロファイルを管理します。

- アクティブ化/非アクティブ化：トラフィック プロファイルをアクティブ化または非アクティブ化するには、スライダをクリックします。トラフィック プロファイルを非アクティブ化すると、そのプロファイルに関連するデータが削除されます。プロファイルを再度アクティブ化する場合は、そのプロファイルに関して作成されたルールがトリガーするようになるまで、PTW の長さだけ待つ必要があります。
- 作成：新しいトラフィック プロファイルを作成するには、[新規プロファイル (New Profile)] をクリックして、[トラフィック プロファイルの設定 \(2275 ページ\)](#) で説明する手順を実行します。また、コピーアイコン (📄) をクリックして、既存のトラフィック プロファイルのコピーを編集することもできます。
- 削除：トラフィック プロファイルを削除するには、削除アイコン (🗑️) をクリックして、選択内容を確認します。
- 編集：既存のトラフィック プロファイルを変更するには、編集アイコン (✎) をクリックして、[トラフィック プロファイルの設定 \(2275 ページ\)](#) で説明する手順を実行します。トラフィック プロファイルがアクティブな場合は、そのプロファイルの名前と説明のみを変更できます。
- グラフ：グラフとしてトラフィック プロファイルを表示するには、グラフアイコン (📊) をクリックします。マルチドメイン展開では、グラフが無関係なドメインに関する情報を公開する場合、先祖ドメインに属しているトラフィック プロファイルのグラフを表示できません。



# トラフィック プロファイルの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

トラフィック プロファイルを高レベルのドメインに制約すると、各子孫リーフ ドメインの同じタイプのトラフィックが集約およびプロファイルされます。システムは、各リーフ ドメインに個別のネットワークマップを作成します。マルチドメイン展開では、ドメイン間のトラフィックをプロファイルすると、予期しない結果になる可能性があります。

## 手順

**ステップ 1** [ポリシー (Policies)] > [相関 (Correlation)] を選択し、[トラフィック プロファイル (Traffic Profiles)] タブをクリックします。

**ステップ 2** [新規プロファイル (New Profile)] をクリックします。

**ステップ 3** プロファイル名を入力し、オプションでプロファイルの説明を入力します。

**ステップ 4** オプションで、トラフィック プロファイルを制約します。

- 設定のコピー：既存のトラフィック プロファイルから設定をコピーするには、[設定のコピー (Copy Settings)] をクリックし、使用するトラフィック プロファイルを選択して [ロード (Load)] をクリックします。
- プロファイル条件：トラッキング対象の接続の情報を使用してトラフィック プロファイルを制約するには、[トラフィック プロファイル条件の追加 \(2276 ページ\)](#) の説明に従って続行します。
- ホスト プロファイル認定：トラッキング対象のホストの情報を使用してトラフィック プロファイルを制約するには、[トラフィック プロファイルへのホスト プロファイル認定の追加 \(2277 ページ\)](#) の説明に従って続行します。
- プロファイルの時間帯 (PTW)：プロファイルの時間帯を変更するには、時間の単位を入力し、[時間 (hour(s)) ]、[日 (day(s)) ]、または [週 (week(s)) ] を選択します。
- サンプリング レート：サンプリング レートを分単位で選択します。
- 非アクティブ期間：[非アクティブ期間の追加 (Add Inactive Period)] をクリックし、ドロップダウン リストを使用して、トラフィック プロファイルを非アクティブなままにする日時と頻度を指定します。非アクティブなトラフィック プロファイルは、相関ルールをトリガーしません。トラフィック プロファイルでは、プロファイルの統計情報に非アクティブな期間のデータを含めません。

**ステップ 5** トラフィック プロファイルを保存します。

- プロファイルを保存し、ただちにデータを収集し始めるには、[保存してアクティブにする (Save & Activate)] をクリックします。

- アクティブ化せずにプロファイルを保存するには、[保存 (Save)] をクリックします。

## トラフィック プロファイル条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

### 手順

**ステップ 1** トラフィック プロファイルエディタの [プロファイル条件 (Profile Conditions)] で、追加する各条件について [条件の追加 (Add condition)] または [複合条件の追加 (Add complex condition)] をクリックします。同レベルの条件は一緒に評価されます。

- 演算子で結ばれた同一のレベルのすべての条件が満たされるべきことを指定するには、[AND] を選択します。
- 演算子で結ばれた同一のレベルの 1 つの条件だけが満たされるべきことを指定するには、[OR] を選択します。

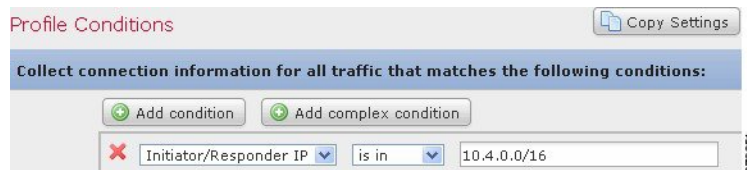
**ステップ 2** [トラフィック プロファイル条件の構文 \(2278 ページ\)](#) と [トラフィック プロファイル条件 \(2271 ページ\)](#) の説明に従い、各条件のカテゴリ、演算子、値を指定します。

演算子として [含まれる (is in)] または [含まれない (is not in)] を選択した場合は、[トラフィック プロファイル条件での複数の値の使用 \(2282 ページ\)](#) に説明してあるように単一の条件で複数の値を選択できます。

カテゴリが IP アドレスを表している場合、演算子として [含まれる (is in)] または [含まれない (is not in)] を選択すると、IP アドレス範囲内にその IP アドレスが含まれるのか、含まれないのかを指定できます。

### 例

次のトラフィック プロファイルは、特定のサブネットの情報を集めます。条件のカテゴリは [イニシエータ/レスポнда IP (Initiator/Responder IP)]、演算子は [含まれる (is in)]、値は 10.4.0.0/16 です。



関連トピック

[Firepower システムの IP アドレス表記法](#) (14 ページ)

## トラフィック プロファイルへのホスト プロファイル認定の追加

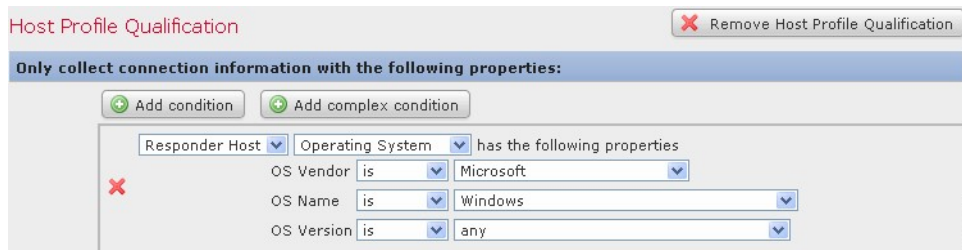
スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

手順

- 
- ステップ 1** トラフィック プロファイル エディタで、[ホスト プロファイル認定の追加 (Add Host Profile Qualification)] をクリックします。
- ステップ 2** [ホスト プロファイル認定 (Host Profile Qualification)] で、追加する各条件について [条件の追加 (Add condition)] または [複合条件の追加 (Add complex condition)] をクリックします。同レベルの条件は一緒に評価されます。
- 演算子で結ばれた同一のレベルのすべての条件が満たされるべきことを指定するには、[AND] を選択します。
  - 演算子で結ばれた同一のレベルの1つの条件だけが満たされるべきことを指定するには、[OR] を選択します。
- ステップ 3** [トラフィック プロファイルのホスト プロファイル限定の構文 \(2279 ページ\)](#) と [トラフィック プロファイル条件 \(2271 ページ\)](#) の説明に従い、各条件のホストタイプ、カテゴリ、演算子、値を指定します。
- 演算子として [含まれる (is in)] または [含まれない (is not in)] を選択した場合は、[トラフィック プロファイル条件での複数の値の使用 \(2282 ページ\)](#) に説明してあるように単一の条件で複数の値を選択できます。
- 

例

次のホスト プロファイル認定によりトラフィック プロファイルが制約され、検出された接続内の応答側ホストで任意のバージョンの Microsoft Windows が実行されている場合にのみ、接続データが収集されます。



## トラフィック プロファイル条件の構文

次の表で、トラフィック プロファイル条件を作成する方法について説明します。トラフィック プロファイルの作成に使用可能な接続データは、トラフィックの特性と検出方法を含む複数の要因によって変わることにご留意してください。

表 238: トラフィック プロファイル条件の構文

次を選択できます。	選択する演算子と内容
アプリケーションプロトコル	アプリケーションプロトコルを1つ以上選択します。
アプリケーションプロトコルカテゴリ	アプリケーションプロトコルカテゴリを1つ以上選択します。
クライアント	クライアントを1つ以上選択します。
クライアントカテゴリ	クライアントカテゴリを1つ以上選択します。
接続タイプ	プロファイルが Firepower システムの管理対象デバイスによってモニタされるトラフィックからの接続データ、またはエクスポートされた NetFlow レコードからの接続データを使用するかどうかを選択します。  接続タイプを指定しない場合、トラフィック プロファイルには両方が含まれます。
接続先 (国) または送信元 (国)	国を1つ以上選択します。
ドメイン	1つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。
イニシエータ IP、レスポнда IP、またはイニシエータ/レスポнда IP	IP アドレス、または IP アドレスの範囲を入力します。  システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

次を選択できます。	選択する演算子と内容
NetFlow デバイス	トラフィック プロファイルの作成に使用するデータの NetFlow エクスポートを選択します。
レスポンド ポート/ICMP コード	ポート番号または ICMP コードを入力します。
セキュリティ インテリジェンス カテゴリ	セキュリティ インテリジェンスのカテゴリを1つ以上選択します。  トラフィック プロファイル条件にセキュリティ インテリジェンスのカテゴリを使用するには、アクセスコントロール ポリシーでそのカテゴリを [ブロック (Block) ] ではなく [モニタ (Monitor) ] に設定する必要があります。
SSL 暗号化セッション	[正常に復号 (Successfully Decrypted) ] を選択します。
トランスポート プロトコル	トランスポート プロトコルとして <b>TCP</b> または <b>UDP</b> と入力します。
Web アプリケーション	Web アプリケーションを1つ以上選択します。
[Web アプリケーションのカテゴリ (Web Application Category) ]	Web アプリケーションのカテゴリを1つ以上選択します。

関連トピック

[接続イベント フィールドの入力の要件](#) (2539 ページ)

[Firepower システムの IP アドレス表記法](#) (14 ページ)

## トラフィック プロファイルのホスト プロファイル限定の構文

ホスト プロファイル限定の条件を作成するときには、まず、トラフィック プロファイルを制約するために使用するホストを選択する必要があります。[レスポンド ホスト (Responder Host) ] または [イニシエータ ホスト (Initiator Host) ] のいずれかを選択できます。ホスト ロールを選択したら、ホスト プロファイル限定の条件の作成を続行します。

NetFlow レコードを使用してネットワーク マップにホストを追加できますが、これらのホストに関する利用可能な情報は限定されています。たとえば、これらのホストに利用可能なオペレーティング システム データは得られません (ただしホスト入力機能を使って指定する場合を除く)。さらに、エクスポートされた NetFlow レコードからの接続データをトラフィック プロファイルで使用する場合、NetFlow レコードには、どのホストが接続のイニシエータで、どのホストがレスポンドであるかを示す情報が含まれないことに注意してください。システムは、NetFlow レコードを処理するとき、それぞれのホストが使用しているポートとそれらのポートが既知かどうかに基づいて、この情報を判断するアルゴリズムを使用します。

暗黙的 (または汎用の) クライアントを照合するには、クライアントに応答するサーバで使われるアプリケーション プロトコルに基づいてホスト プロファイル限定を作成します。接続のイニシエータ (または送信元) として機能するホスト上のクライアントリストに含まれるアプ

リケーションプロトコル名の後にクライアントが続いている場合、そのクライアントは実際には暗黙的クライアントである可能性があります。つまり、検出されたクライアントトラフィックに基づいてではなく、そのクライアントのアプリケーションプロトコルを使用するサーバ応答トラフィックに基づいて、システムがそのクライアントを報告します。

たとえば、ホスト上のクライアントとして **HTTPS クライアント** がシステムにより報告される場合、[アプリケーションプロトコル (Application Protocol) ] を [HTTPS] に設定した [レスポンド ホスト (Responder Host) ] のホスト プロファイル限定を作成します。これは、レスポンドまたは宛先ホストから送られる HTTPS サーバ応答トラフィックに基づいて HTTPS クライアントが汎用クライアントとして報告されるためです。

表 239: ホスト プロファイル限定の構文

次を選択できます。	選択する演算子と内容
[アプリケーションプロトコル (Application Protocol) ] > [アプリケーションプロトコル (Application Protocol) ]	アプリケーションプロトコルを1つ以上選択します。
[アプリケーションプロトコル (Application Protocol) ] > [アプリケーションポート (Application Port) ]	アプリケーションプロトコルのポート番号を入力します。
[アプリケーションプロトコル (Application Protocol) ] > [プロトコル (Protocol) ]	プロトコルを選択します。
[アプリケーションプロトコルカテゴリ (Application Protocol Category) ]	アプリケーションプロトコルカテゴリを1つ以上選択します。
[クライアント (Client) ] > [クライアント (Client) ]	クライアントを1つ以上選択します。
[クライアント (Client) ] > [クライアントバージョン (Client Version) ]	クライアントバージョンを入力します。
[クライアントカテゴリ (Client Category) ]	クライアントカテゴリを1つ以上選択します。
ドメイン	1つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。
[ハードウェア (Hardware) ]	モバイルデバイスのハードウェアモデルを入力します。たとえば、すべての Apple iPhone に一致させるには iPhone と入力します。
[ホストの重要度 (Host Criticality) ]	ホストの重要度を選択します。
[ホストタイプ (Host Type) ]	ホストタイプを1つ以上選択します。通常のホスト、またはいずれかのタイプのネットワークデバイスを選択できます。
[IOC タグ (IOC Tag) ]	IOC タグを1つ以上選択します。

次を選択できます。	選択する演算子と内容
[ジェイルブローケン (Jailbroken) ]	イベントのホストがジェイルブレイクされたモバイルデバイスであることを示すには [はい (Yes) ] を、そうでない場合は [いいえ (No) ] を選択します。
[MAC アドレス (MAC Address) ]>[MAC アドレス (MAC Address) ]	ホストの MAC アドレス全体またはその一部を入力します。
[MAC アドレス (MAC Address) ]>[MAC タイプ (MAC Type) ]	<p>MAC タイプが [ARP/DHCP で検出 (ARP/DHCP Detected) ] されるかどうかを選択します。つまり、次のいずれかです。</p> <ul style="list-style-type: none"> <li>• システムは MAC アドレスがホストに属していることをポジティブに識別した ([ARP/DHCP で検出 (is ARP/DHCP Detected) ])</li> <li>• たとえば、デバイスとホスト間にはルータがあるため、システムはその MAC アドレスを持つ多くのホストを認識している ([ARP/DHCP で検出されない (is not ARP/DHCP Detected) ])</li> <li>• MAC タイプが無関係 ([どれでもない (is any) ])</li> </ul>
[MAC ベンダー (MAC Vendor) ]	ホストが使用するハードウェアの MAC ベンダー全体またはその一部を入力します。
Mobile	イベントのホストがモバイル デバイスであることを示すには [はい (Yes) ] を、そうでない場合は [いいえ (No) ] を選択します。
[NETBIOS 名 (NETBIOS Name) ]	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	<a href="http://www.iana.org/assignments/ethernet-numbers">http://www.iana.org/assignments/ethernet-numbers</a> にリストされているネットワーク プロトコル番号を入力します。
[オペレーティング システム (Operating System) ]>[OS ベンダー (OS Vendor) ]	オペレーティング システムのベンダー名を 1 つ以上選択します。
[オペレーティング システム (Operating System) ]>[OS 名 (OS Name) ]	オペレーティング システムの名前を 1 つ以上選択します。
[オペレーティング システム (Operating System) ]>[OS バージョン (OS Version) ]	オペレーティング システムのバージョンを 1 つ以上選択します。
[トランスポート プロトコル (Transport Protocol) ]	<a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a> にリストされているトランスポート プロトコルの名前または番号を入力します。

次を選択できます。	選択する演算子と内容
VLAN ID (Admin, VLAN ID)	ホストの VLAN ID 番号を入力します。 システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の VLAN タグを使用してこの設定を抑制すると、予期しない結果になる可能性があります。
Web アプリケーション	Web アプリケーションを1つ以上選択します。
[Web アプリケーションのカテゴリ (Web Application Category) ]	Web アプリケーションのカテゴリを1つ以上選択します。
使用可能な任意のホスト属性 (デフォルト コンプライアンス ホワイトリスト ホスト属性を含む)	<p>選択するホスト属性のタイプに応じて、適切な値を次のように指定します。</p> <ul style="list-style-type: none"> <li>ホスト属性タイプが Integer の場合、その属性で定義されている範囲内の整数値を入力します。</li> <li>ホスト属性タイプが Text の場合、テキスト値を入力します。</li> <li>ホスト属性タイプが List の場合、有効なリスト文字列を選択します。</li> <li>ホスト属性タイプが URL の場合、URL 値を入力します。</li> </ul>

## トラフィック プロファイル条件での複数の値の使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Discovery Admin

条件を作成するときに、条件の構文でドロップダウンリストから値を選択できる場合、通常はリストから複数の値を選択できます。

たとえば、ホストで何らかの UNIX フレーバを実行している必要があることを示すホストプロファイル限定をトラフィックプロファイルに追加するには、多数の条件を OR 演算子で結合する代わりに、以下の手順を使用できます。



## 手順

---

- ステップ 1** トラフィック プロファイルまたはホスト プロファイルの資格条件を作成するときに、演算子として [存在する (is in) ] または [存在しない (is not in) ] を選択します。  
ドロップダウン リストがテキスト フィールドに変わります。
- ステップ 2** テキスト フィールド内の任意の場所または [編集 (Edit) ] リンクをクリックします。
- ステップ 3** [使用可能 (Available) ] の下にある複数の値を選択します。
- ステップ 4** 右矢印をクリックして、選択した項目を [選択済み (Selected) ] に移動します。
- ステップ 5** [OK] をクリックします。
-





## 第 93 章

# 修復

以下のトピックでは、修復の設定について説明します。

- [修復の概要 \(2285 ページ\)](#)
- [修復モジュールの管理 \(2299 ページ\)](#)
- [修復インスタンスの管理 \(2300 ページ\)](#)
- [1 つの修復モジュールのインスタンスの管理 \(2301 ページ\)](#)

## 修復の概要

修復は Firepower システムが関連ポリシー違反に応じて起動するプログラムです。

修復を実行すると、システムは修復ステータス イベントを生成します。修復ステータス イベントには、修復の名前、関連ポリシー、修復をトリガーしたルール、終了ステータスメッセージなどの詳細が含まれています。

システムは以下に挙げる複数の修復モジュールをサポートしています。

- Cisco ISE のエンドポイント保護サービス (EPS) : 関連ポリシー違反に関連するホストやネットワークへ送信されるトラフィックを検疫、隔離解除、またはシャットダウンします。
- Cisco IOS Null ルート : 関連ポリシー違反に関連するホストやネットワークへ送信されるトラフィックをブロックします (Cisco IOS バージョン 12.0 以降が必要)。
- Nmap スキャン : ホストをスキャンして、実行中のオペレーティングシステムおよびサーバを決定します。
- 属性値の設定 : 関連ポリシー違反に関連するホストのホスト属性を設定します。



**ヒント** 他のタスクを実行するカスタム モジュールをインストールすることもできます。 *Firepower System Remediation API Guide* を参照してください。

### 修復の実装

修復を実装するには、まず選択したモジュールに対して少なくとも1つのインスタンスを作成します。モジュールごとに複数のインスタンスを作成することができ、各インスタンスは別々に設定できます。たとえば、Cisco IOS Null ルート修復モジュールを使用して複数のルータと通信するには、そのモジュールのインスタンスを複数設定します。

次に、ポリシー違反の際に実行するアクションを説明する複数の修復を各インスタンスに追加します。

最後に、相関ポリシーに応じてシステムが修復を開始するように相関ポリシーで修復とルールを関連付けます。

### 修復およびマルチテナンシー

マルチドメイン展開では、どのドメインのレベルでもカスタムの修復モジュールをインストールできます。システム提供のモジュールはグローバルドメインに属します。

先祖ドメインで作成されたインスタンスに修復を追加することはできませんが、現在のドメインで同様に設定されるインスタンスを作成し、そのインスタンスに修復を追加することは可能です。また、先祖ドメインで作成した修復は、相関応答として使用することもできます。

### 関連トピック

[Firepower Management Center アラート応答](#) (2341 ページ)

[Nmap スキャン](#) (2065 ページ)

[ルールとホワイトリストに応答を追加する](#) (2226 ページ)

## Cisco ISE EPS 修復

ISE 導入環境で、エンドポイント保護サービス (EPS) が設定され、有効になっている場合、Firepower Management Center を設定することで、ISE を使った修復を起動させることが可能です。ISE EPS 修復は、完全に設定された状態では、相関ポリシー違反を起こした送信元または宛先ホストに対し、次の緩和アクション (Mitigation Actions) を実行します。

- **検疫 (quarantine)** : エンドポイントのネットワークへのアクセスを制限または拒否します。
- **隔離解除 (unquarantine)** : エンドポイントの検疫ステータスを解除し、ネットワークへのフルアクセスを許可します。
- **シャットダウン (shutdown)** : エンドポイントのNASポートを非アクティブ化し、ネットワークから切断します。

また、ネットワークをホワイトリストに登録 (Whitelist) して、システムが当該アドレスに対して ISE EPS 修復を行わないようにすることも可能です。



(注) 使用する ISE バージョンと構成は、Firepower システムでの ISE の使用方法に影響を与えます。詳細については、[ISE アイデンティティ ソース \(2126 ページ\)](#) を参照してください。

ISE EPS アクションの詳細については、『Cisco Identity Services Engine User Guide』を参照してください。

## ISE EPS 修復の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスクバリ管理者

送信元または宛先ホストで ISE EPS 修復を実行することによって、相関ポリシー違反に回答できます。

### 始める前に

- ISE サーバ上で EPS 操作を設定します。
- [ユーザ制御用 ISE の設定 \(2128 ページ\)](#) の説明に従って ISE への接続を設定します。

### 手順

- 
- ステップ 1 [ポリシー (Policies)] > [アクション (Actions)] > [インスタンス (Instances)] を選択します。
- ステップ 2 [ISE EPS インスタンスの追加 \(2287 ページ\)](#) の説明に従って pxGrid 緩和インスタンスを追加します。
- ステップ 3 [ISE EPS 修復の追加 \(2288 ページ\)](#) の説明に従って 1 つ以上の ISE EPS 修復を追加します。
- 

### 次のタスク

- [ルールとホワイトリストに回答を追加する \(2226 ページ\)](#) の説明に従って相関ポリシー違反への回答として修復を割り当てます。

## ISE EPS インスタンスの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスクバリ管理者

ISE EPS インスタンスを作成し、ロギングタイプごとに個々の修復をグループ化します。

手順

- 
- ステップ1 [ポリシー (Policies)] > [アクション (Actions)] > [インスタンス (Instances)] を選択します。
  - ステップ2 [新規インスタンスの追加 (Add a New Instance)] リストから、モジュールタイプとして [pxGrid Mitigation(v1.0)] を選択し、[追加 (Add)] をクリックします。
  - ステップ3 [インスタンス名 (Instance Name)] と [説明 (Description)] に入力します。
  - ステップ4 [ログギングの有効化 (Enable Logging)] オプションを設定し、システム ログギングを有効または無効にします。
  - ステップ5 [作成 (Create)] をクリックします。
- 

次のタスク

- [セット属性値修復の追加 \(2298 ページ\)](#) の説明に従って ISE EPS 修復を作成します。

関連トピック

- [Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

ISE EPS 修復の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスカバリ管理者

関連ポリシー違反に含まれる送信元または宛先ホストで [緩和アクション (Mitigation Actions)] を実行するため、インスタンス内に 1 つ以上の ISE EPS 修復を作成します。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- [ISE EPS インスタンスの追加 \(2287 ページ\)](#) の説明に従って ISE EPS インスタンスを作成します。

手順

- 
- ステップ1 [ポリシー (Policies)] > [アクション (Actions)] > [インスタンス (Instances)] を選択します。
  - ステップ2 修復を追加するインスタンスの横にある表示アイコン (🔍) をクリックします。

- ステップ 3** [設定済み修復 (Configured Remediations)] セクションで、[宛先の緩和 (Mitigate Destination)] または [送信元の緩和 (Mitigate Source)] を選択し、[追加 (Add)] をクリックします。
- コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 4** [修復名 (Remediation Name)] と [説明 (Description)] に入力します。
- ステップ 5** 次のいずれかの緩和アクションを選択します。[検疫 (quarantine)]、[隔離解除 (unquarantine)]、[シャットダウン (shutdown)]。
- ステップ 6** (オプション) ホワイトリストに目的の IP アドレスまたは範囲を入力し、修復から除外します。
- ステップ 7** [作成 (Create)] をクリックし、次に [完了 (Done)] をクリックします。

#### 次のタスク

- 相関ポリシー違反への応答として修復を割り当てます (ルールとホワイトリストに応答を追加する (2226 ページ) を参照)。

## Cisco IOS Null ルート修復

Cisco IOS Null ルート修復モジュールでは、シスコ「null route」コマンドを使って、個別の IP アドレスまたは IP アドレスの範囲をブロックすることができます。これにより、ホストまたはネットワークに送信されるすべてのトラフィックがルータの NULL インターフェイスにルーティングされ、ドロップされます。違反ホストまたはネットワークから送信されるトラフィックはブロックされません。



- (注) ディスカバリまたはホスト入力イベントに基づく相関ルールへの応答として接続先ベースの修復を使用しないでください。これらのイベントは、送信元ホストに関連付けられます。



- 注意** Cisco IOS 修復がアクティブになる際、タイムアウト期間はありません。IP アドレスまたはネットワークのブロックを解除するには、ルータから手動でルーティング変更をクリアする必要があります。

## Cisco IOS ルータ用修復の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスカバリ管理者



(注) 検出またはホスト入力イベントに基づく関連ルールへの応答として、宛先ベースの修復を使用しないでください。これらのイベントは、送信元ホストに関連付けられます。



**注意** Cisco IOS 修復がアクティブになる際、タイムアウト期間はありません。IP アドレスまたはネットワークのブロックを解除するには、ルータから手動でルーティング変更をクリアする必要があります。

### 始める前に

- Cisco ルータが Cisco IOS 12.0 以降を実行していることを確認します。
- ルータへのレベル 15 の管理アクセス権を持っていることを確認します。

### 手順

- ステップ 1** Cisco ルータまたは IOS ソフトウェアに付属のドキュメントの説明に従って、Cisco ルータで Telnet を有効にします。
- ステップ 2** Firepower Management Center で、使用する予定の各 Cisco IOS ルータに対する Cisco IOS ヌルルートインスタンスを追加します。[Cisco IOS インスタンスの追加 \(2291 ページ\)](#) を参照してください。
- ステップ 3** 関連ポリシーに違反した場合にルータで実現する応答のタイプに基づき、インスタンスごとに修復を作成します。
- [Cisco IOS ブロック宛先の修復の追加 \(2292 ページ\)](#)
  - [Cisco IOS ブロック宛先ネットワークの修復の追加 \(2293 ページ\)](#)
  - [Cisco IOS ブロック送信元の修復の追加 \(2294 ページ\)](#)
  - [Cisco IOS ブロック送信元ネットワークの修復の追加 \(2295 ページ\)](#)



### 次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（[ルールとホワイトリストに応答を追加する \(2226 ページ\)](#) を参照）。

### Cisco IOS インスタンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスクバリ管理者

修復を送信するルータが複数ある場合は、各ルータに対して別々のインスタンスを作成します。

### 始める前に

- ルータまたはIOS ソフトウェアのドキュメントの説明に従って、Cisco IOS ルータの Telnet アクセスを設定します。

### 手順

- ステップ 1** [ポリシー (Policies) ]>[アクション (Actions) ]>[インスタンス (Instances) ]を選択します。
- ステップ 2** [新しいインスタンスの追加 (Add a New Instance) ]リストから [Cisco IOS Null ルート (Cisco IOS Null Route) ]を選択し、[追加 (Add) ]をクリックします。
- ステップ 3** [インスタンス名 (Instance Name) ]と [説明 (Description) ]を入力します。
- ステップ 4** [ルータ IP (Router IP) ]フィールドに、修復のために使用する Cisco IOS ルータの IP アドレスを入力します。
- ステップ 5** [ユーザ名 (Username) ]フィールドに、ルータの Telnet ユーザ名を入力します。このユーザは、ルータでレベル 15 管理アクセスを持っている必要があります。
- ステップ 6** [接続パスワード (Connection Password) ]フィールドに、Telnet ユーザのパスワードを入力します。
- ステップ 7** [イネーブルパスワード (Enable Password) ]フィールドに、Telnet ユーザのイネーブルパスワードを入力します。これは、ルータの特権モードに入るために使用するパスワードです。
- ステップ 8** [ホワイトリスト (White List) ]フィールドに、修復から除外する IP アドレスまたは範囲を 1 行につき 1 つ入力します。

(注) システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 9 [作成 (Create) ] をクリックします。

### 次のタスク

- [Cisco IOS ブロック宛先の修復の追加 \(2292 ページ\)](#)、[Cisco IOS ブロック宛先ネットワークの修復の追加 \(2293 ページ\)](#)、[Cisco IOS ブロック送信元の修復の追加 \(2294 ページ\)](#)、および [Cisco IOS ブロック送信元ネットワークの修復の追加 \(2295 ページ\)](#) の説明に従い、[関連ポリシー](#) で使用する特定の修復を追加します。

### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## Cisco IOS ブロック宛先の修復の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスカバリ管理者

Cisco IOS ブロック宛先修復は、ルータから、[関連ポリシー違反](#) に関与している宛先ホストに送信されるトラフィックをブロックします。この修復を、検出またはホスト入力イベントに基づく [関連ルール](#) への応答として使用しないでください。これらのイベントは、送信元ホストに関連付けられています。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

### 始める前に

- [Cisco IOS インスタンスの追加 \(2291 ページ\)](#) の説明に従い、Cisco IOS インスタンスを追加します。

### 手順

ステップ 1 [ポリシー (Policies) ] > [アクション (Actions) ] > [インスタンス (Instances) ] を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン (🔍) をクリックします。

ステップ 3 [設定されている修復 (Configured Remediations) ] セクションで、[宛先のブロック (Block Destination) ] を選択し、[追加 (Add) ] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名 (Remediation Name) ] と [説明 (Description) ] を入力します。

ステップ5 [作成 (Create) ]をクリックし、次に[完了 (Done) ]をクリックします。

#### 次のタスク

- 相関ポリシー違反への応答として修復を割り当てます (ルールとホワイトリストに応答を追加する (2226 ページ) を参照)。

#### Cisco IOS ブロック宛先ネットワークの修復の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスクバリ管理者

Cisco IOS ブロック宛先ネットワーク修復は、ルータから、相関ポリシー違反に関与している宛先ホストのネットワークに送信されるトラフィックをブロックします。この修復を、検出またはホスト入力イベントに基づく相関ルールへの応答として使用しないでください。これらのイベントは、送信元ホストに関連付けられています。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

#### 始める前に

- [Cisco IOS インスタンスの追加 \(2291 ページ\)](#) の説明に従い、Cisco IOS インスタンスを追加します。

#### 手順

ステップ1 [ポリシー (Policies) ]>[アクション (Actions) ]>[インスタンス (Instances) ]を選択します。

ステップ2 修復を追加するインスタンスの横にある表示アイコン (🔍) をクリックします。

ステップ3 [設定されている修復 (Configured Remediations) ]セクションで、[宛先ネットワークのブロック (Block Destination Network) ]を選択し、[追加 (Add) ]をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ4 [修復名 (Remediation Name) ]と[説明 (Description) ]を入力します。

ステップ5 [ネットマスク (Netmask) ]フィールドに、サブネットマスクを入力するか、またはCIDR表記を使用して、トラフィックをブロックするネットワークを記述します。

たとえば、1つのホストがルールをトリガーとして使用したときにクラスCネットワーク全体へのトラフィックをブロックするには、ネットマスクとして255.255.255.0または24を使用します。

別の例として、トリガーのIPアドレスを含む30個のアドレスへのトラフィックをブロックするには、ネットマスクとして255.255.255.224または27を指定します。この場合、IPアドレス10.1.1.15が修復をトリガーとして使用し、10.1.1.1と10.1.1.30の間のすべてのIPアドレスがブロックされます。トリガーのIPアドレスのみをブロックするには、このフィールドは空のままにして、32を入力するか、または255.255.255.255を入力します。

**ステップ6** [作成 (Create)] をクリックし、次に [完了 (Done)] をクリックします。

### 次のタスク

- 関連ポリシー違反への応答として修復を割り当てます (ルールとホワイトリストに応答を追加する (2226 ページ) を参照)。

### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## Cisco IOS ブロック送信元の修復の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスカバリ管理者

Cisco IOS ブロック送信元修復は、ルータから、関連ポリシー違反に關与している送信元ホストに送信されるトラフィックをブロックします。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

### 始める前に

- [Cisco IOS インスタンスの追加 \(2291 ページ\)](#) の説明に従い、Cisco IOS インスタンスを追加します。

### 手順

**ステップ1** [ポリシー (Policies)] > [アクション (Actions)] > [インスタンス (Instances)] を選択します。

**ステップ2** 修復を追加するインスタンスの横にある表示アイコン (🔍) をクリックします。

**ステップ 3** [設定されている修復 (Configured Remediations) ]セクションで、[送信元のブロック (Block Source) ]を選択し、[追加 (Add) ]をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 4** [修復名 (Remediation Name) ]と[説明 (Description) ]を入力します。

**ステップ 5** [作成 (Create) ]をクリックし、次に[完了 (Done) ]をクリックします。

### 次のタスク

- 関連ポリシー違反への応答として修復を割り当てます (ルールとホワイトリストに応答を追加する (2226 ページ) を参照)。

### Cisco IOS ブロック送信元ネットワークの修復の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスカバリ管理者

Cisco IOS ブロック送信元ネットワーク修復は、ルータから、関連ポリシー違反に関与している送信元ホストのネットワークに送信されるトラフィックをブロックします。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

### 始める前に

- [Cisco IOS インスタンスの追加 \(2291 ページ\)](#) の説明に従い、Cisco IOS インスタンスを追加します。

### 手順

**ステップ 1** [ポリシー (Policies) ]>[アクション (Actions) ]>[インスタンス (Instances) ]を選択します。

**ステップ 2** 修復を追加するインスタンスの横にある表示アイコン (🔍) をクリックします。

**ステップ 3** [設定されている修復 (Configured Remediations) ]セクションで、[送信元ネットワークのブロック (Block Source Network) ]を選択し、[追加 (Add) ]をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 4** [修復名 (Remediation Name) ]と[説明 (Description) ]を入力します。

**ステップ 5** [ネットマスク (Netmask)] フィールドに、トラフィックをブロックするネットワークの説明となるサブネット マスクまたは CIDR 表記を入力します。

たとえば、1つのホストがルールをトリガーとして使用したときにクラス C ネットワーク全体へのトラフィックをブロックするには、ネットマスクとして 255.255.255.0 または 24 を使用します。

別の例として、トリガーの IP アドレスを含む 30 個のアドレスへのトラフィックをブロックするには、ネットマスクとして 255.255.255.224 または 27 を指定します。この場合、IP アドレス 10.1.1.15 が修復をトリガーとして使用し、10.1.1.1 と 10.1.1.30 の間のすべての IP アドレスがブロックされます。トリガーの IP アドレスのみをブロックするには、このフィールドは空のままにして、32 を入力するか、または 255.255.255.255 を入力します。

**ステップ 6** [作成 (Create)] をクリックし、次に [完了 (Done)] をクリックします。

#### 次のタスク

- 関連ポリシー違反への応答として修復を割り当てます (ルールとホワイトリストに**応答を追加する (2226 ページ)** を参照)。

#### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## Nmap スキャン修復

Firepower システムには、Nmap™ という、ネットワーク調査およびセキュリティ監査を目的としたオープンソースのアクティブスキャナが統合されています。Nmap 修復を使用して、関連ポリシー違反に対応できます。これは、Nmap スキャン修復をトリガーします。

Nmap スキャンの詳細については、[Nmap スキャン \(2065 ページ\)](#) を参照してください。

## セット属性値修復

トリガーイベントが発生したホストでホスト属性値を設定することにより、関連ポリシー違反に対応できます。テキストのホスト属性の場合、イベントの説明を属性値として使用できます。

### セット属性修復の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスクバリ管理者

手順

- ステップ1 [ポリシー (Policies)] > [アクション (Actions)] > [インスタンス (Instances)] を選択します。
- ステップ2 [セット属性値インスタンスの追加 \(2297 ページ\)](#) の説明に従って、セット属性インスタンスを作成します。
- ステップ3 [セット属性値修復の追加 \(2298 ページ\)](#) の説明に従って、セット属性修復を追加します。

次のタスク

- [相関ポリシー違反への応答として修復を割り当てます \(ルールとホワイトリストに応答を追加する \(2226 ページ\)\)](#) を参照。

関連トピック

- [定義済みホスト属性 \(2677 ページ\)](#)
- [ユーザ定義のホスト属性 \(2677 ページ\)](#)

セット属性値インスタンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスカバリ管理者

手順

- ステップ1 [ポリシー (Policies)] > [アクション (Actions)] > [インスタンス (Instances)] を選択します。
- ステップ2 [新しいインスタンスの追加 (Add a New Instance)] リストから [セット属性値 (Set Attribute Value)] を選択し、[追加 (Add)] をクリックします。
- ステップ3 [インスタンス名 (Instance Name)] と [説明 (Description)] を入力します。
- ステップ4 [作成 (Create)] をクリックします。

次のタスク

- [セット属性値修復の追加 \(2298 ページ\)](#) の説明に従って、セット属性修復を作成します。

## セット属性値修復の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスカバリ管理者

セット属性値修復は関連ポリシー違反に関与したホストにホスト属性を設定します。属性を設定する各属性の値について修復を作成します。テキスト属性の場合、トリガーイベントの説明を属性値として使用できます。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

### 始める前に

- [セット属性値インスタンスの追加 \(2297 ページ\)](#) の説明に従って、セット属性インスタンスを作成します。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクション (Actions)] > [インスタンス (Instances)] を選択します。

**ステップ 2** 修復を追加するインスタンスの横にある表示アイコン (🔍) をクリックします。

**ステップ 3** [設定されている修復 (Configured Remediations)] セクションで、[セット属性値 (Set Attribute Value)] を選択し、[追加 (Add)] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 4** [修復名 (Remediation Name)] と [説明 (Description)] を入力します。

**ステップ 5** 送信元データ、宛先データをもつイベントへの応答としてこの修復を使用するには、[イベントが決定するホストを更新 (Update Which Host(s) From Event)] オプションを選択します。

**ステップ 6** テキスト属性の場合、以下に従い [属性値にイベントからの説明を使用 (Use Description From Event For Attribute Value)] を指定します。

- イベントの説明を属性値として使用するには、[オン (On)] をクリックし、設定する [属性値 (Attribute Value)] を入力します。
- 修復の [属性値 (Attribute Value)] 設定を属性値として使用するには、[オフ (Off)] をクリックします。

**ステップ 7** [作成 (Create)] をクリックし、次に [完了 (Done)] をクリックします。



次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（[ルールとホワイトリストに応答を追加する \(2226 ページ\)](#) を参照）。

## 修復モジュールの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスカバリ管理者

マルチドメイン展開では、現在のドメインでインストールされた修復モジュールが表示されます。このモジュールは削除可能です。また、先祖ドメインでインストールされたモジュールも表示されますが、これは削除できません。下位ドメインの修復モジュールを管理するには、そのドメインに切り替えます。

手順

**ステップ 1** [ポリシー (Policies)] > [アクション (Actions)] > [モジュール (Modules)] を選択します。

**ステップ 2** 修復モジュールを管理します。

- 設定：モジュールの [モジュール詳細 (Module Detail)] ページを表示して、そのモジュールのインスタンスと修復を設定するには、表示アイコン (🔍) をクリックします。マルチドメイン展開では、[モジュール詳細 (Module Detail)] ページを使用して、先祖ドメインでインストールされたモジュールに対応する現在のドメイン内のインスタンスを追加、削除、または編集することはできません。代わりに、[インスタンス (Instances)] ページ ([ポリシー (Policies)] > [アクション (Actions)] > [インスタンス (Instances)]) を使用します。[修復インスタンスの管理 \(2300 ページ\)](#) を参照してください。
- 削除：使用されていないカスタム モジュールを削除するには、削除アイコン (🗑️) をクリックします。システム付属のモジュールは削除できません。
- インストール：カスタム モジュールをインストールするには、[ファイルの選択 (Choose File)] をクリックしてモジュールを参照し、[インストール (Install)] をクリックします。詳細については、*Firepower System Remediation API Guide*を参照してください。

## 修復インスタンスの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスカバリ管理者

[インスタンス (Instances)] ページには、すべての修復モジュールのすべての設定済みインスタンスがリスト表示されます。

マルチドメイン展開では、現在のドメインで作成された修復インスタンスが表示されます。このインスタンスは編集可能です。また、先祖ドメインで作成されたインスタンスも表示されますが、これは編集できません。下位ドメインの修復インスタンスを管理するには、そのドメインに切り替えます。

先祖ドメインで作成したインスタンスに修復を追加することはできませんが、同様の設定済みインスタンスを現在のドメインに作成して、そのインスタンスに修復を追加することはできます。また、先祖ドメインで作成した修復は、関連応答として使用することもできます。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクション (Actions)] > [インスタンス (Instances)] を選択します。

**ステップ 2** 修復インスタンスを管理します。

- 追加：インスタンスを追加するには、インスタンスを追加する修復モジュールを選択して、[追加 (Add)] をクリックします。システム付属のモジュールについては、次を参照してください。
  - [ISE EPS インスタンスの追加 \(2287 ページ\)](#)
  - [Cisco IOS インスタンスの追加 \(2291 ページ\)](#)
  - [Nmap スキャン インスタンスの追加 \(2082 ページ\)](#)
  - [セット属性値インスタンスの追加 \(2297 ページ\)](#)

カスタムモジュールを追加する際のヘルプは、そのモジュールのドキュメントを参照してください (使用可能な場合)。

- 設定：インスタンスの詳細を設定して、インスタンスに修復を追加するには、表示アイコン (🔍) をクリックします。

- 削除：使用されていないインスタンスを削除するには、削除アイコン (🗑️) をクリックします。

## 1つの修復モジュールのインスタンスの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	管理者 ディスカバリ管理者

[モジュール詳細 (Module Detail)] ページには、特定の修復モジュールに設定されたインスタンスと修復がすべて表示されます。

マルチドメイン展開では、現在のドメインと先祖ドメインにインストールされた修復モジュールの [モジュール詳細 (Module Detail)] ページにアクセスできます。ただし、[モジュール詳細 (Module Detail)] ページを使用して、先祖ドメインにインストールされているモジュールに対応する現在のドメイン内のインスタンスを追加、削除または編集することはできません。代わりに、[インスタンス (Instances)] ページ ([ポリシー (Policies)] > [アクション (Actions)] > [インスタンス (Instances)]) を使用します。[修復インスタンスの管理 \(2300 ページ\)](#) を参照してください。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクション (Actions)] > [モジュール (Modules)] を選択します。

**ステップ 2** 管理するインスタンスを持つ修復モジュールの横にある表示アイコン (🔍) をクリックします。

**ステップ 3** 修復インスタンスを管理します。

- 追加：インスタンスを追加するには、[追加 (Add)] をクリックします。システム付属のモジュールについては、次を参照してください。
  - [ISE EPS インスタンスの追加 \(2287 ページ\)](#)
  - [Cisco IOS インスタンスの追加 \(2291 ページ\)](#)
  - [Nmap スキャン インスタンスの追加 \(2082 ページ\)](#)
  - [セット属性値インスタンスの追加 \(2297 ページ\)](#)

カスタムモジュールのインスタンスを追加する際のヘルプは、そのモジュールのドキュメントを参照してください (提供されている場合)。

- 設定：インスタンスの詳細を設定して、インスタンスに修復を追加するには、表示アイコン (🔍) をクリックします。
  - 削除：使用されていないインスタンスを削除するには、削除アイコン (🗑️) をクリックします。
-



## 第 **XXII** 部

### レポートとアラート

- [レポートの操作 \(2305 ページ\)](#)
- [アラート応答による外部アラート \(2341 ページ\)](#)
- [侵入イベントに関する外部アラート \(2351 ページ\)](#)





## 第 94 章

# レポートの操作

以下のトピックでは、Firepower システムでレポートを操作する方法について説明します。

- [レポートの概要 \(2305 ページ\)](#)
- [リスク レポート \(2305 ページ\)](#)
- [標準レポートの概要 \(2307 ページ\)](#)
- [生成されたレポートの操作について \(2336 ページ\)](#)

## レポートの概要

Firepower システムは、次の 2 つのタイプのレポートを提供します。

- [リスク レポート \(2305 ページ\)](#) - ネットワーク上で検出されたリスクの高レベルサマリ。
- [標準レポートの概要 \(2307 ページ\)](#) - Firepower システムのあらゆる側面に関する詳細でカスタマイズ可能なレポート。

## リスク レポート

リスク レポートは、組織で検出されたリスクの概要を理解しやすい形で示す、移植可能なサマリです。これらのレポートを使用することで、システムへのアクセス権がない人々や、ネットワークセキュリティのエキスパートではない人々とも、リスク領域に関する情報やそれらのリスクに対処するための推奨案を共有できます。これらのレポートは、ネットワークセキュリティへの投資領域に関する話し合いを促進することを目的としています。

## リスク レポートの生成、表示および印刷

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Maintenance User

標準レポートのテンプレートは、リスク レポートには適用されません。

レポートは現在のドメインに関するものになります。

各リスク レポートは、HTML ファイルとして生成されます。

リスク レポートの生成をスケジュールするには、[レポートの生成の自動化 \(227 ページ\)](#) を参照してください。

### 始める前に

- 概要を取得するリスクを検出するように、システムが設定されていることを確認します。
- レポートを電子メールで送信しようとしていて、まだリレーホストを設定していない場合は、ここで設定できます。詳細については、[メール リレー ホストおよび通知アドレスの設定 \(971 ページ\)](#) を参照してください。

### 手順

**ステップ 1** [概要 (Overview)] > [レポート (Reporting)] を選択します。

**ステップ 2** [レポート テンプレート (Report Templates)] タブをクリックします。

**ステップ 3** 目的のレポートの [レポートの生成 (Report)] アイコンをクリックします。

**ステップ 4** 情報を入力します。

- [入力パラメータ (Input Parameters)] セクションに入力した情報は、レポートのタイトル ページに表示されます。これらのフィールドは、空のままでもかまいません。

**ステップ 5** [生成 (Generate)] をクリックします。

**ステップ 6** [OK] をクリックします。

### 次のタスク

- リスク レポートを表示、ダウンロード、移動、または削除するには、[生成されたレポートの操作について \(2336 ページ\)](#) を参照してください。



- ほとんどのサポート対象ブラウザから、リスク レポートを PDF に出力できます。最適な結果を得るために、ブラウザの印刷または印刷プレビューの設定で、背景色、画像、およびオプションでヘッダーとフッターを有効にします。サポートされるページサイズは、A4 および US Letter です。

## 標準レポートの概要

Firepower システムは柔軟なレポート作成システムを提供しており、Firepower Management Center で表示されるイベントビューやダッシュボードを使用して、複数のセクションがあるレポートを短時間で簡単に生成できます。独自のカスタム レポートを最初から設計することもできます。

レポートは、通信しようとしている内容が含まれるドキュメントファイルで、PDF、HTML、または CSV 形式になります。レポート テンプレートは、データの検索設定とレポートおよびそのセクションの形式を指定します。Firepower システムには強力なレポート デザインが含まれていて、レポート テンプレートの設計を自動的に行います。Web インターフェイスに表示されるイベント ビュー テーブルやダッシュボードのグラフィックの内容を複製できます。

レポート テンプレートは必要な数だけ作成できます。各レポート テンプレートは、レポートの個々のセクションを定義し、レポートの内容を作成するデータベース検索設定を指定し、表示形式（表、グラフ、詳細表示など）とタイムフレームも指定します。さらに、テンプレートでは、表紙や目次の情報、ドキュメント ページにヘッダーとフッターを付けるかどうかなどのドキュメント属性も指定します（PDF 形式のレポートでのみ指定可能）。レポート テンプレートを 1 つの設定パッケージファイルとしてエクスポートし、別の Firepower Management Center にインポートして再使用できます。

テンプレートに入力パラメータを組み込んで実用性を向上させることができます。入力パラメータを使用すると、同じレポートを用途に合わせて異なる様々なレポートに変えることができます。入力パラメータのあるレポートを生成するときには、生成プロセスで各入力パラメータの値を入力するよう求められます。ユーザが入力する値は、レポートの内容をその 1 回だけ決定するものです。たとえば、侵入イベントのレポートを作成する検索の宛先 IP フィールドに入力パラメータを使用できます。この場合、レポートの生成時に、宛先 IP アドレスの入力を求められたときに特定の部門のネットワーク セグメントを指定できます。その結果、この特定の部門に関する情報だけが含まれるレポートが生成されます。

## レポートの設計について

### レポート テンプレート

レポート テンプレートを使用して、レポートの各セクション内のデータの内容と形式や、レポート ファイルのドキュメント属性（表紙、目次、ページヘッダー、ページフッター）を定義します。レポートの生成後、削除しない限りテンプレートは再利用可能な状態になります。

レポートには、1 つ以上の情報セクションが含まれます。個々のセクションごとに形式（テキスト、表、またはグラフ）を選択します。セクションの形式の選択内容によっては、組み込め

るデータが制約される場合があります。たとえば、円グラフの形式を使用すると、特定の表に時間ベースの情報を表示できません。いつでもセクションのデータの基準や形式を変更して、表示を最適にすることができます。

定義済みイベント ビューのレポートの初期設計をベースにするか、定義済みのダッシュボード、ワークフロー、または要約から内容をインポートして設計を開始できます。空のテンプレートシェルから始めて、1つずつセクションを追加したり属性を定義したりすることもできます。



- (注) マルチドメイン導入では、先祖ドメインに属するレポートテンプレートを表示することはできませんが、編集することはできません。これらのテンプレートからレポートを生成するには、テンプレートを現在のドメインにコピーする必要があります。







## レポート テンプレート フィールド

表 240: レポート セクション タイトル バー エレメント

属性 (Attribute)	定義 (Definition)
セクション タイトル	レポート内に表示される際には、セクション名を含みます。このシステムでは、レポート セクション ページに長いセクション タイトル名が表示されると、セクション タイトル名を切り捨てます。
セクション タイトル アイコン	(+) セクションを複製します。(−) セクションを最小化します。(✕) 確認後セクションを削除します。

表 241: レポート セクション フィールド

フィールド名	定義 (Definition)
テーブル	セクションデータの抽出元のテーブルを選択できるドロップダウンメニューを表示します。
プリセット (Preset)	定義済み検索設定のドロップダウンメニューを表示します。新しい検索設定を定義する際に、該当する事前設定を選択して、検索条件を初期化できます。

フィールド名	定義 (Definition)
フォーマット (Format)	<p>セクション データ フォーマットを選択できるアイコンを表示します。次のオプションがあります。</p> <p> 棒グラフ：選択した変数の数量を比較します。</p> <p> 折れ線グラフ：選択した変数の時間の経過に伴う傾向/変化を示します。時間ベースのテーブルにのみ使用できます。</p> <p> 円グラフ：選択した各変数を全体の割合として示します。数量がゼロの変数はグラフからドロップされます。ごくわずかな数量は、ラベル [その他 (Other)] カテゴリに集められます。</p> <p> 表形式の表示：レコードごとの属性の値を示します。要約や統計のデータには使用できません。</p> <p> 詳細表示：パケット (侵入イベントの場合) やホストプロファイル (ホスト イベントの場合) など、特定のイベントに関連付けられた複合オブジェクトのデータを示します。フォーマットは、この種のオブジェクトが関係する特定のイベント タイプだけに使用できます。出力が多数要求されている場合には、パフォーマンスが低下することがあります。</p>
検索またはフィルタ (Search or Filter)	<p>検索フィルタまたはアプリケーションフィルタのドロップダウンメニューを表示します。</p> <p>ほとんどのテーブルの場合、定義済みまたは保存済みの [検索 (Search)] を使用してレポートを制約できます。編集アイコン () をクリックして、新しい検索を作成することもできます。</p> <p>アプリケーション統計表では、ユーザ定義のアプリケーションの [フィルタ (Filter)] を使用して、レポートを制約できます。</p>
X 軸 (X-Axis)	<p>選択したグラフの X 軸の使用可能なデータ列のドロップダウンメニューを表示します。グラフ チャートを選択する場合にのみ表示されます。折れ線グラフの場合、X 軸の値は常に [時刻 (Time)] です。棒グラフと円グラフの場合、X 軸の値として [時刻 (Time)] を選択できません。</p>
Y 軸 (Y-Axis)	<p>選択したグラフの Y 軸の使用可能なデータ カラムのドロップダウンメニューを表示します。</p>

フィールド名	定義 (Definition)
セクションの説明 (Section Description)	セクション内で検索データの前にある説明テキストを定義します。テキストと入力パラメータの組み合わせを入力します。新しいセクションのデフォルトは、 <code>\$(Time Window)</code> と <code>\$(Constraints)</code> の2つの入力パラメータのセットです。
時間枠 (Time Window)	セクションに表示されるデータの時間枠を定義します。セクションで時間ベースのテーブルを検索する場合、チェックボックスを選択して、レポートのグローバル時間枠を継承できます。または、セクションの特定の時間枠を設定することもできます。
結果 (Results)	[トップ (Top)] または [ボトム (Bottom)] を選択して、セクションに含めるレコードの最大数を入力します。
カラー (Color)	セクション内でグラフ化されるデータの色を定義します。必要に応じて、1つ以上の色を選択します。

## レポート テンプレートの作成

レポート テンプレートは、独自のデータベース クエリから個別に構築されたセクションのフレームワークです。

新しいレポートテンプレートを作成するには、新しいテンプレートを作成する、既存のテンプレートを使用する、イベント ビューをテンプレートのベースにする、ダッシュボードまたはワークフローをインポートするという方法があります。

既存のレポートテンプレートをコピーしない場合は、まったく新しいテンプレートを作成できます。テンプレート作成の最初の手順として、セクションを追加したり形式設定したりできるフレームワーク シェルを生成します。次に、ご希望の順序で、個々のテンプレート セクションを設計し、レポート ドキュメントの属性を設定します。

各テンプレートセクションは、検索設定やフィルタによって生成されたデータセットで構成され、表示モードを確定する形式の仕様（表や円グラフなど）があります。出力に含めるデータレコードのフィールドを選択し、タイムフレームと表示するレコード数も選択して、さらにセクションの内容を確定します。



(注) セクションプレビューユーティリティを使用して、カラムの選択内容や、円グラフの色などの出力の特性を検査します。このインジケータは、設定済みの検索設定を必ずしも正確に反映するとは限りません。

テンプレートから生成したレポートには、表紙、ヘッダーとフッター、ページ番号など、すべてのセクションにまたがって機能を制御する複数のドキュメント属性があります。

CSVをドキュメントの形式として選択した場合は、ドキュメントの属性を設定できないことに注意してください。

既存のテンプレートの中に適切なモデルがあれば、そのテンプレートをコピーして属性を編集することで、新しいレポートテンプレートを作成できます。また、Cisco から一連の定義済みレポートテンプレートも提供されています。これらのテンプレートは、[レポート (Reports)] タブのテンプレートの一覧で確認できます。

イベントビューからレポートテンプレートを作成し、必要に応じて変更することができます。セクションを追加したり、自動的に組み込まれるセクションを変更したり、セクションを削除したりできます。

ダッシュボード、ワークフロー、統計の要約をインポートして、新しいレポートをすばやく作成できます。インポートすると、ダッシュボードのウィジェットグラフィックごと、およびワークフローのイベントビューごとにセクションが作成されます。最も重要な情報に焦点が当たるように不要なセクションを削除できます。

### カスタムレポートテンプレートの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

#### 手順

- ステップ 1 [概要 (Overview)] > [レポート (Reporting)] を選択します。
- ステップ 2 [レポートテンプレート (Report Templates)] タブをクリックします。
- ステップ 3 [レポートテンプレートの作成 (Create Report Template)] をクリックします。
- ステップ 4 必要に応じて、[レポートタイトル (Report Title)] フィールドに新しいテンプレートの名前を入力し、[保存 (Save)] をクリックします。
- ステップ 5 レポートタイトルに入力パラメータを追加するには、タイトル内でパラメータ値を表示する位置にカーソルを置き、入力パラメータの挿入アイコン (📌) をクリックします。
- ステップ 6 必要に応じて、[レポートセクション (Report Sections)] タイトルバーの下にある追加アイコンのセットを使用し、セクションを挿入します。
- ステップ 7 [保存 (Save)] をクリックします。
- ステップ 8 [レポートテンプレートの設定 \(2315 ページ\)](#) の説明に従ってセクションコンテンツを設定します。

ヒント セクションのウィンドウの下部にある [プレビュー (Preview)] をクリックして、選択したカラムのレイアウトやグラフィックの形式を表示できます。

ステップ9 [詳細 (Advanced) ] をクリックし、[レポートテンプレート内のドキュメント属性 \(2326 ページ\)](#) の説明に従って PDF および HTML レポートの属性を設定します。


#### 既存のテンプレートからのレポートテンプレートの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

#### 手順

ステップ1 [概要 (Overview) ] > [レポート (Reporting) ] を選択します。

ステップ2 [レポートテンプレート (Report Templates) ] タブをクリックします。

ステップ3 コピーするレポートテンプレートの横にあるコピーアイコン () をクリックします。

ステップ4 [レポートタイトル (Report Title) ] フィールドに、名前を入力します。

ステップ5 [保存 (Save) ] をクリックします。

ステップ6 必要に応じてテンプレートを変更します。

#### イベントビューからのレポートテンプレートの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

#### 手順

ステップ1 レポートに含めるイベントをイベントビューに入力します。

- イベント検索設定を使用して、表示するイベントを定義します。
- イベントビューに該当するイベントが表示されるまでワークフローをドリルダウンします。

ステップ2 イベントビューのページから、[レポートデザイナー (Report Designer) ] をクリックします。

[レポートセクション (Report Sections) ] ページが表示され、キャプチャされるワークフロー内のビューごとにセクションが示されます。

**ステップ3** オプションで、[レポート タイトル (Report Title) ] フィールドに新しい名前を入力し、[保存 (Save) ] をクリックします。

**ステップ4** 次の操作を実行できます。

- 表紙、目次、開始ページ番号、またはヘッダーおよびフッター テキストを追加します： [詳細設定 (Advanced Settings) ] をクリックします。
- 改ページを追加します： 改ページの追加アイコン (📄) をクリックし、新しい改ページオブジェクトを、テンプレートの下部から新しいページを開始するセクションの先頭にドラッグします。
- テキスト セクションを追加します： テキスト セクションの追加アイコン (📄) をクリックし、新しいテキスト セクションを、テンプレートの下部からレポート テンプレート内で表示する位置にドラッグします。
- セクションのタイトルを変更します： タイトルバーでセクションタイトルをクリックし、セクション タイトルを入力して、[OK] をクリックします。
- レポート セクションを設定します。各セクションのフィールド設定を調整します。

**ヒント** セクションの現在のカラムのレイアウトやグラフの形式を表示する場合は、そのセクションの [プレビュー (Preview) ] リンクをクリックします。

- レポートからテンプレート セクションを除外します： セクションのタイトルバーで削除アイコン (✖) をクリックし、削除を確認します。

(注) 一部のワークフロー内の最後のレポート セクションには詳細ビューが含まれ、ワークフローに応じてパケット、ホストプロファイル、または脆弱性が示されません。レポートの生成時に、これらの詳細ビューがあるイベントを多数取得すると、Firepower Management Center のパフォーマンスに影響を与えることがあります。

**ステップ5** [保存 (Save) ] をクリックします。

### ダッシュボードまたはワークフローのインポートによるレポート テンプレートの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

#### 手順

**ステップ1** レポート内で複製するダッシュボード、ワークフロー、または要約を識別します。

**ステップ2** [概要 (Overview) ] > [レポート (Reporting) ] を選択します。

**ステップ3** [レポート テンプレート (Report Templates) ] タブをクリックします。

## [インポートレポートセクション (Import Report Sections)] のデータソースオプション

- ステップ 4** [レポートテンプレートの作成 (Create Report Template)] をクリックします。
- ステップ 5** [レポートタイトル (Report Title)] フィールドに新しいレポートテンプレートの名前を入力します。
- ステップ 6** [保存 (Save)] をクリックします。
- ステップ 7** インポートセクションアイコン (🌐) をクリックします。[インポートレポートセクション (Import Report Sections)] のデータソースオプション (2314 ページ) で説明されているデータソースのいずれかを選択できます。
- ステップ 8** ドロップダウンメニューからダッシュボード、ワークフロー、または要約を選択します。
- ステップ 9** 追加するデータソースの、[インポート (Import)] をクリックします。
- ダッシュボードの場合、ウィジェットグラフィックごとに独自のセクションがあります。ワークフローの場合、イベントビューごとに独自のセクションがあります。
- ステップ 10** 必要に応じてセクションの内容を変更します。
- (注) 一部のワークフロー内の最後のレポートセクションには詳細ビューが含まれ、ワークフローに応じてパケット、ホストプロファイル、または脆弱性が示されます。レポートの生成時に、これらの詳細ビューがあるイベントを多数取得すると、Firepower Management Center のパフォーマンスに影響を与えることがあります。
- ステップ 11** [保存 (Save)] をクリックします。

## [インポートレポートセクション (Import Report Sections)] のデータソースオプション

表 242: [インポートレポートセクション (Import Report Sections)] ウィンドウのデータソースオプション

選択オプション	インポート対象
ダッシュボードのインポート (Import Dashboard)	選択したダッシュボード上のカスタム分析ウィジェット。
ワークフローのインポート (Import Workflow)	定義済みのワークフローまたはカスタムワークフロー。 選択項目の形式は次のようになっています。 Table - Workflow name たとえば、Connection Events - Traffic by Port は、Connection Events テーブルから生成された Traffic by Port ワークフロー内のビューをインポートします。



選択オプション	インポート対象
インポート要約セクション (Import Summary Sections)	次の一般的な要約： <ul style="list-style-type: none"> <li>• 侵入の詳細サマリー (Intrusion Detailed Summary)</li> <li>• 侵入の概要サマリー (Intrusion Short Summary)</li> <li>• ディスカバリの詳細サマリー (Discovery Detailed Summary)</li> <li>• ディスカバリの概要サマリー (Discovery Short Summary)</li> </ul>

## レポート テンプレートの設定

レポートテンプレートを作成すれば、そのテンプレートを変更およびカスタマイズできます。さまざまなレポートセクションの属性を変更して、セクションとそのデータ表示の内容を調整できます。

レポートテンプレート内の各セクションでは、データベース テーブルを照会して、そのセクションの内容を生成します。セクションのデータ形式を変更する際にも同じデータクエリーが使用されますが、形式のタイプごとの分析の目的に従って、セクションに表示されるフィールドが変わります。たとえば、侵入イベントの表形式の表示では、イベントレコードごとに多数のデータフィールドがセクションに入力され、円グラフのセクションでは、選択した各属性が表すすべての一致レコードの割合が示され、個々のイベントに関する詳細情報は表示されません。棒グラフのセクションでは、特定の属性を持つ一致レコードの合計数が比較されます。折れ線グラフでは、1つの属性に関係する一致レコード数の変化が時系列で要約されます。折れ線グラフは時間ベースのデータの場合のみ使用でき、ホスト、ユーザ、サードパーティの脆弱性などに関する情報の場合は使用できません。

レポートセクションの検索設定やフィルタは、セクションの内容のベースになるデータベースクエリーを指定します。ほとんどのテーブルの場合、定義済み検索設定か保存済み検索設定を使用してレポートを制約するか、新しい検索設定を即座に作成することができます。

- 定義済み検索設定は特定のイベントテーブルの検索サンプルの役割を果たし、レポートに含めようとしている、ネットワークに関する重要情報にクイック アクセスできます。
- 保存済みイベント検索設定には、自分や他のユーザが作成したすべてのパブリック イベント検索設定と、自分で保存したすべてのプライベート イベント検索設定が含まれます。
- 現在のレポートテンプレートの保存済み検索設定は、そのレポートテンプレート自体に限りアクセスできます。保存済みレポートテンプレートの検索設定の名前は、末尾が文字列「Custom Search」になります。ユーザは、レポートの設計時にこれらの検索設定を作成します。

[アプリケーションの統計 (Application Statistics)] テーブルにユーザ定義のアプリケーションフィルタを使用して、レポートに制約を適用します。

セクション内にテーブルのデータを組み込む場合、データレコード内のどのフィールドを表示するか選択できます。テーブル内のすべてのフィールドを包含対象または除外対象にできます。レポートの目的を達成するのに必要なフィールドを選択し、それによって配列したりソートしたりします。

テンプレートにテキストセクションを追加して、レポート全体や個々のセクションに概要などのカスタム テキストを用意することができます。

テンプレート内のどのセクションの前後にも改ページを追加できます。この機能は、複数のセクションから成るレポートで、各種セクションの概要を示すテキストページがある場合に特に便利です。

レポートテンプレートの時間枠によって、テンプレートのレポート作成期間が定義されます。



- (注) セキュリティ アナリストは、自分が作成したレポート テンプレートだけを編集できます。マルチドメイン導入では、先祖ドメインのレポートテンプレートは編集できませんが、レポートテンプレートをコピーして子孫バージョンを作成することができます。

## レポート テンプレート セクションのテーブルとデータ形式の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

### 手順

- ステップ 1** [レポート テンプレート (Rreport Template)] セクションで、[テーブル (Table)] ドロップダウンメニューを使用して、問い合わせるテーブルを選択します。
- 選択したテーブルで使用できる出力形式ごとに、アイコンが[形式 (Format)] フィールドに表示されます。
- ステップ 2** セクションに該当する出力形式のアイコンを選択します。
- ステップ 3** 検索制約を変更するには、[検索 (Search)] フィールドか[ファイルタ (Filter)] フィールドの横にある編集アイコン (✎) クリックします。
- ステップ 4** グラフ出力形式 (円グラフや棒グラフなど) の場合、ドロップダウンメニューを使用して、[X 軸 (X-Axis)] と [Y 軸 (Y-Axis)] のパラメータを調整します。
- X 軸の値を選択すると、互換性のある値だけが Y 軸のドロップダウンメニューに表示されます。その逆も同様です。
- ステップ 5** テーブル出力の場合、出力内のカラム、表示順序、ソート順序を選択します。

**ステップ 6** [保存 (Save) ] をクリックします。

**関連トピック**

[レポート テンプレート フィールド \(2308 ページ\)](#)

レポート テンプレート セクションの検索またはフィルタの指定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

**手順**

**ステップ 1** [レポート テンプレート (Rreport Template) ] セクションで、[テーブル (Table) ] ドロップダウンメニューからクエリを行うデータベース テーブルを選択します。

- ほとんどのテーブルでは、[検索 (Search) ] ドロップダウン リストが表示されます。
- [アプリケーション統計 (Application Statistics) ] テーブルでは、[フィルタ (Filter) ] ドロップダウン リストが表示されます。

**ステップ 2** レポートの制約に使用する検索かフィルタを選択します。

編集アイコン (✎) をクリックして、検索条件を表示したり、新しい検索を作成したりできます。

**関連トピック**

[アプリケーションフィルタ \(439 ページ\)](#)

表形式のセクションに表示される検索フィールドの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

**手順**

**ステップ 1** 表形式のレポート セクションで、[フィールド (Fields) ] パラメータの横にある編集アイコン (✎) をクリックします。

**ステップ 2** セクションを変更する場合、フィールドを追加/削除し、望むカラムの順番にそれらのフィールドアイコンをドラッグします。

**ステップ3** どの列でもソート順序を変更する場合、各フィールドアイコンのドロップダウンリストを使用して、ソート順序および優先順位を設定する必要があります。

**ステップ4** [OK] をクリックします。

## レポート テンプレートへのテキスト セクションの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

テキスト セクションには、複数のフォント サイズやフォント スタイル (太字や斜体など) を使用できるリッチ テキスト、入力パラメータ、インポート済みイメージを使用できます。



**ヒント** テキスト セクションは、レポートやそのセクションの概要説明に役立ちます。

### 手順

**ステップ1** レポート テンプレート エディタで、テキスト セクション追加アイコン (📄) をクリックします。

**ステップ2** 新しいテキスト セクションを、レポート テンプレート内のご希望の位置にドラッグします。

**ステップ3** テキスト セクションをページの最初または最後に移動するには、テキスト セクションの前または後に改ページを挿入します。

**ステップ4** テキスト セクションの総称名を変更するには、タイトルバーのセクション名をクリックし、新しい名前を入力します。

**ステップ5** テキスト セクションの本文に形式設定済みのテキストやイメージを追加します。

レポートの生成時に動的に更新する入力パラメータを組み込むことができます。

**ステップ6** [保存 (Save) ] をクリックします。


### 関連トピック

[入力パラメータ](#) (2322 ページ)

## レポート テンプレートへの改ページの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

## 手順

- ステップ 1** レポート テンプレート エディタで、改ページアイコン (  ) をクリックします。  
改ページがテンプレートの下部に表示されます。
- ステップ 2** 改ページを、セクションの前後のご希望の場所にドラッグします。
- ステップ 3** [保存 (Save) ] をクリックします。

## グローバル時間枠とレポート テンプレート セクション

時間ベースのデータ (侵入イベントや検出イベントなど) があるレポート テンプレートにはグローバル時間枠があります。この時間枠は、テンプレート内の時間ベースのセクションでデフォルトで作成時に継承されます。グローバル時間枠を変更すると、グローバル時間枠を継承するように設定されているセクションのローカル時間枠が変更されます。[時間枠の継承 (Inherit Time Window) ] チェックボックスをクリアすると、個々のセクションの時間枠の継承を無効にできます。それから、ローカル時間枠を編集できます。



- (注) グローバル時間枠の継承は、侵入イベントや検出イベントなど、時間ベースのテーブルからのデータがあるレポート セクションだけに適用されます。ネットワーク アセット (ホストやデバイス) と関連情報 (脆弱性など) を報告するセクションの場合、各時間枠を個別に設定する必要があります。


## レポート テンプレートとそのセクションのグローバル時間枠の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst



- ヒント** レポート内のセクションごとに別の時間枠を使用できます。たとえば、最初のセクションを月の要約にして、残りのセクションで週レベルの詳細情報へドリルダウンするようにできます。この場合、セクション レベルの時間枠を個別に設定します。

## 手順

- ステップ 1** レポート テンプレート エディタで [生成 (Generate) ] をクリックします。
- ステップ 2** グローバル時間枠を変更するには、時間枠のアイコン (  ) をクリックします。
- ステップ 3** [イベント時間枠 (Events Time Window) ] タブで時間設定を変更します。

## レポート テンプレート セクションのローカル時間枠の設定

**ステップ 4** [適用 (Apply)] をクリックします。

**ステップ 5** [生成 (Generate)] をクリックしてレポートを生成し、[はい (Yes)] をクリックして確認します。

## レポート テンプレート セクションのローカル時間枠の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

## 手順

**ステップ 1** テンプレートの [レポート セクション (Report Sections)] ページで、セクションの [時間枠の継承 (Inherit Time Window)] チェック ボックスが存在する場合はクリアします。

**ステップ 2** セクションのローカル時間枠を変更するには、時間枠のアイコン (🕒) をクリックします。

(注) 統計テーブルからのデータがあるセクションでは、スライド式の時間枠のみ使用できます。

**ステップ 3** [イベント時間枠 (Events Time Window)] で [適用 (Apply)] をクリックします。

**ステップ 4** [保存 (Save)] をクリックします。

## レポート テンプレート セクションの名前変更

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

## 手順

**ステップ 1** レポート テンプレート エディタで、セクション ヘッダーの現在のセクション名をクリックします。

**ステップ 2** 新しいセクション名を入力します。

**ステップ 3** [OK] をクリックします。

## レポートテンプレートセクションのプレビュー

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

プレビュー機能は、表形式の表示のフィールドのレイアウトとソート順序や、円グラフの色などのグラフの読みやすさに関する重要な特性を表示します。

## 手順

- 
- ステップ1** レポートテンプレートセクションの編集中は、いつでも、そのセクションの [プレビュー (Preview) ] をクリックできます。
- ステップ2** プレビューを閉じるには、[OK] をクリックします。
- 

## レポートテンプレートセクションでの検索

レポートが正常に作成されるかどうかは、レポートのセクションへの入力内容を決める検索設定の定義が重要な要素になります。Firepower システムには検索エディタが備わっており、レポートテンプレートで使用できる検索設定を表示したり、新しいカスタム検索設定を定義したりできます。

## レポートテンプレートのセクションの検索

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

## 手順

- 
- ステップ1** レポートテンプレート内の関連するセクションから、[検索 (Search) ] フィールドの横にある編集アイコン (✎) をクリックします。
- ステップ2** 事前定義済みの検索に基づいてカスタム検索を作成する場合は、[保存済み検索 (Saved Searches) ] ドロップダウンリストから事前定義された検索を選択する必要があります。
- このリストには、このテーブルに対して使用可能な事前定義済みの検索設定がすべて表示されます。システム規模の事前定義済み検索設定とレポート固有の事前定義済み検索設定も含まれています。
- ステップ3** 該当するフィールドで検索条件を編集します。

特定のフィールドでは、制約にイベント検索設定と同じ演算子 (<や<>など) を含めることができます。複数の条件を入力すると、すべての基準を満たすレコードだけが検索で返されます。

**ステップ 4** 制約値を入力する代わりに、ドロップダウンメニューから入力パラメータを挿入する場合は、入力パラメータ アイコン (🌐) をクリックする必要があります。

(注) レポートの検索設定の制約を編集すると、システムにより *section custom search* という名前で編集済みの検索設定が保存されます。*section* は、セクションのタイトルバーに示される文字列 *custom search* の前の名前の部分です。保存するカスタム検索設定の名前をわかりやすくするには、セクション名を変更した後で編集済みの検索設定を保存するようにしてください。保存したレポートの検索設定の名前は変更できません。

**ステップ 5** [OK] をクリックします。

## 入力パラメータ

レポートの生成時に動的に更新できる入力パラメータをレポートテンプレート内で使用できます。入力パラメータのアイコン (🌐) は、入力パラメータを処理できるフィールドを示します。次の 2 種類の入力パラメータがあります。

- 定義済みの入力パラメータは、内部システム関数か設定情報によって解決されます。たとえば、レポートの生成時に、システムにより  $\$<Time>$  パラメータは現在の日時に置き換えられます。
- ユーザ定義の入力パラメータは、セクション検索で制約を行えます。入力パラメータを使用して検索設定を制約すると、レポートの生成時に要求者から値を収集するようにシステムに指示できます。この方法で、テンプレートを変更せずに、レポートを生成時に動的に調整して特定のデータのサブセットを表示できます。たとえば、レポートセクションの検索設定の [接続先 IP (Destination IP)] フィールドに入力パラメータを指定できます。指定後、レポートの生成時に、特定の部門の IP ネットワークのセグメントを入力して、その部門のデータだけを取得できます。

文字列タイプの入力パラメータを定義して、電子メール (件名または本文)、レポートファイル名、テキストセクションなどのレポートの特定のフィールドに動的テキストを追加することもできます。すべて同じテンプレートを利用し、カスタマイズしたレポートファイル名、電子メールアドレス、電子メール メッセージを使用して、さまざまな部門用にレポートをパーソナライズできます。

### 定義済み入力パラメータ

表 243: 定義済み入力パラメータ

このパラメータを入力すると、	テンプレートに次の情報が含まれます :
$\$<Logo>$	選択した更新ロゴ



このパラメータを入力すると、	テンプレートに次の情報が含まれます：
\$<Report Title>	レポート タイトル
\$<Time>	レポートを実行する日付、時刻、粒度 1 秒
\$<Month>	現在の月
\$<Year>	現在の西暦
\$<System Name>	Firepower Management Center 名
\$<Model Number>	Firepower Management Center のモデル番号
\$<Time Window>	レポート セクションに現在適用されている時間窓
\$<Constraints>	レポート セクションに現在適用されている検索制約

表 244: 定義済み入力パラメータの使用法

パラメータ	レポートテンプレート カバー ページ	レポートテンプレート レポート タイトル	レポートテンプレート セクションの説明	レポートテンプレート 本文セクション	レポート ファイル名の作成	レポート 電子メールの主題、本文の作成
\$<Logo>	Yes	No	No	No	No	No
\$<Report Title>	Yes	No	Yes	Yes	Yes	Yes
\$<Time>	Yes	Yes	Yes	Yes	Yes	Yes
\$<Month>	Yes	Yes	Yes	Yes	Yes	Yes
\$<Year>	Yes	Yes	Yes	Yes	Yes	Yes
\$<System Name>	Yes	Yes	Yes	Yes	Yes	Yes
\$<Model Number>	Yes	Yes	Yes	Yes	Yes	Yes
\$<Time Window>	No	No	Yes	No	No	No
\$<Constraints>	No	No	Yes	No	No	No

ユーザ定義の入力パラメータ

入力パラメータを使用して、検索設定の実用性を向上させます。入力パラメータにより、レポートの生成時に要求者から値を収集するようにシステムに指示できます。この方法で、検索設定を変更せずに、レポートを生成時に動的に制約して特定のデータのサブセットを表示できます。たとえば、レポートセクションの[宛先 IP (Destination IP)] フィールドに入力パラメータを指定して、部門レベルでセキュリティ イベントをドリルダウンできます。レポートの生成時に、特定の部門の IP ネットワークのセグメントを入力して、その部門のデータだけを取得できます。

入力パラメータのタイプにより、そのパラメータを使用できる検索フィールドが決まります。特定のタイプは、該当するフィールドでのみ使用できます。たとえば、ユーザパラメータを文字列タイプとして定義すると、テキストフィールド内への挿入には使用できますが、IP アドレスを使用するフィールドでは使用できません。

定義する入力パラメータごとに名前とタイプがあります。

表 245: ユーザ定義の入力パラメータのタイプ

パラメータのタイプ	使用先のフィールド内のデータ
ネットワーク/IP (Network/IP)	CIDR 形式の IP アドレスまたはネットワーク セグメント
Application	アプリケーションプロトコル、クライアントアプリケーション、または Web アプリケーションの名前
イベント メッセージ (Event Message)	イベント ビュー メッセージ
Device	Management Center または管理対象デバイス
[ユーザ名 (Username) ]	イニシエータ ユーザやレスポнда ユーザなどのユーザ ID
番号 (VLAN ID、Snort ID、Vuln ID) (Number (VLAN ID, Snort ID, Vuln ID))	VLAN ID、Snort ID、または脆弱性 ID
文字列	アプリケーションや OS のバージョン、注記、説明などのテキストフィールド

#### ユーザ定義の入力パラメータの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

#### 手順

- ステップ 1 レポート テンプレート エディタで、[詳細 (Advanced) ] をクリックします。
- ステップ 2 入力パラメータ追加アイコン (🔧) をクリックします。
- ステップ 3 パラメータの [名前 (Name) ] を入力します。
- ステップ 4 [タイプ (Type) ] ドロップダウン リストから値を選択します。
- ステップ 5 [OK] をクリックしてパラメータを追加します。
- ステップ 6 [OK] をクリックしてエディタに戻ります。

## ユーザ定義の入力パラメータの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

レポートテンプレートの[入力パラメータ (Input Parameters)] セクションに、テンプレートに使用可能なユーザ定義パラメータがすべてリストされます。

## 手順

- ステップ1 レポートテンプレート エディタで、[詳細設定 (Advanced)] をクリックします。
- ステップ2 変更するパラメータの横にある編集アイコン (✎) をクリックします。
- ステップ3 [名前 (Name)] に新しい名前を入力します。
- ステップ4 [タイプ (Type)] ドロップダウンリストを使用して、パラメータ タイプを変更します。
- ステップ5 [OK] をクリックして変更を保存します。
- ステップ6 入力パラメータを削除するには、入力パラメータの横にある削除アイコン (🗑) をクリックし、確認します。
- ステップ7 [OK] をクリックしてレポートテンプレート エディタに戻ります。

## ユーザ定義の入力パラメータによる検索の制約

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

定義した入力パラメータは、そのパラメータのタイプと一致する検索フィールドでのみ使用できます。たとえば、**ネットワーク/IP** タイプのパラメータは、CIDR 形式の IP アドレスまたはネットワーク セグメントを受け入れるフィールドだけで使用できます。

## 手順

- ステップ1 レポートテンプレート エディタで、セクション内の [検索 (Search)] フィールドの横にある編集アイコン (✎) をクリックします。
- 入力パラメータを使用できるフィールドは、入力パラメータのアイコン (🟢) のマークが付けられます。

## レポート テンプレート内のドキュメント属性

**ステップ 2** フィールドの横にある入力パラメータのアイコン (🟢) をクリックして、ドロップダウンメニューから入力パラメータを選択します。

ユーザ定義の入力パラメータは、アイコン (🔒) のマークが付けられます。

**ステップ 3** [OK] をクリックします。

## レポート テンプレート内のドキュメント属性

レポートを生成する前に、レポートの外観に影響を与えるドキュメント属性を設定できます。これらの属性には、オプションの表紙と目次が含まれます。一部の属性のサポートは、レポートの形式に PDF、HTML、CSV のいずれを選択したかによって異なります。

表 246: ドキュメント属性のサポート

属性 (Attribute)	PDF のサポート	HTML のサポート	CSV のサポート
表紙	可能、オプションでロゴと外観のカスタマイズ	可能、オプションでロゴと外観のカスタマイズ	No
目次	Yes	Yes	No
ページのヘッダーとフッター	可能、オプションでフィールド内にテキストかロゴ	No	No
カスタムの開始ページ番号	Yes	No	No
先頭ページに番号を付けないオプション	Yes	No	No

## レポート テンプレート内のドキュメント属性の編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

## 手順

**ステップ 1** レポート テンプレート エディタで、[詳細 (Advanced)] をクリックします。

**ステップ 2** 次の選択肢があります。

- 表紙の追加: 表紙を追加するには、[表紙を含める (Include Cover Page)] チェックボックスをオンにします。

- 表示のカスタマイズ：表紙のデザインを編集するには、[表紙のカスタマイズ \(2327ページ\)](#) を参照してください。
- 目次の追加：目次を追加するには、[目次を含める (Include Table of Contents)] チェックボックスをオンにします。
- ロゴの管理：テンプレートに関連付けられたロゴイメージを管理するには、[レポートテンプレートのロゴの管理 \(2327ページ\)](#) を参照してください。
- ヘッダーとフッターの設定：テンプレートのヘッダーとフッターの要素を指定するには、[ヘッダー (Header)] フィールドと [フッター (Footer)] フィールドのドロップダウンリストを使用します。
- 最初のページ番号の設定：レポートの最初のページ番号を指定するには、[ページ番号の開始 (Page Number Start)] の値を入力します。
- 最初のページ番号の表示：レポートの最初のページのページ番号を表示するには、[最初のページに番号を付けますか (Number First Page?)] チェックボックスをオンにします。このオプションを選択すると、表紙には番号が付けられません。

**ステップ 3** [OK] をクリックして変更を保存します。

## 表紙のカスタマイズ

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

レポートテンプレートの表紙をカスタマイズできます。表紙には、複数のフォントサイズやフォントスタイル（太字や斜体など）を使用できるリッチテキスト、入力パラメータ、インポート済みイメージを使用できます。

### 手順

**ステップ 1** レポートテンプレートエディタで、[詳細 (Advanced)] をクリックします。

**ステップ 2** [表紙のデザイン (Cover Page Design)] の横にある編集アイコン (✎) をクリックします。

**ステップ 3** リッチテキストエディタで表紙のデザインを編集します。

**ステップ 4** [OK] をクリックします。

## レポートテンプレートのロゴの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

Firepower Management Center で複数のロゴを保存し、さまざまなレポートテンプレートに関連付けることができます。ロゴの関連付けは、テンプレートを設計する際に設定します。テンプレートをエクスポートすると、エクスポートパッケージにロゴが含まれます。

Firepower Management Center にロゴをアップロードすると、そのロゴは次のものに使用できません。

- Firepower Management Center のすべてのレポートテンプレート、または
- マルチドメイン展開では、現在のドメイン内のすべてのレポートテンプレート

ロゴ画像は、PNG 形式、JPG 形式、または GIF 形式することができます。

レポート内のロゴは、Firepower Management Center にアップロードされているいずれかの JPG 画像に変更できます。たとえば、テンプレートを再使用する場合は、別の組織のロゴをレポートに関連付けることができます。

アップロードしたロゴは、削除できます。ロゴを削除すると、そのロゴが使用されているすべてのテンプレートから削除されます。削除を取り消すことはできません。事前定義済みのシスコロゴは削除できない点に注意してください。

## 手順

**ステップ 1** レポートテンプレートエディタで、[詳細 (Advanced)] をクリックします。

テンプレートに現在関連付けられているロゴは、[一般設定 (General Settings)] の [ロゴ (Logo)] の下に表示されます。

**ステップ 2** ロゴの横にある編集アイコン (✎) をクリックします。

**ステップ 3** 次の選択肢があります。

- 追加：新しいロゴを追加します。詳細については、[新しいロゴの追加 \(2328 ページ\)](#) を参照してください。
- 変更：レポートテンプレートのロゴを変更します。詳細については、[レポートテンプレートのロゴの変更 \(2329 ページ\)](#) を参照してください。
- 削除：ロゴを削除します。詳細については、[ロゴの削除 \(2329 ページ\)](#) を参照してください。

## 新しいロゴの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

手順

- ステップ1 レポートテンプレートエディタで、[詳細 (Advanced)] をクリックします。
- ステップ2 [ロゴ (Logo)] フィールドの横にある編集アイコン (✎) をクリックします。
- ステップ3 [ロゴのアップロード (Upload Logo)] をクリックします。
- ステップ4 [参照 (Browse)] ボタンをクリックし、ファイルの場所を参照し、[開く (Open)] をクリックします。
- ステップ5 [アップロード (Upload)] をクリックします。
- ステップ6 新しいロゴを現在のテンプレートに関連付けるには、それを選択し、[OK] をクリックします。

レポートテンプレートのロゴの変更

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

手順

- ステップ1 レポートテンプレートエディタで、[詳細 (Advanced)] をクリックします。
- ステップ2 [ロゴ (Logo)] フィールドの横にある編集アイコン (✎) をクリックします。
- ステップ3 [ロゴの選択 (Select Logo)] ダイアログで、レポートテンプレートに関連付けるロゴを選択します。
- ステップ4 [OK] をクリックします。

ロゴの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

手順

- ステップ1 レポートテンプレートエディタで、[詳細 (Advanced)] をクリックします。
- ステップ2 [ロゴ (Logo)] フィールドの横にある編集アイコン (✎) をクリックします。

ステップ3 [ロゴの選択 (Select Logo)] ダイアログで、削除するロゴを選択します。

ステップ4 [ロゴの削除 (Delete Logo)] をクリックします。

ステップ5 [OK] をクリックします。

## レポート テンプレートの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

マルチドメイン展開では、現在のドメインで作成されたレポート テンプレートが表示されます。このテンプレートは編集可能です。先祖ドメインで作成されたレポート テンプレートも表示されますが、これは編集できません。下位のドメインのレポート テンプレートを表示および編集するには、そのドメインに切り替えます。システムによって表示されるレポートは、現在のドメインで作成されたもののみです。

### 手順

ステップ1 [概要 (Overview)] > [レポート (Reporting)] を選択します。

ステップ2 [レポート テンプレート (Report Templates)] タブをクリックします。

ステップ3 次の選択肢があります。

- 削除：削除するテンプレートの横にある削除アイコン (🗑️) をクリックして確認します。  
システム付属のレポート テンプレートは削除できません。セキュリティアナリストは、自分が作成したレポート テンプレートのみを削除できます。マルチドメイン展開では、現在のドメインに属しているレポート テンプレートのみを削除できます。
- 編集：レポート テンプレートを編集する場合は、[レポート テンプレートの編集 \(2331 ページ\)](#) を参照してください。
- エクスポート：レポート テンプレートをエクスポートする場合は、[レポート テンプレートのエクスポート \(2332 ページ\)](#) を参照してください。  
  
ヒント また、標準設定のエクスポート プロセスを使用してレポート テンプレートをエクスポートすることもできます。[設定のエクスポート \(214 ページ\)](#) を参照してください。
- インポート：レポート テンプレートをインポートする場合は、[設定のインポート \(214 ページ\)](#) を参照してください。



## レポートテンプレートの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成されたレポートテンプレートが表示されます。このテンプレートは編集可能です。先祖ドメインで作成されたレポートテンプレートも表示されますが、これは編集できません。下位のドメインのレポートテンプレートを表示および編集するには、そのドメインに切り替えます。

## 手順

**ステップ 1** [概要 (Overview)] > [レポート (Reporting)] を選択します。

**ステップ 2** [レポートテンプレート (Report Templates)] タブをクリックします。

**ステップ 3** 編集するテンプレートの編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 4** 次の選択肢があります。

- 改ページを追加します。 [レポートテンプレートへの改ページの追加 \(2318 ページ\)](#) を参照してください。
- テキスト セクションを追加します。 [レポートテンプレートへのテキストセクションの追加 \(2318 ページ\)](#) を参照してください。
- [レポートテンプレートの設定 \(2315 ページ\)](#) の説明に従ってセクションコンテンツを設定します。
- 入力パラメータを作成します。 [ユーザ定義の入力パラメータの作成 \(2324 ページ\)](#) を参照してください。
- 入力パラメータを編集します。 [ユーザ定義の入力パラメータの編集 \(2325 ページ\)](#) を参照してください。
- ドキュメントの属性を編集します。 [レポートテンプレート内のドキュメント属性の編集 \(2326 ページ\)](#) を参照してください。
- テンプレートセクションを検索します。 [レポートテンプレートのセクションの検索 \(2321 ページ\)](#) を参照してください。
- [詳細設定 (Advanced)] をクリックし、 [レポートテンプレート内のドキュメント属性 \(2326 ページ\)](#) の説明に従ってドキュメント属性を設定します。
- グローバル時間枠を設定します。 [レポートテンプレートとそのセクションのグローバル時間枠の設定 \(2319 ページ\)](#) を参照してください。
- ローカル時間枠を設定します。 [レポートテンプレートセクションのローカル時間枠の設定 \(2320 ページ\)](#) を参照してください。

- 検索フィールドを設定します。表形式のセクションに表示される検索フィールドの設定（2317 ページ）を参照してください。
- 表とデータ形式を設定します。レポート テンプレート セクションのテーブルとデータ形式の設定（2316 ページ）を参照してください。
- 検索とフィルタを指定します。レポート テンプレート セクションの検索またはフィルタの指定（2317 ページ）を参照してください。

## レポート テンプレートのエクスポート

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

### 手順

- ステップ 1 [概要 (Overview)] > [レポート (Reporting)] を選択します。
- ステップ 2 [レポート テンプレート (Report Templates)] タブを選択します。
- ステップ 3 エクスポートするテンプレートのエクスポートアイコン (📄) をクリックします。
- ステップ 4 [ファイルの保存 (Save file)] と [OK] をクリックして、ローカル コンピュータにファイルを保存します。

## レポートの生成について

### レポートの生成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

レポート テンプレートを作成してカスタマイズすると、レポート生成の準備は完了です。生成プロセスでは、レポートの形式 (HTML、PDF、または CSV) を選択できます。レポートのグローバル時間枠を調整することもできます。この時間枠は、免除していないすべてのセクションに一貫した時間枠を適用します。

PDF レポートの場合：

- Unicode (UTF-8) 文字を使用したファイル名はサポートされません。

- 特殊な Unicode ファイル名が含まれるレポートセクション（ファイルイベントやマルウェア イベントで表示されるセクションなど）では、そのファイル名は書き直された形式で表示されます。

レポートテンプレートの検索の指定にユーザ入力パラメータが含まれている場合、生成プロセスで値を入力するよう求められ、このレポートの実行内容がデータのサブセットに合わせて調整されます。

DNS サーバの設定および IP アドレス解決が有効化されている場合、正常に解決されたホスト名がレポートに取り込まれます。

マルチドメイン展開では、先祖ドメインでレポートを生成すると、そのレポートにはすべての子孫ドメインからの結果を含めることができます。特定のリーフドメインのレポートを生成するには、そのドメインに切り替えます。

## 手順

- 
- ステップ 1** [概要 (Overview)] > [レポート (Reporting)] を選択します。
- ステップ 2** [レポート テンプレート (Report Templates)] タブをクリックします。
- ステップ 3** レポートの生成に使用するテンプレートの横にあるレポートアイコン (📄) をクリックします。
- コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ヒント** 先祖のテンプレートからレポートを生成するには、そのテンプレートを現在のドメインにコピーします。
- ステップ 4** 必要に応じて、レポート名を設定します。
- 新しい [ファイル名 (File Name)] を入力します。新しい名前を入力しないと、システムはレポートテンプレートで指定した名前を使用します。
  - 入力パラメータのアイコン (⊕) を使用して、1つ以上の入力パラメータをファイル名に追加します。
- ステップ 5** 対応するアイコン (HTML、PDF、または CSV) をクリックして、レポートの出力形式を選択します。
- ステップ 6** グローバル時間枠を変更する場合は、時間枠のアイコン (🕒) をクリックします。
- (注) グローバル時間枠の設定は、個々のレポートセクションのうちグローバル設定を継承するように設定されているものの内容だけに影響します。
- ステップ 7** [入力パラメータ (Input Parameters)] セクションに表示されるフィールドの値を入力します。
- ヒント** フィールドにワイルドカード文字 \* を入力すると、ユーザパラメータを無視できます。こうすると、検索設定がユーザパラメータで制約されなくなります。

(注) システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、リテラルのIPアドレスまたはVLANタグを使用してレポート結果を制約すると、予期しない結果になる可能性があります。

**ステップ 8** 電子メールリレーホストを Firepower Management Center 構成で有効化した場合は、[電子メール (Email)] をクリックして、レポートの生成時にレポートが自動的に電子メール配信されるようにします。

**ステップ 9** プロンプトが表示されたら、[OK][生成 (Generate)] をクリックして確認します。

**ステップ 10** 次の選択肢があります。

- レポートリンクをクリックして、新しいウィンドウにレポートを表示します。
- [OK] をクリックして、レポートテンプレートエディタに戻ります。

## レポートの生成オプション

レポートの生成オプションは、以下のように設定できます。

- 1 回のみまたは定期的のいずれかの将来のレポート生成をスケジュールします。[レポートの生成の自動化 \(227 ページ\)](#) を参照してください。毎日、毎週、毎月など、さまざまな範囲のタイムフレームに基づいたスケジュールでもカスタマイズできます。
- スケジューラを使用してメールレポートを配信します。タスクをスケジュールする前に、レポートテンプレートとメールリレーホストを設定する必要があります。
- レポートを生成すると、そのレポートが受信者リストにメールの添付ファイルとして自動的に送信されます。レポートを電子メールで配信するように、メールリレーホストを適切に設定する必要があります。
- 新しく生成されたレポートファイルを、設定されたリモートストレージの場所に保存します。リモートストレージを使用するには、まずリモートストレージの場所を設定します。



(注) リモートに保存してから、ローカルストレージに切り替えた場合、リモートストレージ内のレポートは [レポート (Reports)] タブのリストに表示されません。同様に、あるリモートストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

## レポートの生成時の電子メール配布

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

### 手順

**ステップ 1** [概要 (Overview)] > [レポート (Reporting)] を選択します。

**ステップ 2** [レポート テンプレート (Report Templates)] タブをクリックします。

**ステップ 3** レポートの生成に使用するテンプレートの横にあるレポート アイコン (📄) をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ヒント** 先祖のテンプレートからレポートを生成するには、そのテンプレートを現在のドメインにコピーします。

**ステップ 4** このウィンドウの [電子メール (Email)] セクションを展開します。

**ステップ 5** [電子メール オプション (Email Options)] フィールドで、[電子メールの送信 (Send Email)] を選択します。

**ステップ 6** [受信者リスト (Recipient List)]、[CC] および [BCC] フィールドで、カンマ区切りリストの形式で受信者の電子メールアドレスを入力します。

**ステップ 7** [件名 (Subject)] フィールドに、電子メールの件名を入力します。

**ヒント** [件名 (Subject)] フィールドやメッセージ本文に入力パラメータを使用して、電子メール内にタイムスタンプや Firepower Management Center の名前などの情報を動的に生成できます。

**ステップ 8** 必要に応じて、電子メールの本文にカバー レターを入力します。

**ステップ 9** [OK] をクリックして確定します。

### 関連トピック

[メール リレー ホストおよび通知アドレスの設定 \(971 ページ\)](#)

## 将来のレポートのスケジュール

[レポートの生成の自動化 \(227 ページ\)](#) を参照してください。

# 生成されたレポートの操作について

以前に生成されたレポートには、[レポート (Reports)] タブのページからアクセスして操作します。

## レポートの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

[レポート (Reports)] タブには、以前に生成されたすべてのレポートと、そのレポート名、生成日時、生成したユーザ、そのレポートがローカルに保存されたかリモートに保存されたかが一覧表示されます。ステータスのカラムには、レポートがすでに生成されているか、生成キュー内にある (スケジュール済みタスクの場合など) か、それとも生成できなかった (ディスク領域不足などの理由で) かが示されます。

管理者アクセス権を持つユーザはすべてのレポートを表示でき、その他のユーザは自分が生成したレポートだけを表示できることに注意してください。

マルチドメイン展開では、現在のドメインで作成されたレポートだけを表示できます。

[レポート (Reports)] タブのページには、ローカルに保存されたレポートがすべて示されます。現在リモートストレージが設定されている場合、リモートに保存されたレポートも示されます。リモートで保存されたレポートの [場所 (Location)] カラム データは、「Remote」になります。



- (注) リモートに保存してから、ローカルストレージに切り替えた場合、リモートストレージ内のレポートは [レポート (Reports)] タブのリストに表示されません。同様に、あるリモートストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

### 手順

- ステップ 1** [概要 (Overview)] > [レポート (Reporting)] を選択します。
- ステップ 2** [レポート (Reports)] タブをクリックします。
- ステップ 3** 表示するレポートを選択します。

## レポートのダウンロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

ローカルコンピュータにレポートファイルをダウンロードできます。そのコンピュータから、電子メールや他の使用可能な方法で電子的に配布できます。

マルチドメイン導入では、現在のドメインで生成されたレポートのみをダウンロードできません。

### 手順

**ステップ 1** [概要 (Overview)] > [レポート (Reporting)] を選択します。

**ステップ 2** [レポート (Reports)] タブをクリックします。

**ステップ 3** ダウンロードするレポートの横にあるチェックボックスをオンにして、[ダウンロード (Download)] をクリックします。

**ヒント** ページ上のすべてのレポートをダウンロードするには、そのページの左上にあるチェックボックスをオンにします。複数のレポートが複数のページにある場合は、2つ目のチェックボックスが表示されます。これをクリックすると、すべてのページ上のすべてのレポートをダウンロードできます。

**ステップ 4** ブラウザのプロンプトに従って、レポートをダウンロードします。複数のレポートを選択すると、1つの .zip ファイルでダウンロードされます。

## リモートでのレポートの保存

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

[概要 (Overview)] > [レポート (Reporting)] > [レポート (Reports)] ページの下部に、現在設定されているレポートストレージの場所が表示され、ローカル、NFS、SMB ストレージの場合はディスク使用率も表示されます。SSH を使用してリモートストレージにアクセスする場合、ディスク使用率のデータは利用できません。



- (注) リモートに保存してから、ローカルストレージに切り替えた場合、リモートストレージ内のレポートは [レポート (Reports) ] タブのリストに表示されません。同様に、あるリモートストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

#### 始める前に

- リモートストレージの場所を設定します。詳細については、[リモートストレージ管理 \(949 ページ\)](#) を参照してください。

#### 手順

**ステップ 1** [概要 (Overview) ] > [レポート (Reporting) ] を選択します。

**ステップ 2** [レポート (Reports) ] タブを選択します。

**ステップ 3** ページ下部の [レポートのリモートストレージの有効化 (Enable Remote Storage of Reports) ] チェック ボックスをオンにします。

#### 次のタスク

- ローカルストレージからリモートストレージにレポートを移動します ([リモートストレージへのレポートの移動 \(2338 ページ\)](#) を参照)。

#### 関連トピック

[リモートストレージ管理 \(949 ページ\)](#)

[リモートストレージへのレポートの移動 \(2338 ページ\)](#)

## リモートストレージへのレポートの移動

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

バッチモードまたは単独で、ローカルストレージ内のレポートをリモートストレージの場所に移動できます。





- (注) リモートに保存してから、ローカルストレージに切り替えた場合、リモートストレージ内のレポートは[レポート (Reports)]タブのリストに表示されません。同様に、あるリモートストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

#### 始める前に

- リモートストレージの場所を設定します。詳細については、[リモートストレージ管理 \(949 ページ\)](#) を参照してください。

#### 手順

**ステップ 1** [概要 (Overview)] > [レポート (Reporting)] を選択します。

**ステップ 2** [レポート (Reports)] タブを選択します。

**ステップ 3** 移動するレポートの横にあるチェックボックスをオンにして、[移動 (Move)] をクリックします。

**ヒント** ページ上のすべてのレポートを移動するには、そのページの左上にあるチェックボックスをオンにします。レポートのページが複数にわたる場合は、2つ目のチェックボックスが表示されます。すべてのページのすべてのレポートを移動する場合は、このチェックボックスをオンにします。

**ステップ 4** レポートの移動を確認します。

## レポートの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

レポートファイルはいつでも削除できます。この手順ではファイルが完全に削除され、リカバリは不可能になります。レポートの生成に使用したレポートテンプレートがまだ残っていますが、時間枠を拡大したりスライドしたりした場合は、特定のレポートファイルを再生成するのは難しくなることがあります。テンプレートで入力パラメータを使用した場合も、再生成するのが難しくなることがあります。

マルチドメイン導入では、現在のドメインで生成されたレポートのみを削除できます。

## 手順

---

**ステップ 1** [概要 (Overview)] > [レポート (Reporting)] を選択します。

**ステップ 2** [レポート (Reports)] タブをクリックします。

**ステップ 3** 次の選択肢があります。

- [選択項目の削除 (Delete selected)] : 削除するレポートの隣のチェックボックスをオンにしてから、[削除 (Delete)] をクリックします。
- [すべて削除 (Delete all)] : ページ上のすべてのレポートを削除するには、そのページの左上にあるチェックボックスをオンにします。複数のレポートが複数のページにある場合は、2つ目のチェックボックスが表示され、すべてのページ上のすべてのレポートを削除するよう選択できます。

**ステップ 4** 削除を確認します。

---



## 第 95 章

# アラート応答による外部アラート

次のトピックでは、アラート応答を使用して Firepower Management Center から外部イベントアラートを送信する方法を示します。

- [Firepower Management Center アラート応答 \(2341 ページ\)](#)
- [SNMP アラート応答の作成 \(2342 ページ\)](#)
- [Syslog アラート応答の作成 \(2344 ページ\)](#)
- [電子メール アラート応答の作成 \(2347 ページ\)](#)
- [影響フラグ アラートの設定 \(2348 ページ\)](#)
- [検出イベント アラートの設定 \(2348 ページ\)](#)
- [AMP for Firepower アラートの設定 \(2349 ページ\)](#)

## Firepower Management Center アラート応答

SNMP、syslog、または電子メールでの外部イベント通知はクリティカルなシステムのモニタリングに役立ちます。Firepower Management Center はアラート応答を構成して外部サーバと対話します。アラート応答は、電子メール、SNMP、syslog サーバへの接続を表す構成です。これが応答と呼ばれるのは、これを使用して Firepower により検出されたイベントに応答してアラートを送信できるためです。異なるタイプのアラートを異なるモニタリングサーバまたはユーザ（あるいはその両方）に送信するための複数のアラート応答を構成できます。



(注) アラート応答を使用するアラートは、Firepower Management Center によって送信されます。アラート応答を使用しない侵入の電子メールアラートも、Firepower Management Center によって送信されます。対照的に、個別の侵入ルールのトリガーに基づく SNMP および syslog アラートは管理対象デバイスから直接送信されます。詳細については、[侵入イベントに関する外部アラート \(2351 ページ\)](#) を参照してください。

ほとんどの場合、外部アラートに含まれる情報はデータベースにロギングされたいずれかの関連イベントに含まれる情報と同じです。ただし、相関ルールに接続トラッカーが含まれる相関イベントアラートについては、受信する情報はベースのイベントの種類に関係なく、トラフィックプロファイル変更のアラート情報と同じです。

アラート応答の作成や管理は[アラート (Alerts)] ページ ([ポリシー (Policies)] > [アクション (Actions)] > [アラート (Alerts)]) で行います。新しいアラート応答は自動的に有効になります。アラート応答を削除するのではなく無効にすることで、アラートの生成を一時的に止めることができます。

アラート応答を使って SNMP トラップまたは syslog サーバに接続ログを送信している場合 (外部電子メールアラートは接続イベントではサポートされていません)、これらのアラート応答を編集したあとに設定の変更を展開する必要があります。そうしないと、アラート応答への変更はただちに反映されます。

マルチドメイン展開では、アラート応答を作成すると、作成された応答は現在のドメインに属します。このアラート応答は子孫ドメインでも使用できます。

## アラート応答のサポート設定

アラート応答を作成した後、それを使用して、次のような外部アラートを Firepower Management Center から送信できます。

アラート/イベントのタイプ	詳細情報
侵入イベント (インパクト フラグ別)	<a href="#">影響フラグアラートの設定 (2348 ページ)</a>
検出イベント (タイプ別)	<a href="#">検出イベントアラートの設定 (2348 ページ)</a>
ネットワークベースのマルウェアとレトロスペクティブ マルウェアのイベント	<a href="#">AMP for Firepower アラートの設定 (2349 ページ)</a>
関連イベント (関連ポリシー違反ごと)	<a href="#">ルールとホワイトリストに応答を追加する (2226 ページ)</a>
関連イベント (ログルールまたはデフォルトアクション別) (電子メールアラートのサポートなし)	<a href="#">設定可能な接続ロギング (2504 ページ)</a>
ヘルスイベント (ヘルスモジュールおよび重大度レベル別)	<a href="#">ヘルスマニタアラートの作成 (293 ページ)</a>

## SNMP アラート応答の作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any) (Firepower Threat Defense を除く)	任意 (Any)	Admin

SNMPv1、SNMPv2、または SNMPv3 を使用して SNMP アラート応答を作成できます。



- (注) SNMP プロトコルの SNMP バージョンを選択する場合、SNMPv2 では読み取り専用コミュニティのみがサポートされ、SNMPv3 では読み取り専用ユーザのみがサポートされることに注意してください。SNMPv3 は、AES128 での暗号化をサポートします。

SNMP で 64 ビット値をモニタする場合は、SNMPv2 または SNMPv3 を使用する必要があります。SNMPv1 は 64 ビットのモニタリングをサポートしていません。

#### 始める前に

- ネットワーク管理システムで Firepower Management Center の管理情報ベース (MIB) ファイルが必要な場合は、`/etc/sf/DCEALERT.MIB` で取得できます。

#### 手順

- ステップ 1** [ポリシー (Policies) ] > [アクション (Actions) ] > [アラート (Alerts) ] を選択します。
- ステップ 2** [アラートの作成 (Create Alert) ] ドロップダウンメニューから、[SNMP アラートの作成 (Create SNMP Alert) ] を選択します。
- ステップ 3** SNMP 応答を識別する [名前 (Name) ] を入力します。
- ステップ 4** [トラップサーバ (Trap Server) ] フィールドに、SNMP トラップサーバのホスト名または IP アドレスを入力します。
- (注) このフィールドに無効な IPv4 アドレス (192.169.1.456 など) を入力した場合でも、システムは警告を表示しません。無効なアドレスはホスト名として扱われます。
- ステップ 5** [バージョン (Version) ] ドロップダウンリストから、使用する SNMP バージョンを選択します。SNMP v3 がデフォルトです。
- ステップ 6** 使用する SNMP のバージョンに応じて、次のいずれかを実行します。
- SNMP v1 または SNMP v2 の場合は、[コミュニティストリング (Community String) ] フィールドに SNMP コミュニティ名を入力して、手順 12 に進みます。
  - SNMP v3 の場合、[ユーザ名 (User Name) ] フィールドに SNMP サーバで認証するユーザの名前を入力し、次の手順に進みます。
- ステップ 7** [認証プロトコル (Authentication Protocol) ] ドロップダウンリストから、認証に使用するプロトコルを選択します。
- ステップ 8** [認証パスワード (Authentication Password) ] フィールドに、SNMP サーバの認証に必要なパスワードを入力します。
- ステップ 9** [プライバシープロトコル (Privacy Protocol) ] リストから、[なし (None) ] を選択してプライバシープロトコルを使用しないか、または [DES] を選択してプライバシープロトコルにデータ暗号規格を使用します。
- ステップ 10** [プライバシーパスワード (Privacy Password) ] フィールドに、SNMP サーバに必要なプライバシーパスワードを入力します。

**ステップ 11** [エンジン ID (Engine ID)] フィールドに、SNMP エンジンの識別子を偶数桁の 16 進表記で入力します。

SNMPv3 を使用する場合、メッセージの符号化にはエンジン ID 値が使用されます。SNMP サーバでは、メッセージをデコードするためにこの値が必要です。

Firepower Management Center の IP アドレスの 16 進数バージョンを使用することを推奨します。たとえば、Firepower Management Center の IP アドレスが 10.1.1.77 である場合、0a01014D0 を使用します。

**ステップ 12** [保存 (Save)] をクリックします。

## Syslog アラート応答の作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

syslog アラート応答を設定する際、syslog サーバで確実に正しく処理されるようにするために、syslog メッセージに関連付けられる重大度とファシリティを指定できます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。ファシリティと重大度は syslog に示される実際のメッセージには表示されませんが、syslog メッセージを受信するシステムに対して、メッセージの分類方法を指示するために使用されます。



**ヒント** syslog の機能とその設定方法の詳細については、ご使用のシステムのマニュアルを参照してください。UNIX システムでは、syslog および syslog.conf の man ページで概念情報および設定手順が説明されています。

syslog アラート応答の作成時に任意のタイプのファシリティを選択できますが、syslog サーバに基づいて意味のあるものを選択する必要があります。すべての syslog サーバがすべてのファシリティをサポートしているわけではありません。UNIX syslog サーバの場合、syslog.conf ファイルで、どのファシリティがサーバ上のどのログファイルに保存されるかを示す必要があります。

### 始める前に

- syslog サーバがリモート メッセージを受け入れられることを確認します。

### 手順

**ステップ 1** [ポリシー (Policies)] > [アクション (Actions)] > [アラート (Alerts)] を選択します。

**ステップ 2** [アラートの作成 (Create Alert)] ドロップダウンメニューから、[Syslog アラートの作成 (Create Syslog Alert)] を選択します。

**ステップ 3** [名前 (Name)] にアラートの名前を入力します。

**ステップ 4** [ホスト (Host)] フィールドに、syslog サーバのホスト名または IP アドレスを入力します。

(注) このフィールドに無効な IPv4 アドレス (192.168.1.456 など) を入力した場合でも、システムは警告を表示しません。無効なアドレスはホスト名として扱われます。

**ステップ 5** [ポート (Port)] フィールドに、サーバが syslog メッセージに使用するポートを入力します。この値はデフォルトで 514 です。

**ステップ 6** [Syslog アラート ファシリティ \(2345 ページ\)](#) で説明されているとおりに、[ファシリティ (Facility)] リストからファシリティを選択します。

**ステップ 7** [syslog 重大度レベル \(2346 ページ\)](#) で説明されているとおりに、[重大度 (Severity)] リストから重大度を選択します。

**ステップ 8** [タグ (Tag)] フィールドに、syslog メッセージとともに表示するタグ名を入力します。

たとえば、syslog に送信されるすべてのメッセージの前に FromMC を付ける場合、このフィールドに FromMC と入力します。

**ステップ 9** [保存 (Save)] をクリックします。

## Syslog アラート ファシリティ

次の表に、選択可能な syslog ファシリティを示します。

表 247: 使用可能な syslog ファシリティ

ファシリティ	説明
ALERT	アラート メッセージ。
AUDIT	監査サブシステムによって生成されるメッセージ。
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセスメッセージ。多くのシステムで、これらのメッセージはセキュアファイルに転送されます。
CLOCK	クロック デーモンによって生成されるメッセージ。  Windows オペレーティングシステムを実行している syslog サーバは cLOCK ファシリティを使用することに注意してください。

ファシリティ	説明
CRON	クロック デーモンによって生成されるメッセージ。 Linux オペレーティング システムを実行している syslog サーバは CRON ファシリティを使用することに注意してください。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージは表示されるときにコンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。
NTP	NTP デーモンによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザレベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

## syslog 重大度レベル

次の表に、選択可能な標準の syslog 重大度レベルを示します。

表 248: syslog 重大度レベル

水準器	説明
ALERT	ただちに修正する必要がある状態。
CRIT	クリティカルな状態。
DEBUG	デバッグ情報を含むメッセージ。
EMERG	すべてのユーザに配信されるパニック状態。
ERR	エラー状態。



水準器	説明
INFO	情報メッセージ。
NOTICE	エラー状態ではないが、注意が必要な状態。
WARNING	警告メッセージ。

## 電子メールアラート応答の作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

### 始める前に

- Firepower Management Center で、自身の IP アドレスを逆解決できることを確認します。
- [メールリレーホストおよび通知アドレスの設定 \(971 ページ\)](#) の説明に従って、メールリレーホストを設定します。



(注) 電子メールアラートを使用して、接続をログに記録することはできません。

### 手順

- ステップ 1** [ポリシー (Policies)] > [アクション (Actions)] > [アラート (Alerts)] を選択します。
- ステップ 2** [アラートの作成 (Create Alert)] ドロップダウンメニューから、[電子メールアラートの作成 (Create Email Alert)] を選択します。
- ステップ 3** [名前 (Name)] にアラート応答の名前を入力します。
- ステップ 4** [宛先 (To)] フィールドに、アラートを送信する電子メールアドレスをカンマで区切って入力します。
- ステップ 5** [送信元 (From)] フィールドに、アラートの送信者として表示する電子メールアドレスを入力します。
- ステップ 6** [リレーホスト (Relay Host)] の横に表示されるメールサーバが、アラートの送信に使用するサーバであることを確認します。

ヒント 電子メールサーバを変更するには、編集アイコン (✎) をクリックします。

ステップ7 [保存 (Save) ]をクリックします。

## 影響フラグアラートの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin

特定のインパクトフラグを持つ侵入イベントが発生するたびにアラートが生成されるようにシステムを設定できます。インパクトフラグは、侵入データ、ネットワーク検出データ、および脆弱性情報を関連付けることにより、侵入がネットワークに与える影響を評価するのに役立ちます。

### 手順

ステップ1 [ポリシー (Policies) ] > [アクション (Actions) ] > [アラート (Alerts) ]を選択します。

ステップ2 [インパクトフラグアラート (Impact Flag Alerts) ]タブをクリックします。

ステップ3 [アラート (Alerts) ]セクションで、各アラートタイプで使用するアラート応答を選択します。

ヒント 新しいアラート応答を作成するには、任意のドロップダウンリストから[新規 (New) ]を選択します。

ステップ4 [インパクト設定 (Impact Configuration) ]セクションで、該当するチェックボックスをオンにして、各インパクトフラグに対して受信するアラートを指定します。

ステップ5 [保存 (Save) ]をクリックします。

## 検出イベントアラートの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

特定のタイプの検出イベントが発生するたびにアラートが生成されるようにシステムを設定できます。

### 始める前に

- [ネットワーク検出イベントロギングの設定 \(2172 ページ\)](#) の説明に従って、アラートを設定する検出イベント タイプを記録するようにネットワーク検出ポリシーを設定します。

### 手順

**ステップ 1** [ポリシー (Policies) ] > [アクション (Actions) ] > [アラート (Alerts) ] を選択します。

**ステップ 2** [検出イベント アラート (Discovery Event Alerts) ] タブをクリックします。

**ステップ 3** [アラート (Alerts) ] セクションで、各アラートタイプで使用するアラート応答を選択します。

ヒント 新しいアラート応答を作成するには、任意のドロップダウンリストから [新規 (New) ] を選択します。

**ステップ 4** [イベント設定 (Events Configuration) ] セクションで、各検出イベントタイプに対して、受信するアラートに対応するチェックボックスを選択します。

**ステップ 5** [保存 (Save) ] をクリックします。

## AMP for Firepower アラートの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア	マルウェア	任意 (Any)	任意 (Any)	Admin

ネットワークベースのマルウェア イベント (レトロスペクティブ イベントを含む) が発生するたびにアラートが生成されるようにシステムを設定できます。ただし、エンドポイントベースの (AMP for Endpoints) マルウェア イベントではアラートを生成できません。

### 始める前に

- マルウェア クラウドルックアップを実行するファイル ポリシーを設定し、[侵入ポリシーとファイル ポリシーを使用したアクセス制御 \(1359 ページ\)](#) の説明に従って、そのポリシーをアクセス コントロール ルールに関連付けます。

### 手順

**ステップ 1** [ポリシー (Policies) ] > [アクション (Actions) ] > [アラート (Alerts) ] を選択します。

**ステップ 2** [高度なマルウェア保護アラート (Advanced Malware Protections Alerts) ] タブをクリックします。

**ステップ 3** [アラート (Alerts) ] セクションで、各アラートタイプで使用するアラート応答を選択します。

ヒント 新しいアラート応答を作成するには、任意のドロップダウンリストから[新規 (New)] を選択します。

**ステップ 4** [イベント設定 (Event Configuration)] セクションで、各マルウェア イベントタイプに対して、受信するアラートに対応するチェックボックスを選択します。

[すべてのネットワークベースのマルウェア イベント (All network-based malware events)] には [レトロスペクティブ イベント (Retrospective Events)] が含まれることに注意してください。

**ステップ 5** [保存 (Save)] をクリックします。

---



## 第 96 章

# 侵入イベントに関する外部アラート

次のトピックでは、侵入イベントに関する外部アラートを設定する方法について説明します。

- [侵入イベントの外部アラートについて \(2351 ページ\)](#)
- [侵入イベントの SNMP アラートの設定 \(2352 ページ\)](#)
- [侵入イベントの Syslog アラートの設定 \(2354 ページ\)](#)
- [侵入イベントに対する電子メールアラートの設定 \(2356 ページ\)](#)

## 侵入イベントの外部アラートについて

外部侵入イベント通知は、クリティカルなシステム モニタリングに役立ちます。

- **SNMP** : 侵入ポリシーごとに設定し、管理対象デバイスが送信します。SNMP アラートは侵入ルールごとに有効にすることができます。
- **syslog** : 侵入ポリシーごとに設定し、管理対象デバイスが送信します。1つの侵入ポリシーの syslog アラートを有効にすると、ポリシーに含まれるすべてのルールに適用されます。
- **電子メール** : すべての侵入ポリシーに設定され、Firepower Management Center が送信します。電子メールアラートは侵入ルールごとに有効にすることができ、長さや頻度を制限することもできます。

侵入イベントの抑制やしきい値を設定すると、システムは、ルールがトリガーされるたびに侵入イベントを生成しなくなる（したがってアラートを送信しなくなる）場合があるのでご注意ください。

マルチドメイン導入環境では、どのドメインでも外部アラートを設定できます。先祖ドメインでは、システムは子孫ドメインの侵入イベントの通知を生成します。



- (注) Firepower Management Center も SNMP、syslog、および電子メールアラート応答を使って種々の外部アラートを送信します。[Firepower Management Center アラート応答 \(2341 ページ\)](#) を参照してください。システムは、個々の侵入イベントに対するアラートを送信するためにアラート応答を使用しません。

## 関連トピック

[侵入ポリシーの侵入イベント通知のフィルタ](#) (1641 ページ)

## 侵入イベントの SNMP アラートの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入ポリシーで外部 SNMP アラートを有効にした後、トリガー時に SNMP アラートを送信する個々のルールを設定できます。これらのアラートは管理対象デバイスから送信されます。

### 手順

- ステップ 1 侵入ポリシー エディタのナビゲーション ウィンドウで、[詳細設定 (Advanced Settings)] をクリックします。
- ステップ 2 [SNMP アラート (SNMP Alerting)] が有効になっていることを確認し、[編集 (Edit)] をクリックします。  
ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。
- ステップ 3 SNMP バージョンを選択し、[侵入 SNMP アラートのオプション \(2352 ページ\)](#) の説明に従って構成オプションを指定します。
- ステップ 4 ナビゲーション ウィンドウで [ルール (Rules)] をクリックします。
- ステップ 5 [ルール (rules)] ペインで、SNMP アラートを設定するルールを選択し、[アラート (Alerting)] > [SNMP アラートの追加 (Add SNMP Alert)] を選択します。
- ステップ 6 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] を選択して、[変更を確定 (Commit Changes)] をクリックします。  
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 侵入 SNMP アラートのオプション

ネットワーク管理システムで Management Information Base (MIB) ファイルが必要な場合は、Firepower Management Center の `/etc/sf/DCEALERT.MIB` から取得できます。

## SNMP v2 オプション

オプション	説明
トラップタイプ	アラートに表示される IP アドレスに使用するトラップタイプ。 ネットワーク管理システムによって INET_IPV4 アドレスタイプが正常にレンダリングされた場合は、[バイナリとして (as Binary)] を選択します。それ以外の場合は、[文字列として (as String)] を選択します。たとえば、HP OpenView では [文字列として (as String)] が必要になります。
トラップサーバ (Trap Server)	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。
コミュニティストリング (Community String)	コミュニティ名。

## SNMP v3 オプション

管理対象デバイスは、エンジン ID の値を使用して SNMPv3 アラートをエンコードします。アラートをデコードするには、SNMP サーバにこの値が必要です。この値は、送信デバイスの管理インターフェイスの IP アドレスの 16 進数のバージョンで、「01」が付加されています。

たとえば、SNMP アラートを送信するデバイスの管理インターフェイスの IP アドレスが 172.16.1.50 である場合、エンジン ID の値は 0xAC10013201 です。

オプション	説明
トラップタイプ	アラートに表示される IP アドレスに使用するトラップタイプ。 ネットワーク管理システムによって INET_IPV4 アドレスタイプが正常にレンダリングされた場合は、[バイナリとして (as Binary)] を選択します。それ以外の場合は、[文字列として (as String)] を選択します。たとえば、HP OpenView では [文字列として (as String)] が必要になります。
トラップサーバ (Trap Server)	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。
認証パスワード (Authentication Password)	認証に必要なパスワード。SNMP v3 は、設定に応じて Message Digest 5 (MD5) ハッシュ関数またはセキュアハッシュアルゴリズム (SHA) ハッシュ関数のいずれかを使用し、このパスワードを暗号化します。 認証パスワードを指定すると、認証が有効になります。

オプション	説明
プライベートパスワード (Private Password)	<p>プライバシー用の SNMP キー。SNMP v3 は Data Encryption Standard (DES) ブロック暗号を使用して、このパスワードを暗号化します。SNMP v3 パスワードを入力すると、パスワードは初期設定時にはプレーンテキストで表示されますが、暗号化形式で保存されます。</p> <p>プライベートパスワードを指定すると、プライバシーが有効になり、認証パスワードも指定する必要があります。</p>
ユーザ名 (User Name)	SNMP ユーザ名。

## 侵入イベントの Syslog アラートの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入ポリシーでsyslogアラートを有効にすると、管理対象デバイス自体または外部ホスト上のsyslogにすべての侵入イベントが送信されます。外部ホストを指定した場合、syslogアラートは管理対象デバイスから送信されます。

### 手順

- ステップ 1** 侵入ポリシーエディタのナビゲーションウィンドウで、[詳細設定 (Advanced Settings)] をクリックします。
- ステップ 2** [Syslog アラート (Syslog Alerting)] が有効になっていることを確認し、[編集 (Edit)] をクリックします。  
ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。
- ステップ 3** syslog アラートを送信するロギングホストの IP アドレスを入力します。  
このフィールドを空のままにすると、管理対象デバイスは、独自のsyslog機能を使用して侵入イベントをログに記録します。  
システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。
- ステップ 4** 侵入syslogアラートのファシリティとプライオリティ (2355 ページ) の説明に従って、ファシリティと優先度レベルを選択します。



- ステップ 5** 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] を選択して、[変更を確定 (Commit Changes)] をクリックします。
- 変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 侵入 syslog アラートのファシリティとプライオリティ

管理対象デバイスは、特定のファシリティとプライオリティを使用して、侵入イベントを syslog アラートとして送信できるため、ロギングホストがアラートを分類できます。ファシリティには、それを生成したサブシステムを指定します。プライオリティには、その重大度を指定します。これらのファシリティとプライオリティの値は、実際の syslog メッセージには表示されません。

ご使用の環境に基づいて意味のある値を選択します。ローカル設定ファイル (UNIX ベースのロギングホストの `syslog.conf` など) では、どのログファイルにどのファシリティを保存するかを示すことができます。

#### Syslog アラート ファシリティ

ファシリティ	説明
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CRON	クロック デーモンによって生成されるメッセージ。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージは表示されるときにコンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュースサブシステムによって生成されるメッセージ。

ファシリティ	説明
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザレベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

### Syslog アラートのプライオリティ

水準器	説明
EMERG	すべてのユーザにブロードキャストするパニック状態
ALERT	すぐに修正する必要がある状態
CRIT	重大な状態
ERR	エラー状態
WARNING	警告メッセージ
NOTICE	エラー状態ではないが、注意が必要な状態
INFO	通知メッセージ
DEBUG	デバッグ情報を含むメッセージ

## 侵入イベントに対する電子メールアラートの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入の電子メールアラートを有効にした場合、どの管理対象デバイスまたは侵入ポリシーが侵入を検出したかに関係なく、システムは侵入イベントの生成時に電子メールを送信できます。これらのアラートは Firepower Management Center から送信されます。

### 始める前に

- 電子メールアラートを受信するようにメールホストを設定します。[メールリレーホストおよび通知アドレスの設定 \(971 ページ\)](#) を参照してください。
- Firepower Management Center が独自の IP アドレスを逆解決できることを確認します。

## 手順

- ステップ1 [ポリシー (Policies)] > [アクション (Actions)] > [アラート (Alerts)] を選択します。
- ステップ2 [侵入電子メール (Intrusion Email)] タブをクリックします。
- ステップ3 [侵入電子メールアラートのオプション \(2357ページ\)](#) の説明に従って、アラートを生成する侵入ルールや侵入グループを含むアラート オプションを選択します。
- ステップ4 [保存 (Save)] をクリックします。

## 侵入電子メールアラートのオプション

### On/Off

侵入電子メールアラートを有効または無効にします。

### アドレス送信元/宛先 (From/To Addresses)

電子メールの送信者と受信者。受信者のカンマ区切りリストを指定できます。

### 最大アラート数と頻度 (Max Alerts and Frequency)

Firepower Management Center が時間間隔 ([頻度 (Frequency)] ) ごとに送信する電子メールアラートの最大数 ([最大アラート数 (Max Alerts)] ) 。

### 合同アラート (Coalesce Alerts)

同じ送信元 IP とルール ID を持つアラートをグループ化することによって送信されるアラートの数を減らします。

### サマリー出力 (Summary Output)

テキスト制限されたデバイスに適した短いアラートを有効にします。短いアラートには、以下の情報が含まれています。

- Timestamp
- プロトコル
- 送信元と宛先の IP とポート
- メッセージ
- 同じ送信元 IP に対して生成された侵入イベントの数

```
例: 2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0  
snort_decoder: Unknown Datagram decoding problem! (116:108)
```

[サマリー出力 (Summary Output)] を有効にする場合は、[合同アラート (Coalesce Alerts)] も有効にすることを検討してください。テキストメッセージの制限を超えないように、[最大アラート数 (Max Alerts)] を下げることができます。

### タイムゾーン

アラートタイムスタンプのタイムゾーン。

### 特定のルール設定に基づく電子メール警告 (Email Alerting on Specific Rules Configuration)

電子メールアラートを設定するルールを選択できます。



## 第 **XXIII** 部

# イベントとアセットの分析ツール

- [コンテキスト エクスプローラの使用 \(2361 ページ\)](#)
- [ネットワーク マップの使用 \(2391 ページ\)](#)
- [インシデント \(2405 ページ\)](#)
- [ルックアップの使用 \(2413 ページ\)](#)





## 第 97 章

# コンテキスト エクスプローラの使用

以下のトピックでは、Firepower システムでコンテキスト エクスプローラを使用する方法について説明します。

- [コンテキスト エクスプローラについて \(2361 ページ\)](#)
- [Context Explorer の更新 \(2379 ページ\)](#)
- [Context Explorer の時間範囲の設定 \(2379 ページ\)](#)
- [Context Explorer のセクションの最小化および最大化 \(2380 ページ\)](#)
- [Context Explorer データのドリルダウン \(2381 ページ\)](#)
- [コンテキスト エクスプローラのフィルタ \(2382 ページ\)](#)

## コンテキスト エクスプローラについて

Firepower システムの Context Explorer には、モニタ対象ネットワークのステータスに関するコンテキストでの詳細でインタラクティブなグラフィカル情報が表示されます。これには、アプリケーション、アプリケーション統計、接続、位置情報、侵害の兆候、侵入イベント、ホスト、サーバ、セキュリティ インテリジェンス、ユーザ、ファイル（マルウェア ファイルを含む）、関連 URL に関するデータが含まれます。各セクションには、このデータが鮮やかな色の折れ線グラフ、棒グラフ、円グラフ、ドーナツグラフの形式で表示され、グラフとともに詳しいリストが示されます。1 番目のセクションに表示される時間の経過に伴うトラフィックとイベント数の変化を示した折れ線グラフは、ネットワークのアクティビティにおける最近の傾向の概要を示します。

分析を細かく調整するためのカスタムフィルタを容易に作成および適用できます。またグラフ エリアをクリックするか、カーソルをグラフ エリアに置くことでデータ セクションを詳しく調べることができます。過去 1 時間から過去 1 年までの期間を反映するように Explorer の時間範囲を設定することもできます。Context Explorer にアクセスできるユーザは、管理者、セキュリティ アナリスト、またはセキュリティ アナリスト（読み取り専用）のユーザ ロールが割り当てられているユーザだけです。

Firepower システムのダッシュボードは細かくカスタマイズすることができます。このダッシュボードは区分化されており、リアルタイムで更新されます。一方、Context Explorer は手動で更新され、より幅広いデータのコンテキストを提供することを目的としており、アクティブなユーザ操作のために単一で一貫性のあるレイアウトを備えています。

特定のニーズに基づいてネットワークとアプライアンスのリアルタイムのアクティビティをモニタするには、ダッシュボードを使用します。逆に、詳細かつ明確なコンテキストで事前に定義されている最新のデータセットを調査するには、Context Explorer を使用します。たとえば、ネットワークのホストのうち Linux を使用しているホストは 15% であるが、ほぼすべての YouTube トラフィックはこれらのホストによるものであることが判明した場合、Linux ホストのデータのみを表示するフィルタ、YouTube 関連のアプリケーションデータのみを表示するフィルタ、あるいはこの両方のフィルタを簡単に適用できます。コンパクトで対象が絞り込まれているダッシュボードウィジェットとは異なり、Context Explorer の各セクションは、Firepower システムの専門知識を持つユーザと一般的なユーザの両方に役立つ形式で、システムアクティビティを鮮明なビジュアル表現で提供します。

表示されるデータは、管理対象デバイスのライセンスおよび導入状況や、そのデータを提供する機能を設定しているかどうかによって異なります。また、Context Explorer のすべてのセクションで、フィルタを適用して表示するデータを制限することもできます。

マルチドメイン導入では、先祖ドメインで Context Explorer を表示すると、すべてのサブドメインからの集約データが表示されます。リーフドメインでは、そのドメインに固有のデータだけを表示できます。

## ダッシュボードと Context Explorer の違い

次の表に、ダッシュボードと Context Explorer の主な相違点の要約を示します。

表 249: 比較 : ダッシュボードと Context Explorer

機能	ダッシュボード	コンテキストエクスプローラ (Context Explorer)
表示可能なデータ	Firepower システムによってモニタされる任意の対象	アプリケーション、アプリケーション統計、位置情報、の侵害の兆候、侵入イベント、ファイル (マルウェアファイルを含む)、ホスト、セキュリティインテリジェンスイベント、サーバ、ユーザ、および URL
カスタマイズ可能かどうか	<ul style="list-style-type: none"> <li>ダッシュボードで選択されているウィジェットはカスタマイズ可能です</li> <li>個々のウィジェットはさまざまなレベルでカスタマイズ可能です</li> </ul>	<ul style="list-style-type: none"> <li>基本レイアウトは変更できません</li> <li>適用されたフィルタは Explorer URL に示され、後で使用するためにブックマークできます</li> </ul>
データの更新頻度	自動 (デフォルト)、ユーザ設定	手動 (Manual)
データのフィルタリング	一部のウィジェットで可能です (ウィジェット設定を編集する必要があります)	Explorer のすべての部分で可能であり、複数フィルタに対応しています



機能	ダッシュボード	コンテキストエクスプローラ (Context Explorer)
グラフィカル コンテキスト	一部のウィジェット (特にカスタム分析 (Custom Analysis) ) では、データをグラフ形式で表示できます	すべてのデータの豊富なグラフィカル コンテキスト (独自の詳細なドーナツグラフを含む)
関連 Web インターフェイス ページへのリンク	一部のウィジェット	すべてのセクション
表示データの時間範囲	ユーザ設定	ユーザ設定

### 関連トピック

[ダッシュボードについて](#) (247 ページ)

## [時系列のトラフィックおよび侵入イベント数 (Traffic and Intrusion Event Counts Time) ] グラフ

Context Explorer の上部には、時間の経過に伴うトラフィックおよび侵入イベント数の変化を示す折れ線グラフが表示されます。X 軸は時間間隔を示します (選択されている時間枠に応じて、5 分～1 か月の範囲)。Y 軸は、KB 単位のトラフィック (青色の線) と侵入イベント数 (赤色の線) を示します。

X 軸の最小間隔が 5 分であることを注意してください。これに対応するため、選択された時間範囲の開始点と終了点が、システムにより、最も近い 5 分間隔に調整されます。

このセクションには、デフォルトでは選択された時間範囲のすべてのネットワークトラフィックと、生成されたすべての侵入イベントが表示されます。フィルタを適用すると、フィルタに指定されている条件に関連するトラフィックと侵入イベントだけがグラフに表示されます。たとえば、[OS 名 (OS Name) ] に Windows を指定してフィルタリングすると、時間グラフには Windows オペレーティングシステムを使用するホストに関連するトラフィックとイベントだけが表示されます。

侵入イベントデータ ([優先順位 (Priority) ] が High に設定されたものなど) に基づいて Context Explorer をフィルタ処理すると、青色のトラフィックを示す線が非表示になり、侵入イベントだけにより焦点を当てることができます。

トラフィックとイベント数に関する正確な情報を表示するには、グラフの線上の任意のポイントにポインタを置きます。また、色付きの線の 1 つにポインタを置くと、その線がグラフの前面に移動し、コンテキストがより明確になります。

このセクションのデータは、主に [侵入イベント (Intrusion Events) ] テーブルと [接続イベント (Connection Events) ] テーブルから取得されます。

## [侵害の兆候 (Indications of Compromise) ]セクション

コンテキストエクスプローラの [侵害の兆候 (IOC) (Indications of Compromise (IOC)) ]セクションには、モニタ対象ネットワーク上でセキュリティが侵害されている可能性があるホストの概要を示す2つのインタラクティブセクション (トリガーとして使用された主な IOC 種類の割合のビューと、トリガーとして使用された兆候の数をホストごとに表したビュー) が表示されます。

### [兆候別ホスト (Hosts by Indication) ]グラフ

[兆候別ホスト (Hosts by Indication) ]グラフはドーナツ形式であり、モニタ対象ネットワーク上のホストでトリガーとして使用された侵害の兆候 (IOC) を割合で表示します。内側のリングは IOC カテゴリ ([CnC 接続 (CnC Connected) ]や[マルウェア検出 (Malware Detected) ]など) ごとに分割されており、外側のリングではそれがさらに具体的なイベントの種類 ([影響 2 侵入イベント - 管理者として試行 (Impact 2 Intrusion Event — attempted-admin) ]や[ファイル転送中に脅威を検出 (Threat Detected in File Transfer) ]など) ごとに分割されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [ホスト (Hosts) ]テーブルと [侵害の兆候 (Indications of Compromise) ]テーブルから取得されます。

### [ホスト別兆候 (Indications by Host) ]グラフ

[ホスト別兆候 (Indications by Host) ]グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最も IOC が顕著な 15 のホストでトリガーとして使用された固有の侵害の兆候 (IOC) の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [ホスト (Hosts) ]テーブルと [侵害の兆候 (Indications of Compromise) ]テーブルから取得されます。

## [ネットワーク情報 (Network Information) ]セクション

Context Explorer の [ネットワーク情報 (Network Information) ]セクションには、モニタ対象ネットワーク上の接続トラフィックの全体の概要 (トラフィックに関連付けられている送信元、宛先、ユーザ、およびセキュリティゾーン、ネットワーク上のホストで使用されているオペレーティングシステムの内訳、Firepower システムがネットワークトラフィックに対して実行したアクセス制御アクションの割合のビュー) を示す6つのインタラクティブグラフが含まれています。

### [オペレーティングシステム (Operating Systems) ]グラフ

[オペレーティングシステム (Operating Systems) ]グラフはドーナツグラフ形式で、モニタ対象ネットワークのホストで検出されたオペレーティングシステムを割合で表示します。内側の

リングは OS 名 (Windows や Linux など) ごとに分割され、外側のリングではそのデータがさらにオペレーティング システムのバージョン (Windows Server 2008 や Linux 11.x など) ごとに分割されています。密接に関連するいくつかのオペレーティング システム (Windows 2000、Windows XP、Windows Server 2003 など) は 1 つにまとめられます。ごくまれにしか使用されないオペレーティング システムや認識されないオペレーティング システムは [その他 (Other) ] にまとめられます。

このグラフは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Context Explorer の時間範囲を変更しても、グラフは変化しません。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [ホスト (Hosts) ] テーブルから取得されます。

## [送信元 IP 別トラフィック (Traffic by Source IP) ] グラフ

[送信元 IP 別トラフィック (Traffic by Source IP) ] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の送信元 IP アドレスのネットワーク トラフィック カウント (KB/秒) と固有接続数を表示します。リストされた送信元 IP アドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。



- 
- (注) 侵入イベントの情報でフィルタ処理を実行すると、[送信元 IP 別トラフィック (Traffic by Source IP) ] グラフは非表示になります。
- 

このグラフのデータは、主に [接続イベント (Connection Events) ] テーブルから取得されます。

## [送信元ユーザ別トラフィック (Traffic by Source User) ] グラフ

[送信元ユーザ別トラフィック (Traffic by Source User) ] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の送信元ユーザのネットワーク トラフィック カウント (KB/秒) と固有接続数を表示します。リストされた送信元 IP アドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。



- 
- (注) 侵入イベントの情報でフィルタ処理を実行すると、[送信元ユーザ別トラフィック (Traffic by Source User) ] グラフは非表示になります。
- 

このグラフのデータは、主に [接続イベント (Connection Events) ] テーブルから取得されます。このグラフには、権限のあるユーザのデータが表示されます。

## [アクセスコントロールアクション別の接続 (Connections by Access Control Action) ] グラフ

[アクセスコントロールアクション別の接続 (Connections by Access Control Action) ] グラフは円グラフ形式であり、Firepower システム導入でモニタ対象トラフィックに対して実行されたアクセス制御アクション ([ブロック (Block) ] や [許可 (Allow) ] など) の割合のビューを表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。



- (注) 侵入イベントの情報でフィルタ処理を実行すると、[送信元ユーザ別トラフィック (Traffic by Source User) ] グラフは非表示になります。

このグラフのデータは、主に[接続イベント (Connection Events) ] テーブルから取得されます。

## [宛先 IP 別トラフィック (Traffic by Destination IP) ] グラフ

[宛先 IP 別トラフィック (Traffic by Destination IP) ] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の宛先 IP アドレスのネットワークトラフィックカウント (KB/秒) と固有接続数を表示します。リストされた宛先 IP アドレスごとに、青色の棒はトラフィックデータ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。



- (注) 侵入イベントの情報でフィルタ処理を実行すると、[宛先 IP 別トラフィック (Traffic by Destination IP) ] グラフは非表示になります。

このグラフのデータは、主に[接続イベント (Connection Events) ] テーブルから取得されます。

## [入力/出力のセキュリティゾーン別トラフィック (Traffic by Ingress/Egress Security Zone) ] グラフ

[入力/出力のセキュリティゾーン別トラフィック (Traffic by Ingress/Egress Security Zone) ] グラフは棒グラフ形式で、モニタ対象ネットワークで設定されているセキュリティゾーンごとに、その着信/発信ネットワークトラフィックカウント (KB/秒) および固有接続数を表示します。このグラフは、必要に応じて、入力 (デフォルト) セキュリティゾーン情報または出力セキュリティゾーン情報のいずれかを表示するように設定できます。

リストされたセキュリティゾーンごとに、青色の棒はトラフィックデータ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。



**ヒント** グラフに制約を適用して、出力セキュリティゾーンのトラフィックだけが表示されるようにするには、グラフにポインタを置き、表示されたトグルボタンの[出力 (Egress)]をクリックします。デフォルトのビューに戻すには、[入力 (Ingress)]をクリックします。このグラフは、Context Explorer から外部へ移動しても、デフォルトの[入力 (Ingress)]ビューに戻ります。



(注) 侵入イベントの情報でフィルタ処理を実行すると、[入力/出力のセキュリティゾーン別トラフィック (Traffic by Ingress/Egress Security Zone)] グラフは非表示になります。

このグラフのデータは、主に[接続イベント (Connection Events)] テーブルから取得されます。

## [アプリケーション情報 (Information)] セクション

Context Explorer の[アプリケーション情報 (Information)] セクションには、3つのインタラクティブグラフと1つの表形式リストが表示されます。これらのグラフとリストは、モニタ対象ネットワーク上でのアプリケーションアクティビティの概要 (アプリケーションに関連するトラフィック、侵入イベント、およびホストを、各アプリケーションに割り当てられている推定リスクまたは推定ビジネス関連度ごとに編成したもの) を示します。[アプリケーション詳細リスト (Application Details List)] は、各アプリケーションとそのリスク、ビジネス関連度、カテゴリ、ホスト数を示すインタラクティブなリストです。

このセクションのすべての「アプリケーション」インスタンスについて、[アプリケーション情報 (Application Information)] のグラフのセットは、デフォルトでは特にアプリケーションプロトコル (DNS、SSH など) を検査します。クライアントアプリケーション (PuTTY や Firefox など) や Web アプリケーション (Facebook や Pandora など) を特に検査するように [アプリケーション情報 (Application Information)] セクションを設定することもできます。

## [アプリケーション情報 (Application Information)] セクションへのフォーカスの移動

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

**ステップ 1** [分析 (Analysis)] > [コンテキスト エクスプローラ (Context Explorer)] を選択します。

**ステップ 2** [アプリケーション プロトコル情報 (Application Protocol Information) ] セクションにポインタを重ねます。

(注) 以前に同じ Context Explorer セッションでこの設定を変更している場合は、セクションタイトルが [クライアントアプリケーション情報 (Client Application Information) ] または [Web アプリケーション情報 (Web Application Information) ] と表示されることがある点に注意してください。

**ステップ 3** [アプリケーションプロトコル (Application Protocol) ]、[クライアントアプリケーション (Client Application) ]、または [Web アプリケーション (Web Application) ] をクリックします。

## [リスク/ビジネスとの関連性とアプリケーション別トラフィック (Traffic by Risk/Business Relevance and Application) ] グラフ

[リスク/ビジネスとの関連性とアプリケーション別トラフィック (Traffic by Risk/Business Relevance and Application) ] グラフはドーナツ形式で、モニタ対象ネットワークで検出されたアプリケーショントラフィックを、アプリケーションの推定リスク (デフォルト) または推定のビジネスとの関連性 (ビジネス関連度) ごとの割合で表示します。内側のリングは推定のリスクまたはビジネスとの関連性レベル (Medium や High など) ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション (SSH や NetBIOS など) ごとに分割されます。まれにしか検出されないアプリケーションは [その他 (Other) ] にまとめられます。

このグラフは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Context Explorer の時間範囲を変更しても、グラフは変化しません。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。



**ヒント** グラフに制約を適用して、ビジネスとの関連性とアプリケーションごとにトラフィックが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Business Relevance] をクリックします。デフォルトビューに戻すには [リスク (Risk) ] をクリックします。このグラフは、Context Explorer から外部へ移動しても、デフォルトの [リスク (Risk) ] ビューに戻ります。



(注) 侵入イベントの情報でフィルタ処理を実行すると、[リスク/ビジネスとの関連性とアプリケーション別トラフィック (Traffic by Risk/Business Relevance and Application) ] グラフは非表示になります。

このグラフのデータは、主に [接続イベント (Connection Events) ] テーブルと [アプリケーション統計 (Application Statistics) ] テーブルから取得されます。

## [リスク/ビジネスとの関連度別侵入イベントおよびアプリケーション (Intrusion Events by Risk/Business Relevance and Application) ] グラフ

[リスク/ビジネスとの関連度別侵入イベントおよびアプリケーション (Intrusion Events by Risk/Business Relevance and Application) ] グラフはドーナツ形式であり、モニタ対象ネットワークで検出された侵入イベントと、これらのイベントに関連するアプリケーションを、アプリケーションの推定リスク (デフォルト) または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定のリスクまたはビジネスとの関連性レベル (Medium や High など) ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション (SSH や NetBIOS など) ごとに分割されます。稀に検出されるアプリケーションは [その他 (Other) ] にまとめられます。

ドーナツグラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされるか、または (該当する場合には) アプリケーション情報が表示されます。



**ヒント** グラフに制約を適用して、ビジネスとの関連性とアプリケーションごとに侵入イベントが表示されるようにするには、グラフにポインタを置き、表示されるトグルボタンの [ビジネスとの関連性 (Business Relevance) ] をクリックします。デフォルトビューに戻すには [リスク (Risk) ] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [リスク (Risk) ] ビューに戻ることに注意してください。

このグラフのデータは主に [侵入イベント (Intrusion Events) ] テーブルと [アプリケーションの統計 (Application Statistics) ] テーブルから取得されます。

## [リスク/ビジネスとの関連度別ホストおよびアプリケーション (Hosts by Risk/Business Relevance and Application) ] グラフ

[リスク/ビジネスとの関連度別ホストおよびアプリケーション (Hosts by Risk/Business Relevance and Application) ] グラフはドーナツ形式であり、モニタ対象ネットワークで検出されたホストと、これらのホストに関連するアプリケーションを、アプリケーションの推定リスク (デフォルト) または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル ([中 (Medium) ] または [高 (High) ] など) ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション ([SSH] または [NetBIOS] など) ごとに分割されます。非常に少数のアプリケーションは [その他 (Other) ] にまとめられます。

ドーナツグラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。



**ヒント** グラフに制約を適用して、ビジネスとの関連性とアプリケーションに基づいてホストが表示されるようにするには、グラフにポインタを置き、表示されるトグルボタンの [ビジネスとの関連性 (Business Relevance) ] をクリックします。デフォルトビューに戻すには [リスク (Risk) ] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [リスク (Risk) ] ビューに戻ることに注意してください。

このグラフのデータは主に [アプリケーション (Applications)] テーブルから取得されます。

## アプリケーション詳細リスト

[アプリケーション情報 (Application Information)] セクション下部に表示される [アプリケーション詳細リスト (Application Details List)] は、モニタ対象ネットワークで検出される各アプリケーションの推定リスク、推定ビジネス関連度、カテゴリ、ホスト数の情報を示す表です。アプリケーションは、関連ホスト数の降順でリストされます。

[アプリケーション詳細リスト (Application Details List)] テーブルをソートすることはできませんが、テーブル内の項目をクリックして、その情報でフィルタリングまたはドリルダウンしたり、(該当する場合に) アプリケーション情報を表示したりすることができます。このテーブルのデータは主に [アプリケーション (Applications)] テーブルから取得されます。

このリストは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Explorer の時間範囲を変更しても、リストは変化しません。

## [セキュリティ インテリジェンス (Security Intelligence)] セクション

Context Explorer の [セキュリティ インテリジェンス (Security Intelligence)] セクションには、3 つのインタラクティブな棒グラフが表示されます。これらのグラフには、モニタ対象ネットワーク上の、ブラックリストに登録されているトラフィック、または Security Intelligence によってモニタされているトラフィックの全体の概要が示されます。これらのグラフでは、カテゴリ、送信元 IP アドレス、および宛先 IP アドレスに基づいてそれらのトラフィックがソートされ、トラフィックの量 (KB/秒) と該当する接続の数の両方が表示されます。

## [カテゴリ別セキュリティ インテリジェンス トラフィック (Security Intelligence Traffic by Category)] グラフ

[カテゴリ別セキュリティ インテリジェンス トラフィック (Security Intelligence Traffic by Category)] グラフは棒グラフ形式で、モニタ対象ネットワーク上のトラフィックのセキュリティ インテリジェンスの上位のカテゴリに関する、ネットワーク トラフィック カウント (KB/秒) と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続 データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。



(注) 侵入イベントの情報でフィルタ処理を実行すると、[カテゴリ別セキュリティ インテリジェンス トラフィック (Security Intelligence Traffic by Category)] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント (Security Intelligence Events)] テーブルから取得されます。



## [送信元 IP 別セキュリティ インテリジェンス トラフィック (Security Intelligence Traffic by Source IP) ] グラフ

[送信元 IP 別セキュリティ インテリジェンス トラフィック (Security Intelligence Traffic by Source IP) ] グラフは棒グラフ形式で、モニタ対象ネットワーク上でセキュリティ インテリジェンスによってモニタされたトラフィックの上位の送信元 IP アドレスに関する、ネットワーク トラフィック カウント (KB/秒) と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。



- (注) 侵入イベントの情報でフィルタ処理を実行すると、[送信元 IP 別セキュリティ インテリジェンス トラフィック (Security Intelligence Traffic by Source IP) ] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント (Security Intelligence Events) ] テーブルから取得されます。

## [宛先 IP 別セキュリティ インテリジェンス トラフィック (Security Intelligence Traffic by Destination IP) ] グラフ

[宛先 IP 別セキュリティ インテリジェンス トラフィック (Security Intelligence Traffic by Destination IP) ] グラフは棒グラフ形式で、モニタ対象ネットワーク上でセキュリティ インテリジェンスによってモニタされたトラフィックの上位の宛先 IP アドレスに関する、ネットワーク トラフィック カウント (KB/秒) と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。



- (注) 侵入イベントの情報でフィルタ処理を実行すると、[宛先 IP 別セキュリティ インテリジェンス トラフィック (Security Intelligence Traffic by Destination IP) ] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント (Security Intelligence Events) ] テーブルから取得されます。

## [侵入情報 (Intrusion Information) ] セクション

Context Explorer の [侵入情報 (Intrusion Information) ] セクションには 6 つのインタラクティブ グラフと 1 つの表形式リストが表示されます。これらのグラフとリストは、モニタ対象ネットワークの侵入イベントの概要 (侵入イベントに関連付けられている影響レベル、攻撃元、攻撃対象先、ユーザ、優先レベル、およびセキュリティゾーンと、侵入イベントの分類、優先度、カウントを示す詳細なリスト) を示します。

## [影響別侵入イベント (Intrusion Events by Impact) ] グラフ

[影響別侵入イベント (Intrusion Events by Impact) ] グラフは円グラフ形式であり、モニタ対象ネットワークの侵入イベントを推定影響レベル (0~4) のグループごとの割合で表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [侵入イベント (Intrusion Events) ] テーブルと [IDS 統計情報 (IDS Statistics) ] テーブルから取得されます。

## [上位の攻撃者 (Top Attackers) ] グラフ

[上位の攻撃者 (Top Attackers) ] グラフは棒グラフ形式で、モニタ対象ネットワーク上の (侵入イベントを発生させた) 上位の各攻撃元ホスト IP アドレスの侵入イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。

このグラフのデータは、主に [侵入イベント (Intrusion Events) ] テーブルから取得されます。

## [上位のユーザ (Top Users) ] グラフ

[上位のユーザ (Top Users) ] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最大侵入イベント数に関連付けられたユーザと、イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。

このグラフのデータは、主に [IDS のユーザ統計 (IDS User Statistics) ] テーブルと [侵入イベント (Intrusion Events) ] テーブルから取得されます。このグラフには、権限のあるユーザのデータが表示されます。

## [優先度別侵入イベント (Intrusion Events by Priority) ] グラフ

[優先度別侵入イベント (Intrusion Events by Priority) ] グラフは円グラフ形式であり、モニタ対象ネットワークの侵入イベントを、推定優先度レベル ([高 (High) ]、[中 (Medium) ]、[低 (Low) ] など) のグループごとの割合で表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。

このグラフのデータは、主に [侵入イベント (Intrusion Events) ] テーブルから取得されます。

## [上位のターゲット (Top Targets) ] グラフ

[上位のターゲット (Top Targets) ] グラフは棒グラフ形式で、モニタ対象ネットワーク上の (侵入イベントを発生させた接続で攻撃対象となった) 上位のターゲットホスト (攻撃対象ホスト) の IP アドレスの侵入イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。

このグラフのデータは、主に [侵入イベント (Intrusion Events) ] テーブルから取得されます。

## [入力/出力の上位セキュリティゾーン (Top Ingress/Egress Security Zones) ] グラフ

[入力/出力の上位セキュリティゾーン (Top Ingress/Egress Security Zones) ] グラフは棒グラフ形式で、モニタ対象ネットワーク上で設定されている各セキュリティゾーン (グラフ設定に応じて入力または出力) に関連付けられている侵入イベントの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。



### ヒント

グラフに制約を適用して、出力セキュリティゾーンのトラフィックだけが表示されるにするには、グラフにポインタを置き、表示されたトグルボタンの [出力 (Egress) ] をクリックします。デフォルトのビューに戻すには、[入力 (Ingress) ] をクリックします。このグラフは、Context Explorer から外部へ移動しても、デフォルトの [入力 (Ingress) ] ビューに戻ります。

このグラフのデータは、主に [侵入イベント (Intrusion Events) ] テーブルから取得されます。

このグラフは、必要に応じて、入力 (デフォルト) セキュリティゾーン情報または出力セキュリティゾーン情報のいずれかを表示するように設定できます。

## 侵入イベント詳細リスト

[侵入情報 (Intrusion Information) ] セクション下部に表示される [イベント詳細リスト (Event Details List) ] は、モニタ対象ネットワークで検出された各侵入イベントの分類、推定優先度、イベント数の情報を示すテーブルです。イベントは、イベント数の降順でリストされます。

[イベント詳細リスト (Event Details List) ] テーブルはソートできませんが、テーブルの項目をクリックして、その情報でフィルタリングまたはドリルダウンすることができます。このテーブルのデータは主に [侵入イベント (Intrusion Events) ] テーブルから取得されます。

## [ファイル情報 (Files Information) ] セクション

Context Explorer の [ファイル情報 (Files Information) ] セクションには、6つのインタラクティブグラフが表示されます。これらのグラフは、モニタ対象ネットワーク上のファイルとマルウェアイベントの概要を示します。

このうち5つのグラフには、AMP for Firepower データ (ネットワークトラフィックで検出されたファイルのファイルタイプ、ファイル名、マルウェアの性質、これらのファイルを送信 (アップロード) および受信 (ダウンロード) したホスト) が表示されます。最後のグラフには、AMP for Firepower または AMP for Endpoints のどちらかで検出されたかにかかわらず、組織内で検出されたすべてのマルウェア脅威が表示されます。



(注) 侵入情報でフィルタリングすると、[ファイル情報 (File Information) ] セクション全体が非表示になります。

## [上位のファイルタイプ (Top File Types) ] グラフ

[上位のファイルタイプ (Top File Types) ] グラフはドーナツ グラフ形式で、ネットワーク トラフィックで検出されたファイルタイプの割合のビュー (外側のリング) と、ファイルカテゴリーのグループごとの割合のビュー (内側のリング) を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイルイベント (File Events) ] テーブルから取得されます。

## [上位のファイル名 (Top File Names) ] グラフ

[上位のファイル名 (Top File Names) ] グラフは棒グラフ形式で、ネットワーク トラフィックで検出された上位の一意のファイル名の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイルイベント (File Events) ] テーブルから取得されます。

## [性質別ファイル (Files by Disposition) ] グラフ

[性質別ファイル (Files by Disposition) ] グラフは円グラフ形式であり、AMP for Firepower で検出されたファイルのマルウェアの性質の割合のビューを表示します。Firepower Management Center がマルウェアクラウド検索を行ったファイルにのみ性質が設定されることに注意してください。クラウド検索をトリガーしなかったファイルには、N/A という性質が設定されます。Unavailable という性質は、Firepower Management Center がマルウェアクラウド検索を実行できなかったことを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイルイベント (File Events) ] テーブルから取得されます。

## [送信ファイル数上位のホスト (Top Hosts Receiving Files) ] グラフ

[送信ファイル数上位のホスト (Top Hosts Receiving Files) ] グラフは棒グラフ形式で、ネットワーク トラフィックで検出された、送信ファイル数上位のホストの IP アドレスに関するファイルの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。



**ヒント** グラフに制約を適用して、マルウェアを送信したホストだけが表示されるようにするには、グラフにポインタを置き、表示されたトグルボタンの[マルウェア (Malware) ]をクリックします。デフォルトのファイルのビューに戻すには、[ファイル (Files) ]をクリックします。このグラフは、Context Explorer から外部へ移動してもデフォルトのファイルのビューに戻ります。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に[ファイルイベント (File Events) ]テーブルから取得されます。

## [受信ファイル数上位のホスト (Top Hosts Receiving Files) ]グラフ

[受信ファイル数上位のホスト (Top Hosts Receiving Files) ]グラフは棒グラフ形式で、ネットワークトラフィックで検出された、受信ファイル数上位のホストの IP アドレスに関するファイルの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。



**ヒント** グラフに制約を適用して、マルウェアを受信したホストだけが表示されるようにするには、グラフにポインタを置き、表示されたトグルボタンの[マルウェア (Malware) ]をクリックします。デフォルトのファイルのビューに戻すには、[ファイル (Files) ]をクリックします。このグラフは、Context Explorer から外部へ移動してもデフォルトのファイルのビューに戻ります。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に[ファイルイベント (File Events) ]テーブルから取得されます。

## [上位のマルウェア検出 (Top Malware Detections) ]グラフ

[上位のマルウェア検出 (Top Malware Detections) ]グラフは棒グラフ形式で、AMP for Firepower と AMP for Endpoints のいずれによるものかに関係なく、組織で検出された上位のマルウェア脅威の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリルダウンが実行されます。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に[ファイルイベント (File Events) ]テーブルと[マルウェア イベント (Malware Events) ]テーブルから取得されます。

## [地理位置情報 (Geolocation Information)] セクション

Context Explorer の [地理位置情報 (Geolocation Information)] セクションには、3つのインタラクティブなドーナツグラフが表示されます。これらのグラフは、モニタ対象ネットワークのホストがデータを交換している国の概要（イニシエータ国またはレスポンド国ごとの固有接続数、送信元または宛先の国ごとの侵入イベント数、および送信側または受信側の国ごとのファイルイベント数）を示します。

### [イニシエータ/レスポンドの国別接続 (Connections by Initiator/Responder Country)] グラフの表示

[イニシエータ/レスポンドの国別接続 (Connections by Initiator/Responder Country)] グラフはドーナツグラフ形式であり、ネットワーク上での接続にイニシエータ（デフォルト）またはレスポンドとして関わる国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。



**ヒント** グラフに制約を適用して、接続でレスポンドとなっている国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグルボタンの [レスポンド (Responder)] をクリックします。デフォルトビューに戻すには [イニシエータ (Initiator)] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [イニシエータ (Initiator)] ビューに戻ることに注意してください。

このグラフのデータは主に [接続サマリー データ (Connection Summary Data)] テーブルから取得されます。

### [送信元/宛先国別侵入イベント (Intrusion Events by Source/Destination Country)] グラフ

[送信元/宛先国別侵入イベント (Intrusion Events by Source/Destination Country)] グラフはドーナツグラフ形式であり、ネットワーク上の侵入イベントにイベントの送信元（デフォルト）または宛先として関わる国の割合を表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。



**ヒント** グラフに制約を適用して、侵入イベントの宛先となっている国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグルボタンの [宛先 (Destination)] をクリックします。デフォルトビューに戻すには [送信元 (Source)] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [送信元 (Source)] ビューに戻ることに注意してください。

このグラフのデータは主に [侵入イベント (Intrusion Events)] テーブルから取得されます。

## [送信側/受信側の国別ファイルイベント (File Events by Sending/Receiving Country)] グラフ

[送信側/受信側の国別ファイルイベント (File Events by Sending/Receiving Country)] グラフはドーナツグラフ形式であり、ネットワーク上のファイルイベントでファイルの送信側 (デフォルト) または受信側として検出された国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。



### ヒント

グラフに制約を適用して、ファイルを受信する国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグルボタンの [受信者 (Receiver)] をクリックします。デフォルトビューに戻すには [送信者 (Sender)] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [送信者 (Sender)] ビューに戻ることに注意してください。

このグラフのデータは主に [ファイルイベント (File Events)] テーブルから取得されます。

## [URL 情報 (URL Information)] セクション

Context Explorer の [URL 情報 (URL Information)] セクションには、3つのインタラクティブな棒グラフが表示されます。これらのグラフには、モニタ対象ネットワーク上のホストがデータを交換するために使用する URL の全体の概要 (URL に関連付けられているトラフィックと固有接続数を個々の URL、URL カテゴリ、および URL レピュテーションでソートしたもの) が示されます。URL 情報でフィルタ処理を実行することはできません。



(注) 侵入イベントの情報でフィルタ処理を実行すると、[URL 情報 (URL Information)] セクション全体が非表示になります。

このグラフで URL カテゴリとレピュテーションデータを含めるには、URL フィルタリングライセンスを所有している必要があることに注意してください。

## [URL 別トラフィック (Traffic by URL)] グラフ

[URL 別トラフィック (Traffic by URL)] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最も要求される上位 15 の URL のネットワークトラフィックカウント (KB/秒) と固有接続数を表示します。リストされた URL ごとに、青色の棒はトラフィックデータ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

**[URL カテゴリ別トラフィック (Traffic by URL Category) ] グラフ**

- (注) 侵入イベントの情報でフィルタ処理を実行すると、[URL 別トラフィック (Traffic by URL) ] グラフは非表示になります。

このグラフでURLカテゴリとレピュテーションデータを含めるには、URLフィルタリングライセンスを所有している必要があることに注意してください。

このグラフのデータは、主に[接続イベント (Connection Events) ]テーブルから取得されます。

**[URL カテゴリ別トラフィック (Traffic by URL Category) ] グラフ**

[URL カテゴリ別トラフィック (Traffic by URL Category) ] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最も要求される URL カテゴリ (Search Engines や Streaming Media など) のネットワークトラフィックカウント (KB/秒) と固有接続数を表示します。リストされたURLカテゴリごとに、青色の棒はトラフィックデータ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポイントを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。



- (注) 侵入イベントの情報でフィルタ処理を実行すると、[URL カテゴリ別トラフィック (Traffic by URL Category) ] グラフは非表示になります。

このグラフでURLカテゴリとレピュテーションデータを含めるには、URLフィルタリングライセンスを所有している必要があることに注意してください。

このグラフのデータは、主に[URL統計 (URL Statistics) ]テーブルと[接続イベント (Connection Events) ]テーブルから取得されます。

**[URL レピュテーション別トラフィック (Traffic by URL Reputation) ] グラフ**

[URL レピュテーション別トラフィック (Traffic by URL Reputation) ] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最も要求される URL レピュテーショングループ (Well known や Benign sites with security risks など) のネットワークトラフィックカウント (KB/秒) と固有接続数を表示します。リストされた URL レピュテーションごとに、青色の棒はトラフィックデータ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポイントを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。



- (注) 侵入イベントの情報でフィルタ処理を実行すると、[URL レピュテーション別トラフィック (Traffic by URL Reputation) ] グラフは非表示になります。

このグラフでURLカテゴリとレピュテーションデータを含めるには、URLフィルタリングライセンスを所有している必要があることに注意してください。



このグラフのデータは、主に [URL 統計 (URL Statistics)] テーブルと [接続イベント (Connection Events)] テーブルから取得されます。

## Context Explorer の更新

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

Context Explorer は、表示している情報を自動的に更新しません。新しいデータを組み込むには、Explorer を手動で更新する必要があります。

Context Explorer 自体をリロードすると (ブラウザプログラムの更新または Context Explorer から外部へ移動した後に戻る操作などによるリロード)、すべての表示情報が更新されますが、セクション設定 (入力 (Ingress) /出力 (Egress) グラフや [アプリケーション情報 (Application Information)] セクションなど) に対して行った変更は保持されず、また、読み込みに時間がかかることがある点に注意してください。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

**ステップ 1** [分析 (Analysis)] > [コンテキスト エクスプローラ (Context Explorer)] を選択します。

**ステップ 2** 右上にある [リロード (Reload)] をクリックします。

[リロード (Reload)] ボタンは、更新が終了するまでグレー表示になります。

## Context Explorer の時間範囲の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

過去 1 時間 (デフォルト) から過去 1 年までの期間を反映するように、Context Explorer の時間範囲を設定できます。時間範囲を変更しても、Context Explorer は変更を反映するために自動的に更新されないことに注意してください。新しい時間範囲を適用するには、Explorer を手動で更新する必要があります。

時間範囲の変更は、Context Explorer から外部に移動したり、ログインセッションを終了しても維持されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

#### 手順

**ステップ 1** [分析 (Analysis)] > [コンテキスト エクスプローラ (Context Explorer)] を選択します。

**ステップ 2** [リストを表示 (Show the last)] ドロップダウンリストから、時間範囲を選択します。

**ステップ 3** オプションで、新しい時間範囲のデータを表示するには、[リロード (Reload)] をクリックします。

ヒント [フィルタの適用 (Apply Filters)] をクリックすると、時間範囲の更新が適用されます。

## Context Explorer のセクションの最小化および最大化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

Context Explorer では1つ以上のセクションを最小化して非表示にできます。これは、特定のセクションだけを強調する場合や、ビューをシンプルにしたい場合に便利です。[トラフィックおよび侵入イベント数/時間 (Traffic and Intrusion Event Counts Time)] グラフは最小化できません。

Context Explorer のセクションでは、ページを更新したり、アプライアンスからログアウトしたりしても、設定した最小化または最大化の状態が維持されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

#### 手順

**ステップ 1** [分析 (Analysis)] > [コンテキスト エクスプローラ (Context Explorer)] を選択します。

**ステップ 2** セクションを最小化するには、セクションのタイトルバーにある最小化アイコン (☐) をクリックします。

**ステップ3** セクションを最大化するには、最小化されたセクションのタイトルバーにある最大化アイコン (□) をクリックします。

## Context Explorer データのドリルダウン

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

Context Explorer で許容されている詳細レベルよりもさらに詳細にグラフを調べたりデータをリストしたりするには、当該データのテーブルビューにドリルダウンします。( [一定期間のトラフィックおよび侵入イベント (Traffic and Intrusion Events over Time) ] グラフではドリルダウンできないことに注意してください。) たとえば、[送信元 IP 別のトラフィック (Traffic by Source IP) ] グラフの IP アドレスでドリルダウンすると、[接続イベント (Connection Events) ] 表の [アプリケーション詳細付きの接続 (Connections with Application Details) ] ビューが表示されます。このビューには、選択した送信元 IP アドレスに関連するデータのみが表示されます。

調べるデータのタイプに応じて、コンテキストメニューに追加のオプションが表示されることがあります。特定の IP アドレスに関連付けられているデータポイントの場合、選択した IP アドレスのホストまたは whois 情報を表示するためのオプションが表示されます。特定のアプリケーションに関連付けられているデータポイントの場合、選択したアプリケーションに関するアプリケーション情報を表示するためのオプションが表示されます。特定のユーザに関連付けられているデータポイントの場合、ユーザのユーザプロファイルページを表示するためのオプションが表示されます。侵入イベントのメッセージに関連付けられているデータポイントの場合、そのイベントに関連する侵入ルールに関するルールドキュメントを表示するオプションが表示されます。特定の IP アドレスに関連付けられているデータポイントの場合、そのアドレスをブラックリストまたはホワイトリストに追加するためのオプションが表示されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

- ステップ1** [分析 (Analysis) ] > [コンテキスト エクスプローラ (Context Explorer) ] を選択します。
- ステップ2** [一定期間のトラフィックおよび侵入イベント (Traffic and Intrusion Events over Time) ] 以外の任意のセクションで、調査するデータポイントをクリックします。
- ステップ3** 選択するデータポイントに応じて、表示されるオプションが異なります。
  - テーブルビューでこのデータの詳細を表示するには、[詳細な分析を表示 (Drill into Analysis) ] を選択します。

- 特定の IP アドレスに関連付けられているデータ ポイントを選択している場合に、関連するホストに関する詳細情報を参照するには、[ホスト情報の表示 (View Host Information)] を選択します。
- 特定の IP アドレスのデータ ポイントを選択している場合に、そのアドレスで whois 検索を行うには、[Whois] を選択します。
- 特定のアプリケーションに関連付けられているデータ ポイントを選択している場合に、そのアプリケーションに関する詳細情報を参照するには、[アプリケーション情報の表示 (View Application Information)] を選択します。
- 特定のユーザに関連付けられているデータ ポイントを選択している場合に、そのユーザに関する詳細情報を参照するには、[ユーザ情報の表示 (View User Information)] を選択します。
- 特定の侵入イベント メッセージに関連付けられているデータ ポイントを選択している場合に、関連する侵入ルールに関する詳細情報を参照するには、[ルール ドキュメントの表示 (View Rule Documentation)] を選択します。
- 特定の IP アドレスに関連付けられているデータ ポイントを選択している場合に、Security Intelligence グローバルブラックリストまたはホワイトリストにその IP アドレスを追加するには、[今すぐブラックリストに追加 (Blacklist Now)] または [今すぐホワイトリストに追加 (Whitelist Now)] のいずれか該当するオプションを選択します。

## コンテキスト エクスプローラのフィルタ

コンテキスト エクスプローラに最初に表示される基本的で広範なデータをフィルタリングして、ネットワーク上のアクティビティのより詳細な状況を把握することができます。フィルタは URL 情報以外のすべての種類の Firepower システム データに対応し、除外と包含がサポートされており、Context Explorer のグラフ データ ポイントをクリックするだけですぐに適用でき、Explorer 全体に反映されます。一度に最大 20 のフィルタを適用できます。

コンテキスト エクスプローラ データにフィルタを追加する方法はいくつかあります。

- [フィルタの追加 (Add Filter)] ダイアログを使用する。
- コンテキストメニューを使用する (エクスプローラのデータポイントを選択する場合)。
- 特定の詳細表示ページ ([アプリケーションの詳細 (Application Detail)]、[ホストプロファイル (Host Profile)]、[ルールの詳細 (Rule Detail)]、[ユーザプロファイル (User Profile)]) に表示されるテキストリンクを使用する。これらのリンクをクリックすると、コンテキストエクスプローラが自動的に開き、詳細表示ページの当該データに基づいてコンテキストエクスプローラがフィルタリングされます。たとえば、ユーザ jenkins のユーザ詳細ページで [コンテキスト エクスプローラ (Context Explorer)] リンクをクリックすると、エクスプローラにはそのユーザに関連するデータだけが表示されます。

ファイルタイプの中には、相互に互換性がないタイプがあります。たとえば、侵入イベント関連のフィルタ (**Device** や **Inline Result** など) を、接続イベント関連フィルタ (**Access Control Action** など) と同時に適用することはできません。これは、システムでは接続イベントデー

タを侵入イベントデータによってソートできないためです。互換性のないフィルタの同時適用はシステムによって自動的に防止されます。互換性の問題が存在する場合、より後に適用された方のフィルタタイプと互換性のないタイプのフィルタは非表示になります。

複数のフィルタがアクティブな場合、同じデータタイプの値はOR検索条件として扱われます。つまり、いずれか1つの値と一致するデータがすべて表示されます。異なるデータタイプの値はAND検索条件として扱われます。つまり、データは各フィルタデータタイプの1つ以上の値と一致する必要があります。たとえば、Application: 2channel、Application: Reddit、およびUser: edickinsonというフィルタセットで表示されるデータは、ユーザ edickinsonに関連付けられており、かつアプリケーション 2channel またはアプリケーション Redditに関連付けられている必要があります。

マルチドメイン展開では、先祖ドメインでコンテキストエクスプローラを表示している場合に複数の子孫ドメインでフィルタリングできます。この場合、IP Address フィルタも追加する場合は注意してください。システムは、各リーフドメインに個別のネットワークマップを作成します。実際のIPアドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

表示されるデータは、管理対象デバイスのライセンスおよび展開方法やデータを提供する機能を設定するかどうかなどの要因によって異なります。



(注) フィルタは、必要とする正確な Firepower データ コンテキストをいつでも取得できるシンプルかつ俊敏性に優れたツールとして機能します。永続的に設定するものではなく、コンテキストエクスプローラから外部に移動するか、セッションを終了すると消去されます。後で使用するためにフィルタ設定を保存するには、[フィルタ処理されたコンテキストエクスプローラビューの保存 \(2388 ページ\)](#) を参照してください。

## データタイプフィールドオプション

次の表に、フィルタとして使用できるデータタイプと、各データタイプの例と説明を示します。

表 250: フィルタ データタイプ

タイプ (Type)	値の例	定義 (Definition)
アクセス コントロール アクション (Access Control Action)	Allow、Block	トラフィックを許可またはブロックするためにアクセス コントロール ポリシーにより実行されるアクション。
アプリケーション カテゴリ (Application Category)	web browser、email	アプリケーションの主要機能の一般的な分類。
アプリケーション	Facebook、HTTP	アプリケーションの名前。

タイプ (Type)	値の例	定義 (Definition)
アプリケーションのリスク (Application Risk)	Very High、Medium	アプリケーションの推定セキュリティリスク。
アプリケーションタグ (Application Tag)	encrypts communications、sends mail	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを使用できます (タグを使用しないことも可能です)。
アプリケーションタイプ (Application Type)	Client、Web Application	アプリケーションタイプ (アプリケーションプロトコル、クライアント、または Web アプリケーション)。
ビジネスとの関連性 (Business Relevance)	Very Low、High	(娯楽ではない) ビジネスアクティビティに対するアプリケーションの推定関連度。
大陸 (Continent)	North America、Asia	モニタ対象ネットワークで検出されたルーティング可能な IP アドレスに関連付けられている大陸。
国 (Country)	Canada、Japan	モニタ対象ネットワークで検出されたルーティング可能な IP アドレスに関連付けられている国。
Device	device1.example.com、192.168.1.3	モニタ対象ネットワーク上のデバイスの名前または IP アドレス。
ドメイン (Domain)	Asia Division、Europe Division	グラフ表示するネットワークアクティビティを行うデバイスのドメイン。このデータタイプはマルチドメイン展開の場合にのみ存在します。
イベントの分類 (Event Classification)	Potential Corporate Policy Violation、Attempted Denial of Service	侵入イベントの簡単な説明。侵入イベントをトリガーしたルール、デコーダ、またはプリプロセッサにより決定されます。
イベントメッセージ (Event Message)	dns response、P2P	イベントによって生成されるメッセージ。イベントをトリガーしたルール、デコーダ、またはプリプロセッサにより決定されます。
ファイル傾向 (File Disposition)	Malware、Clean	Firepower Management Center によるマルウェアクラウド検索の実行対象ファイルの性質。

タイプ (Type)	値の例	定義 (Definition)
ファイル名	Packages.bz2	ネットワークトラフィックで検出されたファイルの名前。
ファイル SHA256 (File SHA256)	任意の 32 ビット文字列	Firepower Management Center によるマルウェアクラウド検索の実行対象ファイルの SHA-256 ハッシュ値。
ファイルタイプ (File Type)	GZ、SWF、MOV	ネットワークトラフィックで検出されたファイルのタイプ。
ファイルタイプカテゴリ (File Type Category)	Archive、Multimedia、Executables	ネットワークトラフィックで検出されたファイルのタイプの一般カテゴリ。
[IPアドレス (IP Address) ]	192.168.1.3、2001:0db8:85a3::0000/24	IPv4 または IPv6 のアドレス、アドレス範囲、またはアドレスブロック。  IPアドレスを検索すると、そのアドレスが送信元または宛先のいずれかになっているイベントが返されることに注意してください。
影響レベル (Impact Level)	Impact Level 1、Impact Level 2	モニタ対象ネットワークでのイベントの推定影響レベル。
インライン結果 (Inline Result)	dropped、would have dropped	トラフィックがドロップされたか、ドロップされた可能性があるか、またはシステムによりトラフィックが処理されていないかのいずれかです。
IOC カテゴリ (IOC Category)	High Impact Attack、Malware Detected	トリガーとして使用された侵害の兆候 (IOC) イベントのカテゴリ。
IOC イベントタイプ (IOC Event Type)	exploit-kit、malware-backdoor	特定の侵害の兆候 (IOC) に関連付けられている ID。その兆候をトリガーしたイベントを示します。
マルウェア脅威名 (Malware Threat Name)	W32.Trojan.a6b1	マルウェア脅威の名前。
OS 名 (OS Name)	Windows、Linux	オペレーティングシステムの名前。
OS Version	XP、2.6	オペレーティングシステムの特定のバージョン。
[プライオリティ (Priority) ]	high、low	イベントの推定緊急度。

タイプ (Type)	値の例	定義 (Definition)
セキュリティインテリジェンスカテゴリ (Security Intelligence Category)	Malware、Spam	セキュリティインテリジェンスにより判別される危険なトラフィックのカテゴリ。
セキュリティゾーン	My Security Zone、Security Zone X	トラフィックが分析されたインターフェイスのセット。インライン展開の場合は、トラフィックが通過するインターフェイスのセット。
SSL	yes、no	SSL暗号化トラフィックまたはTLS暗号化トラフィック。
ユーザ (User)	wsmith、mtwain	モニタ対象ネットワーク上のホストにログインしたユーザの ID。

## [フィルタの追加 (Add Filter) ] ウィンドウからのフィルタの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

この手順を使用して、[フィルタの追加 (Add Filter) ] ウィンドウでフィルタを最初から作成します。(コンテキストメニューを使用して、クイックフィルタを作成することもできます。)

Context Explorer の左上にある [フィルタ (Filters) ] の下のプラスアイコン (+) をクリックすると表示される [フィルタの追加 (Add Filter) ] ウィンドウには、次の 2 つのフィールドだけが表示されます。

- [データタイプ (Data Type) ] ドロップダウンリストには、Context Explorer に制約を適用するために使用できる多数の Firepower システムデータタイプが含まれています。データタイプの選択後に、そのタイプの固有の値を [フィルタ (Filter) ] フィールドに入力します (たとえば、[大陸 (Continent) ] タイプの場合は値 [アジア (Asia) ] など)。ユーザ支援のため、[フィルタ (Filter) ] フィールドでは、選択したデータタイプのさまざまな値の例がグレー表示で示されます。(フィールドにデータを入力すると、これらは消去されます。)
- [フィルタ (Filter) ] フィールドには、イベント検索と同様に、\* や ! などの特殊検索パラメータを入力できます。フィルタパラメータの前に ! 記号を付けることで排他的なフィルタを作成できます。





(注) 追加したフィルタは自動的に適用されません。Context Explorer でフィルタを表示するには、[フィルタの適用 (Apply Filters)] をクリックする必要があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

- ステップ 1 [分析 (Analysis)] > [コンテキスト エクスプローラ (Context Explorer)] を選択します。
- ステップ 2 左上にある [フィルタ (Filter)] の下で、プラスアイコン (+) をクリックします。
- ステップ 3 [データ タイプ (Data Type)] ドロップダウンリストから、フィルタリングの条件として使用するデータ タイプを選択します。
- ステップ 4 [フィルタ (Filter)] フィールドに、フィルタリングの条件として使用するデータ タイプ値を入力します。
- ステップ 5 [OK] をクリックします。
- ステップ 6 オプションで、前述の手順を繰り返し、必要なフィルタセットが設定されるまで、フィルタを追加します。
- ステップ 7 [フィルタの適用 (Apply Filters)] をクリックします。

関連トピック

- [データ タイプ フィールド オプション \(2383 ページ\)](#)
- [検索の制約 \(2468 ページ\)](#)

## コンテキストメニューからのクイックフィルタの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

Context Explorer のグラフとリストデータを詳しく調べるときに、データ ポイントをクリックし、コンテキストメニューを使用してそのデータに基づいてフィルタ (包含または除外) を簡単に作成できます。コンテキストメニューを使用して、[アプリケーション (Application)]、[ユーザ (User)]、[侵入イベントメッセージ (Intrusion Event Message)] データタイプの情報、あるいは任意の個別ホストでフィルタリングする場合、フィルタウィジェットには、そのデータタイプの該当する詳細ページ (アプリケーションデータの場合は[アプリケーションの詳細 (Application Detail)] など) にリンクするウィジェット情報アイコンが表示されます。URL データではフィルタリングできないことに注意してください。

特定のグラフまたはリストのデータを詳しく調査する場合にもコンテキストメニューを使用できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

#### 手順

---

**ステップ 1** [分析 (Analysis)] > [コンテキスト エクスプローラ (Context Explorer)] を選択します。

**ステップ 2** [一定期間のトラフィックおよび侵入イベント (Traffic and Intrusion Events over Time)] セクションと URL データを含むセクション以外の Explorer セクションで、フィルタリングするデータポイントをクリックします。

**ステップ 3** 次の 2 つの対処法があります。

- このデータにフィルタを追加するには、[フィルタの追加 (Add Filter)] をクリックします。
- このデータに除外フィルタを追加するには、[除外フィルタの追加 (Add Exclude Filter)] をクリックします。このフィルタが適用されると、除外された値に関連付けられていないすべてのデータが表示されます。除外フィルタでは、フィルタ値の前に感嘆符 (!) が表示されます。

---

## フィルタ処理されたコンテキスト エクスプローラ ビューの保存

コンテキストエクスプローラから外部に移動した後、またはセッションを終了した後に、コンテキストエクスプローラのフィルタ設定を保持するには、適切なフィルタを適用したコンテキストエクスプローラのブラウザブックマークを作成します。適用されるフィルタはコンテキストエクスプローラ ページ URL に組み込まれているので、そのページのブックマークを読み込むと、対応するフィルタも読み込まれます。

#### 手順

---

適切なフィルタが適用されたコンテキスト エクスプローラのブラウザブックマークを作成します。

---

## フィルタ データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

**ステップ 1** [分析 (Analysis)] > [コンテキスト エクスプローラ (Context Explorer)] を選択します。

**ステップ 2** 該当するフィルタ ウィジェットの情報アイコン (i) をクリックします。

## フィルタの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

### 手順

**ステップ 1** [分析 (Analysis)] > [コンテキスト エクスプローラ (Context Explorer)] を選択します。

**ステップ 2** 左上の [フィルタ (Filters)] の下で、任意のフィルタ ウィジェットのクリアアイコン (✖) をクリックします。

**ヒント** すべてのフィルタを一括削除するには、[クリア (Clear)] ボタンをクリックします。





## 第 98 章

# ネットワーク マップの使用

ここでは、ネットワーク マップの使用方法について説明します。

- [ネットワーク マップ \(2391 ページ\)](#)
- [カスタム ネットワーク トポロジ \(2399 ページ\)](#)

## ネットワーク マップ

Firepower システムは、ネットワークを通じて送信されるトラフィックをモニタし、トラフィック データを復号化してから、設定されているオペレーティング システムおよびフィンガープリントとそのデータを比較します。このシステムでは、次にそのデータを使用して、ネットワーク マップというネットワークの詳細な表示を生成します。マルチドメイン展開では、システムはリーフ ドメインごとの個々のネットワーク マップを生成します。

システムは、ネットワーク 検出ポリシーのモニタリングで特定された管理対象デバイスからデータを収集します。管理対象デバイスでは、モニタされたトラフィックから直接ネットワーク アセットを検出したり、処理された NetFlow レコードから間接的にネットワーク アセットを検出したりします。複数のデバイスで同じネットワーク アセットを検出した場合、システムではそれらの情報をまとめてそのアセットの複合表示を生成します。

受動的に検出されるデータを補完するには、次のようにします。

- オープンソースの Nmap™ スキャナを使用してホストをアクティブにスキャンして、そのスキャン結果をネットワーク マップに追加します。
- ホスト入力機能を使用して、サードパーティ製のアプリケーションからホストデータを手動で追加できます。

ネットワーク マップには、検出されたホストとネットワーク デバイスの観点から見たネットワーク トポロジが表示されます。

ネットワーク マップを使用すれば、次のことを行えます。

- ネットワークの全体的なビューを即座に入手できます。

- 実行する分析に適したさまざまなビューを選択できます。ネットワークマップの各ビューの形式は、展開可能なカテゴリおよびサブカテゴリを持つ階層ツリーからなる、同一の形式です。カテゴリをクリックすると、展開して、その下のサブカテゴリが表示されます。
- カスタムトポロジ機能を使用してサブネットを整理して識別できます。たとえば、組織の各部署が異なるサブネットを使用している場合、カスタムトポロジ機能を使用して、それらのサブネットに分かりやすいラベルを割り当てることができます。
- 任意のモニタ対象ホストのホストプロファイルにドリルダウンすれば、詳細情報を表示できます。
- アセットの調査が不要になった場合は、そのアセットを削除できます。



(注) システムは、ネットワークマップから削除されたホストに関連付けられているアクティビティを検出した場合、そのホストをネットワークマップに再度追加します。同様に、削除されたアプリケーションは、システムでアプリケーションの変更（たとえば、Apache Web サーバが新しいバージョンにアップグレードされた場合）を検出すると、ネットワークマップに再度追加されます。システムが特定のホストを脆弱にする変更を検出した場合、それらのホストの脆弱性が再びアクティブにされます。



**ヒント** ネットワークマップからホストまたはサブネットを永続的に除外するには、ネットワーク検出ポリシーを変更します。ロードバランサおよびNATデバイスで過剰なイベントまたは無関係なイベントを生成していることが判明した場合は、それらのデバイスをモニタリングから除外することができます。

#### 関連トピック

[ネットワーク検出ポリシーの設定](#) (2149 ページ)

## ホストのネットワーク マップ

[ホスト (Hosts) ] タブのネットワークマップには、ホスト数と、ホストのIPアドレスとMACアドレスのリストが表示されます。各アドレスまたはアドレスの一部は、次のレベルへのリンクです。このネットワークマップビューは、ホストに1つのIPアドレスまたは複数のIPアドレスがあるかを問わず、システムによって検出されたすべての一意のホスト数を表示します。

ホストのネットワークマップを使用して、サブネットによって階層ツリーに整理されたネットワークのホストを参照でき、特定のホストのホストプロファイルにドリルダウンできます。

システムは、ホストをエクスポートされたNetFlowレコードからネットワークマップに追加できますが、これらのホストに使用できる情報は限られます ([NetFlow データと管理対象デバイスデータの違い](#) (2028 ページ) を参照)。

ネットワークのカスタムトポロジを作成して、サブネットに意味のあるラベル（部門名など）を割り当てることができます。これはホストのネットワークマップで表示されます。また、カスタムトポロジで指定した組織に基づいてホストのネットワークマップを表示することもできます。

ホストのネットワークマップからネットワーク全体、サブネット、または個々のホストを削除できます。ホストがネットワークに接続されていないことがわかっている場合など、分析を効率化するために削除できます。システムは削除されたホストに関連付けられたアクティビティを後で検出すると、ネットワークマップにホストを再追加します。ネットワークマップからホストまたはサブネットを永続的に除外するには、ネットワーク検出ポリシーを変更します。



**注意** ネットワーク デバイスをネットワーク マップから削除しないでください。システムがネットワーク トポロジを判断するために必要です。

## ネットワーク デバイスのネットワーク マップ

[ネットワーク デバイス (Network Devices) ] タブのネットワーク マップには、ネットワークの1つのセグメントを別のセグメントに接続するネットワーク デバイス（ブリッジ、ルータ、NAT デバイス、およびロード バランサ）が表示されます。このマップには、IP アドレスで特定されたデバイスと、MAC アドレスで特定されたデバイスがリストされる2つのセクションがあります。

また、このマップには、デバイスに保持されている IP アドレスが1つか複数かに関係なく、システムによって検出されたすべての一意のネットワーク デバイスの数も表示されます。

ネットワークのカスタムトポロジを作成した場合、サブネットに割り当てられているラベルがネットワーク デバイスのネットワーク マップに表示されます。

ネットワーク デバイスを識別するためにシステムで使用される方法には、次のものがあります。

- Cisco Discovery Protocol (CDP) メッセージの分析。ネットワーク デバイスとそれらのタイプを識別できます（シスコ デバイスのみ）。
- スパニングツリープロトコル (STP) の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。

ネットワーク デバイスが CDP を使用して通信している場合、1つ以上の IP アドレスを保持している可能性があります。ネットワーク デバイスが STP を使用して通信している場合は、1つの MAC アドレスのみを保持している可能性があります。

ネットワーク デバイスをネットワーク マップから削除することはできません。これは、システムでそれらの場所を使用してネットワーク トポロジを判断するためです。

ネットワーク デバイスのホスト プロファイルには、[オペレーティング システム (Operating Systems)] セクションではなく [システム (Systems)] セクションがあります。このセクションには、ネットワーク デバイスの背後で検出されたモバイル デバイスすべてのハードウェア プラットフォームが反映された [ハードウェア (Hardware)] 列が含まれています。[システム (Systems)] の下にハードウェア プラットフォームの値が表示され場合、システムは、ネットワーク デバイスの背後で 1 つ以上のモバイル デバイスが検出されたことを示しています。モバイル デバイスはハードウェア プラットフォームの情報を持っていることも、持っていないこともあります。モバイル デバイスではないシステムではハードウェア プラットフォーム情報は検出されないことに注意してください。

## モバイル デバイスのネットワーク マップ

[モバイル デバイス (Mobile Devices)] タブのネットワーク マップには、ネットワークに接続されているモバイル デバイスが表示されます。また、このネットワーク マップには、デバイスに設定されている IP アドレスが 1 つか複数かに関係なく、システムによって検出されたすべての一意のモバイル デバイスの数も表示されます。

各アドレスまたはアドレスの一部分は、次のレベルへのリンクです。また、サブネットまたは IP アドレスを削除することもできます。そして、システムでそのデバイスを再検出すると、そのデバイスをネットワーク マップに再度追加します。

さらに、ドリルダウンしてモバイル デバイスのホスト プロファイルを表示することもできます。

モバイル デバイスを特定するために、システムでは次のことを行います。

- モバイル デバイスのモバイル ブラウザからの HTTP トラフィック内のユーザ エージェントの文字列を分析します。
- 特定のモバイル アプリケーションの HTTP トラフィックをモニタします。

ネットワークのカスタム トポロジを作成した場合、サブネットに割り当てられているラベルがモバイル デバイスのネットワーク マップに表示されます。

## 侵害の兆候のネットワーク マップ

[侵害の兆候 (Indications of Compromise)] タブのネットワーク マップには、ネットワーク上で侵害されたホストが IOS カテゴリ別に編成されて表示されます。影響を受けているホストは各カテゴリの下に表示されます。各アドレスまたはアドレスの一部は、次のレベルへのリンクです。

システムは、ホストのセキュリティ侵害のステータスを判断するために、侵入イベント、セキュリティ インテリジェンス、Cisco Advanced Malware Protection (AMP) を含む複数のソースからのデータを使用します。



[侵害の兆候 (Indications of Compromise)] タブのネットワーク マップから、何らかのセキュリティ侵害を受けたと判断される各ホストのホストプロファイルを表示できます。さらに、IOC カテゴリまたは特定のホストを削除でき (解決済みにする)、これによって当該ホストから IOC タグが削除されます。たとえば、問題が対応済みで、繰り返し発生する可能性が低いと判断した場合に、IOC カテゴリをネットワーク マップから削除できます。

ネットワーク マップのホストや IOC カテゴリを解決済みにしても、ネットワークからは削除されません。システムがその IOC をトリガーする情報を新たに検出すると、解決済みのホストまたは IOC カテゴリはネットワーク マップに再表示されます。

## アプリケーション プロトコルのネットワーク マップ

[アプリケーションプロトコル (Application Protocols)] タブのネットワーク マップには、ネットワークで稼働しているアプリケーションが、アプリケーション名、ベンダー、バージョン、各アプリケーションを実行しているホストを基準とした階層ツリー形式で表示されます。

システムが検出するアプリケーションは、システム ソフトウェアや VDB が更新された場合や、アドオンディテクタをインポートした場合に変わることがあります。各システムまたは VDB アップデートのリリース ノートまたはアドバイザリ テキストには、新規および更新されたディテクタの情報が含まれています。ディテクタを網羅した最新のリストについては、Cisco のサポート サイト (<http://www.cisco.com/cisco/web/support/index.html>) を参照してください。

このネットワーク マップから、特定のアプリケーションを実行している各ホストのホストプロファイルを確認できます。

また、アプリケーションのカテゴリ、すべてのホストで実行されているアプリケーション、あるいは特定のホストで実行されているアプリケーションを削除することもできます。たとえば、あるアプリケーションがホスト上で無効化されているとわかっており、システムによる影響レベルの認定で使用されないようにする場合は、そのアプリケーションをネットワーク マップから削除します。

ネットワーク マップからアプリケーションを削除しても、ネットワークからは削除されません。削除したアプリケーションは、システムがアプリケーションの変更 (たとえば Apache Web サーバが新しいバージョンにアップグレードされた) を検出するか、ユーザがシステムの検出機能を再起動すると、ネットワーク マップに再表示されます。

何を削除するかによって、動作は次のように異なります。

- **アプリケーション カテゴリ** : アプリケーション カテゴリを削除すると、そのアプリケーション カテゴリがネットワーク マップから除去されます。削除したカテゴリの下にあるすべてのアプリケーションは、そのアプリケーションを含むすべてのホストプロファイルから削除されます。

たとえば、[http] を削除した場合、[http] として示されるすべてのアプリケーションがすべてのホストプロファイルから削除され、[http] はネットワーク マップのアプリケーション ビューに表示されなくなります。

- **特定のアプリケーション、ベンダー、バージョン** : これらの要素を削除すると、関連するアプリケーションがネットワーク マップから除去され、そのアプリケーションを含むホストプロファイルからもアプリケーションが除去されます。

たとえば、[http] カテゴリを展開し、[Apache] を削除すると、[Apache] としてリストされているすべてのアプリケーションは、[Apache] の下にリストされているバージョンを問わず、それらを含むホストプロファイルから削除されます。同様に、[Apache] を削除する代わりに、特定のバージョン ([1.3.17] など) を削除すると、影響を受けるホストプロファイルから、選択されたバージョンだけが削除されます。

- 特定の IP アドレス：IP アドレスを削除すると、その IP アドレスがアプリケーション リストから除去され、選択した IP アドレスのホストプロファイルからアプリケーション自体が除去されます。

たとえば、[http]、[Apache]、[1.3.17 (Win32)] の順に展開し、[172.16.1.50:80/tcp] を削除すると、Apache 1.3.17 (Win32) アプリケーションは IP アドレス 172.16.1.50 のホストプロファイルから削除されます。

## [脆弱性 (Vulnerabilities) ] のネットワーク マップ

[脆弱性 (Vulnerabilities) ] タブのネットワーク マップには、システムによってネットワークで検出された脆弱性がレガシーの脆弱性 ID (SVID)、Bugtraq ID、CVE ID、または Snort ID ごとに編成されて表示されます。脆弱性は、デフォルトでは SVID ごとに表示されます。脆弱性は ID 番号順に並べられ、影響を受けるホストが各脆弱性の下にリストされます。

このネットワーク マップから、特定の脆弱性の詳細、および特定の脆弱性の影響を受けるホストのホストプロファイルを表示できます。この情報は、影響を受ける特定のホストに対するその脆弱性によって生じる脅威を評価するために役立ちます。

特定の脆弱性がネットワーク上のホストに該当しないと判断した場合（たとえば、パッチの適用が完了した場合）、その脆弱性を非アクティブ化できます。非アクティブ化された脆弱性はネットワーク マップに表示され続けますが、これまで影響を受けていたそれらのホストの IP アドレスはグレーのイタリック体で表示されます。それらのホストのホストプロファイルには、非アクティブ化された脆弱性は無効と表示されますが、個々のホストについて手動で有効とマークすることができます。

ホスト上のアプリケーションまたはオペレーティングシステムにアイデンティティの競合がある場合、システムは可能性のあるアイデンティティの両方について脆弱性をリスト表示します。アイデンティティの競合が解決された場合、その脆弱性は現在のアイデンティティに関連付けられたままになります。

ネットワーク マップには、デフォルトではパケットにアプリケーションのベンダーとバージョンが含まれている場合にのみ、検出されたアプリケーションの脆弱性が表示されます。ただし、Firepower Management Center の構成でアプリケーションの脆弱性マッピングの設定を有効化することで、ベンダーとバージョンのデータがないアプリケーションの脆弱性をリストするようにシステムを設定できます。

脆弱性 ID (または脆弱性 ID の範囲) の隣の数字は、次の 2 つのカウンタを表しています。

### 影響を受けるホスト数

最初の数字は、1 つまたは複数の脆弱性の影響を受ける 1 台とは限らないホストのカウンタです。1 台のホストが複数の脆弱性の影響を受ける場合、このカウンタは複数回数えら

れます。このため、このカウントがネットワーク上のホスト数を上回ることがありえます。脆弱性を非アクティブ化すると、このカウントはその脆弱性の影響を受ける可能性のあるホスト数の分減少します。1つまたは複数の脆弱性の影響を受ける可能性のあるホストについて、脆弱性を1つも非アクティブ化していない場合、このカウントは表示されません。

#### 影響を受ける可能性のあるホスト数

2番目の数字は、1つまたは複数の脆弱性の影響を受ける可能性があるとしてシステムが判断した1台とは限らないホストの総数のカウントです。

脆弱性を非アクティブ化すると、指定したホストについてのみ脆弱性が非アクティブになります。脆弱と判断されたすべてのホストか、指定した個々の脆弱なホストの脆弱性を非アクティブ化することができます。脆弱性が非アクティブ化されると、該当するホストのIPアドレスはネットワークマップにグレーのイタリック体で表示されます。また、それらのホストのホストプロファイルでは、非アクティブ化された脆弱性が無効と表示されます。

その後でシステムが脆弱性が非アクティブ化されていないホストに（たとえば、ネットワークマップ内の新しいホストに）その脆弱性を検出すると、システムはそのホストの脆弱性をアクティブ化します。新たに検出された脆弱性は明示的に非アクティブ化する必要があります。また、システムでは、ホストのオペレーティングシステムまたはアプリケーションの変更を検出すると、関連付けられている非アクティブ化された脆弱性を再度アクティブ化することがあります。

## ホスト属性のネットワーク マップ

[ホスト属性 (Host Attributes)] タブのネットワーク マップには、ネットワーク上のホストがユーザ定義ホスト属性またはコンプライアンス ホワイトリスト ホスト属性のいずれかを基準に編成されて表示されます。この表示では、定義済みホスト属性を使用してホストを編成することはできません。

ホストを編成するために使用するホスト属性を選択すると、Firepower Management Center はネットワークマップで使用可能なその属性の値をリストし、割り当てられた値に基づいてホストをグループ化します。たとえば、ホワイトリストホスト属性でホストを編成することになると、システムは [準拠 (Compliant)]、[非準拠 (Non-Compliant)]、[評価されていない (Not Evaluated)] カテゴリでホストを表示します。

また、特定のホスト属性値が割り当てられた任意のホストのホストプロファイルを表示することもできます。

#### 関連トピック

[ホストプロファイル内のホスト属性](#) (2676 ページ)

## ネットワーク マップの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Any Security Analyst

### 手順

**ステップ 1** [分析 (Analysis)] > [ホスト (Hosts)] > [ネットワーク マップ (Network Map)] を選択します。

**ステップ 2** 表示するネットワーク マップのタブをクリックします。

**ステップ 3** 必要に応じて、以下の操作を続行します。

- ドメインの選択：マルチドメイン展開では、[ドメイン (Domain)] ドロップダウン リストからリーフ ドメインを選択します。
- ホストのフィルタリング：IP または MAC アドレスでフィルタリングするには、検索フィールドにアドレスを入力します。検索をクリアするには、クリア アイコン (✕) をクリックします。
- ドリル ダウン：カテゴリまたはホスト プロファイルを調べる場合、マップのカテゴリまたはサブネットからドリルダウンします。カスタム トポロジを定義した場合、[ホスト (host)] タブから [(トポロジ) ((topology))] をクリックしてそのトポロジを表示し、デフォルトのビューに戻りたい場合は、[(ホスト) ((hosts))] をクリックします。
- 削除：該当する要素の横にある削除アイコン (🗑️) をクリックし、以下のことを行います。
  - [ホスト (Hosts)]、[ネットワーク デバイス (Network Devices)]、[モバイル デバイス (Mobile Devices)]、[アプリケーション プロトコル (Application Protocols)] タブのマップから要素を削除する。
  - [侵害の兆候 (Indications of Compromise)] タブで IOC カテゴリ、侵害されたホスト、侵害されたホストのグループを解決済みとしてマークを付ける。
  - [脆弱性 (Vulnerabilities)] タブですべてのホストまたは単一ホストの脆弱性を非アクティブ化する。
- 脆弱性クラスの指定：[脆弱性 (Vulnerabilities)] タブで、[タイプ (Type)] ドロップダウン リストから、表示する脆弱性のクラスを選択します。
- 組織属性の指定：[ホスト属性 (Host Attributes)] タブで、[属性 (Attribute)] ドロップダウン リストから属性を選択します。

### 関連トピック

[カスタム ネットワーク トポロジ \(2399 ページ\)](#)

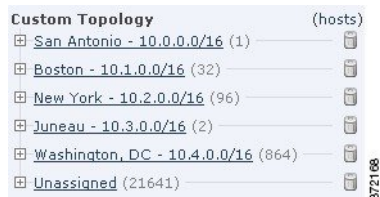
[ホストプロファイル](#) (2655 ページ)

## カスタム ネットワーク トポロジ

ホストおよびネットワーク デバイスのネットワーク マップでサブネットを整理および識別するために、カスタム トポロジ機能を使用します。

たとえば、部門内の各部署が異なるサブネットを使用している場合、カスタム トポロジ機能を使用して、これらのサブネットにラベルを付けられます。

また、カスタム トポロジで指定した部門に基づいてホストのネットワーク マップを表示することもできます。



次のいずれかまたはすべての方法でカスタム トポロジのネットワークを指定できます。

- ネットワーク検出ポリシーからネットワークをインポートして、システムでモニタするように設定したネットワークをトポロジに追加します。
- 手動でネットワークをトポロジに追加します。

[カスタム トポロジ (Custom Topology) ] ページにカスタム トポロジと各トポロジのステータスが一覧表示されます。ポリシー名の隣の電球アイコンが点灯している場合、そのトポロジはアクティブで、ネットワーク マップに影響します。消灯している場合、トポロジは非アクティブです。

### 関連トピック

[ホストのネットワーク マップ](#) (2392 ページ)

[ネットワーク デバイスのネットワーク マップ](#) (2393 ページ)

## カスタム トポロジの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

### 手順

**ステップ 1** [ポリシー (Policies) ] > [ネットワーク検出 (Network Discovery) ] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** ツールバーで [カスタム トポロジ (Custom Topology) ] をクリックします。

**ステップ 3** [トポロジの作成 (Create Topology) ] をクリックします。

**ステップ 4** 名前を入力します。

**ステップ 5** 必要に応じて、[説明 (Description) ] を入力します。

**ステップ 6** トポロジにネットワークを追加します。次の方法のいずれかまたはすべてを使用できます。

- [ネットワーク検出ポリシーからのネットワークのインポート \(2400 ページ\)](#) の説明に従って、ネットワーク検出ポリシーからネットワークをインポートします。
- [手動によるカスタム トポロジへのネットワークの追加 \(2401 ページ\)](#) の説明に従って、手動でネットワークを追加します。

**ステップ 7** [保存 (Save) ] をクリックします。

#### 次のタスク

- トポロジをアクティブ化します。詳細については、[カスタム トポロジのアクティブおよび非アクティブの設定 \(2402 ページ\)](#) を参照してください。

## ネットワーク検出ポリシーからのネットワークのインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

#### 手順

**ステップ 1** ネットワークをインポートするカスタム トポロジにアクセスします。

- カスタム トポロジを作成します。[カスタム トポロジの作成 \(2399 ページ\)](#) を参照してください。
- 既存のカスタム トポロジを編集します。[カスタム トポロジの編集 \(2402 ページ\)](#) を参照してください。

**ステップ 2** [ポリシー ネットワークのインポート (Import Policy Networks) ] をクリックします。

**ステップ 3** [ロード (Load) ] をクリックします。システムにより、ネットワーク検出ポリシーのトポロジ情報が表示されます。

**ステップ 4** トポロジを修正するには、次の手順を実行します。

- トポロジ内のネットワーク名を変更するには、ネットワークの横にある編集アイコン (✎) をクリックし、名前を入力してから [名前の変更 (Rename)] をクリックします。
- トポロジからネットワークを削除するには、削除アイコン (🗑) をクリックしてから [OK] をクリックします。

**ステップ 5** [保存 (Save)] をクリックします。

#### 次のタスク

- トポロジをアクティブ化します。詳細については、[カスタムトポロジのアクティブおよび非アクティブの設定 \(2402 ページ\)](#) を参照してください。

## 手動によるカスタム トポロジへのネットワークの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

#### 手順

**ステップ 1** ネットワークを追加するカスタム トポロジにアクセスします。

- カスタム トポロジを作成します。[カスタムトポロジの作成 \(2399 ページ\)](#) を参照してください。
- 既存のカスタム トポロジを編集します。[カスタムトポロジの編集 \(2402 ページ\)](#) を参照してください。

**ステップ 2** [ネットワークの追加 (Add Network)] をクリックします。

**ステップ 3** ホストとネットワーク デバイスのネットワーク マップでネットワークのカスタム ラベルを追加するには、[名前 (Name)] を入力します。

**ステップ 4** 追加するネットワークを表す [IP アドレス (IP Address)] と [ネットマスク (Netmask)] (IPv4) を入力します。

**ステップ 5** [追加 (Add)] をクリックします。

**ステップ 6** [保存 (Save)] をクリックします。

#### 次のタスク

- トポロジをアクティブ化します。詳細については、[カスタムトポロジのアクティブおよび非アクティブの設定 \(2402 ページ\)](#) を参照してください。

## 関連トピック

[Firepower システムの IP アドレス表記法](#) (14 ページ)

## カスタムトポロジのアクティブおよび非アクティブの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin



(注) 常に1つのカスタムトポロジのみアクティブにできます。複数のトポロジを作成した場合、1つをアクティブ化すると、自動的に現在アクティブなトポロジが非アクティブになります。

## 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

**ステップ 2** [カスタムトポロジ (Custom Topology)] を選択します。

**ステップ 3** アクティブまたは非アクティブにするトポロジの横にあるスライダをクリックします。

## カスタムトポロジの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	リーフのみ	Admin/Discovery Admin

アクティブトポロジに加える変更はただちに有効になります。

## 手順

**ステップ 1** [ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] を選択します。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。



**ステップ2** [カスタム トポロジ (Custom Topology) ]をクリックします。

**ステップ3** 編集するトポロジの横にある編集アイコン (✎) をクリックします。

**ステップ4** [カスタム トポロジの作成 \(2399 ページ\)](#) の説明に従って、トポロジを編集します。

**ステップ5** [保存 (Save) ]をクリックします。

---





## 第 99 章

# インシデント

次のトピックでは、インシデント処理を設定する方法について説明します。

- [インシデント対応について \(2405 ページ\)](#)
- [カスタム インシデント タイプの作成 \(2409 ページ\)](#)
- [インシデントの作成 \(2410 ページ\)](#)
- [インシデントの編集 \(2411 ページ\)](#)
- [インシデント レポートの生成 \(2412 ページ\)](#)

## インシデント対応について

インシデント対応とは、セキュリティポリシーの違反が疑われる場合に組織が取る対応を指します。Firepower システムには、インシデントの調査に関連する情報の収集および処理をサポートする機能が含まれます。これらの機能を使用して、インシデントに関連する可能性のある侵入イベントおよびパケット データを収集することができます。攻撃の影響を軽減するために Firepower システムの外部で実行するアクティビティに関する記録のためのリポジトリとしてインシデントを使用できます。たとえば、セキュリティポリシーによって、ネットワークの安全性に問題のあるホストの検疫が要求される場合は、インシデントにそのことを記録できます。

Firepower システムはインシデントのライフ サイクルもサポートします。これにより、攻撃への対応を進めるごとに、インシデントのステータスを変更できます。インシデントを閉じるときに、学んだ教訓の結果としてセキュリティ ポリシーに加えた変更を記録できます。

## インシデントの定義

一般的に、インシデントとは、セキュリティ ポリシー違反の可能性があると疑われる、1 つ以上の侵入イベントと定義されます。Firepower システムでは、この用語は、インシデントへの応答を追跡するために使用できる機能について記述しています。

一部の侵入イベントは、ネットワーク資産の可用性、機密性、および整合性の点で他のイベントよりも重要になります。たとえば、ポート スキャン検出では、ネットワークでのポート スキャンアクティビティについて通知することができます。しかし、セキュリティ ポリシーでは、ポート スキャンが明確に禁止されていなかったり、優先度の高い脅威とは見なされていない

かったりすることがあります。それで、直接的なアクションの実行はしないで、代わりにすべてのポート スキャンのログを後の調査のために保持しておくことができます。

一方、ネットワーク内のホストが侵害されていることを示す、分散型サービス拒否 (DDoS) 攻撃に関係したイベントをシステムが生成する場合、そのアクティビティはセキュリティポリシーの明確な違反であると考えられます。それで、これらのイベントを調査して追跡できるように、Firepower システムでインシデントを作成する必要があります。

## 共通のインシデント対応プロセス

### 準備 (Preparation)

インシデントの準備には次の 2 通りの方法があります。

- 明確で包括的なセキュリティポリシーと、それらを施行するためのハードウェアおよびソフトウェア リソースを配置する
- インシデントに対応するための明確に定義された計画と、その計画を実行できる適切なトレーニングを受けたチームを配置する

インシデント対応において重要なのは、ネットワークのどの部分が最も大きなリスクとなるかを理解することです。これらのネットワーク セグメントに Firepower システムを展開することで、インシデントがいつどのように発生するかについて理解を深めることができます。また、時間をかけて各管理対象デバイスに対する侵入ポリシーを慎重に調整することによって、生成されるイベントの品質を最大限に高めることができます。

### 検出と通知

インシデントを検出できなければ、インシデントに対応できません。インシデント対応プロセスでは、検出できるセキュリティ関連イベントのタイプと、それらを検出するために使用するメカニズム (ソフトウェアとハードウェアの両方) を識別する必要があります。また、セキュリティポリシーの違反を検出できるケースにも注意する必要があります。積極的あるいは受動的にモニタされないセグメントがネットワークに含まれている場合は、それらのセグメントにも注意する必要があります。

ユーザがネットワークに展開する管理対象デバイスは、それらがインストールされているセグメントのトラフィックの分析、侵入の検知、およびそれらを説明するイベントの生成を行う必要があります。各管理対象デバイスに展開するアクセス コントロール ポリシーが、検出するアクティビティの種類と優先度に影響を与えることに注意してください。インシデントチームが数百のイベントを取捨選択しなくてもよいように、特定のタイプの侵入イベントに対して通知オプションを設定することもできます。特定の優先順位の高い、重大度の高いイベントが検出されたときに自動的に通知するように指定できます。

### 調査と認定

インシデント対応プロセスでは、セキュリティインシデントの検出後に、どのように調査を実施するかを指定する必要があります。一部の組織では、経験の浅いチームメンバーがすべてのインシデントのトリアージを行い、重大度と優先度が比較的に低いケースは自分たちで処理

し、熟練のチームメンバーが重大度と優先度が高いインシデントを処理しています。各チームメンバーがインシデントの重要度を繰り上げる基準について理解するように、エスカレーションプロセスの概要を慎重にまとめる必要があります。

エスカレーションプロセスでは、検出されたイベントがネットワーク資産のセキュリティにどのような影響を与えるかについての理解が不可欠です。たとえば、Microsoft SQL Server を実行するホストに対する攻撃は、それとは異なるデータベースサーバを使用する組織にとって優先度は高くありません。同様に、ネットワークで SQL Server を使用しているものの、すべてのサーバにパッチを適用済みで、その攻撃に対する脆弱性がないことを確信している場合には、その攻撃の重要度は低くなります。しかし、最近誰かが脆弱性のあるバージョンのソフトウェアコピーを（テスト目的などで）インストールしていたりすれば、簡易調査で指摘されるよりも大きな問題が発生するおそれがあります。

Firepower システムは、調査および認定のプロセスをサポートするのに特に適しています。独自のイベント分類を作成し、ネットワークの脆弱性を最も適切に示す方法で、それらを適用することができます。ネットワークのトラフィックによってイベントがトリガーされると、自動的に、そのイベントの優先度判別と認定が行われ、脆弱性があることが判明しているホストに対してどのような攻撃が行われるかを示す特別なインジケータが付けられます。

Firepower システムのインシデントトラッキング機能には、エスカレーションされたインシデントを示すためにユーザが変更できるステータスインジケータも含まれています。

### コミュニケーション (Communication)

すべてのインシデント対応プロセスでは、インシデント対応チームと内部および外部の対象者の間でのインシデントについての連絡の方法が指定されている必要があります。たとえば、どの種類のインシデントが管理介入を必要とし、どのレベルでの介入が必要かを考慮する必要があります。また、プロセスでは、組織の外部との連絡の方法とタイミングが説明されている必要があります。次の点に注意してください。

- あるインシデントについて、法執行機関に通知する必要がありますか。
- ホストがリモートサイトに対する分散型サービス妨害 (DDoS) に関与している場合、そのことを通知しますか。
- CERT 調整センター (CERT/CC) や FIRST などの組織と情報を共有する必要があるでしょうか。

Firepower システムには、HTML、PDF、CSV (カンマ区切り値) などの標準形式で侵入データを収集するために使用できる機能があり、侵入データを他のユーザと簡単に共有できます。

たとえば、CERT/CC は Web サイトのセキュリティインシデントに関する標準情報を収集します。CERT/CC は、Firepower システムから簡単に抽出できる次のような情報を探します。

- 影響を受けるマシンに関する次のような情報
  - ホスト名および IP
  - タイムゾーン
  - ホストの目的や機能

- 攻撃元に関する次のような情報
  - ホスト名および IP
  - タイムゾーン
  - 攻撃者と接触したことがあるかどうか
  - インシデント処理の概算コスト
- 次のようなインシデントの説明
  - 日付
  - 侵入方法
  - 使用された侵入者ツール
  - ソフトウェアバージョンとパッチレベル
  - 侵入者ツールの出力
  - 悪用された脆弱性の詳細
  - 攻撃元
  - その他の関連情報

また、インシデントのコメントセクションを使用して、問題を伝えた日時と相手を記録することができます。

### 封じ込めとリカバリ

インシデント対応プロセスでは、ホストまたはその他のネットワークコンポーネントが侵害された場合に、どのような手順を実行するかを明確に示す必要があります。封じ込めとリカバリの方法には、脆弱性のあるホストへのパッチの適用から、ターゲットのシャットダウンとネットワークからの除去まで、さまざまな選択肢があります。攻撃の性質と重大度によっては、刑事責任を追求する場合に備えて証拠を保存しておくことの重要性を考慮する必要もあります。

Firepower システムのインシデント機能を使用して、インシデントの封じ込めとリカバリのフェーズ中に実行するアクションを記録しておくことができます。

### 学んだ教訓

それぞれのセキュリティインシデントは、攻撃が成功したかどうかに関わりなく、セキュリティポリシーを見直す機会となります。ファイアウォールルールを更新する必要がありますか。パッチ管理に対するより構造化されたアプローチが必要ですか。不正なワイヤレスアクセスポイントは新しいセキュリティ問題となりますか。それぞれの学んだ教訓は、セキュリティポリシーにフィードバックし、次のインシデントへのより良い対処のために役立つ必要があります。

## Firepower システムのインシデントタイプ

作成する各インシデントにインシデントタイプを割り当てることができます。Firepower システムでは、以下のタイプがデフォルトでサポートされます。

- 侵入 (Intrusion)
- サービス妨害 (DoS)
- 不正な管理者アクセス
- Web サイトの改変
- システム整合性の侵害
- デマ ウイルス
- 盗難
- ダメージ
- 不明

独自のインシデントタイプを作成することもできます。

## カスタム インシデントタイプの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

### 手順

**ステップ 1** [分析 (Analysis)] > [侵入 (Intrusions)] > [インシデント (Incidents)] を選択します。

**ステップ 2** [インシデントの作成 (Create Incident)] をクリックします。

**ステップ 3** [タイプ (Type)] エリアで、[タイプ (Types)] をクリックします。

デフォルトのインシデントタイプがページの下部に表示されます。

**ステップ 4** [インシデントタイプ名 (Incident Type Name)] フィールドに、新しいインシデントタイプの名前を入力します。

**ステップ 5** [追加 (Add)] をクリックします。

**ステップ 6** [完了 (Done)] をクリックします。

次にインシデントを作成または編集するときに、新しいインシデントタイプを使用できます。

## インシデントの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

マルチドメイン導入では、現在のドメインで作成されたインシデントのみを表示および変更できます。先祖ドメインでは、任意の子孫ドメインからのインシデントにイベントを追加できません。

### 手順

**ステップ 1** [分析 (Analysis)] > [侵入 (Intrusions)] > [インシデント (Incidents)] を選択します。

**ステップ 2** [インシデントの作成 (Create Incident)] をクリックします。

**ステップ 3** [タイプ (Type)] ドロップダウンメニューから、インシデントを最も適切に説明するオプションを選択します。

**ステップ 4** [滞留時間 (Time Spent)] フィールドに、インシデントで費やした時間の合計を #d #h #m #s の形式で入力します。ここで、# は日数、時間数、分数、秒数を表します。

**ステップ 5** [概要 (Summary)] テキストボックスに、インシデントの簡単な説明 (最大 255 文字の英数字、スペース、記号) を入力します。

**ステップ 6** [コメントを追加 (Add Comment)] テキストボックスに、インシデントのより詳細な説明 (最大 8191 文字の英数字、スペース、記号) を入力します。

**ステップ 7** インシデントにイベントを追加します。

- 選択したイベントを追加するには、クリップボードのイベントを選択して、[インシデントに追加 (Add to Incident)] をクリックします。
- クリップボードからすべてのイベントを追加するには、[すべてをインシデントに追加 (Add All to Incident)] をクリックします。

(注) クリップボードの複数のページにある個々のイベントを追加する場合は、1つのページのイベントを追加してから、他のページのイベントを追加します (ページごとに追加します)。

**ステップ 8** [保存 (Save)] をクリックします。



## インシデントの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

マルチドメイン導入では、現在のドメインで作成されたインシデントのみを表示および変更できます。先祖ドメインでは、すべての子孫ドメインからインシデントにイベントを追加できません。

### 手順

**ステップ 1** [分析 (Analysis)] > [侵入 (Intrusions)] > [インシデント (Incidents)] を選択します。

**ステップ 2** 編集するインシデントの横にある編集アイコン (✎) をクリックします。

**ステップ 3** インシデントの以下の側面を編集できます。

- ステータスの変更
- タイプの変更
- クリップボードからのイベントの追加
- イベントの削除

**ステップ 4** [滞留時間 (Time Spent)] フィールドに、インシデントに費やした追加の時間の合計を入力します。

**ステップ 5** [コメントを追加 (Add Comment)] テキストボックスで、インシデントに対する変更点 (最大 8191 文字の英数字、スペース、および記号) を示します。

**ステップ 6** オプションで、インシデントにイベントを追加したり、削除したりすることができます。

- クリップボードからイベントを追加するには、クリップボードのイベントを選択して、[インシデントに追加 (Add to Incident)] をクリックします。
- クリップボードからすべてのイベントを追加するには、[インシデントにすべてを追加 (Add All to Incident)] をクリックします。
- インシデントから特定のイベントを削除するには、イベントを選択し、[削除 (Delete)] をクリックします。
- インシデントからすべてのイベントを削除するには、[すべて削除 (Delete All)] をクリックします。
- イベントを追加または削除せずにインシデントを更新するには、[保存 (Save)] をクリックします。

## インシデントレポートの生成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

Firepower システムを使用して、インシデントレポートを生成できます。このレポートには、インシデントの概要、インシデントのステータス、およびコメントに加えて、インシデントに追加するイベントの情報を含めることができます。また、レポートにイベントの概要情報を含めるかどうかも指定できます。

### 手順

**ステップ 1** [分析 (Analysis)] > [侵入 (Intrusions)] > [インシデント (Incidents)] を選択します。

**ステップ 2** レポートに含めるインシデントの横にある編集アイコン (✎) をクリックします。

**ステップ 3** 次の 2 つの対処法があります。

- レポートにインシデントのすべてのイベントを含める場合は、[すべてのレポートの生成 (Generate Report All)] をクリックします。
- レポートにインシデントの特定のイベントを含める場合は、目的のイベントの横にあるチェックボックスをオンにしてから、[レポートの生成 (Generate Report)] をクリックします。

**ステップ 4** レポートの名前を入力します。

**ステップ 5** [インシデントレポートのセクション (Incident Report Sections)] で、レポートに含めるインシデントの部分 ([ステータス (status)]、[概要 (summary)]、および [コメント (comments)] のチェックボックスをオンにします。

**ステップ 6** レポートにイベント情報を含める場合は、使用するワークフローを選択し、[レポートのセクション (Report Sections)] で、イベントの概要情報を含めるかどうかを指定します。

**ステップ 7** レポートに含めるワークフロー ページの横にあるチェックボックスをオンにします。

**ステップ 8** レポートに使用する出力形式 ([PDF]、[HTML]、および [CSV]) の横にあるチェックボックスをオンにします。

(注) CSV ベースのインシデントレポートには、イベント情報のみが含まれます。インシデントのステータス、概要、コメントは含まれません。

**ステップ 9** [レポートの生成 (Generate Report)] をクリックして、レポート プロファイルの更新を確認します。



## 第 100 章

# ルックアップの使用

以下のトピックでは、Firepower システムで既知の（または未知の）エンティティに関する情報を検索する方法について説明します。

- [ルックアップの概要](#)（2413 ページ）
- [Whois ルックアップの実行](#)（2413 ページ）
- [IP アドレスの地理位置情報の検出](#)（2414 ページ）

## ルックアップの概要

Firepower Management Center がインターネットに接続している場合、手動ルックアップ機能を使って次の情報を検索できます。

- 任意の IP アドレスについての Regional Information Registries (RIR) 情報 (whois)。
- 任意の IP アドレスについての地理位置情報 (国名、国番号および大陸名) (最新の地理位置情報を確実に使用するように、Firepower Management Center 上の地理位置情報データベース (GeoDB) を定期的に更新することを強くお勧めします)。

### 関連トピック

[地理位置情報データベースの更新](#)（192 ページ）

## Whois ルックアップの実行

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)

## 始める前に

- Firepower Management Center がインターネットにアクセスできることを確認します。[セキュリティ、インターネット アクセス、および通信ポート \(2785 ページ\)](#) を参照してください。

## 手順

**ステップ 1** [分析 (Analysis)] > [検索 (Lookup)] > [Whois] を選択します。

**ステップ 2** IP アドレスを入力して、[検索 (Search)] をクリックします。

## 関連トピック

[コンテキスト メニュー \(32 ページ\)](#)

## IP アドレスの地理位置情報の検出

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center	任意 (Any)	任意 (Any)

地理位置情報ルックアップ機能を使用して、国名、ISO 3166-1 の 3 桁の国番号と、任意の IP アドレスに関連付けられた大陸名を検索します。

## 手順

**ステップ 1** [分析 (Analysis)] > [検索 (Lookup)] > [位置情報 (Geolocation)] を選択します。

**ステップ 2** 1 つ以上の IP アドレスの地理位置情報を表示するには、アドレス (複数可) を入力して、[検索 (Search)] をクリックします。IPv4 アドレス、IPv6 アドレスのいずれか、または両方を指定できます。複数のアドレスは、カンマ、セミコロン、改行、スペース文字を使用して区切ります。

**ヒント** テキストボックスをクリアするには、[クリア (Clear)] をクリックします。

**ステップ 3** データを並べ替えるには、列見出しをクリックします。IP アドレスを除くすべてのフィールドによって並べ替えが可能です。

## 関連トピック

[地理位置情報データベースの更新 \(192 ページ\)](#)



## 第 **XXIV** 部

### ワークフロー（**Workflows**）

- [ワークフロー](#)（2417 ページ）
- [イベントの検索](#)（2467 ページ）
- [カスタム ワークフロー](#)（2479 ページ）
- [カスタム テーブル](#)（2489 ページ）





## 第 101 章

# ワークフロー

以下のトピックでは、ワークフローの使用方法について説明します。

- [概要：ワークフロー](#) (2417 ページ)
- [定義済みワークフロー](#) (2418 ページ)
- [カスタム テーブル ワークフロー](#) (2429 ページ)
- [ワークフローの使用](#) (2429 ページ)
- [ブックマーク](#) (2464 ページ)

## 概要：ワークフロー

ワークフローは Firepower Management Center Web インターフェイス上でユーザに合わせて作成された一連のデータページで、アナリストはワークフローを使用して、システムで生成されたイベントを評価することができます。

Firepower Management Center では、以下のタイプのワークフローを使用できます。

### 定義済みワークフロー

システムに付属のプリセットワークフローです。定義済みのワークフローの編集や削除を行うことはできません。ただし、定義済みワークフローをコピーして、そのコピーをカスタム ワークフローの基礎として使用することができます。

### 保存済みのカスタム ワークフロー

Firepower Management Center に付属の保存済みカスタム テーブルに基づくカスタム ワークフロー。これらのワークフローは編集、削除、コピーすることができます。

### カスタム ワークフロー

特定のニーズに対応するために作成してカスタマイズするワークフロー、またはカスタム テーブルを作成するとシステムによって自動的に生成されるワークフローです。これらのワークフローは編集、削除、コピーすることができます。

通常、ワークフローに表示されるデータは、管理対象デバイスのライセンスおよび展開状況や、データを提供する機能を設定しているかどうかによって異なります。

## 定義済みワークフロー

以下の項で説明する定義済みワークフローは、システムに付属しているものです。定義済みワークフローを編集または削除することはできません。ただし、定義済みワークフローをコピーして、そのコピーをカスタムワークフローのベースとして使用することができます。

### 定義済み侵入イベントのワークフロー

次の表では、Firepower System に備わっている定義済み侵入イベントのワークフローについて説明します。

表 251: 定義済み侵入イベントのワークフロー

ワークフロー名	説明
[接続先ポート (Destination Port) ]	接続先ポートは、通常、アプリケーションに紐付けされているため、このワークフローにより、異常な大容量アラートを経験しているアプリケーションを検出できます。接続先ポートカラムにより、ネットワーク上に存在してはならないアプリケーションを特定できます。
イベント特定	このワークフローでは、2つの有用な特徴を提供します。イベントが頻繁に発生する場合には、次のことを示します： <ul style="list-style-type: none"> <li>• 誤検出</li> <li>• ワーム</li> <li>• 不正確な誤設定ネットワーク</li> </ul> 発生頻度の低いイベントは、対象となる攻撃を最も確実に示す証拠であり、特別な注意を必要とします。
優先度および分類によるイベント	このワークフローでは、イベントとタイプのリストをそれぞれのイベントが発生した回数と共にイベントの優先度の順に示します。
接続先に対するイベント	このワークフローでは、攻撃されているホスト IP アドレスや攻撃の本質のハイレベルビューを提示します。利用可能な場合、攻撃に関与する国に関する情報を確認することもできます。



ワークフロー名	説明
IP 特定	このワークフローでは、最も多くのアラートを発生するホスト IP アドレスを示します。イベント数が最も多いホストは、対外に向けて、受信しているワームタイプのトラフィック（調整を必要とする適切な場所を示す）であるか、またはアラートの原因を決定するために更に調査を必要とします。イベント数が最も少ないホストは、対象となる攻撃を受ける可能性があるため、調査の根拠となります。イベント数が少ない場合は、ホストがネットワークに属していないことを示す場合もあります。
影響度と優先度	このワークフローにより、すぐに再度発生している影響度の高いイベントを検索します。レポートによる影響レベルは、イベントが発生した時間数で示します。この情報を使用して、最も頻繁に再発する影響度の高いイベントを特定できます。これがネットワーク上での広範な攻撃の指標となります。
影響度と送信元	このワークフローにより、進行中の攻撃の送信元を特定できます。レポートされた影響レベルは、イベントに対する関連の送信元 IP アドレスにより示します。たとえば、影響レベルが 1 のイベントは、同じ送信元 IP アドレスから繰り返し発生している場合、これらは特定された脆弱なシステムであり、送信元 IP アドレスを対象としている攻撃者を示すこともあります。
接続先への影響	このワークフローを使用して、脆弱なコンピュータ上で繰り返し発生しているイベントを特定できます。このため、これらのシステムでの脆弱性を指定し、進行中の攻撃を停止できます。
送信元ポート	このワークフローは、最もアラートを発生しているサーバを示します。この情報を使用して、調整が必要なエリアを特定し、注意を要するサーバを決定できます。
送信元と接続先	このワークフローでは、高いレベルのアラートを共有するホスト IP アドレスを特定します。リストのトップのペアは誤検出の可能性もあり、調整が必要なエリアを特定することもあります。評価する必要のないリソースを評価するユーザまたはネットワークに属していないホストについては、対象となる攻撃リストの下部にあるペアを確認できます。

## 定義済みマルウェアのワークフロー

次の表では、Firepower Management Center に備えられた定義済みマルウェアのワークフローについて説明します。定義済みマルウェアのワークフローでは、必ずマルウェアイベントのテーブルビューを使用します。

表 252: 定義済みマルウェアのワークフロー

ワークフロー名	説明
マルウェア サマリ	このワークフローでは、ネットワーク トラフィック内で検出されたか、または AMP for Endpoints Connector によって検出されたマルウェアのリストを提供します。これらのリストは、それぞれの脅威ごとにグループ化されます。
マルウェア イベント サマリ	このワークフローでは、異なるマルウェア イベントのタイプやサブタイプの明細が迅速に表示されます。
ホスト受信マルウェア	このワークフローでは、マルウェアを受信したホスト IP アドレスのリストが表示されます。このリストは、マルウェア ファイル関連の処理ごとにグループ化されます。
ホスト送信マルウェア	このワークフローでは、マルウェアを送信したホスト IP アドレスのリストが表示されます。このリストは、マルウェア ファイル関連の処理ごとにグループ化されます。
アプリケーション導入マルウェア	このワークフローでは、ファイルを受信したホスト IP アドレスのリストが表示されます。このリストは、受信したファイルの関連したマルウェアの処理によってグループ化されます。

## 定義済みファイルのワークフロー

次の表では、Firepower Management Center に備えられる定義済みファイルイベントのワークフローについて説明しています。定義済みファイルイベントのワークフローでは、必ずファイルイベントのテーブルビューを使用します。

表 253: 定義済みファイルのワークフロー

ワークフロー名	説明
ファイル サマリ (File Summary)	このワークフローでは、関連するマルウェアの処理と共に、異なるファイル イベント カテゴリやタイプの明細を迅速に表示します。

ワークフロー名	説明
ホスト受信ファイル (Hosts Receiving Files)	このワークフローでは、ファイルを受信したホスト IP アドレスのリストが表示されます。このリストは、受信したファイルの関連したマルウェアの処理によってグループ化されます。
ホスト送信ファイル (Hosts Sending Files)	このワークフローでは、ファイルを送信したホスト IP アドレスのリストを表示します。このリストは、これらのファイルの関連したマルウェアの処理によってグループ化されます。

## 定義済みキャプチャ ファイルのワークフロー

次の表では、Firepower Management Center での定義済みキャプチャ ファイルのワークフローについて説明しています。定義済みキャプチャファイルのワークフローは、必ずキャプチャファイルのテーブル ビューを使用します。

表 254: 定義済みキャプチャ ファイルのワークフロー

ワークフロー名	説明
キャプチャ ファイル サマリ	このワークフローでは、タイプ、カテゴリ、脅威スコアに基づいてキャプチャ ファイルの詳細を提示します。
ダイナミック分析ステータス (Dynamic Analysis Status)	このワークフローでは、ダイナミック分析用に提示されたか否かに基づいて、キャプチャ ファイルの数を表示します。

## 定義済み接続データのワークフロー

次の表では、Firepower Management Center に備えられる定義済み接続データのワークフローについて説明しています。定義済み接続データ ワークフローでは、必ず接続データのテーブル ビューを使用します。

表 255: 定義済み接続データのワークフロー

ワークフロー名	説明
接続イベント	このワークフローでは、ベーシックな接続に関する情報や検出されたアプリケーション情報のサマリー ビューを提示し、このサマリー ビューを使用して、イベントのテーブル ビューをドリルダウンできます。

ワークフロー名	説明
アプリケーションごとの接続 (Connections by Application)	このワークフローには、検出された接続情報の数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなアプリケーションのグラフが含まれます。
イニシエータごとの接続 (Connections by Initiator)	このワークフローには、ホストが接続トランザクションを開始した接続の数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなホスト IP アドレスのグラフが含まれています。
ポートごとの接続 (Connections by Port)	このワークフローには、検出された接続の数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなポートのグラフが含まれています。
レスポンドごとの接続 (Connections by Responder)	このワークフローには、ホスト IP が接続トランザクションでレスポンドである接続の数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなホスト IP アドレスのグラフが含まれています。
時間の経過ごとの接続 (Connections over Time)	このワークフローには、監視対象のネットワーク セグメントでの時間の経過ごとの合計接続数のグラフが含まれています。
アプリケーションごとのトラフィック (Traffic by Application)	このワークフローには、送信されたキロバイト数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなアプリケーションのグラフが含まれています。
イニシエータごとのトラフィック (Traffic by Initiator)	このワークフローには、各アドレスから送信された合計キロバイト数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなホスト IP アドレスのグラフが含まれています。
ポートごとのトラフィック (Traffic by Port)	このワークフローには、送信されたキロバイト数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなポートのグラフが含まれています。
レスポンドごとのトラフィック (Traffic by Responder)	このワークフローには、各アドレスが受信した合計キロバイト数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなホスト IP アドレスのグラフが含まれています。
時間の経過ごとのトラフィック	このワークフローには、監視対象のネットワーク セグメントで送信される時間の経過ごとの合計キロバイト数のグラフが含まれています。

ワークフロー名	説明
レスポンドごとの一意イニシエータ	このワークフローには、各アドレスでコンタクトした一意イニシエータの数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブな応答ホスト IP アドレスのグラフが含まれています。
イニシエータごとの一意レスポンド (Unique Responders by Initiator)	このワークフローには、アドレスにコンタクトする一意レスポンドの数に基づく、監視対象のネットワーク セグメントでの 10 個の最もアクティブな開始ホスト IP アドレスのグラフが含まれています。

## 定義済みセキュリティ インテリジェンスのワークフロー

次の表では、Firepower Management Center に備えられている定義済みセキュリティ インテリジェンスのワークフローについて説明しています。定義済みセキュリティ インテリジェンスのワークフローでは、必ずセキュリティ インテリジェンス イベントのテーブル ビューを使用します。

表 256: 定義済みセキュリティ インテリジェンスのワークフロー

ワークフロー名	説明
セキュリティ インテリジェンス イベント	このワークフローでは、基礎的なセキュリティ インテリジェンスや検出されたアプリケーション情報のサマリ ビューを表示し、イベントのテーブル ビューをドリルダウンする際に使用できます。
セキュリティ インテリジェンス サマリ	このワークフローは、セキュリティ インテリジェンス イベントのワークフローと同じものですが、セキュリティ インテリジェンス サマリ ページから始まり、カテゴリや数ごとにセキュリティ インテリジェンス イベントのみのリストを表示します。
セキュリティ インテリジェンスと DNS 詳細	このワークフローは、セキュリティ インテリジェンス イベントのワークフローと同じものですが、DNS 詳細のあるセキュリティ インテリジェンス ページから始まり、カテゴリや DNS 関連特性ごとにセキュリティ インテリジェンス イベントのリストを表示します。

## 定義済みホストのワークフロー

次の表では、ホスト データと共に使用できる定義済みワークフローについて説明します。

表 257: 定義済みホストのワークフロー

ワークフロー名	説明
Hosts	このワークフローには、ホストのテーブルビューと、その後ホストビューが含まれます。ホストテーブルに基づくワークフロービューでは、ホストに関連付けられているすべてのIPアドレスのデータを容易に表示できます。
オペレーティングシステムサマリ (Operating System Summary)	このワークフローを用いて、ネットワーク上で使用中のオペレーティングシステムを分析できます。

## 定義済み侵害の兆候のワークフロー

次の表では、IOC（侵害の兆候）と共に使用できる定義済みワークフローについて説明します。

表 258: 定義済み侵害の兆候のワークフロー

ワークフロー名	説明
の侵害の兆候	このワークフローは、数とカテゴリごとにグループ化したIOCデータのサマリービューから始まり、さらにサマリデータをイベントタイプごとに分割した詳細ビューを表示します。  [分析 (Analysis)] > [ホスト (Hosts)] メニューからこのワークフローにアクセスします。
ホストごとの侵害の兆候	このワークフローを使用して、最も侵害する可能性の高いネットワーク上のホストを判断できます (IOCデータに基づく)。  [分析 (Analysis)] > [ホスト (Hosts)] メニューからこのワークフローにアクセスします。

## 定義済みアプリケーションワークフロー

次の表では、アプリケーションデータと共に使用できる定義済みワークフローについて説明しています。

表 259: 定義済みアプリケーションワークフロー

ワークフロー名	説明
アプリケーションのビジネスとの関連性	このワークフローを使用して、ネットワーク上で実行中のそれぞれ予想されるビジネスとの関連性レベルのアプリケーションを分析できます。そのため、ネットワークリソースが適切に使用されているかを監視できます。
アプリケーション カテゴリ	このワークフローを使用して、ネットワーク上で各カテゴリの実行中のアプリケーションを分析できます（電子メール、検索エンジン、ソーシャルネットワーキングなど）。そのため、ネットワークリソースが適切に使用されているかを監視できます。
アプリケーションのリスク	このワークフローを使用して、ネットワーク上でそれぞれ予想されるセキュリティ リスク レベルの実行中のアプリケーションを分析できます。このため、ユーザのアクティビティの考えられるリスクを予想し、適切なアクションを取ることができます。
アプリケーション サマリ	このワークフローを使用して、ネットワークのアプリケーションや関連するホストに関する詳細情報を取得できます。このため、ホストのアプリケーションのアクティビティを正確に調べることができます。
アプリケーション	このワークフローを使用して、ネットワーク上の実行中のアプリケーションを分析できます。このため、ネットワークの使用状況の概要を取得できます。

## 定義済みアプリケーション詳細ワークフロー

次の表では、アプリケーションの詳細とクライアントデータと共に使用できる定義済みワークフローについて説明しています。

表 260: 定義済みアプリケーション詳細ワークフロー

ワークフロー名	説明
アプリケーション詳細 (Application Details)	このワークフローを用いて、ネットワーク上のクライアントアプリケーションをさらに詳しく分析することができます。また、このワークフローでは、クライアントアプリケーションのテーブルビューを表示し、その後ホストビューを表示します。

ワークフロー名	説明
Clients	このワークフローには、クライアントアプリケーションのテーブルビューと、その後にホストビューが含まれます。

## 定義済みサーバのワークフロー

次の表では、サーバデータと共に使用できる定義済みワークフローについて説明します。

表 261: 定義済みサーバのワークフロー

ワークフロー名	説明
数別ネットワーク アプリケーション	このワークフローを使用して、ネットワーク上で最も多く使用されるアプリケーションを分析できます。
ヒット別ネットワーク アプリケーション	このワークフローを使用して、ネットワーク上で最もアクティブなアプリケーションを分析できます。
サーバの詳細	このワークフローを使用して、ベンダや検出されたサーバアプリケーションプロトコルのバージョンを詳細に分析できます。
サーバ	このワークフローには、アプリケーションのテーブルビューと、その後にホストビューが含まれます。

## 定義済みホスト属性のワークフロー

次の表では、ホスト属性データと共に使用できる定義済みワークフローについて説明します。

表 262: 定義済みホスト属性のワークフロー

ワークフロー名	説明
属性 (Attributes)	このワークフローを使用して、ネットワーク上のホスト IP アドレスやホスト ステータスを監視できます。

## 定義済み検出イベントのワークフロー

次の表では、検出データとアイデンティティデータの表示に使用できる定義済みワークフローについて説明しています。



表 263: 定義済み検出イベントワークフロー

ワークフロー名	説明
検出イベント (Discovery Events)	このワークフローでは、テーブルビュー形式の検出イベント詳細リストが提示され、その次にホストビューが提示されます。

## 定義済みユーザワークフロー

次の表では、ユーザ検出データとユーザアイデンティティデータの表示に使用できる定義済みワークフローを説明します。

表 264: 定義済みユーザワークフロー

ワークフロー名	説明
Users	このワークフローでは、ユーザ ID ソースによって収集されるユーザ情報リストが表示されます。

## 定義済み脆弱性のワークフロー

次の表では、Firepower Management Center に備えられている定義済み脆弱性のワークフローについて説明します。

表 265: 定義済み脆弱性のワークフロー

ワークフロー名	説明
脆弱性 (Vulnerabilities)	このワークフローを使用して、ネットワーク上で検出されたホストに適用するこれらのアクティブな脆弱性のみのテーブルビューなど、データベース内の脆弱性を検討できます。このワークフローにより脆弱性詳細ビューが提供され、これには制約に適合するそれぞれの脆弱性に関する詳細な説明が含まれています。

## 定義済みのサードパーティ脆弱性のワークフロー

次の表では、Firepower Management Center に備えられた定義済みのサードパーティ脆弱性のワークフローについて説明します。

表 266: 定義済みのサードパーティ脆弱性のワークフロー

ワークフロー名	説明
IP アドレスごとの脆弱性	このワークフローを使用して、監視対象のネットワーク上のホスト IP アドレスごとに検出されたサードパーティの脆弱性の数をすぐに確認できます。
送信元ごとの脆弱性	このワークフローを使用して、QualysGuard Scanner などサードパーティの脆弱性の送信元ごとに検出されたサードパーティの脆弱性の数をすぐに確認できます。

## 定義済み関連ワークフロー、ホワイトリストワークフロー

関連データ、ホワイトリストイベント、ホワイトリスト違反、修復ステータスイベントのそれぞれのタイプには、定義済みワークフローがあります。

表 267: 定義済み関連ワークフロー

ワークフロー名	説明
関連イベント (Correlation Events)	このワークフローには、関連イベントのテーブルビューが含まれています。
ホワイトリストイベント (White List Events)	このワークフローには、ホワイトリストイベントのテーブルビューが含まれています。
ホスト違反数 (Host Violation Count)	このワークフローには、少なくとも 1 つのホワイトリストに違反しているすべてのホスト IP アドレスのリストを示す一連のページが表示されます。
ホワイトリスト違反 (White List Violations)	このワークフローには、すべての違反を列挙し、リストのトップに直前に検出された違反を示す、ホワイトリスト違反のテーブルビューが含まれています。テーブル内の各列には、検出された違反が 1 つずつ表示されます。
ステータス (Status)	このワークフローには、修復ステータスのテーブルビューを含み、違反したポリシー名、適用された修復名や修復状況が表示されています。

## 定義済みのシステムのワークフロー

Firepower System には、監査イベントやヘルスイベントなどのシステム イベントなど、いくつかの追加のワークフロー、ルール更新インポート、アクティブスキャンの結果をリストにしたワークフローが提供されています。

表 268: 追加の定義済みワークフロー

ワークフロー名	説明
監査ログ (Audit Log)	このワークフローでは、監査イベントをリストした監査ログのテーブルビューを含みます。
ヘルス イベント (Health Events)	このワークフローでは、ヘルス監視ポリシーによりトリガーされるイベントを表示します。
ルール更新インポートログ (Rule Update Import Log)	このワークフローは、成功したルールの更新インポートと失敗したルールの更新インポートに関する情報をリストしたテーブルビューを含みます。
スキャン結果 (Scan Results)	このワークフローには、それぞれ完了したスキャンをリストしたテーブルビューを含みます。

## カスタム テーブル ワークフロー

カスタム テーブルの機能を使用して、複数のイベント タイプのデータを使用するテーブルを作成することができます。これにより、たとえば、ユーザが侵入イベントのデータとディスクバリエーションデータを関連付けるテーブルおよびワークフローを作成して、重要なシステムに影響を及ぼすイベントを簡単に検索できるようになるため、役立ちます。

カスタム テーブルを作成すると、システムは自動的にワークフローを作成します。このテーブルを使って関連するイベントを表示することができます。ワークフローの機能は、使用するテーブルのタイプによって異なります。たとえば、侵入イベントテーブルに基づいたカスタム テーブルのワークフローは、必ずパケットビューで終了します。ただし、検出イベントに基づいたカスタム テーブルのワークフローは、必ずホストビューで終了します。

事前定義のイベント テーブルに基づいたワークフローとは異なり、カスタム テーブルに基づいたワークフローには、他のタイプのワークフローへのリンクがありません。


## ワークフローの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	(ワークフローに応じて) Admin/Maint/Any Security Analyst


## 手順

**ステップ1** [ワークフローの選択 \(2432 ページ\)](#) に記載されているように、適切なメニューパスとオプションを選択します。

**ステップ2** 現在のワークフロー内で移動します。

- 選択したイベント データタイプで利用可能な列をすべて表示するには、テーブル ビュー ページを使用します。[テーブルビューページの使用 \(2440 ページ\)](#) を参照してください。
- 選択したイベント データタイプで利用可能な列のサブセットを表示するには、ドリルダウン ページを使用します。[ドリルダウン ページの使用 \(2439 ページ\)](#) を参照してください。
- ワークフローの次のページの対応する行を表示するには、青い下矢印アイコン () をクリックします。
- マルチページワークフローのページ間を移動するには、各ページの下部にあるツールを使用します。[ワークフローページのトラバーサルツール \(2436 ページ\)](#) を参照してください。
- 別のタイプのイベントに対してワークフロー内で適用された同じ制約を表示するには、[移動先 (Jump to) ] をクリックし、ドロップダウンリストからイベント ビューを選択します。

**ステップ3** 現在のワークフローの表示を変更します。

- ページ上で1つ以上の行のチェックボックスにマークを付けて、処理を反映させる行を表示し、ページの下部にあるいずれかのボタン ([表示 (View) ] ボタンなど) をクリックして、選択したすべての行に対してそのアクションを実行します。
- 行の上部にあるチェックボックスにマークを付けて、ページ上のすべての行を選択し、ページの下部にあるいずれかのボタン ([表示 (View) ] ボタンなど) をクリックして、ページ上のすべての行に対してそのアクションを実行します。
- 非表示にする列ヘッダーの閉じるアイコン () をクリックして、表示する列を制約します。表示されるポップアップ ウィンドウで、[適用 (Apply) ] をクリックします。




**ヒント** 他のカラムを表示または非表示にするには、[適用 (Apply) ] をクリックする前に、該当するチェックボックスをオンまたはオフにします。無効にした列をビューに戻すには、展開の矢印をクリックして検索の制約を展開し、[無効な列 (Disabled Columns) ] の下の列名をクリックします。

- 選択したフィールドに対して選択した値でデータ ビューを制約します。詳細については、[イベントビューの制約 \(2460 ページ\)](#) および [複合イベントビューの制約 \(2462 ページ\)](#) を参照してください。
- イベントビューの時間の制約を変更します。ページの右上隅に表示される日付の範囲は、ワークフローに含めるイベントの時間範囲を設定します。詳細については、[イベント時間の制約 \(2451 ページ\)](#) を参照してください。

(注) イベントビューを時間によって制約している場合は、(グローバルかイベントに特有かに関係なく) アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベントビューに表示されることがあります。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

- データを列でソートするには、列の名前をクリックします。ソート順序を反転させるには、もう一度列の名前をクリックします。矢印のアイコンは、データのソート基準になっている列、およびソートが昇順である (▲) か、または降順である (▼) かを表します。
- ワークフローページのリンクをクリックして、アクティブな制約を使用しているページを表示します。ワークフロー ページのリンクは、事前定義されたワークフロー テーブルビュー、およびドリルダウンページの左上隅の、イベントの上で、ワークフロー名の下に示されます。

**ステップ 4** 現在のワークフロー内の追加データを表示します。

- ファイルのトラジェクトリ マップを新しいウィンドウで表示するには、ファイル名と SHA-256 ハッシュ値の列のネットワーク ファイル トラジェクトリ アイコンをクリックします。アイコンは、ファイル ステータスによって異なります。 [ファイル トラジェクトリ アイコン \(2436 ページ\)](#) を参照してください。
- IP アドレスに関連付けられたホスト プロファイルのポップアップ ウィンドウを表示するには、IP アドレスの列のホスト プロファイル アイコンをクリックします。アイコンは、ファイル ステータスによって異なります。 [ホスト プロファイルのアイコン \(2437 ページ\)](#) を参照してください。
- ファイルに関連付けられた最も高い脅威スコアの動的分析サマリーレポートを表示するには、いずれかの脅威スコア列の脅威スコアアイコンをクリックします。アイコンは、ファイルの最も高い脅威スコアによって異なります。 [脅威スコアアイコン \(2437 ページ\)](#) を参照してください。
- ユーザ プロファイル情報を表示するには、いずれかのユーザ ID 列でユーザ アイコン ( 、または侵害の兆候に関連付けられたユーザの場合は  ) をクリックします。ユーザ アイコンは、そのユーザがデータベースにない場合 (つまり、AMP for Endpoints Connector ユーザの場合) は淡色表示されます。
- サードパーティの脆弱性の脆弱性詳細を表示するには、いずれかのサードパーティの脆弱性の ID 列の脆弱性アイコン (  ) をクリックします。
- 集約データ ポイントを表示する場合は、ポイントをフラグ アイコンの上に合わせて国名を表示します。
- 個々のデータ ポイントを表示する場合は、フラグ アイコンをクリックして、 [位置情報 \(GeoLocation\) \(2440 ページ\)](#) に記載されている地理位置情報詳細を表示します。

**ステップ 5** 別のワークフローに移動します。

別のワークフローを使用して同じイベントタイプを表示するには、ワークフローのタイトルの横にある（ワークフローの切り替え）をクリックして、使用するワークフローを選択します。スキャン結果には別のワークフローを使用できないことに注意してください。

## ユーザ ロールによるワークフローへのアクセス

ワークフローへのアクセスはユーザのロールにより異なります。詳細については、次の表を参照してください。

ユーザ ロール	アクセス可能なワークフロー
管理者 (Administrator)	すべてのワークフローにアクセスできます。また、Administrator は監査ログ、スキャン結果、およびルール更新のインポートログにアクセスできる唯一のユーザです。
メンテナンスユーザ	ヘルス イベントにアクセスできます。
セキュリティアナリストとセキュリティアナリスト (読み取り専用)	侵入、マルウェア、ファイル、接続、検出、脆弱性、関連、ヘルスワークフローにアクセスできます。

## ワークフローの選択

Firepower システムには、次の表に記載されているデータのタイプに対して、事前定義のワークフローが用意されています。

表 269: ワークフローを使用する機能

機能	メニューパス	オプション
侵入イベント	[分析 (Analysis) ]> [侵入 (Intrusions) ]	イベント 確認済みイベント クリップボード [インシデント (Incidents) ]
マルウェア イベント	[分析 (Analysis) ]> [ファイル (Files) ]	マルウェア イベント
ファイル イベント	[分析 (Analysis) ]> [ファイル (Files) ]	ファイル イベント
キャプチャ ファイル	[分析 (Analysis) ]> [ファイル (Files) ]	キャプチャファイル (Captured Files)

機能	メニューパス	オプション
接続イベント	[分析 (Analysis) ]>[接続 (Connections) ]	イベント
セキュリティ インテリジェンス イベント	[分析 (Analysis) ]>[接続 (Connections) ]	セキュリティ インテリジェンス イベント
ホスト イベント	[分析 (Analysis) ]>[ホスト (Hosts) ]	ネットワーク マップ Hosts Indications of Compromise アプリケーション アプリケーション詳細 (Application Details) サーバ ホスト属性 (Host Attributes) 検出イベント (Discovery Events)
ユーザ イベント	[分析 (Analysis) ]>[ユーザ (Users) ]	ユーザ アクティビティ Users
脆弱性イベント	[分析 (Analysis) ]>[脆弱性 (Vulnerabilities) ]	脆弱性 サードパーティの脆弱性
関連イベント	[分析 (Analysis) ]>[関連 (Correlation) ]	関連イベント (Correlation Events) ホワイトリスト イベント (White List Events) ホワイトリスト違反 (White List Violations) ステータス (Status)
監査イベント	[システム (System) ]>[モニタリング (Monitoring) ]	監査 (Audit)
ヘルス イベント	[ヘルス (Health) ]>[イベント (Events) ]	適用対象外
ルール更新インポート ログ	[システム (System) ]>[更新 (Updates) ]	適用対象外
スキャン結果	[ポリシー (Policies) ]>[アクション (Actions) ]>[スキャナ (Scanners) ]	適用対象外

上記の表に記載されているいずれかの種類のデータを表示する場合、そのデータのデフォルトのワークフローの最初のページにイベントが表示されます。イベントビューの設定項目を設定することによって、別のデフォルトワークフローを指定することができます。ワークフローへのアクセス権限は、ユーザの役割によって異なります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

#### 関連トピック

[イベントビュー設定の設定](#) (37 ページ)

## ワークフローのページ

ワークフローのタイプによってデータは異なりますが、すべてのワークフローで共通の機能セットを共有しています。ワークフローには、数種類のページを含めることができます。ユーザがワークフローのページ上で実行できるアクションは、ページのタイプによって異なります。

ワークフローのドリルダウンのページとテーブルビューのページを使用すれば、データのビューをすばやく絞り込むことができるため、分析にとって重要なイベントに集中できます。テーブルビューのページとドリルダウンのページの両方で、ユーザが表示するイベントセットに制約を適用したり、ワークフローをナビゲートしたりするために使用できる機能が多数サポートされています。ドリルダウンページ、またはワークフロー内のテーブルビューでデータを表示する場合、ソートに使用できる任意のカラムに基づいてデータを昇順または降順でソートできます。1つのワークフローのページに表示できるイベント数よりも多くのイベントがデータベースに含まれている場合は、ページの下部にあるリンクをクリックして、さらにイベントを表示できます。これらのリンクの1つをクリックすると時間枠が自動的に一時停止されるため、同じイベントが2回表示されません。準備ができれば時間枠の一時停止を解除できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

#### テーブルビュー

ページがデフォルトで有効になっている場合、テーブルビューには、ワークフローのベースとなるデータベースの各フィールドに対するカラムが含まれています。

テーブルビューでカラムを無効にし、それによって同じ行が複数生成される場合、Firepower システムによってイベントビューに [カウント (Count)] カラムが追加されます。テーブルビューページで1つの値をクリックすると、その値によって制約することができます。カスタムワークフローを作成する場合は、[テーブルビューの追加 (Add Table View)] をクリックしてテーブルビューを追加します。



## ドリルダウン ページ

ドリルダウン ページは、通常テーブル ビューのページに移動する前に調査対象を絞り込むために使用する中間ページです。ドリルダウンページには、データベースで使用できるカラムのサブセットが含まれています。

たとえば、検出イベントのドリルダウン ページには、[IP アドレス (IP Address) ]、[MAC アドレス (MAC Address) ]、および [時刻 (Time) ] カラムだけが含まれています。また、侵入イベントのドリルダウン ページには、[優先順位 (Priority) ]、[影響フラグ (Impact Flag) ]、[インラインの結果 (Inline Result) ]、および [メッセージ (Message) ] カラムが含まれています。

ドリルダウンページを使用すれば、表示するイベントの範囲を絞り込んだり、ワークフローで先へ進んだりできます。ドリルダウンページで1つの値をクリックすると (たとえば、その値で制約を加えて、ワークフローの次のページに進んだ場合)、選択した値に一致するイベントをさらに詳しく調べることができます。ドリルダウンページで値をクリックした場合、次のページがテーブル ビューであっても、値が存在するカラムは無効になりません。事前定義のワークフローのドリルダウン ページには、必ず [カウント (Count) ] カラムがあることに注意してください。カスタム ワークフローを作成する場合は、[ページの追加 (Add Page) ] をクリックしてドリルダウン ページを追加します。

## グラフ

接続データに基づくワークフローには、グラフ ページ (接続グラフとも呼ばれる) を含めることができます。

たとえば接続グラフには、一定期間にシステムで検出された接続の数を示す線グラフを表示することができます。一般的に接続グラフは、ドリルダウンページと同様に、ユーザが調査対象を絞り込むために使用する中間ページです。

## 最終ページ

ワークフローの最終ページは、ワークフローがベースとするイベントのタイプによって異なります。

- ホスト ビューとは、アプリケーション、アプリケーションの詳細、検出イベント、ホスト、侵害の兆候 (IOC)、サーバ、ホワイトリスト違反、ホスト属性、またはサードパーティ製の脆弱性に基づいたワークフローの最終ページです。このページからホスト プロファイルを表示することにより、ユーザは、複数のアドレスを持つホストに関連付けられているすべての IP アドレス上のデータを簡単に表示することができます。
- ユーザの詳細ビューとは、ユーザとユーザアクティビティに基づいたワークフローの最終ページです。
- 脆弱性の詳細ビューとは、Cisco の脆弱性に基づいたワークフローの最終ページです。
- パケット ビューは、侵入イベントに基づいたワークフローの最終ページです。

他の種類のイベント (監査ログ イベントやマルウェア イベントなど) に基づいたワークフローには、最終ページがありません。

ワークフローの最終ページで詳細セクションを展開して、ワークフローの進行中に絞り込んだセットの各オブジェクトについて、具体的な情報を表示することができます。Web インターフェイスでは、ワークフローの最終ページに制約が表示されませんが、以前に設定した制約は保持されており、データのセットに適用されます。

## ワークフロー ページのナビゲーション ツール

ワークフローのページには、ページ間の移動と、イベントの分析中に表示する情報の選択を容易にする視覚的なキューが用意されています。

## ワークフロー ページのトラバーサル ツール

ワークフローに複数のデータ ページが含まれている場合は、各ページの下部にワークフロー内のページ数と、ページ間を移動するために使用できるツールが表示されます。これらのツールを次の表に示します。

表 270: ワークフロー ページのトラバーサル ツール




ページのトラバーサル ツール	操作
ページ番号 (別のページを表示するには、表示する番号を入力して Enter キーを押します。)	別のページを表示する
>	次のページを表示する
<	前のページを表示する
>	最後のページに移動する
<	最初のページに移動する

## ファイル トラジェクトリ アイコン

ワークフロー ページで、新しいウィンドウにファイルのトラジェクトリ マップを表示する機会があるときは、ネットワーク トラジェクトリ アイコンが表示されます。このアイコンは、ファイルのステータスによって変わります。

表 271: ファイル トラジェクトリ アイコン





ファイル トラジェクトリ アイコン	ファイル ステータス
	正常
	マルウェア

ファイルトラジェクトリアイコン	ファイルステータス
	カスタム検出
	不明
	使用不可

## ホスト プロファイルのアイコン

ワークフロー ページでは、IP アドレスに関連付けられたホスト プロファイルをポップアップ ウィンドウで表示することができ、ホスト プロファイルアイコンが表示されます。ホスト プロファイルのアイコンがグレー表示になっている場合は、ネットワーク マップ内にそのホストが存在することができないため、ホスト プロファイルを表示できません (0.0.0.0 など)。このアイコンは、ホストのステータスによって異なって表示されます。

表 272: ホスト プロファイルのアイコン

ホスト プロファイルのアイコン	ホストステータス
	ホストは潜在的に危険にさらされているとタグ付けされていません。
	ホストは、トリガーされた侵害の兆候 (IOC) ルールによって潜在的に危険にさらされているとタグ付けされています。
	ブラックリスト化されています (セキュリティインテリジェンス データに基づいて、トラフィック フィルタリングを実行している場合にのみ表示されます)。
	ブラックリスト化され、モニタに設定されています (セキュリティインテリジェンス データに基づいて、トラフィック フィルタリングを実行している場合にのみ表示されます)。

## 脅威スコア アイコン

ワークフロー ページで、ファイルに関連付けられているスコアが最も高い脅威に関する動的分析サマリ レポートを表示すると、脅威スコアアイコンが表示されます。このアイコンは、ファイルの最も高い脅威スコアに応じて異なります。

表 273: 脅威スコア アイコン

脅威スコア アイコン	脅威スコア レベル
	低 (Low)
	中規模 (Medium)
	高 (High)
	非常に高い (Very high)

## ワークフロー ツールバー

ワークフローの各ページには、関連する機能へすばやくアクセスするためのツールバーがあります。次の表で、ツールバー上の各リンクについて説明します。

表 274: ワークフロー ツールバーのリンク

機能	説明
このページをブックマーク	後でそのページに戻れるように、現在のページをブックマークします。ブックマークすると、表示中のページに適用されている制約が取得され、データがまだ存在している場合は後で同じデータに戻ることができます。
レポート作成者	現在制約されているワークフローを選択基準として使用して、レポート デザイナを開きます。
ダッシュボード	現行のワークフローに関連するダッシュボードを開きます。たとえば、[接続イベント (Connection Events)] ワークフローは [接続サマリ (Connection Summary)] ダッシュボードと関連付けられています。
ブックマークの表示	ユーザが選択できる、保存したブックマークのリストを表示します。
検索 (Search)	ワークフローのデータについて高度な検索を実行できる [検索 (Search)] ページが表示されます。下向きの矢印アイコンをクリックし、保存済みの検索を選択して使用することもできます。

### 関連トピック

[イベントビューからのレポートテンプレートの作成 \(2312 ページ\)](#)

[ダッシュボードについて \(247 ページ\)](#)

[イベントの検索 \(2467 ページ\)](#)

[ブックマーク](#) (2464 ページ)

[ブックマークの作成](#) (2465 ページ)

[ブックマークの表示](#) (2465 ページ)

## ドリルダウン ページの使用

スマート ライセ ンス	従来のライセンス	サポートされるデ バイス	サポートされるド メイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst (ワークフローに 応じて異なりま す)

### 手順

**ステップ 1** 「[表 269: ワークフローを使用する機能](#)」の説明に従って、適切なメニューパスとオプションを選択してワークフローにアクセスします。

**ステップ 2** すべてのワークフローで、次のオプションを選択できます。

- 特定の値に制限して、次のワークフロー ページにドリルダウンするには、行内の値をクリックします。この処理はドリルダウンページでのみ可能でることに注意してください。テーブルの行内の値をクリックしても、テーブルビューが制約されるだけで、次のページにはドリルダウンしません。
- いくつかのイベントによって制約したまま次のワークフローページにドリルダウンするには、次のワークフロー ページに表示させるイベントの横のチェック ボックスを選択し、[表示 (View) ] をクリックします。
- 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[すべて表示 (View All) ] をクリックします。

**ヒント** テーブル ビューでは、必ずページ名に「Table View」が含まれます。

## テーブル ビュー ページの使用

スマート ライセ ンス	従来のライセンス	サポートされるデ バイス	サポートされるド メイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst (ワークフローに 応じて異なりま す)

テーブル ビュー ページには、ドリルダウン、ホストビュー、パケットビュー、脆弱性の詳細ページでは利用できない機能が用意されています。これらの機能は次のように使用します。

### 手順

**ステップ 1** [ワークフローの選択 \(2432 ページ\)](#) の説明に従って、適切なメニューパスとオプションを選択してワークフローにアクセスします。

**ステップ 2** ワークフローの名前の下に表示されるワークフローパスからテーブル ビューを選択します。

**ステップ 3** 必要に応じて、次に示す機能を使用してテーブルビュー内に配置したり、移動したりします。

- 無効なカラムのリストを表示するには、[検索制約 (Search Constraints)] の展開矢印 (▼) をクリックします。
- 無効なカラムのリストを非表示するには、[検索制約 (Search Constraints)] の折りたたみ矢印 (▲) をクリックします。
- 無効になったカラムをイベント ビューに戻すには、[検索制約 (Search Constraints)] の展開アイコン (▼) をクリックして検索制約を展開し、[無効カラム (Disabled Columns)] の下にあるカラム名をクリックします。
- カラムを表示または非表示 (無効) には、各カラム名の横にあるクリア アイコン (✕) をクリックします。表示されるポップアップウィンドウで、該当するチェックボックスをオンまたはオフにして、どのカラムを表示するかを指定し、[適用 (Apply)] をクリックします。

## 位置情報 (GeoLocation)

地理位置情報機能によって、ルート可能な IP アドレスの地理的な送信元についてのデータ (国や大陸など) が提供されます。この情報は、イベント、資産のプロファイル、コンテキストエクスペローラ、ダッシュボードやその他の分析ツールで使用できます。



(注) 国間を移動するモバイルデバイスやその他のホストが検出された場合、システムは特定の国ではなく大陸名を報告する可能性があります。

地理位置情報データを使用してネットワークトラフィックをフィルタできます。たとえば、接続の発信元または終端が、組織と関連性のない国であるかどうかを判別できます。インライン展開では、これらの接続をブロックするか、またはレート制限を行うことができます。

地理位置情報データはシステムの地理位置情報データベース (GeoDB) 内に保存されます。シスコでは、GeoDB の定期的な更新を提供しています。[概要 (About) ] ページ ([ヘルプ (Help) ] > [概要 (About) ]) に GeoDB の現在の更新バージョンが表示されています。

GeoDB の更新を許可する場合、Firepower Management Center Web インターフェイスで小さな国旗のアイコンと ISO 国番号をクリックして特定の IP アドレスに関する地理位置情報の詳細を取得することができます。地理情報の詳細情報 (2441 ページ) を参照してください。また、サードパーティのマッピングツールを使用して、検出された場所を特定することもできます。GeoDB を更新しない場合、これらの詳細情報は取得できません。

[接続のサマリ (Connection Summary) ] ダッシュボードなど、集約的な地理位置情報から詳細の地理位置情報を表示することはできません。

#### 関連トピック

[ネットワーク条件](#) (377 ページ)

[地理位置情報オブジェクト](#) (443 ページ)

[関連ポリシーとルールの概要](#) (2223 ページ)

[トラフィック プロファイル条件](#) (2271 ページ)

[地理位置情報データベースの更新](#) (192 ページ)

## 地理情報の詳細情報

可用性に応じて、[地理情報の詳細 (Geolocation Details) ] ページに多数のフィールドが表示される場合があります。次の表で、これらのフィールドの情報について示します。(情報がないフィールドは表示されません。)

表 275: 地理情報の詳細フィールド

フィールド	目次
国 (Country)	ホスト IP アドレスに関連付けられている国が国旗とともに示されます。大陸はカッコ内に表示されます。例: United States (North America)、Equatorial Guinea (Africa)
地域	ホストが存在する国の州、県、またはその他の小区域。例: VA、35
市区町村郡 (City)	ホストが存在する市。例: Seattle、Fukuoka
[郵便番号 (Postal Code) ]	ホストが存在する地域の郵便番号。例: 361000、90210

フィールド	目次
緯度/経度 (Latitude/Longitude)	ホストの場所の正確な座標。例：40.0375, -76.1053、53.4050, -0.5484
マップ	外部のマッピングサイト (Google Maps、Yahoo Maps、Bing Maps、OpenStreetMap など) へのリンク。ホストのおよその位置のコンテキスト マップを表示するには、リンクをクリックします。
タイムゾーン (Timezone)	ホストの場所のタイムゾーン (該当する場合には夏時間が示されます)。例：GMT+8:00、GMT-4:00 (In DST)
ASN	ホスト IP アドレスに関連付けられている自律システム番号 (ASN)、およびその ASN に関する追加情報。例：14618 (Amazon.com Inc.)、4837 (Cncgroup China169 Backbone)
ISP	ホストの IP アドレスに関連付けられているインターネット サービス プロバイダー (ISP)。例：Atlantic Broadband、China Unicom Ip Network
自宅/会社 (Home/Business)	ホストの接続が自宅または会社のどちらの目的であることを示します。
Organization	ホストの IP アドレスに関連付けられている組織。例：Amazon.com、Bank of America
ドメイン名 (Domain Name)	ホストの IP アドレスに関連付けられているドメイン名。例：amazonaws.com、xmcnc.net
接続タイプ (Connection Type)	ホストの IP アドレスに関連付けられている接続タイプ。例：Broadband、DSL
プロキシタイプ (Proxy Type)	使用するプロキシのタイプ。例：Anonymous、Corporate

## 接続イベントグラフ

システムは、テーブル形式のドリルダウン ページを使ったワークフローや最終的なイベントのテーブル表示に加えて、5 分間隔で集計されたデータを使用して、特定の接続データをグラフィック表示することができます。グラフ表示できるのは、データを集約するのに使用する情報 (送信元と宛先の IP アドレス (およびこれらのホストに関連するユーザ)、宛先ポート、トランスポート プロトコルとアプリケーション プロトコル) のみです。





**ヒント** セキュリティ インテリジェンス イベントを関連する接続イベントとは別にグラフ表示することはできません。セキュリティ インテリジェンスのフィルタリング アクティビティの概要をグラフィック表示するには、ダッシュボードとコンテキスト エクスプローラを使用します。

接続グラフは 3 種類あります。

- 円グラフは、1 つのデータセットのデータをカテゴリ分けして表示します。
- 棒グラフは、1 つあるいは複数のデータセットのデータをカテゴリ分けして表示します。
- 折れ線グラフは、時間の経過に伴って 1 つあるいは複数のデータセットのデータをプロットします。標準ビューあるいは速度 (変化のペース) ビューを使用します。



**(注)** システムは、トラフィック プロファイルを線グラフで表示します。他の接続グラフと同様に操作可能ですが、いくつか規制があります。トラフィック プロファイルを表示するには、管理者 アクセス権が必須です。

ワークフロー テーブルと同様に、ワークフロー グラフもドリル ダウンし、制約を加えることで分析的を絞ることができます。

棒グラフおよび折れ線グラフはどちらも複数のデータセットを表示できます。つまり、各 X 軸 データ ポイントに対し、Y 軸に複数の値を表示できます。たとえば、一意のイニシエータとレスポンドの総数を表示することができます。円グラフでは、1 つのデータセットのみ表示できます。

X 軸または Y 軸、もしくは両方を変更することによって、接続グラフにさまざまなデータやデータセットを表示できます。円グラフでは、X 軸を変更すると独立変数が変わり、Y 軸を変更すると従属変数を変ります。

**関連トピック**

[接続の概要 \(グラフ用集約データ\)](#) (2522 ページ)

## 接続イベント グラフの使用法

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	(ワークフローに応じて) Admin/Maint/Any Security Analyst

Firepower Management Center では、検索する情報に応じて、接続イベント グラフを表示したり操作したりできます。

接続グラフにアクセスしたときに表示されるページは、使用するワークフローによって異なります。接続イベントのテーブルビューで終了する、事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

## 手順

**ステップ 1** [分析 (Analysis)] > [接続 (Connections)] > [イベント (Events)] を選択します。

(注) 接続イベントテーブルがグラフの代わりに表示される場合、または別のグラフを表示する場合は、ワークフロータイトルの横にある (ワークフローの切り替え) をクリックし、グラフが含まれる事前定義されたワークフローまたはカスタムワークフローを選択します。接続グラフを含むすべての事前定義された接続イベント ワークフローは、接続のテーブルビューで終了します。

**ステップ 2** 次の選択肢があります。

- [時間範囲 (Time Range)] : 時間範囲を調整する場合は (グラフがブランクの場合に役立ちます) 、 [時間枠の変更 \(2455 ページ\)](#) を参照してください。
- [フィールド名 (Field Name)] : ユーザが図示可能なデータの詳細については、 [接続およびセキュリティインテリジェンスイベントフィールド \(2523 ページ\)](#) を参照してください。
- [ホスト プロファイル (Host Profiles)] : IP アドレスのホスト プロファイルを表示するには、発信側または応答側による接続データが表示されているグラフで、棒グラフの棒または円グラフの扇形をクリックし、[ホスト プロファイルの表示 (View Host Profile)] を選択します。
- [ユーザ プロファイル (User Profile)] : ユーザ プロファイル情報を表示するには、発信側ユーザによる接続データが表示されているグラフで、棒グラフの棒または円グラフの扇形をクリックし、[ユーザ プロファイルの表示 (View User Profile)] を選択します。
- [その他の情報 (Other Information)] : 図示されたデータに関する詳細については、折れ線グラフの点、棒グラフの棒、または円グラフの扇形の上にカーソルを置きます。
- [固定 (Constrain)] : ワークフローを次のページに進めずに接続グラフを X 軸 (独立した変数) 基準で固定するには、折れ線グラフの点、棒グラフの棒、または円グラフの扇形をクリックし、[表示方法 (View by)] オプションを選択します。
- [データ選択 (Data Selection)] : グラフに表示されるデータを変更するには、[X 軸 (X-Axis)] または [Y 軸 (Y-Axis)] をクリックし、図示する新しいデータを選択します。X 軸を [時間 (Time)] に変更、または [時間 (Time)] から変更すると、グラフ タイプも変更されます。Y 軸を変更すると、表示されるデータセットに影響します。

- [データセット (Datasets) ]: グラフのデータセットを変更するには、[データセット (Datasets) ]をクリックし、新しいデータセットを選択します。
- [切り離し (Detach) ]: デフォルトの時間範囲に影響を与えずにさらに分析を実行できるように接続グラフを分離するには、[切り離し (Detach) ]をクリックします。  
**ヒント** コピーを作成するには、分離したグラフで[新規ウィンドウ]をクリックします。分離した各グラフ上で、別々の分析ができるようになります。トラフィックプロファイルは、分離したグラフです。
- [詳細 (Drill-Down) ]: ワークフローで次のページにドリルダウンするには、折れ線グラフの点、棒グラフの線、または円グラフの扇形をクリックし、[詳細 (Drill-Down) ]を選択します。折れ線グラフで点をクリックすると、次のページの時間枠は、クリックした点を中心とする 10 分間に変更されます。棒グラフの棒または円グラフの扇形をクリックすると、その棒または扇形が表す基準に基づいて次のページが制約されます。
- [エクスポート (Export) ]: グラフの接続データを CSV (カンマ区切り値) ファイルとしてエクスポートするには、[データのエクスポート (Export Data) ]を選択します。次に、[CSV ファイルのダウンロード (Download CSV File) ]をクリックし、ファイルを保存します。
- [グラフ タイプ (Graph Type) ]: [折れ線 (Line) ]- 標準と速度 (変化のペース) の折れ線グラフを切り替えるには、[速度 (Velocity) ]をクリックし、[標準 (Standard) ]または[速度 (Velocity) ]を選択します。
- [グラフ タイプ (Graph Type) ]: [棒と円 (Bar and Pie) ]- 棒グラフと円グラフを切り替えるには、[棒グラフに切り替え (Switch to Bar) ]または[円グラフに切り替え (Switch to Pie) ]をクリックします。円グラフには複数のデータセットを表示できないため、複数のデータセットを持つ棒グラフから円グラフに切り替えた場合、円グラフは自動的に選択された1つのデータセットだけを表示します。表示するデータセットを選択する際、Firepower Management Center は、発信側と応答側の統計情報よりも全体の統計情報を優先し、応答側の統計情報よりも発信側の統計情報を優先します。
- [ページ間の移動 (Navigate Between Pages) ]: 現在のワークフローで現在の制約を保持したままページ間を移動するには、ワークフロー ページの左上にある該当するページリンクをクリックします。
- [イベント ビュー間の移動 (Navigate Between Event Views) ]: 他のイベント ビューに移動して関連するイベントを表示するには、[移動先 (Jump to) ]をクリックし、ドロップダウンリストからイベント ビューを選択します。
- [再センタリング (Recenter) ]: 時間範囲の長さを変更せずにある時点を中心に折れ線グラフを再センタリングするには、その点をクリックし、[再センタリング (Recenter) ]を選択します。
- [ズーム (Zoom) ]: ズームインまたはズームアウトしながらある時点を中心に折れ線グラフを再センタリングするには、その点をクリックし、[ズーム (Zoom) ]を選択してから新しい時間枠を選択します。

(注) 分離したグラフを使用している場合を除いて、制約、再センタリング、およびズームすると Firepower Management Center のデフォルトの時間範囲が変わります。

#### 例：接続グラフの制約

##### 例：円グラフの X 軸と Y 軸の変更

ある期間の接続のグラフについて考えてみましょう。グラフ上の点をポートによって制約すると、検出された接続イベント数に基づいて、最もアクティブだった 10 のポートを示す棒グラフが表示されますが、クリックした点を中心とする 10 分間の時間枠によって制約されます。

棒の 1 つをクリックし、[発信側 IP による表示 (View by Initiator IP)] を選択してグラフをさらに制約すると、それまでと同じ 10 分間の時間枠だけでなく、クリックした棒が表示するポートでも制約された新しい棒グラフが表示されます。

ポートごとのキロバイト数を表示する円グラフについて考えてみましょう。この場合、X 軸は **レスポンドポート**、Y 軸は **キロバイト** です。この円グラフは、ある間隔に監視対象ネットワークで送信されたデータの合計キロバイト数を表します。円の中の扇形は、各ポートで検出されたデータの比率を表します。

- グラフの X 軸を **アプリケーション プロトコル** に変更すると、引き続き円グラフは送信データの合計キロバイト数を表しますが、円の中の扇形は検出された各アプリケーション プロトコルの送信データの比率を表します。
- グラフの Y 軸を **パケット** に変更すると、円グラフはある間隔に監視対象ネットワークで送信された合計パケット数を表し、円の中の扇形は各ポートで検出された合計パケット数の割合を表します。

#### 関連トピック

[ワークフローの使用](#) (2429 ページ)

[イベント ビュー設定の設定](#) (37 ページ)

#### 接続グラフ データ オプション

X 軸または Y 軸、もしくは両方を変更することによって、接続グラフにさまざまなデータを表示できます。円グラフでは、X 軸を変更すると独立変数が変わり、Y 軸を変更すると従属変数が変わります。

表 276: X軸オプション

X 軸オプション	グラフの種類	次の基準でこのデータをグラフ化する
アプリケーションプロトコル (Application Protocol)	棒グラフまたは円グラフ	最もアクティブな 10 個のアプリケーションプロトコルに基づいて
Device	棒グラフまたは円グラフ	最もアクティブな 10 台の管理対象デバイスに基づいて
イニシエータ IP (Initiator IP)	棒グラフまたは円グラフ	最もアクティブな 10 個のイニシエータホスト IP アドレスに基づいて
イニシエータユーザ (Initiator User)	棒グラフまたは円グラフ	最もアクティブな 10 名のイニシエータユーザに基づいて
レスポнда IP (Responder IP)	棒グラフまたは円グラフ	最もアクティブな 10 個のレスポндаホスト IP アドレスに基づいて
レスポндаポート (Responder Port)	棒グラフまたは円グラフ	最もアクティブな 10 個のレスポндаポートに基づいて
送信元デバイス (Source Device)	棒グラフまたは円グラフ	最もアクティブな 10 個の NetFlow データ エクスポートと、Firepower システムの管理対象デバイスによって検出されたすべての接続の Firepower という名前の送信元デバイスに基づいて。
時刻 (Time)	ライン	時系列  Y 軸と [時刻 (Time) ] を切り替えることでグラフの種類も変わり、データセットを変更できます。

表 277: Y軸オプション

Y 軸オプション	X軸の基準を使用してこのデータをグラフ化する
バイト (Bytes)	送信バイト数
接続 (Connections)	接続数

Y 軸オプション	X軸の基準を使用してこのデータをグラフ化する
KB (KBytes)	送信キロバイト数
KB/秒 (KBytes Per Second)	KB/秒
パケット (Packets)	送信パケット数
固有のホスト (Unique Hosts)	検出された固有のホスト数
固有のアプリケーション プロトコル (Unique Application Protocols)	固有のアプリケーション プロトコル数
固有ユーザ (Unique Users)	固有ユーザ数

### 複数のデータセットの接続グラフ

棒グラフおよび折れ線グラフはどちらも複数のデータセットを表示できます。つまり、各 X 軸データポイントに対し、Y 軸に複数の値を表示できます。たとえば、一意のイニシエータとレスポンドの総数を表示することができます。



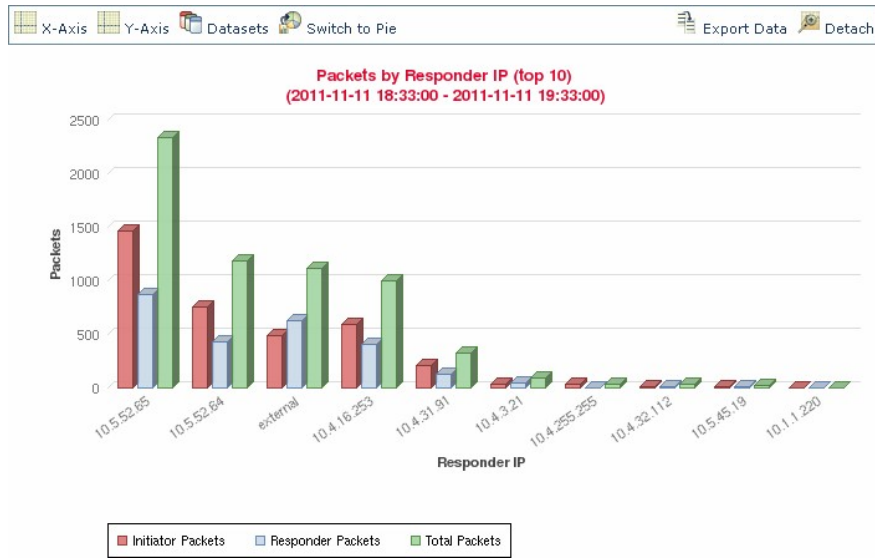
- (注) 円グラフには複数のデータセットを表示できません。複数のデータセットを持つ棒グラフから円グラフに切り替えた場合、円グラフは自動的に選択された1つのデータセットだけを表示します。表示するデータセットを選択する際、Firepower Management Center は、イニシエータとレスポンドの統計情報よりも全体の統計情報を優先し、イニシエータの統計情報よりもレスポンドの統計情報を優先します。

折れ線グラフでは、複数のデータセットは複数の線として、それぞれ異なる色で表示されます。たとえば次のグラフは、監視対象ネットワークにおいて1時間の間に検出された一意のイニシエータの合計数と一意のレスポンドの合計数を表示しています。



371.989

棒グラフでは、複数のデータセットが X 軸データ ポイントごとに色分けされた棒として表示されます。たとえば次の棒グラフは、監視対象ネットワーク上で送信されたパケットの合計数と、イニシエータによって送信されたパケット数、レスポндаによって送信されたパケット数を表示しています。



371.988

### 接続グラフ データセットオプション

次の表では、接続グラフの x 軸に表示できるデータセットについて説明します。

表 278: データセット オプション

y 軸が表示されている場合は、	データベースとして選択できます。
接続 (Connections)	デフォルトのみです。監視対象のネットワークで検出された接続数 ([接続 (Connections)]) です。これは、トラフィックプロファイルグラフ用の唯一のオプションです。
KB (KBytes)	以下を組み合わせています。 <ul style="list-style-type: none"> <li>• 監視対象のネットワークで送信される合計キロバイト ([合計キロバイト (Total KBytes)])</li> <li>• 監視対象のネットワークでホスト IP アドレスから送信されるキロバイト数 ([イニシエータのキロバイト (Initiator KBytes)])</li> <li>• 監視対象のネットワークでホスト IP アドレスによって受信されるキロバイト数 ([レスポンドのキロバイト (Responder KBytes)])</li> </ul>
KB/秒 (KBytes Per Second)	デフォルトのみです。監視対象ネットワーク上で送信される合計キロバイト/秒 ([合計キロバイト/秒 (Total KBytes Per Second)]) です。
パケット	以下を組み合わせています。 <ul style="list-style-type: none"> <li>• 監視対象ネットワークで送信される合計パケット ([合計パケット (Total Packets)])</li> <li>• 監視対象ネットワークのホスト IP アドレスから送信されたパケット数 ([イニシエータ パケット (Initiator Packets)])</li> <li>• 監視対象ネットワークのホスト IP アドレスによって受信されたパケット数 ([レスポンド パケット (Responder Packets)]) です。</li> </ul>



y 軸が表示されている場合は、	データベースとして選択できます。
固有のホスト (Unique Hosts)	以下を組み合わせています。 <ul style="list-style-type: none"> <li>監視対象ネットワークの固有セッションイニシエータ数 ([固有イニシエータ (Unique Initiators) ]) です。</li> <li>監視対象ネットワークの固有セッションレスポンド数 ([固有レスポンド (Unique Responders) ])</li> </ul>
固有のアプリケーションプロトコル (Unique Application Protocols)	デフォルトのみです。監視対象ネットワークの固有のアプリケーションプロトコル数 ([固有アプリケーションプロトコル (Unique Application Protocols) ]) です。
固有ユーザ (Unique Users)	デフォルトのみです。監視対象のネットワークでのセッションイニシエータにログインした固有ユーザ数 ([固有イニシエータ ユーザ (Unique Initiator Users) ]) です。

## イベント時間の制約

各イベントには、そのイベントがいつ発生したかを示すタイムスタンプがあります。時間枠（時間範囲とも呼ばれる）を設定することによって、いくつかのワークフローに表示される情報を制約することができます。

時間によって制約できるイベントに基づいたワークフローには、ページの上部に時間範囲を表す行が含まれています。デフォルトでは、シスコアプライアンス上のワークフローは、1時間前が開始時間として設定された時間枠を使用します。たとえば、午前 11:30 にログインした場合、午前 10:30～11:30 の間に発生したイベントが表示されます。時間が経過するにしたがって、時間枠が拡張されます。午後 12:30 には、午前 10:30～午後 12:30 の間に発生したイベントが表示されます。

イベントビューの設定で独自のデフォルト時間枠を設定することによって、この動作を変更することができます。これにより、次の 3 つのプロパティが影響を受けます。

- 時間枠のタイプ（静的、拡張、またはスライディング）
- 時間枠の長さ
- 時間枠の数（複数の時間枠、または単一のグローバル時間枠）

ページの上にある時間範囲をクリックして [日時 (Date/Time) ] ポップアップ ウィンドウを表示し、デフォルトの時間枠の設定に関係なく、イベントの分析中に時間枠を手動で変更することができます。設定した時間枠の数、および使用しているアプライアンスのタイプに応じて

[日時 (Date/Time) ]ウィンドウを使用して、表示しているイベントのタイプに対するデフォルトの時間枠を変更することもできます。

最後に、時間枠は一時停止することができるため、時間枠の変更と削除、または必要のないイベントを追加することなく、ワークフローで提供されたデータを調べることができます。ページの下部にあるリンクをクリックしてイベントの他のページを表示する場合は、異なるワークフローページで同じイベントを表示しないように、時間枠が自動的に一時停止することに注意してください。準備ができたなら時間枠の一時停止を解除できます。

#### 関連トピック

[イベント ビュー設定の設定 \(37 ページ\)](#)

[接続およびセキュリティ インテリジェンス イベント テーブルの使用 \(2548 ページ\)](#)

## イベントの時間枠のカスタマイズ

デフォルトの時間枠に関係なく、イベントの分析中に時間枠を手動で変更することができます。



(注) 手動による時間枠の設定は、現在のセッションについてのみ有効です。いったんログアウトしてからもう一度ログインすると、時間枠はデフォルトにリセットされます。

ユーザが設定した時間枠の数によっては、1つのワークフローの時間枠の変更が、アプライアンス上の他のワークフローに影響を与えることがあります。たとえば、単一のグローバル時間枠がある場合、1つのワークフローの時間枠を変更すると、アプライアンス上の他のすべてのワークフローの時間枠が変更されます。一方、複数の時間枠を使用している場合は、監査ログまたはヘルスイベントのワークフローの時間枠を変更しても、他の時間枠には影響を与えませんが、他の種類のイベントの時間枠を変更すると、時間で制約できるすべてのイベント（監査イベントとヘルスイベントは除く）が影響を受けます。

すべてのワークフローを時間によって制約できるわけではないため、時間枠の設定は、ホスト、ホスト属性、アプリケーション、アプリケーションの詳細、脆弱性、ユーザ、またはホワイトリスト違反に基づいたワークフローには影響を与えないことに注意してください。

[日付/時刻 (Date/Time) ]ウィンドウの [時間枠 (Time Window) ]タブを使用して、時間枠を手動で設定します。デフォルトの時間枠設定で設定した時間枠の数によって、タブのタイトルは以下のいずれかになります。

- [イベントの時間枠 (Events Time Window) ] : 複数の時間枠を設定し、監査ログまたはヘルスイベントのワークフロー以外のワークフローに対して時間枠を設定している場合
- [ヘルス モニタリングの時間枠 (Health Monitoring Time Window) ] : 複数の時間枠を設定し、ヘルスイベントのワークフローに対して時間枠を設定している場合
- [監査ログの時間枠 (Audit Log Time Window) ] : 複数の時間枠を設定し、監査ログに対して時間枠を設定している場合
- [グローバル時間枠 (Global Time Window) ] : 単一の時間枠を設定している場合

時間枠を設定する場合には、最初に、使用する時間枠のタイプを決定する必要があります。

- 静的 (*static*) の時間枠では、特定の開始時刻から特定の終了時刻までの間に生成されたすべてのイベントが表示されます。
- 拡張 (*expanding*) の時間枠では、特定の開始時刻から現在までの間に生成されたすべてのイベントが表示されます。そして、時間の経過とともに時間枠が拡張され、新しいイベントがイベントビューに追加されます。
- スライディング (*sliding*) の時間枠では、特定の開始時刻 (たとえば、1週間前) から現在までの間に生成されたすべてのイベントが表示されます。そして、時間の経過とともに時間枠が「スライド」するため、設定した範囲 (この例では、過去1週間) のイベントのみが表示されます。

選択したタイプによって、[日付/時刻 (Date/Time) ] ウィンドウが変化し、さまざまな設定オプションが提供されます。



(注) Firepower システムでは、タイムゾーンの設定に指定された時間に基づいて、24 時間の時計を使用します。

### 時間枠の設定

次の表で、[時間枠 (Time Window) ] タブで設定できるさまざまな項目について説明します。

表 279: 時間枠の設定

設定	時間枠のタイプ	説明
[時間枠タイプ (time window type) ] ドロップダウン リスト	適用対象外	<p>使用する時間枠のタイプとして、[静的 (<i>static</i>) ]、[拡張 (<i>expanding</i>) ]、または [スライディング (<i>sliding</i>) ] のいずれかを選択します。</p> <p>イベントビューを時間で制約している場合は、(グローバルであるかイベントに特有であるかに関係なく) アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベントビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。</p>

設定	時間枠のタイプ	説明
[開始時刻 (Start Time) ] カレンダー	[静的 (static) ] および [拡張 (expanding) ]	<p>時間枠の開始日と時刻を指定します。すべての時間枠の最大時間範囲は、1970年1月1日午前0時 (UTC) ~ 2038年1月19日午前3時14分7秒です。</p> <p>カレンダーを使用する代わりに、下記で説明するプリセットオプションを使用することもできます。</p>
[終了時刻 (End Time) ] カレンダー	静的	<p>時間枠の終了日と時刻を指定します。すべての時間枠の最大時間範囲は、1970年1月1日午前0時 (UTC) ~ 2038年1月19日午前3時14分7秒です。</p> <p>拡張時間枠を使用している場合は、[終了時刻 (End Time) ] カレンダーがグレー表示になり、終了時刻が「現在の時刻 (Now) 」と示されることに注意してください。</p> <p>カレンダーを使用する代わりに、下記で説明するプリセットオプションを使用することもできます。</p>
[最後を表示 (Show the Last) ] フィールドおよびドロップダウンリスト	[スライディング (sliding) ]	スライディング時間枠の長さを設定します。
[プリセット (Presets) ] : [最後 (Last) ]	すべて	リスト内のいずれかの時間範囲をクリックし、アプライアンスのローカル時刻に基づいて時間枠を変更します。たとえば、[1週間 (1 week) ] をクリックすると、最後の1週間を反映するように時間枠が変わります。プリセットをクリックすると、選択したプリセットを反映するようにカレンダーが変わります。

設定	時間枠のタイプ	説明
[プリセット (Presets) ] : [現在 (Current) ]	[静的 (static) ] および [拡張 (expanding) ]	<p>リスト内のいずれかの時間範囲をクリックし、アプライアンスのローカル時刻と日付に基づいて時間枠を変更します。プリセットをクリックすると、選択したプリセットを反映するようにカレンダーが変わります。</p> <p>次の点に注意してください。</p> <ul style="list-style-type: none"> <li>• 現在の日付は午前 0 時から始まる</li> <li>• 現在の週は日曜日の午前 0 時から始まる</li> <li>• 現在の月は、月の最初の日の午前 0 時から始まる</li> </ul>
[プリセット (Presets) ] : [同期先 (Synchronize with) ]	すべて (グローバルな時間枠を使用している場合は使用不可)	<p>以下のいずれかをクリックします。</p> <ul style="list-style-type: none"> <li>• [イベントの時間枠 (Events Time Window) ] : 現在の時間枠とイベントの時間枠を同期する場合</li> <li>• [ヘルス モニタリングの時間枠 (Health Monitoring Time Window) ] : 現在の時間枠とヘルスマニタリングの時間枠を同期する場合</li> <li>• [監査ログの時間枠 (Audit Log Time Window) ] : 現在の時間枠と監査ログの時間枠を同期する場合</li> </ul>

時間枠の変更

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst (ワークフローに応じる)

## 手順

**ステップ 1** 時間により制約されたワークフローで、時間範囲のアイコン (🕒) をクリックし、[日付と時間 (Date/Time)] ウィンドウを開きます。

**ステップ 2** [イベントの時間枠 (Events Time Window)] タブで、[時間枠の設定 \(2453 ページ\)](#) に記載されているように時間枠を設定します。

ヒント 時間枠をデフォルトの設定に戻すには、[リセット (Reset)] をクリックします。

**ステップ 3** [適用 (Apply)] をクリックします。

## イベントのデフォルト時間枠

イベントの分析中に、[日付/時間 (Date/Time)] ウィンドウの [設定 (Preferences)] タブを使用し、表示しているイベントのタイプに対するデフォルトの時間枠を (イベントビューの設定を使用せずに) 変更することができます。

この方法でデフォルトの時間枠を変更すると、表示しているイベントのタイプのデフォルト時間枠のみが変わります。たとえば、複数の時間枠を設定している場合に [設定 (Preferences)] タブでデフォルトの時間枠を変更すると、イベント、ヘルス モニタリング、または監査ログ ウィンドウのいずれかの設定が変更されます。つまり、最初のタブで示されている時間枠が変更されます。1 つの時間枠を設定している場合に [設定 (Preferences)] タブでデフォルトの時間枠を変更すると、イベントのすべてのタイプのデフォルト時間枠が変わります。

## 関連トピック

[デフォルト時間枠 \(41 ページ\)](#)

## イベントタイプのデフォルトの時間枠オプション

次の表で、[設定 (Preferences)] タブで設定できるさまざまな設定について説明します。

表 280: 時間枠の設定

設定	説明
更新間隔 (Refresh Interval)	イベントビューの更新間隔を分単位で設定します。ゼロを入力すると、更新オプションは無効になります。
時間枠の数 (Number of Time Windows)	使用する時間枠の数を指定します。 <ul style="list-style-type: none"> <li>監査ログ、ヘルス イベント、および時間によって制約可能なイベントに基づいたワークフローに対してそれぞれ別のデフォルト時間枠を設定する場合は、[複数 (Multiple)] を選択します。</li> <li>すべてのイベントに適用されるグローバルな時間枠を使用する場合は、[単一 (Single)] を選択します。</li> </ul>

設定	説明
デフォルト時間枠 : [最後を表示 - スライディング (Show the Last - Sliding) ]	<p>この設定を選択すると、指定する長さのスライディングのデフォルト時間枠を設定できます。</p> <p>アプライアンスは、特定の開始時刻（たとえば1時間前）から現在までに生成されたすべてのイベントを表示します。イベントビューの変更と共に、時間枠は「スライド」して、常に最後の1時間内のイベントが表示されます。</p>
デフォルト時間枠 : [最後を表示 - 静的/拡張 (Show the Last - Static/Expanding) ]	<p>この設定を選択すると、指定する長さの、静的または拡張のデフォルト時間枠を設定できます。</p> <p><b>静的な時間枠の場合</b> ([終了時間を使用 (Use End Time) ] チェックボックスをオンにした場合)、アプライアンスは特定の開始時間（1時間前などの）から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベントビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。</p> <p><b>拡張時間枠の場合</b> ([終了時間を使用 (Use End Time) ] チェックボックスをオフにした場合)、アプライアンスは特定の開始時間（1時間前などの）から現在までに生成されたすべてのイベントを表示します。イベントビューを変更すると、時間枠は現在まで拡張されます。</p>
デフォルト時間枠 : [本日 - 静的/拡張 (Current Day - Static/Expanding) ]	<p>この設定を選択すると、現在の日付に対して静的または拡張のデフォルト時間枠を設定できます。現在の日付は、現行セッションのタイムゾーン設定に基づいて午前0時に始まります。</p> <p><b>静的な時間枠の場合</b> ([終了時間を使用 (Use End Time) ] チェックボックスをオンにした場合)、アプライアンスは午前0時から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベントビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。</p> <p><b>拡張時間枠の場合</b> ([終了時間を使用 (Use End Time) ] チェックボックスをオフにした場合)、アプライアンスは午前0時から現在までに生成されたすべてのイベントを表示します。イベントビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に24時間を超えて分析を続けた場合、この時間枠は24時間よりも長くなる可能性があることに注意してください。</p>

## イベントタイプのデフォルトの時間枠の変更

設定	説明
デフォルト時間枠：[今週 - 静的/拡張 (Current Week - Static/Expanding) ]	<p>この設定を選択すると、現在の週に対して静的または拡張のデフォルト時間枠を設定できます。現在の週は、現行セッションのタイムゾーン設定に基づいて直前の日曜日の午前0時に始まります。</p> <p><b>静的な時間枠の場合</b> ([終了時間を使用 (Use End Time) ] チェックボックスをオンにした場合)、アプライアンスは午前0時から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベントビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。</p> <p><b>拡張時間枠の場合</b> ([終了時間を使用 (Use End Time) ] チェックボックスをオフにした場合)、アプライアンスは日曜日の午前0時から現在までに生成されたすべてのイベントを表示します。イベントビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に1週間を超えて分析を続けた場合、この時間枠は1週間よりも長くなる可能性があることに注意してください。</p>

## イベントタイプのデフォルトの時間枠の変更

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst

## 手順

- ステップ 1 時間により制約されたワークフローで、時間範囲のアイコン (🕒) をクリックし、[日付と時間 (Date/Time) ] ウィンドウを開きます。
- ステップ 2 [優先 (Preferences) ] タブをクリックし、[イベントタイプのデフォルトの時間枠オプション \(2456 ページ\)](#) に記載されているようにプリファレンスを変更します。
- ステップ 3 [設定の保存 (Save Preferences) ] をクリックします。
- ステップ 4 次の2つの対処法があります。
  - 使用しているイベントビューに新しいデフォルト時間枠の設定を適用するには、[適用 (Apply) ] をクリックして [日付と時間 (Date/Time) ] ウィンドウを閉じてイベントビューをリフレッシュします。



- デフォルトの時間枠設定を適用せずに分析を続けるには、[適用 (Apply)] をクリックせずに [日付と時間 (Date/Time)] ウィンドウを閉じます。

## 時間枠の進行

時間枠は一時停止することができます。これにより、ワークフローから提供されたデータのスナップショットを調べることができます。一時停止が解除されたワークフローが更新されると、それによって、調査したいイベントが削除されたり、調査対象外のイベントが追加されたりすることがあるため、この機能は役立ちます。

静的 (static) の時間枠は一時停止できないことに注意してください。また、イベントの時間枠の一時停止はダッシュボードに影響を与えず、ダッシュボードの一時停止もイベントの時間枠の一時停止に影響を与えません。

分析が完了したら、時間枠の一時停止を解除できます。時間枠の一時停止を解除すると、設定に従って時間枠が更新されます。また、一時停止を解除した時間枠を反映するようにイベントビューも更新されます。

1つのワークフローのページに表示できるイベント数よりも多くのイベントがデータベースに含まれている場合は、ページの下部にあるリンクをクリックして、さらにイベントを表示できます。リンクをクリックすると、同じイベントが2回表示されないように時間枠が自動的に一時停止します。

### 時間枠の一時停止/一時停止解除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst (ワークフローによる)

### 手順

時間で制約されているワークフローでは、目的の時間範囲コントロールを選択できます。

- 時間枠を一時停止するには、時間範囲コントロールの一時停止アイコン (⏸) をクリックします。
- 時間枠の一時停止を解除するには、時間範囲コントロールの再生アイコン (▶) をクリックします。

## イベントビューの制約

ワークフローページに表示される情報は、ユーザが設定した制約によって異なります。たとえばイベントワークフローを最初に開いた場合、情報は、最後の1時間に生成されたイベントに制約されています。

ワークフローの次のページに進んで、表示されるデータを特定の値で制約する場合は、ページでこれらの値を持つ行を選択し、[表示 (View)] をクリックします。現在の制約を保持し、すべてのイベントを含めた状態でワークフローの次のページに進むには、[すべて表示 (View All)] を選択します。



(注) 複数の不可算値を持つ行を選択し、[表示 (View)] を選択すると、複合的な制約が作成されません。

ワークフローのデータを制約するための3番目の方法があります自身が選択した値を持つ行のみが表示されるようページを制約し、ページの上部に示される制約リストに選択した値を追加するには、ページの行で値をクリックします。たとえば、記録された接続のリストを表示する場合には、アクセス制御を使用して、自身が許可したものがリストに示されるよう制約する場合は、[アクション (Action)] カラムで [許可 (Allow)] をクリックします。他の例では、侵入イベントを表示する場合には、宛先ポートが 80 のイベントのみがリストに示されるよう制約する場合は、[宛先ポート/ICMP コード (Destination Port/ICMP Code)] カラムで [80 (http) /tcp (80 (http)/tcp)] をクリックします。



ヒント モニタルールの条件に基づいて接続イベントを制約するための手順は少し異なり、いくつかの追加手順が必要になる場合があります。また、関連付けられているファイルや侵入情報によって接続イベントを制約することはできません。

検索を使用して、ワークフローの情報を制約することもできます。1つのカラム内の複数の値について制約する場合は、この機能を使用します。たとえば、2つのIPアドレスに関連しているイベントを表示する場合は、[検索の編集 (Edit Search)] をクリックし、[検索 (Search)] ページで対象の [IP アドレス (IP address)] フィールドを変更して両方のアドレスが含まれるようにして、[検索 (Search)] をクリックします。

検索ページで入力した検索条件はページの上部に制約として表示され、これに従って制約されたイベントが合わせて表示されます。Firepower Management Center では、複合的な制約でない限り、他のワークフローにナビゲートしたときにも現在の制約が適用されます。

検索する場合は、検索対象のテーブルに検索の制約を適用するかどうか注意到する必要があります。たとえば、クライアントデータは接続サマリーでは使用できません。接続で検出されたクライアントに基づいて接続イベントを検索し、結果を接続サマリーイベントビューで表示すると、Firepower Management Center では、制約が設定されていない場合と同じように接続データが表示されます。無効な制約は、非適用 (N/A) とラベルが付けられ、取り消し線が付けられます。

## イベントの制約

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst (ワークフローに応じて異なります)

### 手順

**ステップ 1** [ワークフローの選択 \(2432 ページ\)](#) の説明に従って適切なメニューパスとオプションを選択し、ワークフローにアクセスします。

**ステップ 2** すべてのワークフローで、次のオプションを選択できます。

- ビューを単一の値と一致するイベントに制約するには、ページの行内の目的の値をクリックします。
- ビューを複数の値と一致するイベントに制約するには、その値を持つイベントのチェックボックスをオンにし、[表示 (View)] をクリックします。  
(注) 行に複数の不可算値が含まれている場合は、複合的な制約が追加されます。
- 制約を解除するには、[制約の検索 (Search Constraints)] の展開矢印 (▼) をクリックし、展開された [制約の検索 (Search Constraints)] リストで制約の名前をクリックします。
- 検索ページを使用して制約を編集するには、[検索の編集 (Edit Search)] をクリックします。
- 保存済み検索として制約を保存するには、[検索の保存 (Save Search)] をクリックし、クエリに名前を付けます。  
(注) 複合的な制約が含まれているクエリは保存できません。
- 別のイベント ビューで同じ制約を使用するには、[移動先 (Jump to)] をクリックし、イベント ビューを選択します。  
(注) 別のワークフローに切り替えると、複合的な制約は保持されません。
- 制約の表示を切り替えるには、[制約の検索 (Search Constraints)] の展開矢印 (▼) または [制約の検索 (Search Constraints)] の折りたたみ開矢印 (▲) をクリックします。制約のリストが長く、画面の大半を占有する場合に、この機能は役立ちます。

## 複合イベントビューの制約

複合的な制約は、特定のイベントに対するすべての不可算値に基づいています。複数の不可算値を持つ行を選択する場合は、ページ上の対象行におけるすべての不可算値と一致するイベントのみを取得する複合的な制約を設定します。たとえば、送信元 IP アドレスが 10.10.31.17 で、宛先 IP アドレスが 10.10.31.15 である行と、送信元 IP アドレスが 172.10.10.17 で宛先 IP アドレスが 172.10.10.15 である行を選択すると、次のすべての結果が取得されます。

- 送信元 IP アドレスが 10.10.31.17 で、かつ宛先 IP アドレスが 10.10.31.15 のイベント
- または
- 送信元 IP アドレスが 172.10.31.17 で、かつ宛先 IP アドレスが 172.10.31.15 のイベント

複合的な制約と単純な制約を組み合わせると、複合的な制約の各セットに単純な制約が追加されます。たとえば、上記に記載されている複合的な制約に対して、プロトコル値 `tcp` の単純な制約を追加すると、次のすべての結果が取得されます。

- 送信元 IP アドレスが 10.10.31.17 で、かつ宛先 IP アドレスが 10.10.31.15 で、かつプロトコルが `tcp` であるイベント
- または
- 送信元 IP アドレスが 172.10.31.17 で、かつ宛先 IP アドレスが 172.10.31.15 で、かつプロトコルが `tcp` であるイベント

複合的な制約について、検索および検索の保存を実行することはできません。また、別のワークフローに切り替えるのに、イベントビューのリンクを使用した場合、または [ワークフロー切り替え (switch workflow)] をクリックした場合は、複合的な制約は保持できません。複合的な制約が適用されているイベントビューをブックマークしても、制約はブックマークに保存されません。

## 複合イベントビュー制約の使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst (ワークフローに応じて異なります)

### 手順

- ステップ 1** [ワークフローの選択 \(2432 ページ\)](#) の説明に従って、適切なメニューパスとオプションを選択してワークフローにアクセスします。

ステップ2 複合制約を管理する場合、次の選択肢があります。

- 複合制約を作成するには、カウント以外の値を持つ1つ以上の行を選択し、[表示 (View)] をクリックします。
- 複合制約をクリアするには、[検索制約 (Search Constraints)] の展開矢印 (■) をクリックし、[複合制約 (Compound Constraints)] をクリックします。

## ワークフロー間のナビゲーション

ワークフロー ページの [移動 (Jump to...)] ドロップダウン リストのリンクを使用して、他のワークフローへ移動できます。ドロップダウンリストを選択し、追加のワークフローを表示および選択します。

新しいワークフローを選択すると、(適切な場合は)、選択する行で共有されているプロパティおよび設定する制約が、新しいワークフローで使用されます。設定した制約またはイベントのプロパティが、新しいワークフローのフィールドにマップされない場合は、これらはドロップされます。また、ワークフローを切り替えた場合には、複合的な制約は保持されません。キャプチャファイルのワークフローの制約は、ファイルおよびマルウェアのイベントワークフローのみに転送されます。



- (注) 所定の時間範囲のイベント数を表示する場合、詳細なデータを利用できるイベントの数が、イベントの総数に反映されないことがあります。これは、ディスク領域の使用率を管理するために、古いイベントの詳細がシステムによってブルーニングされることがあるために発生します。イベント詳細のブルーニングを最小限にするために、対象の展開にとって最も重要なイベントだけを記録するようにイベント ログgingを調整できます。

時間枠を一時停止していない場合、または静的な時間枠を設定していない場合、ワークフローを変更したときに時間枠も変更されることに注意してください。

この機能により、疑わしいアクティビティの調査が強化されます。たとえば、接続データを表示していて、内部ホストが異常に大量のデータを外部サイトに転送していることに気付いた場合は、応答側の IP アドレスとポートを制約として選択し、[アプリケーション (Applications)] ワークフローへ移動することができます。[アプリケーション (Applications)] ワークフローは応答側の IP アドレスとポートを IP アドレスとポートの制約として使用し、アプリケーションの種類などの追加情報を表示することができます。ページの上にある [ホスト (Hosts)] をクリックして、リモートホストのホストプロファイルを表示することもできます。

アプリケーションに関する詳細を検索した後で、[相関イベント (Correlation Events)] を選択して接続データ ワークフローに戻る、制約から応答側の IP アドレスを削除する、制約にインシエンタの IP アドレスを追加する、[アプリケーションの詳細 (Application Details)] を選択して、データをリモートホストに転送するときに開始側のホストでユーザがどのクライアントを使用しているかを確認する、といったことができます。ポートの制約は、[アプリケーション詳細 (Application Details)] ページには転送されないことに注意してください。ローカルホス

トを制約として保持したまま、追加情報を検索するために他のナビゲート ボタンを使用することもできます。

- ローカル ホストがいずれかのポリシーに違反しているかどうかを検出するには、IP アドレスを制約として保持したまま [移動 (Jump to) ] ドロップダウンリストから [関連イベント (Correlation Events) ] を選択します。
- ホストに対して侵入ルールがトリガーされた (侵害を表している) かどうかを確認するには、[移動 (Jump to) ] ドロップダウンリストから [侵入イベント (Intrusion Events) ] を選択します。
- ローカル ホストのホスト プロファイルを表示し、ホストが、悪用された可能性のある脆弱性の影響を受けやすくなっているかどうかを判断するには、[移動 (Jump to) ] ドロップダウンリストから [ホスト (Hosts) ] を選択します。

## ブックマーク

イベントの分析の特定の場所と時間にすばやく戻りたい場合には、ブックマークを作成します。ブックマークは、次の情報が含まれます。

- 使用中のワークフロー
- ワークフローの表示中の部分
- ワークフローのページ番号
- 検索の制約
- 無効になっているカラム
- 使用している時間範囲

あるユーザが作成したブックマークは、ブックマーク アクセスを持っているすべてのユーザ アカウントで利用できます。これは、より詳細な分析を必要とするイベントセットを発見した場合、簡単にブックマークを作成し、適切な権限を持った他のユーザに調査を引き継ぐことが可能であることを意味します。



- (注) ブックマークに表示されているイベントが (ユーザによって直接、またはデータベースの自動クリーンアップによって) 削除されると、そのブックマークにあった元のイベントは表示されなくなります。

## ブックマークの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst (ワークフローに応じて異なります)

マルチドメイン導入では、現在のドメインで作成されたブックマークのみを表示できます。

### 手順

**ステップ 1** イベントの分析中に、表示されている対象のイベントで[このページをブックマーク (Bookmark This Page) ]をクリックします。

**ステップ 2** [名前 (Name) ]フィールドに、名前を入力します。

**ステップ 3** [ブックマークの保存 (Save Bookmark) ]をクリックします。

## ブックマークの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst (ワークフローに応じて異なります)

マルチドメイン導入では、現在のドメインで作成されたブックマークのみを表示できます。

### 手順

すべてのイベント ビューで、以下の 2 つの方法を選択できます。

- [ブックマークの表示 (View Bookmarks) ]の上にポインタを合わせ、ドロップダウンメニューから目的のブックマークをクリックします。
- [ブックマークの表示 (View Bookmarks) ]をクリックし、[ブックマークの表示 (View Bookmarks) ]ページで目的のブックマーク名をクリックするか、その横にある表示アイコン (🔍) をクリックします。

- (注) 最初にブックマークに表示されていたイベントが（ユーザによって直接、またはデータベースの自動クリーンアップによって）削除されると、そのブックマークにはイベントの元のセットは表示されません。
-





## 第 102 章

# イベントの検索

以下のトピックでは、ワークフロー内のイベントの検索方法について説明します。

- [イベントの検索 \(2467 ページ\)](#)
- [シェルによるクエリのオーバーライド \(2476 ページ\)](#)

## イベントの検索

Firepower システムでは、データベース テーブルにイベントとして保存される情報が生成されます。イベントには、アプライアンスがイベントを生成する原因となったアクティビティを示すいくつかのフィールドが含まれます。ご使用の環境用にカスタマイズされた、さまざまなイベント タイプの検索を作成および保存し、後で再使用するために保存できます。

検索設定を保存するときには、その検索設定の名前を付け、それを自分だけで使用するか、それともアプライアンスの全ユーザが使用できるようにするかを指定します。カスタム ユーザロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。以前に検索設定を保存した場合、それをロードし、必要に応じて修正して、検索を開始することができます。カスタム分析のダッシュボード ウィジェット、レポート テンプレート、カスタム ユーザロールも、保存した検索を使用できます。保存済みの検索設定がある場合、[検索 (Search)] ページからそれらを削除できます。

いくつかのイベント タイプに関しては、Firepower システムに備わっている定義済みの検索設定をサンプルとして使用すると、ネットワークについての重要な情報にすばやくアクセスできます。ネットワーク環境に合わせて定義済み検索設定のフィールドを変更し、検索設定を保存して、後で再利用することができます。

検索の種類に応じて、使用できる検索条件は異なりますが、メカニズムは同じです。検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。



(注) カスタム テーブルの検索には、若干異なる手順が必要です。

### 関連トピック

- [カスタム テーブルの検索 \(2498 ページ\)](#)

## 検索の制約

データベーステーブルごとに、検索を制約する値を入力できる独自の検索ページがあります。入力した値は、そのテーブルに定義されているフィールドに適用されます。フィールドのタイプによっては、特殊なシンタックスを使用して、ワイルドカード文字や数値の範囲などの基準を指定できます。

検索結果はワークフローページに表示され、カラム式レイアウトでテーブルの各フィールドが表示されます。一部のデータベース テーブルは、ワークフロー ページにカラムとして表示されないフィールドを使用した検索も行えます。ワークフローページで結果を確認する際に、該当する制約が検索結果に適用されているかどうかを判別するには、展開アイコン (■) をクリックして、検索に現在有効になっている制約を表示します。

### 一般的な検索の制約

イベントを検索するときは、次の一般的な注意事項を順守してください。

- すべてのフィールドで否定 (!) を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を1つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、A, B, "C, D, E" を検索すると、指定したフィールドに「A」または「B」または「C, D, E」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、A, B, "C, D, E" をこれらの文字の1つまたは複数を含むことができるフィールドで検索すると、指定したフィールドにAまたはB、またはC、D、Eのすべてを含むレコードが一致します。
- フィールドでその情報を利用できないイベントを示すには、そのフィールドで n/a を指定します。フィールドに情報が入力されているイベントを示すには !n/a を使用します。
- 多くの数値フィールドの前には、より大きい (>)、以上 (>=)、より小さい (<)、以下 (<=)、等しい (=) または等しくない (<>) の演算子を付けることができます。



**ヒント** 長い複雑な値を（SHA-256ハッシュ値など）を含むフィールドを検索する場合は、ソース資料から検索基準値をコピーし、検索ページの適切なフィールドに貼り付けることができます。

## 検索で使用するワイルドカードと記号

検索ページの多くのテキストフィールドでは、文字列内の文字に一致させるために、アスタリスク (\*) を使用することができます。たとえばnet\*と指定すると、network、netware、netscapeなどに一致します。

英数字以外の文字（アスタリスク文字を含む）を検索するには、検索文字列を引用符で囲みます。たとえば、次の文字列を検索するとします。

```
Find an asterisk (*)
```

この場合は、次のように入力します。

```
"Find an asterisk (*)"
```

ワイルドカードを使用できるテキストフィールドで、文字列の部分一致を検索するには、ワイルドカードを使用する**必要**があります。たとえば、ページビューを含む（つまりメッセージが「Page View」である）すべての監査レコードを監査ログ内で検索する場合、「Page」を検索しても結果は返されません。代わりに、「Page\*」と指定してください。

一部のフィールドでは、アスタリスクを使用せずにフィールドの内容をすべてまたは一部検索することができます。完全一致の場合は、検索文字列を引用符で囲む必要があります。引用符で囲まなかった場合は、部分一致が実行されます。たとえば、フィールド検索で、引用符を使用せずに Scan Completed with Detection という文字列を検索すると、該当フィールドに次の文字列が含まれているレコードと、該当フィールドが検索文字列と完全に一致するレコードが返されます。

```
Scan Completed, No Detections  
Scan completed With Detections
```

## 検索でのオブジェクトとアプリケーションのフィルタ

Firepower システムでは、ネットワーク構成の一部として使用可能な名前付きオブジェクト、オブジェクトグループ、およびアプリケーションフィルタを作成できます。検索を実行または保存するときには、検索条件としてこれらのオブジェクト、グループ、およびフィルタを使用できます。

検索を実行するときに、オブジェクト、オブジェクトグループ、およびアプリケーションフィルタは\${object\_name}という形式で表示されます。たとえば、オブジェクト名ten\_ten\_networkであるネットワークオブジェクトは、検索では\${ten\_ten\_network}と表されます。

検索基準としてオブジェクトを使用できる検索フィールドの横にはオブジェクト追加アイコン (+) が表示され、これをクリックすることができます。

## 関連トピック

[オブジェクト マネージャ](#) (424 ページ)

## 検索で指定する時間制約

時間値を指定できる検索条件フィールドで使用可能な形式を、次の表に示します。

表 281: 検索フィールドにおける時間指定

時間の形式	例
today [at HH:MMam pm]	today today at 12:45pm
YYYY-DDMM- HH:MM:SS	2006-03-22 14:22:59

時間値の前に、以下のいずれか 1 つの演算子を指定できます。

表 282: 時間指定の演算子

演算子	例	説明
<	< 2006-03-22 14:22:59	2006 年 3 月 22 日午後 2 時 23 分より前のタイムスタンプを持つイベントを返します。
>	> today at 2:45pm	今日の午後 2 時 45 分より後のタイムスタンプを持つイベントを返します。

## 検索での IP アドレス

検索で IP アドレスを指定するときには、個別の IP アドレス、複数アドレスのカンマ区切りリスト、アドレスブロック、またはハイフン (-) で区切った IP アドレス範囲を入力することができます。また、否定を使用することもできます。

IPv6 をサポートする検索（侵入イベント、接続データ、相関イベントの検索など）では、IPv4 アドレス、IPv6 アドレス、および CIDR/プレフィックス長アドレス ブロックを任意に組み合わせ入れて入力できます。IP アドレスを使用してホストを検索した場合、結果には、少なくとも 1 つの IP アドレスが検索条件と一致するホストがすべて含まれます（つまり、IPv6 のアドレスの検索では、プライマリアドレスが IPv4 であるホストが返されることがあります）。

CIDR またはプレフィックス長の表記を使用して IP アドレスのブロックを指定する場合、Firepower システムは、マスクまたはプレフィックス長で指定されたネットワーク IP アドレスの部分のみを使用します。たとえば 10.1.2.3/8 と入力すると、Firepower システムは 10.0.0.0/8 を使用します。

IP アドレスをネットワーク オブジェクトによって表すことができるため、IP アドレス検索フィールドの横にあるネットワーク オブジェクト追加アイコン (+) をクリックして、ネットワーク オブジェクトを IP アドレス検索基準として使用することもできます。

表 283: 使用可能な IP アドレス構文

指定する項目	タイプ	例
単一の IP アドレス	その IP アドレス。	192.168.1.1 2001:db8::abcd
リストを使用した複数の IP アドレス	IP アドレスからなるカンマ区切りリスト。カンマの前後にスペースを追加しないでください。	192.168.1.1,192.168.1.2 2001:db8::b3ff,2001:db8::0202
CIDR ブロックまたはプレフィックス長で指定できる IP アドレスの範囲	IPv4 CIDR または IPv6 プレフィックス表記の IP アドレス ブロック。	192.168.1.0/24 これは、サブネット マスク 255.255.255.0 である 192.168.1.0 ネットワーク内の任意の IP を指定します (つまり 192.168.1.0 から 192.168.1.255 まで)。
CIDR ブロックやプレフィックスで指定できない IP アドレスの範囲	ハイフンを使用した IP アドレス範囲。ハイフンの前後にスペースを入力しないでください。	192.168.1.1-192.168.1.5 2001:db8::0202-2001:db8::8329
他の方法で否定を使用して IP アドレスまたは IP アドレス範囲を指定	IP アドレス、ブロック、または範囲の先頭に感嘆符を付ける。	192.168.0.0/32,!192.168.1.10 !2001:db8::/32 !192.168.1.10,!2001:db8::/32

### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## 検索での管理対象デバイス

管理対象デバイスを制約として使用して検索を作成する場合、[デバイス (Device)] 検索条件フィールドに次のいずれかを指定できます。

- 管理対象デバイス名、IP アドレス、またはホスト名
- デバイス グループ名
- デバイス スタック名
- 7000 または 8000 シリーズ デバイス高可用性ペアの名前

システムでグループ、デバイス高可用性ペア、またはスタックの一致が検出されると、検索を実行するために、そのグループ名、デバイス高可用性ペア名、またはスタック名が適切なメン

バー デバイス名に置き換えられます。デバイス フィールドのデバイス グループ、デバイス高可用性ペア、またはスタックを使用する検索を保存すると、デバイスフィールドで指定した名前がシステムによって保存され、検索が実行されるたびにデバイス名の置換が再度実行されます。

## 検索でのポート

Firepower System では、検索においてポート番号の特定の構文に対応しています。次の入力が可能です。

- 1つのポート番号
- コンマで区切られたポート番号リスト
- ポート番号範囲を示すのにダッシュで区切られた2つのポート番号
- ポート番号の後ろにスラッシュで区切ってプロトコルの略語（侵入イベントを検索する場合のみ）
- 特定のポートの否定を示すエクスクラメーションマークの後ろにポート番号またはポート番号範囲



(注) ポート番号またはポート範囲を指定する場合はスペースは使用しないでください。

表 284: ポート構文例

例	説明
21	ポート 21 でのすべてのイベント（TCP イベントや UDP イベントなど）を戻します。
!23	ポート 23 のイベントを除き、すべてのイベントを戻します。
25/tcp	ポート 25 の TCP 関連侵入イベントをすべて戻します。
21/tcp,25/tcp	ポート 21、25 の TCP 関連侵入イベントをすべて戻します。
21-25	ポート 21 から 25 のイベントをすべて戻します。

## 検索のイベント フィールド

イベントを検索するときは、検索条件として次のフィールドを使用できます。

- [監査ログのワークフロー フィールド \(2773 ページ\)](#)

- アプリケーションデータ フィールド (2728 ページ)
- アプリケーションの詳細データ フィールド (2731 ページ)
- キャプチャされたファイルのフィールド (2642 ページ)
- ホワイト リスト イベントのフィールド (2762 ページ)
- 接続およびセキュリティ インテリジェンス イベント フィールド (2523 ページ)
- 関連イベントのフィールド (2757 ページ)
- ディスカバリ イベントのフィールド (2706 ページ)
- [ヘルス イベント (Health Events) ] テーブル (306 ページ)
- ホスト属性データ フィールド (2716 ページ)
- ホスト データ フィールド (2708 ページ)
- ファイルおよびマルウェア イベント フィールド (2617 ページ)
- 侵入イベント フィールド (2557 ページ)
- ルール アップデートのインポート ログの詳細ビュー (188 ページ)
- 修復ステータスのテーブル フィールド (2767 ページ)
- Nmap スキャン結果のフィールド (2094 ページ)
- サーバ データ フィールド (2724 ページ)
- サードパーティの脆弱性データのフィールド (2740 ページ)
- ユーザ関連フィールド (2741 ページ)
- 脆弱性データのフィールド (2733 ページ)
- ホワイト リスト違反のフィールド (2764 ページ)

## 検索の実行

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

### 手順

ステップ 1 [分析 (Analysis) ] > [検索 (Search) ] を選択します。

ヒント また、ワークフローの任意のページから [検索 (Search)] をクリックすることもできます。

- ステップ2 テーブルのドロップダウンリストから、検索するイベントまたはデータのタイプを選択します。
- ステップ3 該当するフィールドに検索条件を入力します。 [検索の制約 \(2468 ページ\)](#) を参照してください。
- ステップ4 将来検索を再度使用する場合は、その検索を保存します。詳細については、 [検索設定の保存 \(2474 ページ\)](#) を参照してください。
- ステップ5 [検索 (Search)] をクリックして、検索を開始します。検索結果は、検索されるテーブルのデフォルトワークフローで表示され、該当する場合には時間で制約されます。

#### 次のタスク

- ワークフローを使用して検索結果を分析する場合は、 [ワークフローの使用 \(2429 ページ\)](#) を参照してください。

#### 関連トピック

[イベント ビュー設定の設定 \(37 ページ\)](#)

## 検索設定の保存

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成された保存済みの検索が表示されます。これは編集できます。先祖ドメインで作成された保存済みの検索も表示されますが、これは編集できません。下位のドメインで作成された検索を表示および編集するには、そのドメインに切り替えます。

#### 始める前に

- [検索の実行 \(2473 ページ\)](#) で説明するように検索条件を設定するか、 [保存済み検索設定のロード \(2475 ページ\)](#) で説明するように保存した検索をロードします。

#### 手順

- ステップ1 [検索 (Search)] ページから、自分だけがアクセスできるように検索設定をプライベートとして保存する場合は、[プライベート (Private)] チェックボックスをオンにします。



**ヒント** カスタムユーザロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。

**ステップ 2** 次の 2 つの対処法があります。

- ロードした検索設定の新しいバージョンを保存する場合は、[新規に保存 (Save As New)] をクリックします。
- 新しい検索結果を保存する場合や、同じ名前を使用してカスタム検索を上書きする場合は、[保存 (Save)] をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

## 保存済み検索設定のロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成された保存済みの検索が表示されます。これは編集できます。先祖ドメインで作成された保存済みの検索も表示されますが、これは編集できません。下位のドメインで作成された検索を表示および編集するには、そのドメインに切り替えます。

### 手順

**ステップ 1** [分析 (Analysis)] > [検索 (Search)] を選択します。

**ヒント** また、ワークフローの任意のページから [検索 (Search)] をクリックすることもできます。

**ステップ 2** テーブルのドロップダウンリストから、検索するイベントまたはデータのタイプを選択します。

**ステップ 3** [カスタム検索 (Custom Searches)] リストまたは [定義済みの検索 (Predefined Searches)] リストから、ロードする検索を選択します。

**ステップ 4** 別の検索条件を使用するには、検索の制約を変更します。

**ステップ 5** 変更した検索を将来再度使用する場合は、検索を保存しておきます。詳細については、[検索設定の保存 \(2474 ページ\)](#) を参照してください。

**ステップ 6** [検索 (Search)] をクリックします。

## シェルによるクエリのオーバーライド

システム管理者は、シェルベースのクエリ管理ツールを使用して、実行時間の長いクエリを検出および停止することができます。

クエリ管理ツールでは指定した分数よりも実行時間が長いクエリを検索し、それらのクエリを停止することができます。ユーザがクエリを停止すると、このツールにより監査ログと `syslog` にイベントが記録されます。

Firepower Management Center でのシェルアクセスを持つローカル作成されたユーザだけが、`admin` ユーザであることに注意してください。シェルアクセスを与える外部認証オブジェクトを使用する場合、シェルアクセス フィルタに一致するユーザもまたシェルにログインできます。



(注) Web インターフェイス内の検索ページを終了しても、クエリは停止しません。長い時間をかけて結果を返すクエリは、クエリ実行中にシステム全体のパフォーマンスに影響を与えます。

## シェルベースのクエリ管理の構文

実行時間が長いクエリを管理するには、次の構文を使用します。

```
query_manager [-v] [-l [minutes]] [-k query_id [...]] [--kill-all minutes]
```

表 285: `query_manager` オプション

オプション	説明
<code>-h, --help</code>	短いヘルプ メッセージを出力します。
<code>-l, --list [minutes]</code>	指定された時間 (分単位) を超えるすべてのクエリをリストします。デフォルトで、1分より長くかかっているすべてのクエリを表示します。
<code>-k, --kill query_id [...]</code>	指定された ID を持つクエリを強制終了します。オプションは複数の ID を取得する場合があります。
<code>--kill-all minutes</code>	指定された時間 (分単位) を超えるすべてのクエリを強制終了します。
<code>-v, --verbose</code>	完全な SQL クエリを含む詳細な出力。



注意 シェルアクセスを、システム管理者のみに制限する必要があります。

## 実行時間が長いクエリの停止

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	admin またはシェル アクセスが付与されたユーザ

### 手順

- 
- ステップ 1** ssh を使用して Firepower Management Center に接続します。
- ステップ 2** [シェルベースのクエリ管理の構文 \(2476 ページ\)](#) で説明された構文を使用して、sudo で query\_manager を実行します。
-

■ 実行時間が長いクエリの停止



## 第 103 章

# カスタム ワークフロー

次のトピックでは、カスタム ワークフローの使用方法について説明します。

- [カスタム ワークフローの概要 \(2479 ページ\)](#)
- [保存済みカスタム ワークフロー \(2480 ページ\)](#)
- [カスタム ワークフローの作成 \(2481 ページ\)](#)
- [カスタム ワークフローの使用と管理 \(2485 ページ\)](#)

## カスタム ワークフローの概要

シスコが提供する事前定義のカスタム ワークフローがニーズに合わない場合は、カスタム ワークフローを作成して管理することができます。

カスタム ワークフローは、組織に特有のニーズに合わせて作成するワークフローです。カスタム ワークフローを作成する場合は、ワークフローのベースとなるイベント（またはデータベーステーブル）の種類を選択します。Firepower Management Center では、カスタム ワークフローをカスタム テーブルのベースにすることができます。また、カスタム ワークフローに含まれるページを選択することもできます。カスタム ワークフローには、ドリルダウン、テーブルビュー、ホストまたはパケット ビューのページを含めることができます。

イベント評価プロセスが変わった場合には、新しいニーズを満たすようにカスタム ワークフローを編集することができます。事前定義のワークフローは編集できないことに注意してください。



**ヒント** 任意のイベント タイプについて、デフォルト ワークフローとしてカスタム ワークフローを設定することができます。

## 保存済みカスタム ワークフロー

Firepower Management Center は、変更可能な定義済みのワークフローの他に保存済みのカスタム ワークフローを含みます。それぞれのワークフローは、カスタム テーブルに基づき、いずれも変更可能です。

マルチドメイン展開では、これらの保存されたワークフローは、グローバルドメインに属し、下位ドメインでは変更できません。

表 286: 保存済みカスタム ワークフロー

ワークフロー名	説明
影響度、優先度、ホストの重要度によるイベント	このワークフローを使用して、ネットワークにとって重要であり、現在脆弱であり、現在攻撃を受けている可能性のあるホストを迅速に選択して、そのホストに焦点を合わせることができます。 このワークフローは、宛先重要度のカスタム テーブルのある侵入イベントに基づいています。
優先度および分類によるイベント	このワークフローでは、イベントとタイプのリストをそれぞれのイベントが発生した回数と共にイベントの優先度の順に示します。 このワークフローは、侵入イベントのカスタム テーブルに基づきます。
宛先、影響度、ホストの重要度を有するイベント	このワークフローを使用して、ネットワークにとって重要であり、現在脆弱であるホストの最新の攻撃を検出できます。 このワークフローは、宛先重要度のカスタム テーブルのある侵入イベントに基づいています。
サーバのデフォルト ワークフローのあるホスト	このワークフローを使用すると、サーバのカスタム テーブルと共にホストの基本的な情報をすぐに表示できます。 このワークフローは、サーバのカスタム テーブルのあるホストに基づきます。
宛先重要度のデフォルト ワークフローのある侵入イベント	このワークフローを使用すると、宛先重要度のカスタム テーブルと共に侵入イベントの基本的な情報をすぐに表示できます。 このワークフローは、宛先重要度のカスタム テーブルのある侵入イベントに基づいています。

ワークフロー名	説明
送信元重要度のデフォルト ワークフローのある侵入イベント	このワークフローを使用すると、送信元重要度のカスタム テーブルと共に侵入イベントの基本的な情報をすぐに表示できます。  このワークフローは、送信元重要度のカスタム テーブルのある侵入イベントに基づいています。
サーバとホストの詳細	このワークフローを使用して、ネットワークで最も高頻度で使用されているサーバやそのサーバを稼働しているホストを決定できます。  このワークフローは、サーバのカスタム テーブルのあるホストに基づきます。

## カスタム ワークフローの作成

シスコが提供する事前定義のカスタム ワークフローがニーズに合わない場合は、カスタム ワークフローを作成することができます。



**ヒント** 新しいカスタム ワークフローを作成する代わりに、別のアプライアンスからカスタム ワークフローをエクスポートし、それを自身のアプライアンスへインポートすることができます。その後でニーズに合わせて、インポートしたワークフローを編集することができます。

カスタム ワークフローを作成する場合は、次の操作を行います。

- ワークフローのソースとなるテーブルを選択する
- ワークフローの名前を指定する
- ワークフローにドリル ダウン ページおよびテーブル ビュー ページを追加する

ワークフローの各ドリル ダウン ページでは、次のことができます。

- Web インターフェイスのページの上部に表示される名前を指定する
- 1 ページにつき最大 5 個のカラムを含める
- デフォルトのソート順（昇順または降順）を指定する

ワークフロー ページの順序において、任意の場所にテーブル ビュー ページを追加することができます。これらのページには編集可能なプロパティ（ページ名、ソート順、ユーザ定義可能なカラム位置など）がありません。



(注) カスタム ワークフローには、イベントのドリルダウンページまたはテーブルビューを少なくとも1つ追加する必要があります。



(注) テーブルタイプに [脆弱性 (Vulnerabilities)] を選択し、テーブルカラムに [IP アドレス (IP Address)] を追加しても、検索機能を使用して特定の IP アドレスまたはアドレスのブロックを表示するようワークフローを制約しない限り、カスタムワークフローを使用して脆弱性を表示する場合に [IP アドレス (IP Address)] カラムは表示されません。

カスタムワークフローの最終ページは、次の表に記載されているように、ワークフローのベースにしているテーブルによって異なります。これらの最終ページは、ワークフローを作成したときにデフォルトで追加されます。

表 287: カスタムワークフローの最終ページ

イベント/アセットタイプ	最終ページ
ディスカバリ イベント	ホスト
脆弱性	脆弱性の詳細
サードパーティの脆弱性	ホスト
Users	Users
侵害の兆候	ホスト
侵入イベント	パケット

システムは、他の種類のイベント (監査ログやマルウェア イベントなど) に基づくカスタムワークフローには最終ページを追加しません。

接続データに基づくカスタムワークフローもその他のカスタムワークフローと同様です。ただし、接続データに基づくカスタムワークフローには接続の要約データを含むドリルダウンページや個々の接続とテーブルビューページを含むドリルダウンページを入れることができます。

## 非接続データに基づくカスタムワークフローの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst



## 手順




- ステップ 1** [分析 (Analysis)] > [カスタム (Custom)] > [カスタム ワークフロー (Custom Workflows)] を選択します。
- ステップ 2** [カスタム ワークフローの作成 (Create Custom Workflow)] をクリックします。
- ステップ 3** [名前 (Name)] フィールドにワークフローの名前を入力します。
- ステップ 4** 必要に応じて、[説明 (Description)] を入力します。
- ステップ 5** [テーブル (Table)] ドロップダウンリストから、対象とするテーブルを選択します。
- ステップ 6** ワークフローに1つ以上のドリルダウンページを追加する場合は、[ページの追加 (Add Page)] をクリックします。
- ステップ 7** [ページ名 (Page Name)] フィールドにページの名前を入力します。
- ステップ 8** [カラム 1 (Column 1)] で、ソートの優先順位およびテーブルのカラムを選択します。このカラムは、ページの最も左のカラムとして表示されます。
- 例 :**
- たとえば、対象とする宛先ポートを示すページを作成し、カウントでページをソートするには、[ソートの優先順位 (Sort Priority)] ドロップダウンリストから [2] を選択し、[フィールド (Field)] ドロップダウンリストから [宛先ポート/ICMP コード (Destination Port/ICMP Code)] を選択します。
- ステップ 9** ページに表示するすべてのフィールドが指定されるまで、含めるフィールドの選択とソートの優先順位の設定を続けます。
- ステップ 10** ワークフローにテーブル ビュー ページを追加するには、[テーブル ビューの追加 (Add Table View)] をクリックします。
- ステップ 11** [保存 (Save)] をクリックします。

## カスタム接続データ ワークフローの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

接続データに基づいたカスタム ワークフローは他のカスタム ワークフローと似ていますが、ドリルダウンページとテーブル ビュー ページだけでなく、接続データ グラフのページも含めることができます。必要に応じて、ワークフローにそれぞれのタイプのページを任意の数だけ、任意の順序で含めることができます。それぞれの接続データ グラフのページには1つのグラフ (線グラフ、棒グラフ、または円グラフ) が含まれます。線グラフと棒グラフには、複数のデータセットを含めることができます。

## 手順

- ステップ 1** [分析 (Analysis)] > [カスタム (Custom)] > [カスタム ワークフロー (Custom Workflows)] を選択します。
- ステップ 2** [カスタム ワークフローの作成 (Create Custom Workflow)] をクリックします。
- ステップ 3** [名前 (Name)] フィールドにワークフローの名前を入力します。
- ステップ 4** 必要に応じて、[説明 (Description)] を入力します。
- ステップ 5** [テーブル (Table)] ドロップダウンリストから、[接続イベント (Connection Events)] を選択します。
- ステップ 6** ワークフローに1つ以上のドリルダウンページを追加する場合は、次の2つのオプションがあります。
- 個々の接続に関するデータが含まれているドリルダウン ページを追加するには、[ページの追加 (Add Page)] をクリックします。
  - 接続の概要データが含まれているドリルダウン ページを追加するには、[サマリー ページの追加 (Add Summary Page)] をクリックします。
- ステップ 7** [ページ名 (Page Name)] フィールドにページの名前を入力します。
- ステップ 8** [カラム 1 (Column 1)] で、ソートの優先順位およびテーブルのカラムを選択します。このカラムは、ページの最も左のカラムとして表示されます。
- ステップ 9** ページに表示するすべてのフィールドが指定されるまで、含めるフィールドの選択とソートの優先順位の設定を続けます。
- 例：
- たとえば、監視対象ネットワーク経由で転送されるトラフィックの量を表示するページを作成し、トラフィックの転送量が最も多い応答側によってページをソートするには、[ソートの優先順位 (Sort Priority)] ドロップダウンリストで [1] を選択し、[フィールド (Field)] ドロップダウンリストで [応答側のバイト数 (Responder Bytes)] を選択します。
- ステップ 10** ワークフローに1つ以上のグラフ ページを追加する場合は、[グラフの追加 (Add Graph)] をクリックします。
- ステップ 11** [グラフ名 (Graph Name)] フィールドにページの名前を入力します。
- ステップ 12** ページに含めるグラフのタイプを選択します。
- 線グラフ 
  - 棒グラフ 
  - 円グラフ 
- ステップ 13** グラフの X 軸と Y 軸を選択し、グラフ化するデータの種類を指定します。
- 円グラフでは、X 軸は独立変数を表し、Y 軸は従属変数を表します。
- ステップ 14** グラフに含めるデータセットを選択します。
- 円グラフには1つのデータセットしか含めることができないことに注意してください。

**ステップ 15** 接続データのテーブル ビューを追加するには、[テーブル ビューの追加 (Add Table View)] をクリックします。

テーブル ビューは設定できません。

**ステップ 16** [保存 (Save)] をクリックします。

## カスタム ワークフローの使用と管理

ワークフローが、事前定義のイベント テーブルまたはカスタム テーブルのいずれに基づいているかによって、ワークフローの表示に使用する方法が異なります。

カスタム ワークフローが事前定義のイベント テーブルに基づいている場合は、アプライアンスに付属しているワークフローにアクセスするのと同じ方法でアクセスします。たとえば、ホストテーブルに基づいているカスタムワークフローにアクセスするには、[分析 (Analysis)] > [ホスト (Hosts)] > [ホスト (Hosts)] を選びます。また、カスタム ワークフローがカスタム テーブルに基づいている場合は、[カスタム テーブル (Custom Tables)] ページからアクセスする必要があります。

イベント評価プロセスが変わった場合には、新しいニーズを満たすようにカスタム ワークフローを編集することができます。事前定義のワークフローは編集できないことに注意してください。



**ヒント** 任意のイベント タイプについて、デフォルト ワークフローとしてカスタム ワークフローを設定することができます。

## 事前定義されたテーブルに基づいたカスタム ワークフローの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst (ワークフローに応じて異なります)

### 手順

**ステップ 1** [ワークフローの選択 \(2432 ページ\)](#) の説明に従って、カスタム ワークフローのベースとなるテーブルについて、適切なメニュー パスとオプションを選択します。

- ステップ2** カスタム ワークフローも含め、別のワークフローを使用するには、現在のワークフロー タイトルの横にある [(ワークフローの切り替え) ((switch workflow))] をクリックします。
- ステップ3** イベントが表示されず、ワークフローを時間によって制約できる場合は、時間範囲の調整が必要なことがあります (イベント時間の制約 (2451 ページ) を参照)。

## カスタム テーブルに基づいたカスタム ワークフローの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成されたカスタム ワークフローが表示されます。これは編集できます。先祖ドメインで作成されたカスタム ワークフローも表示されますが、これは編集できません。下位のドメインのカスタム ワークフローを表示および編集するには、そのドメインに切り替えます。

### 手順

- ステップ1** [分析 (Analysis)] > [カスタム (Custom)] > [カスタム テーブル (Custom Tables)] を選択します。
- ステップ2** 表示するカスタム テーブルの隣にある表示アイコン (🔍) をクリックするか、またはカスタム テーブルの名前をクリックします。
- ステップ3** カスタム ワークフローも含め、別のワークフローを使用するには、現在のワークフロー タイトルの横にある [(ワークフローの切り替え) ((switch workflow))] をクリックします。
- ステップ4** イベントが表示されず、ワークフローを時間によって制約できる場合は、時間範囲の調整が必要なことがあります (イベント時間の制約 (2451 ページ) を参照)。

## カスタム ワークフローの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成されたカスタム ワークフローが表示されます。これは編集できます。先祖ドメインで作成されたカスタム ワークフローも表示されますが、これは編集できません。下位のドメインのカスタム ワークフローを表示および編集するには、そのドメインに切り替えます。

## 手順

---

**ステップ 1** [分析 (Analysis)] > [カスタム (Custom)] > [カスタムワークフロー (Custom Workflows)] を選択します。

**ステップ 2** 編集するワークフロー名の横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ワークフローに必要な変更を加えます。

**ステップ 4** [保存 (Save)] をクリックします。

---





## 第 104 章

# カスタム テーブル

次のトピックでは、カスタム テーブルの使用方法について説明します。

- [カスタム テーブルの概要 \(2489 ページ\)](#)
- [定義済みのカスタム テーブル \(2489 ページ\)](#)
- [ユーザ定義のカスタム テーブル \(2494 ページ\)](#)
- [カスタム テーブルの検索 \(2498 ページ\)](#)

## カスタム テーブルの概要

Firepower システムがネットワークに関する情報を収集し、Firepower Management Center がその情報を一連のデータベーステーブルに保存します。結果として生成される情報を表示するためにワークフローを使用する場合、Firepower Management Center はそれらのテーブルのいずれかからデータを取り出します。たとえば、[カウントに基づいたネットワーク アプリケーション (Network Applications by Count)] ワークフローの各ページのカラムは、[アプリケーション (Applications)] テーブルのフィールドから取得されます。

さまざまなテーブルのフィールドを結合することにより、ネットワークのアクティビティの分析が向上する場合、カスタム テーブルを作成できます。たとえば、定義済みの [ホスト属性 (Host Attributes)] テーブルのホスト重大度情報と、定義済みの [接続データ (Connection Data)] テーブルのフィールドを結合してから、新しいコンテキストで接続データを検証できます。

定義済みのテーブルまたはカスタム テーブルのどちらについても、カスタム ワークフローを作成できます。

## 定義済みのカスタム テーブル

カスタム テーブルには、2つまたは3つの定義済みテーブルのフィールドを含みます。Firepower System は、いくつかのシステム定義のカスタム テーブルと共に配布されますが、特定のニーズに適合する情報のみを含む追加のカスタム テーブルを作成できます。

たとえば、Firepower System は、侵入イベントとホストデータを相関するシステム定義のカスタム テーブルと共に配布されます。そのため、クリティカル システムに影響を及ぼすイベントを検索でき、1つのワークフローにその検索結果を表示できます。

マルチドメイン展開では、定義済みのカスタム テーブルは、グローバルドメインに属し、下位ドメインで変更することはできません。

次の表では、システムと共に提供されるカスタム テーブルについて説明します。

表 288: システム定義カスタム テーブル

テーブル	説明
ホストとサーバ (Hosts with Servers)	ホスト テーブルおよびサーバ テーブルのフィールドを含み、ネットワーク上で実行されている検出されたアプリケーションに関する情報やこれらのアプリケーションを実行するホストに関する基本的なオペレーティング システム情報を提供します。
侵入イベントと宛先重要度 (Intrusion Events with Destination Criticality)	侵入イベント テーブルとホスト テーブルのフィールドを含み、侵入イベントに関する情報と各侵入イベントに含まれる宛先ホストのホスト重要度を提供します。 このテーブルを使用して、ホスト重要度の高い宛先ホストに関与する侵入イベントを検索できます。
侵入イベントと送信元重要度 (Intrusion Events with Source Criticality)	侵入イベント テーブルとホスト テーブルのフィールドを含み、侵入イベントに関する情報と各侵入イベントに含まれる送信元ホストのホスト重要度を提供します。 このテーブルを使用して、ホスト重要度の高い送信元ホストに関与する侵入イベントを検索できます。

## 可能なテーブルの組み合わせ

カスタム テーブルを作成する場合、関連データのある定義済みのテーブルのフィールドを組み合わせることができます。次の表では、新しいカスタム テーブルを作成するために組み合わせることのできる定義済みのテーブルを列挙します。2つ以上の定義済みのカスタム テーブルのフィールドを組み合わせるカスタム テーブルを作成できます。



表 289: カスタム テーブルの組み合わせ

組み合わせ可能なカスタム テーブル	フィールド
アプリケーション	<ul style="list-style-type: none"> <li>• 相関イベント (Correlation Events)</li> <li>• 侵入イベント (Intrusion Events)</li> <li>• 接続サマリ データ (Connection Summary Data)</li> <li>• ホスト属性 (Host Attributes)</li> <li>• アプリケーションの詳細 (Application Details)</li> <li>• 検出イベント (Discovery Events)</li> <li>• 接続イベント (Connection Events)</li> <li>• ホスト (Hosts)</li> <li>• サーバ</li> <li>• ホワイトリスト イベント (White List Events)</li> </ul>
相関イベント (Correlation Events)	<ul style="list-style-type: none"> <li>• アプリケーション</li> <li>• ホスト属性 (Host Attributes)</li> <li>• ホスト (Hosts)</li> </ul>
侵入イベント (Intrusion Events)	<ul style="list-style-type: none"> <li>• アプリケーション</li> <li>• ホスト属性 (Host Attributes)</li> <li>• ホスト (Hosts)</li> <li>• サーバ</li> </ul>
接続サマリ データ (Connection Summary Data)	<ul style="list-style-type: none"> <li>• アプリケーション</li> <li>• ホスト属性 (Host Attributes)</li> <li>• ホスト (Hosts)</li> <li>• サーバ</li> </ul>

組み合わせ可能なカスタム テーブル	フィールド
の侵害の兆候 (Host Indications of Compromise)	<ul style="list-style-type: none"> <li>• アプリケーション</li> <li>• アプリケーションの詳細 (Application Details)</li> <li>• キャプチャ ファイル (Captured Files)</li> <li>• 接続イベント (Connection Events)</li> <li>• 接続サマリ データ (Connection Summary Data)</li> <li>• 相関イベント (Correlation Events)</li> <li>• 検出イベント (Discovery Events)</li> <li>• ホスト属性 (Host Attributes)</li> <li>• ホスト (Hosts)</li> <li>• 侵入イベント (Intrusion Events)</li> <li>• セキュリティインテリジェンスイベント (Security Intelligence Events)</li> <li>• サーバ</li> <li>• ホワイト リスト イベント (White List Events)</li> </ul>
ホスト属性 (Host Attributes)	<ul style="list-style-type: none"> <li>• アプリケーション</li> <li>• 相関イベント (Correlation Events)</li> <li>• 侵入イベント (Intrusion Events)</li> <li>• 接続サマリ データ (Connection Summary Data)</li> <li>• アプリケーションの詳細 (Application Details)</li> <li>• 検出イベント (Discovery Events)</li> <li>• 接続イベント (Connection Events)</li> <li>• ホスト (Hosts)</li> <li>• サーバ</li> <li>• ホワイト リスト イベント (White List Events)</li> </ul>

組み合わせ可能なカスタム テーブル	フィールド
アプリケーションの詳細 (Application Details)	<ul style="list-style-type: none"> <li>• アプリケーション</li> <li>• ホスト属性 (Host Attributes)</li> <li>• ホスト (Hosts)</li> </ul>
検出イベント (Discovery Events)	<ul style="list-style-type: none"> <li>• アプリケーション</li> <li>• ホスト属性 (Host Attributes)</li> <li>• ホスト (Hosts)</li> </ul>
接続イベント (Connection Events)	<ul style="list-style-type: none"> <li>• アプリケーション</li> <li>• ホスト属性 (Host Attributes)</li> <li>• ホスト (Hosts)</li> <li>• サーバ</li> </ul>
セキュリティ インテリジェンス イベント (Security Intelligence Events)	<ul style="list-style-type: none"> <li>• アプリケーション</li> <li>• ホスト属性 (Host Attributes)</li> <li>• ホスト (Hosts)</li> <li>• サーバ</li> </ul>
ホスト (Hosts)	<ul style="list-style-type: none"> <li>• アプリケーション</li> <li>• 相関イベント (Correlation Events)</li> <li>• 侵入イベント (Intrusion Events)</li> <li>• 接続サマリ データ (Connection Summary Data)</li> <li>• ホスト属性 (Host Attributes)</li> <li>• アプリケーションの詳細 (Application Details)</li> <li>• 検出イベント (Discovery Events)</li> <li>• 接続イベント (Connection Events)</li> <li>• サーバ</li> <li>• ホワイト リスト イベント (White List Events)</li> </ul>

組み合わせ可能なカスタム テーブル	フィールド
サーバ	<ul style="list-style-type: none"> <li>• アプリケーション</li> <li>• 侵入イベント (Intrusion Events)</li> <li>• 接続サマリ データ (Connection Summary Data)</li> <li>• ホスト属性 (Host Attributes)</li> <li>• 接続イベント (Connection Events)</li> <li>• ホスト (Hosts)</li> </ul>
ホワイトリストイベント (White List Events)	<ul style="list-style-type: none"> <li>• アプリケーション</li> <li>• ホスト属性 (Host Attributes)</li> <li>• ホスト (Hosts)</li> </ul>

1 つのテーブルのフィールドを別のテーブルの 1 つ以上のフィールドにマッピングすることもあります。たとえば、定義済みの [宛先の重要度による侵入イベント (Intrusion Events with Destination Criticality)] のカスタムテーブルを侵入イベントテーブルとホストテーブルのフィールドと組み合わせます。侵入イベントテーブルの各イベントは、そのイベントに関連付けられた 2 つの IP アドレス、送信元 IP アドレスと宛先 IP アドレスがあります。しかしホストテーブル内の「イベント」は、それぞれ 1 つのホスト IP アドレスを示します (ホストには複数の IP アドレスがあることもあります)。このため、侵入イベントテーブルとホストテーブルに基づいてカスタム テーブルを作成すると、ホストテーブルで表示されたデータを侵入イベントテーブルのホスト送信元 IP アドレスまたはホスト宛先 IP アドレスに適用できるかを選択する必要があります。

新しいカスタムテーブルを作成すると、テーブル内のすべての列を表示するデフォルトのワークフローが自動的に作成されます。また、定義済みのテーブルのように、ネットワークの分析に使用するデータについてカスタムテーブルを検索できます。定義済みのテーブルを使用して可能であるように、カスタム テーブルに基づいてレポートを作成できます。

## ユーザ定義のカスタム テーブル



### ヒント

新しいカスタムテーブルを作成する代わりに、別の Firepower Management Center からカスタムテーブルをエクスポートし、Firepower Management Center にインポートすることができます。

カスタム テーブルを作成するには、Firepower システムに付属しているどの定義済みテーブルに、カスタムテーブルに組み込むフィールドが含まれているかを判断します。その後、組み込

むフィールドを選択できます。さらに、必要に応じて、共通フィールドのフィールドマッピングを設定することもできます。



**ヒント** [ホスト (Hosts) ]テーブルを含むデータでは、1つの IP アドレスではなく、1つのホストのすべての IP アドレスに関連したデータを表示できます。

例として、[相関イベント (Correlation Events) ]テーブルと[ホスト (Hosts) ]テーブルのフィールドを結合するカスタム テーブルについて考慮します。このカスタム テーブルを使用して、相関ポリシーの違反に関係するホストの詳細情報を取得できます。注意すべき点として、[相関イベント (Correlation Events) ]テーブルの送信元 IP アドレスと宛先 IP アドレスのどちらと一致する [ホスト (Hosts) ]テーブル データを表示するかを決定する必要があります。

このカスタム テーブルのイベントのテーブル ビューを表示する場合、相関イベントが 1 行に 1 つずつ表示されます。次の情報を含むようにカスタム テーブルを設定できます。

- イベントが生成された日時
- 違反された相関ポリシーの名前
- 違反をトリガーとして使用した規則の名前
- 相関イベントに関係する送信元ホスト (開始ホスト) に関連付けられた IP アドレス
- 送信元ホストの NetBIOS 名
- 送信元ホストが実行しているオペレーティング システムおよびバージョン
- 送信元ホストの重大度



**ヒント** 宛先ホスト (応答ホスト) の同じ情報を表示する同様のカスタム テーブルを作成することもできます。

## カスタム テーブルの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Any/Admin

### 手順

**ステップ 1** [分析 (Analysis) ] > [カスタム (Custom) ] > [カスタム テーブル (Custom Tables) ] を選択します。

**ステップ 2** [カスタム テーブルの作成 (Create Custom Table) ] をクリックします。

- ステップ 3** [名前 (Name) ]フィールドに、カスタム テーブルの名前を入力します。
- 例：  
たとえば、Correlation Events with Host Information (Src IP) と入力します。
- ステップ 4** [テーブル (Tables) ]ドロップダウンリストから、[相関イベント (Correlation Events) ]を選択します。
- ステップ 5** [フィールド (Fields) ]で[時間 (Time) ]を選択し、[追加 (Add) ]をクリックして、相関イベントが生成された日時を追加します。
- ステップ 6** 手順5を繰り返して、[ポリシー (Policy) ]および[ルール (Rule) ]フィールドを追加します。
- ヒント CtrlまたはShiftを押しながらクリックすることにより、複数のフィールドを選択できます。また、クリックしてドラッグすることで、隣接する複数の値を選択できます。ただし、テーブルに関連したイベントのテーブルビューでフィールドが表示される順序を指定する場合は、フィールドを一度に1つずつ追加します。
- ステップ 7** [テーブル (Tables) ]ドロップダウンリストから[ホスト (Hosts) ]を選択します。
- ステップ 8** [IP アドレス (IP Address) ]、[NetBIOS 名 (NetBIOS Name) ]、[OS 名 (OS Name) ]、[OS バージョン (OS Version) ]、[ホストの重大度 (Host Criticality) ]フィールドをカスタム テーブルに追加します。
- ステップ 9** [相関イベント (Correlation Events) ]の隣にある[共通フィールド (Common Fields) ]で、[送信元 IP (Source IP) ]を選択します。
- 相関イベントに関係する送信元ホスト (開始ホスト) 用に手順8で選択したホスト情報を表示するように、カスタム テーブルが設定されます。
- ヒント 相関イベントに関係する宛先ホスト (応答ホスト) に関する詳細なホスト情報を表示するカスタム テーブルを作成する場合も、この手順に従いますが、[送信元 IP (Source IP) ]ではなく、[送信先 IP (Destination IP) ]を選択します。
- ステップ 10** [保存 (Save) ]をクリックします。

## カスタム テーブルの変更

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Any/Admin

マルチドメイン展開では、現在のドメインで作成されたカスタム テーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタム テーブルも表示されますが、これは編集できません。下位のドメインのカスタム テーブルを表示および編集するには、そのドメインに切り替えます。

## 手順

- ステップ 1** [分析 (Analysis)] > [カスタム (Custom)] > [カスタム テーブル (Custom Tables)] を選択します。
- ステップ 2** 編集するテーブルの横にある編集アイコン (✎) をクリックします。
- 代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3** 除外するフィールドの横にある削除アイコン (🗑) をクリックして、テーブルからフィールドを除外することもできます。
- (注) レポートで現在使用中のフィールドを削除すると、それらのフィールドを使用しているセクションをそれらのレポートから除外するか確認するプロンプトが表示されます。
- ステップ 4** 必要に応じて、その他の変更を実行します。
- ステップ 5** [保存 (Save)] をクリックします。

## カスタム テーブルの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Any/Admin

マルチドメイン導入では、現在のドメインで作成されたカスタムテーブルが表示されます。これは削除できます。先祖ドメインで作成されたカスタムテーブルも表示されますが、これは削除できません。下位のドメインのカスタムテーブルを削除するには、そのドメインに切り替えます。

## 手順

- ステップ 1** [分析 (Analysis)] > [カスタム (Custom)] > [カスタム テーブル (Custom Tables)] を選択します。
- ステップ 2** 削除するカスタム テーブルの隣にある削除アイコン (🗑) をクリックします。
- コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

## カスタム テーブルに基づいたワークフローの表示

スマート ライセ ンス	従来のライセンス	サポートされるデ バイス	サポートされるド メイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Any/Admin

カスタム テーブルを作成すると、そのデフォルトのワークフローがシステムによって自動的に作成されます。このワークフローの最初のページには、イベントのテーブルビューが表示されます。カスタム テーブルに侵入イベントを含める場合、ワークフローの 2 番目のページはパケット ビューになります。それ以外の場合、ワークフローの 2 番目のページはホスト ページになります。カスタム テーブルに基づいて、独自のカスタム ワークフローを作成することもできます。



### ヒント

カスタム テーブルに基づいてカスタム ワークフローを作成する場合、それをそのテーブルのデフォルトのワークフローとして指定できます。

同じ手法を使用して、定義済みのテーブルに基づいたイベントビューに使用するカスタム テーブルでイベントを表示できます。

マルチドメイン展開では、現在のドメインで作成されたカスタム テーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタム テーブルも表示されますが、これは編集できません。下位のドメインのカスタム テーブルを表示および編集するには、そのドメインに切り替えます。

### 手順

- ステップ 1** [分析 (Analysis)] > [カスタム (Custom)] > [カスタム テーブル (Custom Tables)] を選択します。
- ステップ 2** 表示するワークフローに関連するカスタム テーブルの隣にある表示アイコン (🔍) をクリックします。

## カスタム テーブルの検索

スマート ライセ ンス	従来のライセンス	サポートされるデ バイス	サポートされるド メイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Any/Admin

マルチドメイン展開では、現在のドメインで作成されたカスタム テーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタム テーブルも表示されますが、これは編



集できません。下位のドメインのカスタムテーブルを表示および編集するには、そのドメインに切り替えます。

#### 手順

- ステップ 1** [分析 (Analysis)] > [カスタム (Custom)] > [カスタム テーブル (Custom Tables)] を選択します。
- ステップ 2** 検索するカスタム テーブルの隣にある表示アイコン (🔍) をクリックします。
- ヒント カスタムワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(ワークフローの切り替え) ((switch workflow))] をクリックします。
- ステップ 3** [検索 (Search)] をクリックします。
- ヒント 別の種類のイベントやデータについてデータベースを検索する場合は、その種類をテーブル ドロップダウンリストから選択します。
- ステップ 4** 該当するフィールドに、検索条件を入力します。
- 複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。
- ヒント 検索基準としてオブジェクトを使用する場合は、検索フィールドの横にあるオブジェクト アイコン (+) をクリックします。
- ステップ 5** 必要に応じて、検索を保存する場合は、[プライベート (Private)] チェックボックスをオンにして、プライベートとして検索を保存すると、その検索に本人のみがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。
- ヒント カスタムユーザロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。
- ステップ 6** 必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。
- [保存 (Save)] をクリックして、検索条件を保存します。[プライベート (Private)] チェックボックスをオンにすると、その検索は本人のアカウントでのみ表示できるようになります。
  - 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[新規に保存 (Save As New)] をクリックします。[プライベート (Private)] チェックボックスをオンにすると、その検索は本人のアカウントでのみ保存および表示できるようになります。
- ステップ 7** [検索 (Search)] をクリックして、検索を開始します。

検索結果は、現在の時間範囲によって制限されている、カスタム テーブルのデフォルトのワークフローに表示されます (該当する場合)。

---



## 第 **XXV** 部

### イベントとアセット

- [接続ロギング \(2503 ページ\)](#)
- [接続イベントとセキュリティインテリジェンス イベント \(2521 ページ\)](#)
- [侵入イベントの操作 \(2555 ページ\)](#)
- [ファイル/マルウェア イベントとネットワーク ファイル トラジェクトリ \(2613 ページ\)](#)
- [ホスト プロファイルの使用 \(2655 ページ\)](#)
- [ディスクバリ イベントの操作 \(2689 ページ\)](#)
- [相関イベントとコンプライアンス イベント \(2755 ページ\)](#)
- [システムの監査 \(2771 ページ\)](#)





## 第 105 章

# 接続ロギング

次のトピックでは、モニタ対象ネットワークでホストから実行される接続を記録するよう Firepower システムを設定する方法について説明します。

- [接続ロギングについて \(2503 ページ\)](#)
- [接続ロギング ストラテジー \(2504 ページ\)](#)
- [トンネル ルールおよびプレフィルタ ルールによる接続のロギング \(2513 ページ\)](#)
- [SSL ルールによる復号可能接続のロギング \(2514 ページ\)](#)
- [セキュリティ インテリジェンスによる接続のロギング \(2515 ページ\)](#)
- [アクセス制御ルールによる接続のロギング \(2516 ページ\)](#)
- [ポリシーのデフォルト アクションによる接続のロギング \(2517 ページ\)](#)
- [長い URL のロギングの制限 \(2518 ページ\)](#)

## 接続ロギングについて

システムは管理対象デバイスで検出された接続のログを生成できます。このログは接続イベントと呼ばれます。ルールやポリシーの設定を行うことで、ログに記録する接続の種類、接続をログに記録するタイミング、およびデータを保存する場所をきめ細かく制御できます。セキュリティ インテリジェンス イベントと呼ばれる特別な接続イベントは、レピュテーションベースのセキュリティ インテリジェンス機能によってブラックリストに登録（ブロック）された接続を表します。

接続イベントには、検出されたセッションに関するデータも含まれています。個々の接続イベントで入手可能な情報はいくつかの要因に応じて異なりますが、一般的には次のものがあります。

- タイムスタンプ、送信元と宛先の IP アドレス、入出力ゾーン、接続を処理したデバイスなど、基本的な接続特性
- アプリケーション、要求される URL、または接続に関連付けられているユーザなど、システムによって検出または推測される追加の接続特性
- どの設定がトラフィックを処理したか、接続が許可またはブロックされていたかどうか、暗号化された接続および復号された接続に関する詳細など、接続がログに記録された理由に関するメタデータ



- (注) エクスポートした NetFlow レコードから生成された接続データを使い、管理対象デバイスで収集された接続ログを補うことができます。これは、Firepower システムの管理対象デバイスでモニタできないネットワーク上に NetFlow 対応ルータやその他のデバイスを配置した場合に特に有効です。

#### 関連トピック

[Firepower システムの NetFlow データ](#) (2027 ページ)

## 接続ロギングストラテジー

部門のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。目標が生成するイベントの数を抑えパフォーマンスを向上させることである場合は、分析のために重要な接続のロギングのみを有効にします。しかし、プロファイリングの目的でネットワークトラフィックの広範な表示が必要な場合は、追加の接続のロギングを有効にできます。



- ヒント** 接続データの詳細な分析を実行するため、シスコはクリティカルな接続の終了を Firepower Management Center データベースに記録することを推奨します。

システムは 1 つの接続をさまざまな理由でロギングすることがあるため、1 か所でロギングを無効にしても、一致する接続がロギングされないとは限りません。また、接続イベントストレージを無効にしない限り、システムが自動でロギングする接続もあります。検出したファイアウォール、マルウェア、侵入、インテリジェントアプリケーションバイパス (IAB) に関連する接続がその例です。

以下はロギングできません。

- 8000 シリーズのファーストパスルールでファーストパスされた接続
- カプセル化された接続がアクセス制御によって検査されるプレーンテキスト、パススルートンネルの外部セッション

## 設定可能な接続ロギング

重要な接続のみがロギングされるように、ルールごとの接続ロギングを有効にします。あるルールに対し接続ロギングを有効にすると、システムはそのルールによって処理されたすべての接続をロギングします。

また、ポリシーのデフォルトアクションにより処理された接続をロギングすることもできます。ルールやデフォルトアクションにより (アクセス制御の場合は、ルールのインスペクション設定により)、ロギングのオプションは異なります。

### プレフィルタ ポリシー：ルールとデフォルト アクション

プレフィルタ ポリシーによりファースト パスまたはブロックする接続（すべてのプレーン テキスト、パススルー トンネルを含む）をロギングすることができます。

プレフィルタは、外部ヘッダーを基準にしてトラフィックを処理します。ロギングするトンネルでは、結果の接続イベントには、外部のカプセル化ヘッダー情報が含まれます。

継続分析の対象となるトラフィックについては、一致する接続が他の設定によってロギングされることもあるかもしれませんが、プレフィルタポリシーによるロギングは無効となります。システムは内部ヘッダーを使ってすべての継続分析を行います。つまり、システムは、許可されたトンネル内の各接続を個別に処理、ロギングします。

### SSL ポリシー：ルールとデフォルト アクション

SSL ルールまたは SSL ポリシーのデフォルト アクションに一致する接続をロギングすることができます。

ブロックされた接続の場合、システムは即座にセッションを終了し、イベントを生成します。監視対象の接続やアクセス コントロール ルールに渡す接続の場合、システムはセッションが終了するとイベントを生成します。

### アクセス コントロール ポリシー：セキュリティ インテリジェンスによる判断

接続がレピュテーションベースのセキュリティ インテリジェンス機能によってブラックリスト 登録（ブロック）される場合は、その接続をログに記録できます。

オプションで、セキュリティ インテリジェンス フィルタリングにはモニタ専用設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブラックリスト 登録されるはずの接続をシステムがさらに分析できるだけでなく、ブラックリストと一致する接続をログに記録することもできます。セキュリティ インテリジェンス モニタリングによって、セキュリティ インテリジェンス情報を使用してトラフィック プロファイルを作成することもできます。

セキュリティ インテリジェンスのフィルタリングの結果、システムが接続イベントをロギングすると、一致するセキュリティ インテリジェンス イベントもロギングされます。そのイベントは特殊なタイプの接続イベントで、個別に表示および分析することができ、また個別に保存、プルーニングされます。接続でブラックリスト 登録された IP アドレスを特定できるように、IP アドレスの横にあるホスト アイコンは、ブラックリスト 登録された IP アドレスとモニタされた IP アドレスではイベント ビューアで少々異なる表示になっています。

### アクセス コントロール ポリシー：ルールとデフォルト アクション

アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに一致する接続をロギングすることができます。

#### 関連トピック

[アクションと接続ロギング](#) (2509 ページ)

## 自動接続ロギング

接続イベントのストレージを無効にしない限り、システムは他のロギング設定に関係なく、Firepower Management Center データベースに次の接続終了イベントを保存します。

### 侵入に関連付けられた接続

システムは、接続がアクセス コントロール ポリシーのデフォルトアクションで処理されなければ、侵入イベントに関連付けられた接続を自動的にログに記録します。

アクセス コントロールのデフォルトアクションに関連付けられた侵入ポリシーによって侵入イベントが生成された場合、システムは、そのイベントに関連する接続の終了を自動的にログに記録しません。代わりに、デフォルトのアクション接続のロギングを明示的に有効にする必要があります。これは、接続データをログに記録する必要がない、侵入防御専用の展開環境で役立ちます。

ただし例外として、デフォルトアクションの接続開始ロギングを有効にした場合はその限りではありません。この場合、関連付けられた侵入ポリシーがトリガーされると、システムは接続の開始だけでなく、接続の終了もログに記録します。

### ファイル イベントとマルウェア イベントに関連付けられた接続

システムは、ファイル イベントとマルウェア イベントに関連付けられた接続を自動的にログに記録します。



- (注) NetBIOS-ssn (SMB) トラフィックのインスペクションによって生成されるファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。システムはクライアントまたはサーバがセッションを終了した後に接続イベントを生成します。

### インテリジェント アプリケーション バイパスに関連付けられた接続

システムは、IABに関連付けられたバイパスされた、およびバイパスされるはずだった接続をログに記録します。

## 接続開始のロギングと終了のロギングの比較

接続は、次の例外となるブロックされたトラフィックを除き、接続開始時あるいは終了時にログを記録することができます。

- ブロックされたトラフィック：ブロックされたトラフィックは、さらに検査されることなくすぐさま拒否されるため、通常、ブロックされたトラフィックやブラックリストに登録されたトラフィックについては、接続開始イベントのみ記録可能です。ログに記録される個々の接続終了はありません。



- ブロックされた暗号化トラフィック：SSLポリシーで接続のログギングを有効にすると、システムは接続開始イベントではなく接続終了イベントをログに記録します。これは、システムは接続がセッション内で最初のパケットを使用して暗号化されているかどうかを判定できず、暗号化されたセッションを即座にブロックできないためです。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をログギングします。何らかの理由で接続をモニタリングすると、接続終了ログギングが強制されます。単一のブロックされていない接続の場合、接続終了イベントには、接続開始イベントに含まれるすべての情報に加えて、セッション期間中に収集された情報も含まれます。

次の表では、接続開始イベントと接続終了イベントの違い（それぞれをログギングする利点を含む）を詳細に説明します。

表 290: 接続開始イベントと接続終了イベントの比較

	接続開始イベント	接続終了イベント
次の場合に生成可能です	システムが接続の開始を検出した場合（または、イベントの生成がアプリケーションまたはURLの識別に依存する場合は最初の数パケットの後）	システムが以下の状態の場合 <ul style="list-style-type: none"> <li>• 接続のクローズを検出した場合</li> <li>• 一定期間後に接続の終了を検出しない場合</li> <li>• メモリ制約によりセッションを追跡できなくなった場合</li> </ul>
次のものについてログギングが可能です	SSLポリシーによってブロックされた接続を除くすべての接続	すべての接続。ただし、すべての場所で接続終了ログギングを設定できない場合があります。
次を含みます	最初のパケット（または、イベントの生成がアプリケーションまたはURLの識別に依存する場合は最初の数パケット）で判定できる情報のみ	接続開始イベント内のすべての情報と、セッション期間を通してトラフィックを検査して判別された情報（たとえば伝送されたデータ総量、接続の最後のパケットのタイムスタンプなど）

	接続開始イベント	接続終了イベント
次の場合に有用です	<p>次のものをロギングする場合</p> <ul style="list-style-type: none"> <li>• ブロックされた接続。</li> <li>• 接続終了情報はユーザにとって重要ではないので、接続の開始のみ</li> </ul>	<p>目的</p> <ul style="list-style-type: none"> <li>• SSL ポリシーによって処理される暗号化接続をロギングする場合</li> <li>• セッションの期間にわたって収集された情報であらゆる種類の詳細な分析を実行する場合、またはその情報を使用して相関ルールをトリガーする場合</li> <li>• カスタム ワークフローで接続の概要（集約接続データ）を表示する場合、グラフ形式で接続データを表示する場合、またはトラフィック プロファイルを作成して使用する場合</li> </ul>

## Firepower Management Center と外部ロギング

接続イベントとセキュリティ インテリジェンス イベントは Firepower Management Center データベースにロギングできます（Web インターフェイスの [イベントビューア（Event Viewer）]）。Firepower Management Center に保存できるイベントの数はモデルによって異なります。アラート応答と呼ばれる接続を設定し、それを使って外部 syslog や SNMP トラップ サーバにイベントをロギングすることもできます。

Firepower Management Center データベースにロギングすると、Firepower システムのレポート、分析、およびデータ相関関係の多くの機能を活用できます。次に例を示します。

- ダッシュボードおよびコンテキストエクスプローラでは、システムによってロギングされた接続をグラフ形式によって一目で確認できます。
- イベントビューには、システムによってロギングされた接続の詳細情報が提示され、グラフ形式や表形式で表示したり、レポートに要約することもできます。
- トラフィック プロファイリングは、接続データを使用して正常なネットワーク トラフィックのプロファイルを作成します。ユーザはそのプロファイルを基準として使用して、異常な動作を検出および追跡できます。
- 相関ポリシーを使用して、イベントを生成し、特定のタイプの接続またはトラフィック プロファイルの変更に対する応答（アラートや外部修復など）をトリガーできます。



- (注) これらの機能を使用するには、接続（ほとんどの場合、接続の開始ではなく接続の終了）を Firepower Management Center データベースにロギングする **必要があります**。システムがクリティカルな接続（ログに記録された侵入、禁止されたファイルおよびマルウェアに関連付けられているもの）を自動的にロギングするのはこのためです。

#### 関連トピック

[Firepower Management Center アラート応答](#) (2341 ページ)

## アクションと接続ロギング

接続ロギングを設定する場合、ルールアクションおよびポリシーのデフォルトアクションにより、一致するトラフィックをシステムがどのように検査、処理するのかだけでなく、一致するトラフィックの詳細をいつ、どのようにロギングするかが決まります。接続イベントには、接続がロギングされた理由を記述したメタデータが含まれています。メタデータにはトラフィックがどの設定によって処理されたかなどの情報が含まれます。

#### 関連トピック

[トンネルとプレフィルタ ルールのコンポーネント](#) (1408 ページ)

[SSL ルールのアクション](#) (1477 ページ)

[アクセス コントロールルールのアクション](#) (1353 ページ)

[接続およびセキュリティ インテリジェンス イベントフィールド](#) (2523 ページ)

## FastPath された接続のロギング

FastPath された接続や非暗号化トンネルをロギングできます。ロギングには、プレフィルタポリシーの以下のルールとアクションに一致するトラフィックを含めることができます。

- トンネルルール：[ファストパス (FastPath) ]アクション (外部セッションをロギングします)
- プレフィルタ ルール：[ファストパス (FastPath) ]アクション

FastPath されたトラフィックはアクセス コントロールと QoS の残りをバイパスするため、FastPath された接続の接続イベントに含まれる情報は限られます。8000 シリーズ FastPath ルールで FastPath された接続をロギングすることはできません。

## モニタされた監視接続のロギング

システムは常に、以下の設定と一致するトラフィックの接続終了をロギングします。このことは、トラフィックに一致する他のルールがなく、デフォルトアクションのロギングを有効にしている場合でも該当します。

- セキュリティインテリジェンス：モニタするように設定されたブラックリスト (セキュリティ インテリジェンス イベントも生成されます)

- SSL ルール : [ モニタ (Monitor) ] アクション
- アクセス コントロール ルール : [ モニタ (Monitor) ] アクション

システムは、1つの接続が1つのモニタールールに一致するたびに1つの別個のイベントを生成するわけではありません。1つの接続が複数のモニタールールに一致する可能性があるため、各接続イベントには、接続が一致する最初の8つのモニター アクセス コントロール ルールに関する情報だけでなく、最初の一致する SSL モニター ルールに関する情報を含めて表示することができます。

同様に、外部 syslog または SNMP トラップ サーバに接続イベントを送る場合、システムは1つの接続が1つのモニタールールに一致するたびに1つの別個のアラートを送信するわけではありません。代わりに、接続の終了時にシステムから送られるアラートに、接続が一致したモニター ルールの情報が含まれます。

## 信頼されている接続のロギング

信頼されている接続の開始と終了をロギングできます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- アクセス コントロール ルール : [ 信頼する (Trust) ] アクション
- アクセス コントロール のデフォルト アクション : [ すべてのトラフィックを信頼する (Trust All Traffic) ]

信頼されている接続には、ディープインスペクションまたはディスカバリは適用されません。したがって、信頼されている接続の接続イベントに含まれる情報は限られます。

システムは、接続を検出したデバイスに応じて異なる方法で、信頼アクセスコントロールルールによって処理された TCP 接続をロギングします。

- 7000 および 8000 シリーズ デバイスでは、信頼ルールによって最初のパケットで検出された TCP 接続は、すでに有効になっているモニター ルールの有無に応じて異なるイベントを生成します。モニタールールがアクティブな場合、システムはパケットを評価し、接続開始および接続終了イベントを生成します。アクティブなモニタールールがない場合、システムは接続終了イベントだけを生成します。
- 他のすべてのモデルでは、信頼ルールによって最初のパケットで検出された TCP 接続は、接続終了イベントだけを生成します。システムは、最後のセッションパケットの1時間後にイベントを生成します。

## ブロックされた接続のロギング

ブロックされた接続をロギングできます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- トンネル ルール : [ ブロック (Block) ]
- プレフィルタ ルール : [ ブロック (Block) ]

- プレフィルタのデフォルトアクション：[すべてのトンネルトラフィックをブロック (Block all tunnel traffic) ]
- セキュリティインテリジェンス：ブロックするブラックリストが設定されます (セキュリティインテリジェンス イベントも生成されます)
- SSL ルール：[ブロック (Block) ]および[リセットしてブロック (Block with reset) ]
- SSL のデフォルトアクション：[ブロック (Block) ]および[リセットしてブロック (Block with reset) ]
- アクセスコントロールルール：[ブロック (Block) ]、[リセットしてブロック (Block with reset) ]、[インタラクティブブロック (Interactive Block) ]
- アクセスコントロールのデフォルトアクション：[すべてのトラフィックをブロック (Block All Traffic) ]

トラフィックをブロックできるデバイスは、インライン (つまり、ルーテッドインターフェイス、スイッチドインターフェイス、トランスペアレントインターフェイス、インラインインターフェイスのペア) で展開されているもののみです。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。



#### 注意

サービス妨害 (DoS) 攻撃の間にブロックされた TCP 接続をロギングすると、システムパフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロックルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニターするかどうかを検討します。

#### ブロックされた接続の接続開始ロギングと接続終了ロギングとの比較

ブロックされた接続をロギングするときは、システムがその接続をどのようにロギングするかは接続がブロックされた理由によって異なります。これは、接続ログに基づいて関連ルールを設定する際に留意しておくことが重要です。

- 暗号化されたトラフィックをブロックする SSL ルールおよび SSL ポリシーのデフォルトアクションの場合、システムは接続終了イベントをロギングします。これは、システムが接続がセッション内で最初のパケットを使用して暗号化されているかどうかを決定できないためです。
- 他のブロッキングアクションについては、システムは接続開始イベントをロギングします。一致するトラフィックは、追加のインスペクションなしで拒否されます。

#### バイパスされるインタラクティブブロックのロギング

インタラクティブブロッキングアクセスコントロールルール (このルールではユーザが禁止されている Web サイトを参照するとシステムによって警告ページが表示されます) を使用す

ると、接続終了ロギングを設定できます。その理由は、警告ページをユーザがクリックスルーすると、その接続は新規の、許可された接続と見なされ、システムによってモニタとロギングができるためです。

したがって、[インタラクティブ ブロック (Interactive Block)] ルールまたは [リセットしてインタラクティブ ブロック (Interactive Block with reset)] ルールにパケットが一致する場合、システムは以下の接続イベントを生成できます。

- ユーザの要求が最初にブロックされ警告ページが表示されたときの接続開始イベント。このイベントにはアクション [インタラクティブ ブロック (Interactive Block)] または [リセットしてインタラクティブ ブロック (Interactive Block with reset)] が関連付けられます。
- 複数の接続開始または終了イベント (ユーザが警告ページをクリックスルーし、要求した最初のページをロードした場合)。これらのイベントには [許可 (Allow)] アクションおよび理由 [ユーザ バイパス (User Bypass)] が関連付けられます。

## 許可された接続のロギング

許可された接続をロギングができます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- SSL ルール : [複合 (Decrypt)] アクション
- SSL ルール : [複合しない (Do not decrypt)] アクション
- SSL のデフォルト アクション : [複合しない (Do not decrypt)] アクション
- アクセス コントロール ルール : [許可 (Allow)] アクション
- アクセスコントロールのデフォルトアクション : [ネットワーク検出のみ (Network Discovery Only)] および任意の侵入防御オプション

これらの設定に対するロギングを有効にすると、接続が確実にロギングされると同時に、インスペクションおよびトラフィック処理の次のフェーズが許可 (または指定) されます。SSL ロギングは常に接続終了ロギングですが、アクセスコントロール設定で接続開始ロギングも可能にすることができます。

トンネルおよびプレフィルタールールでの [分析 (Analyze)] アクションを使用してアクセスコントロールで接続を続行することもできますが、このアクションを使用するルールではロギングが無効にされます。ただし、他の設定を使用して、一致する接続をロギングすることもできます。許可されたトンネルのカプセル化されたセッションは、個別に評価されてロギングされます。

アクセス コントロール ルールまたはデフォルト アクションでトラフィックを許可する場合、関連する侵入ポリシーを使用してトラフィックをさらに検査し、侵入をブロックすることができます。アクセス コントロール ルールでは、ファイル ポリシーを使用して、マルウェアを含む禁止されたファイルを検出し、ブロックすることもできます。接続イベントストレージを無効にしない限り、システムは、侵入イベント、ファイル イベント、マルウェア イベントに関連する許可された接続のほとんどを自動的にロギングします。詳細については、[自動接続ロギ](#)

ング (2506ページ) を参照してください。ペイロードが暗号化される接続には、ディープインスペクションは適用されません。したがって、暗号化接続の接続イベントに含まれる情報は限られることに注意してください。

### 許可された接続のファイルおよびマルウェア イベントのロギング

ファイルポリシーによってファイルが検出またはブロックされると、以下のいずれかのイベントが Firepower Management Center データベースにロギングされます。

- ファイル イベント：検出またはブロックされたファイル（マルウェア ファイルを含む）を表します
- マルウェア イベント：検出されたまたはブロックされたマルウェア ファイルのみを表します
- レトロスペクティブ マルウェア イベント：以前に検出されたファイルでのマルウェア処理が変化した場合に生成されます

このロギングは、アクセス コントロールルールごとに無効にすることができます。または、ファイルイベントおよびマルウェア イベントストレージを完全に無効にすることもできます。



(注) Cisco では、ファイルイベントおよびマルウェア イベントのロギングを有効のままにすることを推奨しています。

## トンネルルールおよびプレフィルタールールによる接続のロギング

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Admin/Access Admin/Network Admin

### 始める前に

- ルール アクションを [ブロック (Block) ] または [ファストパス (Fastpath) ] に設定します。[分析 (Analyze) ] アクションのロギングは無効にします。これにより、接続のアクセス制御が引き続き可能になり、接続の処理とロギングは別の設定で決定されます。

## 手順

- ステップ 1** プレフィルタポリシーエディタで、ロギングを設定するルールのある編集アイコン (✎) をクリックします。
- 代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 2** [ロギング (Logging)] タブをクリックします。
- ステップ 3** [接続の開始時にロギングする (Log at Beginning of Connection)] または [接続の終了時にロギングする (Log at End of Connection)] を指定します。
- パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。ブロックされたトラフィックは、それ以上の検査なしで即座に拒否されるため、[ブロック (Block)] ルールの場合は接続終了時のイベントはロギングできません。
- ステップ 4** 接続イベントの送信先を指定します。
- 接続イベントについて Firepower Management Center ベースの分析を実行する場合は、イベントをイベントビューアに送信します。
- ステップ 5** [保存 (Save)] をクリックしてルールを保存します。
- ステップ 6** [保存 (Save)] をクリックしてポリシーを保存します。

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

# SSL ルールによる復号可能接続のロギング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

## 手順

- ステップ 1** SSLポリシーエディタで、ロギングを設定するルールのある編集アイコン (✎) をクリックします。



代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 2** [ロギング (Logging) ] タブをクリックします。

**ステップ 3** [接続の終了時にロギングする (Log at End of Connection) ] をオンにします。

モニタ対象トラフィックに対して、接続の終了時のロギングが必要になります。

**ステップ 4** 接続イベントの送信先を指定します。

接続イベントについて Firepower Management Center ベースの分析を実行する場合は、イベントをイベントビューアに送信します。モニタ対象トラフィックに対して、これが必要になります。

**ステップ 5** [保存 (Save) ] をクリックしてルールを保存します。

**ステップ 6** [保存 (Save) ] をクリックしてポリシーを保存します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## セキュリティ インテリジェンスによる接続のロギング

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

#### 手順

**ステップ 1** アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス (Security Intelligence) ] タブをクリックします。

**ステップ 2** ロギング アイコン (🔍) をクリックして、次の条件を使用するセキュリティ インテリジェンス ロギングを有効にします。

- IP アドレス別 : [ネットワーク (Networks) ] の横にあるロギング アイコンをクリックします。
- URL 別 : [URL (URLs) ] の横にあるロギング アイコンをクリックします。
- ドメイン名別 : [DNS ポリシー (DNS Policy) ] ドロップダウンリストの横にあるロギング アイコンをクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベースポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。

**ステップ 3** [接続のロギング (Log Connections)] チェックボックスをオンにします。

**ステップ 4** 接続イベントとセキュリティ インテリジェンス イベントの送信先を指定します。

Firepower Management Center ベースの分析を実行する場合や、ブラックリストに登録されたオブジェクトをモニタ専用を設定する場合は、イベントをイベント ビューアに送信します。

**ステップ 5** [OK] をクリックしてロギング オプションを設定します。

**ステップ 6** [保存 (Save)] をクリックしてポリシーを保存します。

### 次のタスク

- 設定変更を展開します。 [設定変更の導入 \(350 ページ\)](#) を参照してください。

## アクセス制御ルールによる接続のロギング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

ルールアクションと詳細検査のオプションの選択によって、ロギング オプションは異なります。 [アクションと接続ロギング \(2509 ページ\)](#) を参照してください。

### 手順

**ステップ 1** アクセス コントロール ポリシー エディタで、ロギングを設定するルールの横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) が表示される場合、設定は先祖ポリシーから継承され、先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 2** [ロギング (Logging)] タブをクリックします。

**ステップ 3** [接続の開始時にロギングする (Log at Beginning of Connection)] または [接続の終了時にロギングする (Log at End of Connection)] を指定します。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。

**ステップ 4** (オプション) [ファイルのロギング (Log Files)] チェックボックスをオンにして、接続に関連付けられているファイル イベントとマルウェア イベントをロギングします。

シスコは、このオプションを有効のままにすることを推奨します。

**ステップ 5** 接続イベントの送信先を指定します。

接続イベントに対し、Management Center ベースの分析を実行する場合や、ルールアクションが [モニタ (Monitor)] の場合は、イベントを Firepower Management Center に送信します。

**ステップ 6** [保存 (Save)] をクリックしてルールを保存します。

### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## ポリシーのデフォルトアクションによる接続のロギング

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

ポリシーのデフォルトアクションにより、システムがポリシー内のルールの内いずれにも一致しないトラフィックを処理する方法が決定されます (ただし、トラフィックの照合およびロギングを実行し、トラフィックの処理や調査は実行しないアクセス コントロール ポリシーと SSL ポリシー内のモニタ ルールを除きます)。

また、システムが複合化できないセッションをロギングする方法は、SSL ポリシーのデフォルトアクションのロギング設定でも制御されます。

### 始める前に

- プレフィルタのデフォルトアクションロギングについては、デフォルトアクションを [すべてのトンネルトラフィックをブロック (Block all tunnel traffic)] に設定します。[すべてのトンネルトラフィックを許可 (Allow all tunnel traffic)] アクションのロギングは無効になります。これにより、接続のアクセス制御が引き続き可能になり、接続の処理とロギングは別の設定で決定されます。

### 手順

**ステップ 1** ポリシー エディタで、[デフォルトアクション (Default Action)] ドロップダウンリストの横にあるロギングアイコン (📄) をクリックします。

**ステップ 2** 一致する接続をロギングするタイミングを指定します。

- 接続の開始時にロギングする：SSL のデフォルト アクションではサポートされていません。
- 接続の終了時にロギングする：アクセス制御の [すべてのトラフィックをブロック (Block All Traffic) ] デフォルト アクションまたはプレフィルタの [すべてのトンネルトラフィックをブロック (Block all tunnel traffic) ] デフォルト アクションを選択するとサポートされなくなります。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。アクセス コントロール ポリシーでは、設定が先祖ポリシーから継承されることもあります。

**ステップ 3** 接続イベントの送信先を指定します。

接続イベントについて Firepower Management Center ベースの分析を実行する場合は、イベントをイベント ビューアに送信します。

**ステップ 4** [OK] をクリックします。

**ステップ 5** [保存 (Save) ] をクリックしてポリシーを保存します。

#### 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。

## 長い URL のロギングの制限

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

HTTP トラフィックの接続の終了イベントは、監視対象ホストによって要求された URL を記録します。URL の保管を無効にすることや保管する URL 文字数を制限することで、システムパフォーマンスが向上する可能性があります。URL のロギングを無効化しても（保管する文字数を 0 にしても）、URL フィルタリングには影響しません。システムは、要求された URL に基づいてトラフィックをフィルタリングします。それらの URL を記録しない場合も同じです。

## 手順

---

**ステップ 1** アクセスコントロールポリシーエディタで、[詳細 (Advanced)] タブをクリックして、[一般設定 (General Settings)] の横にある編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔒) が表示される場合、設定は先祖ポリシーから継承され、先祖ドメインに属しており、設定を変更する権限がありません。設定がロック解除されている場合は、[ベースポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。

**ステップ 2** [接続イベントで保存する URL の最大文字数 (Maximum URL characters to store in connection events)] を入力します。

**ステップ 3** [OK] をクリックします。

**ステップ 4** [保存 (Save)] をクリックしてポリシーを保存します。

---

## 次のタスク

- 設定変更を展開します。[設定変更の導入 \(350 ページ\)](#) を参照してください。





## 第 106 章

# 接続イベントとセキュリティインテリジェンス イベント

次のトピックでは、接続およびセキュリティ イベント テーブルを使用する方法について説明します。

- [接続イベントについて \(2521 ページ\)](#)
- [接続およびセキュリティ インテリジェンス イベント フィールド \(2523 ページ\)](#)
- [接続およびセキュリティ インテリジェンス イベント テーブルの使用 \(2548 ページ\)](#)
- [デバイス サマリー ページの表示 \(2553 ページ\)](#)

## 接続イベントについて

システムは、管理対象デバイスが検出した接続のログを生成することができます。このログは接続イベントと呼ばれます。ルールやポリシーの設定を行うことで、ログに記録する接続の種類、接続をログに記録するタイミング、およびデータを保存する場所をきめ細かく制御できます。セキュリティインテリジェンス イベントは特殊な接続イベントで、レピュテーションベースのセキュリティインテリジェンス機能によってブラックリストに登録されている（ブロックされた）接続を表します。詳細については、[接続ロギング \(2503 ページ\)](#) を参照してください。

### 関連トピック

[セキュリティ インテリジェンスについて \(1375 ページ\)](#)

## 接続イベントとセキュリティ インテリジェンス イベントの比較

セキュリティ インテリジェンス イベントは、レピュテーションベースのセキュリティ インテリジェンス機能によりセッションがブラックリストに登録された（ブロックされた）ときに生成される接続イベントです。

ただし、各セキュリティ インテリジェンス イベントには同一の接続イベントがあり、セキュリティ インテリジェンス イベントを個別に表示、分析できます。また、システムはセキュリティ インテリジェンス イベントを個別に保存およびプルーニングします。

システムは、より多くのリソースを消費する評価を行う前に、セキュリティインテリジェンスを実施することに注意してください。接続がセキュリティインテリジェンスによってブロックされた場合、結果として生成されるイベントには、その後の評価によってシステムで収集されることになっていた情報（ユーザ ID など）が含まれません。



(注) 本書では違ふと明記されていない限り、接続イベントに関する情報は、セキュリティインテリジェンス イベントに関する情報でもあります。

## NetFlow 接続

管理対象デバイスで収集された接続データを捕うために、NetFlow エクスポートによってブロードキャストされたレコードを使用して接続イベントを生成できます。この方法が特に役立つのは、NetFlow エクスポートが、管理対象デバイスでモニタしているネットワークとは別のネットワークをモニタしている場合です。

システムは NetFlow レコードを単方向の接続終了イベントとして Firepower Management Center データベースに記録します。これらの接続に関して使用可能な情報は、アクセスコントロールポリシーで検出された接続の情報とは若干異なります。[NetFlow データと管理対象デバイスデータの違い \(2028 ページ\)](#) を参照してください。

### 関連トピック

[Firepower システムの NetFlow データ \(2027 ページ\)](#)

## 接続の概要（グラフ用集約データ）

Firepower システムは 5 分間隔で収集された接続データを集約し、接続の概要を作成します。この概要を使用して、接続グラフとトラフィックプロファイルがシステムで生成されます。必要に応じて、接続の概要データに基づいてカスタム ワークフローを作成できます。これは、個々の接続イベントに基づいたワークフローと同じように使用できます。

セキュリティ インテリジェンス イベント専用の接続の概要はないことに注意してください。ただし、対応する接続終了イベントは接続の概要データに集約できます。

集約するには、複数の接続が以下の状態である必要があります。

- 接続終了を表している
- 送信元と宛先の IP アドレスが同じで、レスポнда（宛先）のホストで同じポートを使用している
- 同じプロトコルを使用している（TCP または UDP）
- 同じアプリケーションプロトコルを使用している
- 同じ Firepower システム管理対象デバイスまたは同じ NetFlow エクスポートによって検出される



各接続の概要には、接続数など全トラフィック統計情報が含まれています。NetFlow エクスポートは単一方向接続を生成するので、接続の概要では、NetFlow データに基づく接続ごとに接続数が 2 ずつ増えます。

接続の概要には、概要内の集約された接続に関するすべての情報が含まれているわけではありませんので注意してください。たとえば、接続の概要に集約される接続にはクライアント情報が使用されないため、概要にクライアント情報は含まれません。

## 長時間接続

接続データを集約する 5 分間隔の 2 回以上に監視対象のセッションがまたがる場合、その接続は長時間接続と見なされます。接続サマリーで接続数を計算する際には、長時間接続が開始された 5 分間隔の回のみカウントします。

また、長時間接続において発信側と応答側が送信したパケット数とバイト数を計算する際は、システムは 5 分間隔の各回で実際に送信されたパケット数とバイト数を報告しません。代わりにシステムは、送信された合計パケット数と合計バイト数、接続の長さ、5 分間隔の各回で接続のどの部分が行われたかに基づいて、一定の送信速度を仮定し、値を推定します。

## 外部応答側からの統合接続サマリー

接続データの保存に必要なスペースを減らし、接続グラフのレンダリングを高速化するために、システムは次の場合に接続サマリーを統合します。

- 接続に関連するホストの 1 つが監視対象のネットワーク上にない場合
- 外部ホストの IP アドレス以外で、サマリー内の接続がサマリー集約条件を満たす場合

イベントビューアで接続サマリーを表示する場合や、接続グラフを使用する場合、システムは非監視対象ホストの IP アドレスの代わりに [外部 (external)] と表示します。

この集約の結果として、外部応答側を含む接続サマリーまたはグラフから接続データのテーブルビューにドリルダウンしようとする（つまり、個別の接続データへのアクセス）、テーブルビューには情報が何も表示されません。

# 接続およびセキュリティ インテリジェンス イベント フィールド

表形式およびグラフィカル ワークフローを使用して表示や検索ができる接続およびセキュリティ インテリジェンス イベントには、次に示すフィールドがあります。個別のイベントで利用可能な情報は、システムがいつ、なぜ、どのようにして接続を記録したかによって異なることに注意してください。



- (注) 各セキュリティ インテリジェンス イベントには、同一の、個別に保存された接続イベントがあります。すべてのセキュリティ インテリジェンス イベントに、入力済みの [セキュリティ インテリジェンス カテゴリ (Security Intelligence Category) ] フィールドがあります。

接続グラフは接続サマリーに基づいているため、接続サマリーを制約しているのと同じ条件が接続グラフを制約します。検索ページのアスタリスク (\*) が付いたフィールドは、接続グラフおよび接続サマリーを制約します。無効な検索条件を使用して接続サマリーを検索し、カスタム ワークフローの接続サマリー ページを使用して結果を見る場合、無効な条件には適用不可 (N/A) としてラベルが付けられ、取り消し線が引かれます。

### 全般情報 (General Information)

#### アクセス コントロール ポリシー (Access Control Policy)

接続をモニタしたアクセス コントロール ポリシー。

#### アクセス コントロール ルール (Access Control Rule)

接続を処理したアクセス コントロール ルールまたはデフォルト アクションと、その接続に一致した最大 8 つのモニター ルール。

接続が 1 つのモニター ルールに一致した場合、Firepower Management Center は接続を処理したルールの名前を表示し、その後モニター ルール名を表示します。接続が複数のモニター ルールに一致したときは、イベント ビューアは一致したモニター ルールの数を Default Action + 2 Monitor Rules などと表示します。

接続に一致した最初の 8 つのモニター ルールのリストをポップアップ ウィンドウに表示するには、[N モニター ルール (NMonitor Rules) ] をクリックします。

#### アクション (Action)

接続をロギングした設定に関連付けられているアクション。

セキュリティ インテリジェンスによってモニタされている接続の場合、そのアクションは、接続によってトリガーされる最初のモニタ以外のアクセス コントロール ルールのアクションであるか、またはデフォルト アクションです。同様に、モニター ルールに一致するトラフィックは常に後続のルールまたはデフォルト アクションによって処理されるため、モニター ルールによってロギングされた接続と関連付けられたアクションが [モニター (Monitor) ] になることはありません。ただし、モニター ルールに一致する接続の関連ポリシー違反をトリガーする可能性があります。

アクション	説明
許可 (Allow)	アクセスコントロールによって明示的に許可された、またはユーザがインタラクティブ ブロックをバイパスしたために許可された接続。

アクション	説明
ブロック (Block)、リセットしてブロック (Block with reset)	次を含むブロックされた接続： <ul style="list-style-type: none"> <li>• プレフィルタポリシーによってブロックされたトンネルおよびその他の接続</li> <li>• セキュリティインテリジェンスによってブラックリストに載せられた接続</li> <li>• SSL ポリシーによってブロックされた暗号化接続</li> <li>• 侵入ポリシーによってエクスプロイトがブロックされた接続</li> <li>• ファイルポリシーによってファイル (マルウェアを含む) がブロックされた接続。</li> </ul> システムが侵入またはファイルをブロックする接続では、アクセスコントロールの許可ルールを使用してディープインスペクションを呼び出す場合にも、システムはブロックを表示します。
高速パス (Fastpath)	プレフィルタポリシーによって高速パスが適用された暗号化されていないトンネルおよびその他の接続。
インタラクティブブロック (Interactive Block)、リセット付きインタラクティブブロック (Interactive Block with reset)	システムがインタラクティブブロックルールを使用してユーザの HTTP 要求を最初にブロックしたときにログに記録された接続。システムにより表示される警告ページでユーザがクリックスルーすると、そのセッションでログに記録されるその後の接続に許可アクションが付きます。
信頼 (Trust)	アクセスコントロールによって信頼された接続。デバイスモデルに応じて、システムは信頼された TCP 接続を別にログに記録します。 <a href="#">信頼されている接続のログギング (2510 ページ)</a> を参照してください。
デフォルトアクション (Default Action)	アクセスコントロールポリシーのデフォルトアクションによって処理される接続。

**接続 (Connections)**

接続サマリーに含まれる接続数。長時間接続 (複数回の接続サマリー間隔にまたがる接続) の場合、最初の接続サマリー間隔の分だけ増加します。[接続 (Connections)] 条件を使用した検索で意味のある結果を表示するには、接続サマリーページを持つカスタムワークフローを使用する必要があります。

### メンバー数 (Count)

各行に表示される情報に一致する接続数。[カウント (Count)] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。カスタムワークフローを作成し、ドリルダウンページに [カウント (Count)] カラムを追加しない場合、各接続は個別に表示され、パケット数とバイト数は合計されません。

### エンドポイント ロケーション (Endpoint Location)

ISE で指定された、ユーザの認証に ISE を使用したネットワーク デバイスの IP アドレス。

### エンドポイント プロファイル (Endpoint Profile)

ISE で指定されたユーザのエンドポイント デバイス タイプ。

### 最初のパケットまたは最後のパケット (First Packet or Last Packet)

セッションの最初または最後のパケットが検出された日時。

### イニシエータ/レスポнда バイト (Initiator/Responder Bytes)

セッション イニシエータまたはセッション レスポндаが送信した合計バイト数。

### イニシエータ/レスポнда パケット (Initiator/Responder Packets)

セッション イニシエータが送信した合計パケット数。

### イニシエータ ユーザ (Initiator User) (サマリーおよびグラフを制約)

セッション イニシエータにログインしていたユーザ。このフィールドに [認証なし (No Authentication)] が入力されている場合、ユーザ トラフィックは次のようになります。

- 関連付けられたアイデンティティ ポリシーがないアクセス コントロール ポリシーに一致しました。
- アイデンティティ ポリシーのいずれのルールにも一致しませんでした。

### IOC

マルウェア イベントが、接続に関与したホストに対する侵入の痕跡 (IOC) をトリガーしたかどうか。

### ネットワーク分析ポリシー (Network Analysis Policy)

イベントの生成に関連付けられているネットワーク分析ポリシー (NAP) (ある場合)。

### プレフィルタ ポリシー (Prefilter Policy)

接続を処理したプレフィルタ ポリシー。

### 理由 (Reason)

多くの場合に接続がロギングされた1つまたは複数の原因。完全なリストについては、[接続イベントの理由 \(2537 ページ\)](#) を参照してください。

IP ブロック、DNS ブロック、および URL ブロックの理由による接続には、固有のイニシエータ レスポнда ペアごとに 15 秒のしきい値があります。システムがこれらのいずれかの接続をブロックした後、イベントを生成した時点から 15 秒の間、この 2 つのホスト間

で接続がブロックされたとしても、ポートやプロトコルの違いに関わらず、接続イベントを生成しません。

### セキュリティ コンテキスト (Security Context)

ASA FirePOWER でマルチ コンテキスト モードで処理される接続で、トラフィックが通過した仮想ファイアウォール グループを特定するメタデータ。

### セキュリティ グループ タグ (Security Group Tag)

接続に関係するパケットのセキュリティ グループ タグ (SGT) 属性。SGT は、信頼ネットワーク内での、トラフィックの送信元の権限を指定します。セキュリティ グループ アクセス (Cisco TrustSec と Cisco ISE の両方に共通の機能) は、パケットがネットワークに入るときに属性を適用します。

### セキュリティ インテリジェンスのカテゴリ (Security Intelligence Category)

接続でブラックリストに記載された IP アドレスを表すか、もしくはそれを含む、ブラックリストに記載されたオブジェクトの名前。セキュリティ インテリジェンスのカテゴリは、ネットワーク オブジェクトまたはグループ、ブラックリスト、カスタムセキュリティ インテリジェンスのリストまたはフィード、またはインテリジェンスフィードのカテゴリのいずれかの名前にすることができます。

インテリジェンス フィードのカテゴリの詳細については、[セキュリティ インテリジェンス オプション \(1380 ページ\)](#) を参照してください。

### TCP フラグ (TCP Flags)

NetFlow データから生成された接続において、接続で検出された TCP フラグ。このフィールドを検索する場合は、TCP フラグのカンマ区切りリストを入力することで、これらのフラグが 1 つ以上あるすべての接続が表示されます。

### 時刻 (Time)

システムが接続を接続サマリーに集約するために使用した 5 分間隔の終了時刻。このフィールドは検索できません。

### トラフィック (KB) (Traffic (KB)) (検索のみ)

接続で送信されたデータの総量 (キロバイト単位)。

### 合計パケット (Total Packets) (検索のみ)

接続で送信された合計パケット数。

### トンネル/プレフィルタ ルール (Tunnel/Prefilter Rule)

トンネルルール、プレフィルタ ルール、または接続を処理したプレフィルタ ポリシーのデフォルトアクション。

## Networking

### 宛先ポート/ICMP コード (Destination Port/ICMP Code) (サマリーおよびグラフを制約)

セッション レスポンダが使用するポートまたは ICMP コード。

**DNS クエリ (DNS Query)**

ドメイン名を検索するために接続でネーム サーバに送信された DNS クエリ。

**DNS レコード タイプ (DNS Record Type)**

接続で送信された DNS クエリを解決するために使用された DNS リソース レコードのタイプ。

**DNS レスポンス (DNS Response)**

問い合わせ時に接続でネーム サーバに返された DNS レスポンス。

**DNS シンクホール名 (DNS Sinkhole Name)**

システムが接続をリダイレクトしたシンクホール サーバの名前。

**DNS TTL**

DNS サーバが DNS リソース レコードをキャッシュする秒数。

**HTTP 応答コード (HTTP Response Code)**

クライアントからの接続経由の HTTP 要求に応じて送信される HTTP ステータス コード。

**入力/出力セキュリティ ゾーン (Ingress/Egress Security Zone)**

接続に関連付けられた入力または出力のセキュリティ ゾーン。

再区分されたカプセル化接続では、元の入力セキュリティゾーンの代わりに、割り当てたトンネルゾーンが入力フィールドに表示されます。出力フィールドは空白です。

**イニシエータ/レスポнда IP (Initiator/Responder IP) (サマリーおよびグラフを制約)**

セッションイニシエータまたはレスポндаの IP アドレス (および DNS 解決が有効化されている場合はホスト名)。ブラックリストに記載された接続でブラックリストに記載された IP アドレスを識別できるように、ブラックリストに記載された IP アドレスの横のアイコンは見た目が少し異なります。

プレフィルタ ポリシーによってブロックされるか、高速パスが適用されたプレーンテキストのパススルートンネルでは、これらの IP アドレスはトンネルエンドポイント (トンネルの両側のネットワーク デバイスのルーテッド インターフェイス) を表します。

**クライアントのオリジナル IP (Original Client IP)**

X-Forwarded-For (XFF)、True-Client-IP、またはカスタム定義の HTTP ヘッダーからの、元のクライアント IP アドレス。このフィールドに入力するには、元のクライアントに基づいてプロキシトラフィックを処理するアクセス コントロールルールを有効にする必要があります。

**プロトコル (Protocol) (サマリーおよびグラフを制約、検索のみ)**

接続に使用されるトランスポートプロトコルです。特定のプロトコルを検索するには、名前を使用するか、<http://www.iana.org/assignments/protocol-numbers> に記載されたプロトコルの番号を指定します。

**送信元ポート/ICMP タイプ (Source Port/ICMP Type) (サマリーおよびグラフを制約)**

セッション イニシエータが使用するポートまたは ICMP タイプ。

**VLAN ID (Admin. VLAN ID)**

接続をトリガーしたパケットに関連付けられている最内部 VLAN ID。

**位置情報 (GeoLocation)****イニシエータ/レスポンド国 (Initiator/Responder Country)**

ルーティング可能な IP が検出された場合の、セッション イニシエータまたはレスポンドの IP アドレスに関連付けられた国。システムにより、国旗のアイコンと、国の ISO 3166-1 alpha-3 国番号が表示されます。国旗アイコンの上にポインタを移動すると、国の完全な名称が表示されます。

**イニシエータ/レスポンド大陸 (Initiator/Responder Continent)**

ルーティング可能な IP が検出された場合の、セッション イニシエータまたはレスポンドの IP アドレスに関連付けられた大陸。

**クライアントのオリジナル国 (Original Client Country)**

元のクライアントの IP アドレスが属する国。この値を取得するために、システムは元のクライアント IP アドレスを X-Forwarded-For (XFF)、True-Client-IP、またはカスタム定義の HTTP ヘッダーから抽出し、それを地理位置情報データベース (GeoDB) を使用して国にマップします。このフィールドに入力するには、元のクライアントに基づいてプロキシトラフィックを処理するアクセス コントロールルールを有効にする必要があります。

**Device****デバイス (Device) (サマリーおよびグラフを制約)**

接続を検出した管理対象デバイス。または、NetFlow データから生成された接続の場合は、データを処理した管理対象デバイス。

**ドメイン (Domain)**

接続を検出した管理対象デバイスのドメイン。または、NetFlow データから生成された接続の場合は、データを処理した管理対象デバイスのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合にのみ表示されます。

**入力/出力インターフェイス (Ingress/Egress Interface)**

接続に関連付けられた入力または出力のインターフェイス。展開に非同期のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインターフェイスセットに属する場合があります。

**SSL****SSL の実際の動作 (SSL Actual Action) (検索のみ)**

システムが SSL ポリシーの暗号化トラフィックに適用したアクション。システムにより、検索ワークフローのページの [SSL ステータス (SSL Status) ] フィールドにフィールド値が表示されます。

アクション	説明
ブロック (Block) / リセットしてブロック (Block With Reset)	ブロックされた暗号化接続を表します。
複合 (再署名) (Decrypt (Resign))	再署名サーバ証明書を使用して復号された発信接続を表します。
復号 (キーの置き換え) (Decrypt (Replace Key))	置き換えられた公開キーと自己署名サーバ証明書を使用して復号された発信接続を表します。
復号 (既知のキー) (Decrypt (Known Key))	既知の秘密キーを使用して復号された着信接続を表します。
デフォルトアクション (Default Action)	接続がデフォルトアクションによって処理されたことを示しています。
復号しない (Do Not Decrypt)	システムが復号しなかった接続を表します。



### SSL 証明書ステータス (SSL Certificate Status)

これは、認証ステータスの SSL ルール条件が設定されている場合にのみ適用されます。暗号化されたトラフィックが SSL ルールに一致すると、このフィールドに次のサーバの証明書のステータス値の 1 つ以上が表示されます。

- 自署 (Self Signed)
- 有効 (Valid)
- 署名が無効 (Invalid Signature)
- 発行元が無効 (Invalid Issuer)
- 期限切れ
- 不明
- まだ有効ではない (Not Valid Yet)
- 失効 (Revoked)

復号できないトラフィックが SSL ルールと一致する場合、このフィールドには [未チェック (Not Checked) ] と表示されます。

### SSL 証明書情報 (SSL Certificate Information) (検索のみ)

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- 件名/発行元共通名 (Subject/Issuer Common Name)
- 件名/発行元組織 (Subject/Issuer Organization)
- 件名/発行元組織ユニット (Subject/Issuer Organization Unit)
- 有効期間の開始/終了 (Not Valid Before/After)
- シリアル番号 (Serial Number)
- 証明書フィンガープリント (Certificate Fingerprint)
- 公開キー フィンガープリント (Public Key Fingerprint)

### SSL 暗号スイート (SSL Cipher Suite)

接続を暗号化するのに使用される暗号スイートを表すマクロ値。暗号スイート値の指定については、[www.iana.org/assignments/tls-parameters/tls-parameters.xhtml](http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml) を参照してください。

### 接続に適用された SSL 暗号化 (SSL Encryption applied to the connection) (検索のみ)

**yes** または **no** を [SSL (SSL) ] 検索フィールドに入力することで、SSL 暗号化された接続または暗号化されていない接続が表示されます。

### SSL 予想アクション (SSL Expected Action) (検索のみ)

有効な SSL ルールで指定された、暗号化トラフィックに適用されると予想されるアクション。[SSL の実際の動作 (SSL Actual Action) ] にリストされている値を入力します。

### SSL 失敗理由 (SSL Failure Reason)

システムが暗号化されたトラフィックの復号に失敗した理由：

- 不明
- 不一致 (No Match)
- Success
- キャッシュされていないセッション (Uncached Session)
- 不明な暗号スイート (Unknown Cipher Suite)
- サポートされていない暗号スイート (Unsupported Cipher Suite)
- サポートされていない SSL バージョン (Unsupported SSL Version)
- SSL 圧縮の使用 (SSL Compression Used)
- パッシブ モードで復号できないセッション (Session Undecryptable in Passive Mode)
- ハンドシェイク エラー (Handshake Error)
- 復号エラー (Decryption Error)
- 保留サーバ名カテゴリ ルックアップ (Pending Server Name Category Lookup)
- 保留共通名カテゴリ ルックアップ (Pending Common Name Category Lookup)
- 内部エラー (Internal Error)
- ネットワーク パラメータを使用できません (Network Parameters Unavailable)
- 無効なサーバ証明書の処理 (Invalid Server Certificate Handle)
- サーバ証明書フィンガープリントを使用できません (Server Certificate Fingerprint Unavailable)
- サブジェクト DN をキャッシュできません (Cannot Cache Subject DN)
- 発行元 DN をキャッシュできません (Cannot Cache Issuer DN)
- 不明の SSL バージョン (Unknown SSL Version)
- 外部証明書リストを使用できません (External Certificate List Unavailable)
- 外部証明書フィンガープリントを使用できません (External Certificate Fingerprint Unavailable)
- 内部証明書リストが無効です (Internal Certificate List Invalid)
- 内部証明書リストを使用できません (Internal Certificate List Unavailable)
- 内部証明書を使用できません (Internal Certificate Unavailable)
- 内部証明書フィンガープリントを使用できません (Internal Certificate Fingerprint Unavailable)

- サーバ証明書検証を使用できません (Server Certificate Fingerprint Unavailable)
- サーバ証明書検証エラー (Server Certificate Validation Failure)
- 無効なアクション (Invalid Action)

フィールド値は、検索ワークフローのページの [SSL ステータス (SSL Status) ] フィールドに表示されます。

#### SSL フロー エラー (SSL Flow Error)

エラーが SSL セッション中に発生した場合はエラー名および 16 進数コード。エラーが発生しない場合は [成功 (Success) ]。

#### SSL フロー フラグ (SSL Flow Flags)

暗号化された接続の最初の 10 個のデバッグ レベルフラグ。ワークフローページでは、すべてのフラグを表示するには、省略記号 (...) をクリックします。

#### SSL フロー メッセージ (SSL Flow Messages)

次のキーワードは、暗号化トラフィックが SSL ハンドシェイク時にクライアントとサーバ間で交換される指定されたメッセージタイプに関連付けられていることを示します。詳細については、<http://tools.ietf.org/html/rfc5246>を参照してください。

- HELLO\_REQUEST
- CLIENT\_ALERT
- SERVER\_ALERT
- CLIENT\_HELLO
- SERVER\_HELLO
- SERVER\_CERTIFICATE
- SERVER\_KEY\_EXCHANGE
- CERTIFICATE\_REQUEST
- SERVER\_HELLO\_DONE
- CLIENT\_CERTIFICATE
- CLIENT\_KEY\_EXCHANGE
- CERTIFICATE\_VERIFY
- CLIENT\_CHANGE\_CIPHER\_SPEC
- CLIENT\_FINISHED
- SERVER\_CHANGE\_CIPHER\_SPEC
- SERVER\_FINISHED
- NEW\_SESSION\_TICKET
- HANDSHAKE\_OTHER

- APP\_DATA\_FROM\_CLIENT
- APP\_DATA\_FROM\_SERVER

### SSL ポリシー (SSL Policy)

接続を処理した SSL ポリシー。

### SSL ルール (SSL Rule)

接続を処理した SSL ルールまたはデフォルトアクションと、その接続に一致した最初のモニタールール。接続が1つのモニタールールに一致した場合、Firepower Management Center は接続を処理したルールの名前を表示し、その後モニタールール名を表示します。

### SSL セッション ID (SSL Session ID)

SSL ハンドシェイク時にクライアントとサーバ間でネゴシエートされた16進数セッションID。

### SSL ステータス (SSL Status)

暗号化された接続を記録した、[SSL の実際の動作 (SSL Actual Action)] (SSL ルール、デフォルトアクション、または復号できないトラフィックアクション) に関連したアクション。ロックアイコン (🔒) は、SSL 証明書の詳細にリンクしています。証明書を利用できない場合 (たとえば、SSL ハンドシェイクエラーにより接続がブロックされる場合)、ロックアイコンはグレー表示になります。

システムが暗号化接続を復号できなかった場合は、[SSL の実際の動作 (SSL Actual Action)] (実行された復号不能のトラフィックアクション) と、[SSL 失敗理由 (SSL Failure Reason)] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [Do Not Decrypt (Unknown Cipher Suite)] が表示されます。

このフィールドを検索する場合は、[SSL の実際の動作 (SSL Actual Action)] と [SSL 失敗理由 (SSL Failure Reason)] の1つ以上の値を入力することで、システムが処理した、または復号に失敗した暗号化トラフィックが表示されます。

### SSL 件名/発行元国 (SSL Subject/Issuer Country) (検索のみ)

暗号化証明書に関連付けられた件名または発行元国の2文字のISO 3166-1 alpha-2 国番号。

### SSL チケット ID (SSL Ticket ID)

SSL ハンドシェイク時に送信されたセッションチケット情報の16進数のハッシュ値。

### SSL バージョン (SSL Version)

接続の暗号化に使用された SSL または TLS プロトコルバージョン。

- 不明
- SSLv2.0
- SSLv3.0
- TLSv1.0

- TLSv1.1
- TSLv1.2

### Application

#### アプリケーション プロトコル (Application Protocol) (サマリーおよびグラフを制約)

接続で検出された、ホスト間の通信を表すアプリケーション プロトコル。

#### アプリケーション プロトコル カテゴリとタグ (Application Protocol Category and Tag)

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

#### アプリケーションのリスク (Application Risk)

接続で検出されたアプリケーショントラフィックに関連付けられたリスク。「非常に高い (Very High)」、「高 (High)」、「中 (Medium)」、「低 (Low)」、「非常に低い (Very Low)」のいずれかとなります。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

#### ビジネスとの関連性 (Business Relevance)

接続で検出されたアプリケーショントラフィックに関連するビジネス関連性: Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネス関連性があります。このフィールドでは、それらのうち最も低いもの (関連が最も低い) が表示されます。

#### クライアントおよびクライアント バージョン (Client and Client Version)

接続で検出されたクライアントのクライアント アプリケーションとバージョン。

接続で使用されている特定のクライアントをシステムが特定できなかった場合、このフィールドは汎用的な名称としてアプリケーションプロトコル名の後に「client」という語を付加して FTP client などと表示します。

#### クライアント カテゴリとタグ (Client Category and Tag)

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

#### HTTP リファラ (HTTP Referrer)

接続で検出された HTTP トラフィックの要求 URL のリファラを示す HTTP リファラ (他の URL へのリンクを提供した Web サイト、他の URL からリンクをインポートした Web サイトなど)。

#### 参照ホスト (Referenced Host)

接続のプロトコルが HTTP または HTTPS の場合、このフィールドにはそれぞれのプロトコルが使用していたホスト名が表示されます。

#### ユーザ エージェント (User Agent)

接続で検出された HTTP トラフィックから取得したユーザ エージェント文字列アプリケーションの情報。

### Web アプリケーション (Web Application)

接続で検出された HTTP トラフィックの内容または要求された URL を表す Web アプリケーション。

Web アプリケーションがイベントの URL に一致しない場合、そのトラフィックは通常、参照先のトラフィックです (アドバタイズメントのトラフィックなど)。システムは、参照先のトラフィックを検出すると、参照元のアプリケーションを保存し (可能な場合)、そのアプリケーションを Web アプリケーションとして表示します。

HTTP トラフィックに含まれる特定の Web アプリケーションをシステムが特定できなかった場合、このフィールドには [Web ブラウジング (Web Browsing)] と表示されます。

### Web アプリケーションのカテゴリとタグ (Web Application Category and Tag)

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

### URL

#### URL、URL カテゴリ、および URL レピュテーション (URL, URL Category, and URL Reputation)

セッション中に監視対象のホストによって要求された URL と、関連付けられたカテゴリおよびレピュテーション (利用できる場合)。

システムが SSL アプリケーションを識別またはブロックする場合、要求された URL は暗号化トラフィック内にあるため、システムは、SSL 証明書に基づいてトラフィックを識別します。したがって SSL アプリケーションの場合、このフィールドは証明書に含まれる一般名を表示します。

### NetFlow

#### NetBIOS ドメイン (NetBIOS Domain)

セッションで使用された NetBIOS ドメイン。

#### NetFlow 送信元/宛先の自律システム (NetFlow Source/Destination Autonomous System)

NetFlow データから生成された接続の場合、接続のトラフィックの送信元または宛先に対する、Border Gateway Protocol の自律システム番号。

#### NetFlow 送信元/宛先のプレフィックス (NetFlow Source/Destination Prefix)

NetFlow データから生成された接続の場合、送信元または宛先の IP アドレスに、送信元と宛先のプレフィックス マスクが追加されたもの。

#### NetFlow 送信元/宛先 TOS (NetFlow Source/Destination TOS)

NetFlow データから生成された接続の場合、接続トラフィックが NetFlow 対応デバイスに入ったか、NetFlow エクスポートから出たときの Type of Service (TOS) バイトの設定。

### NetFlow SNMP 入出力 (NetFlow SNMP Input/Output)

NetFlow データから生成された接続の場合、接続トラフィックが NetFlow 対応デバイスに入ったか、NetFlow エクスポートから出た際のインターフェイスのインターフェイスインデックス。

### ソース デバイス (Source Device) (サマリーおよびグラフを制約)

接続の生成に使用されたデータをブロードキャストする NetFlow エクスポートの IP アドレス。管理対象デバイスによって接続が検出された場合、このフィールドには Firepower と表示されます。

### QoS

#### QoS がドロップされたイニシエータのバイト数 (QoS-Dropped Initiator Bytes) /QoS がドロップされたレスポンドのバイト数 (QoS-Dropped Responder Bytes)

レート制限によりセッションイニシエータまたはセッションレスポンドからドロップされたバイト数。

#### QoS がドロップされたイニシエータのパケット数 (QoS-Dropped Initiator Packets) /QoS がドロップされたレスポンドのパケット数 (QoS-Dropped Responder Packets)

レート制限によりセッションイニシエータまたはセッションレスポンドからドロップされたパケット数。

#### QoS が適用されたインターフェイス (QoS-Applied Interface)

レート制限された接続で、レート制限を適用するインターフェイスの名前。

#### QoS ポリシー (QoS Policy)

接続のレートを制限する QoS ポリシー。


#### QoS ルール (QoS Rule)

接続のレートを制限する QoS ルール。


### 関連イベント (Associated Events)

接続に関連付けられたイベントの検索に、接続やセキュリティインテリジェンスのイベントの検索ページは使用できません。

### ファイル (Files)

接続に関連付けられたファイルイベント (ある場合)。ファイルの表示アイコン  は、ファイルのリストにリンクしています。アイコンの数字は、その接続で検出またはブロックされたファイル数 (マルウェアファイルを含む) を示します。

### 侵入イベント (Intrusion Events)

接続に関連付けられた侵入イベント (ある場合)。侵入イベントの表示アイコン  は、イベントのリストにリンクしています。

## 接続イベントの理由

接続イベントの [理由 (Reason)] フィールドには、次の状況で接続がロギングされた理由が表示されます。

理由 (Reason)	説明
コンテンツ制限 (Content Restriction)	セーフサーチまたは YouTube EDU 機能のいずれかに関連したコンテンツ制限を実施するために、パケットが変更されました。
DNS ブロック (DNS Block)	ドメイン名とセキュリティインテリジェンスデータに基づいて、インスペクションなしで接続が拒否されました。DNS ブロックの理由は、DNS ルールアクションに応じて、[ブロック (Block)]、[ドメインが見つかりません (Domain not found)]、[シンクホール (Sinkhole)] のアクションと対として組み合わせられます。
DNS モニタ (DNS Monitor)	システムはドメイン名とセキュリティインテリジェンスデータに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニタするように設定されています。
ファイルブロック (File Block)	ファイルまたはマルウェアファイルが接続に含まれており、システムがその送信を防いでいます。[ファイルブロック (File Block)] の理由は必ず [ブロック (Block)] のアクションと対として組み合わせられます。
ファイルカスタム検出 (File Custom Detection)	カスタム検出リストにあるファイルが接続に含まれており、システムがその送信を防いでいます。
ファイルモニタ (File Monitor)	システムが接続において特定のファイルの種類を検出しました。
ファイル復帰許可 (File Resume Allow)	ファイル送信がはじめに [ファイルブロック (Block Files)] ルールまたは [マルウェアブロック (Block Malware)] ファイルルールによってブロックされました。ファイルを許可する新しいアクセスコントロールポリシーが展開された後、HTTP セッションが自動的に再開しました。この理由はインライン展開のみで表示されます。
ファイル復帰ブロック (File Resume Block)	ファイル送信がはじめに [ファイル検出 (Detect Files)] ルールまたは [マルウェアクラウドルックアップ (Malware Cloud Lookup)] ファイルルールによって許可されました。ファイルをブロックする新しいアクセスコントロールポリシーが展開された後、HTTP セッションが自動的に停止しました。この理由はインライン展開のみで表示されます。
インテリジェントアプリケーションバイパス (Intelligent App Bypass)	インテリジェントアプリケーションバイパス (IAB) モード： <ul style="list-style-type: none"> <li>アクションが [信頼 (Trust)] の場合、IAB はバイパスモードでした。一致するトラフィックは、追加のインスペクションなしで通過しました。</li> <li>アクションが [許可 (Allow)] の場合、IAB はテストモードでした。一致するトラフィックは、追加のインスペクションに使用できました。</li> </ul>



理由 (Reason)	説明
侵入ブロック (Intrusion Block)	接続で検出されたエクスプロイト (侵入ポリシー違反) をシステムがブロックしたか、ブロックするはずでした。[侵入ブロック (Intrusion Block)] の原因は、ブロックされたエクスプロイトの場合は[ブロック (Block)]、ブロックされるはずだったエクスプロイトの場合は[許可 (Allow)] のアクションと対として組み合わせられます。
侵入モニタ (Intrusion Monitor)	接続で検出されたエクスプロイトをシステムが検出したものの、ブロックしなかったことを示します。これは、トリガーされた侵入ルールの状態が[イベントを生成する (Generate Events)] に設定されている場合に発生します。
IP ブロック (IP Block)	IP アドレスとセキュリティインテリジェンスデータに基づいて、インスペクションなしで接続が拒否されました。[IP ブロック (IP Block)] の原因は必ず[ブロック (Block)] のアクションと対として組み合わせられます。
IP モニタ (IP Monitor)	システムは IP アドレスとセキュリティインテリジェンスデータに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニタするように設定されています。
SSL ブロック (SSL Block)	システムが SSL インスペクション設定に基づいて暗号化接続をブロックしました。[SSL ブロック (SSL Block)] の理由は必ず[ブロック (Block)] のアクションと対として組み合わせられます。
URL ブロック (URL Block)	URL とセキュリティインテリジェンスデータに基づいて、インスペクションなしで接続が拒否されました。[URL ブロック (URL Block)] の原因は必ず[ブロック (Block)] のアクションと対として組み合わせられます。
URL モニタ (URL Monitor)	システムは URL とセキュリティインテリジェンスデータに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニタするように設定されています。
ユーザ バイパス (User Bypass)	最初にユーザの HTTP 要求をブロックしましたが、ユーザのクリックによって警告ページからサイトを表示しました。[ユーザバイパス (User Bypass)] の理由は必ず[許可 (Allow)] のアクションと対として組み合わせられます。

## 接続イベント フィールドの入力の要件

接続イベント、セキュリティインテリジェンスイベント、接続サマリーで利用可能な情報は、いくつかの要因によって異なります。

### アプライアンス モデルおよびライセンス

多くの機能は、ターゲットデバイスで特定のライセンス付与対象の機能を有効にしなければ使用できません。また、一部のモデルでしか使用できない機能も多くあります。

たとえば、NGIPSv デバイスは SSL インспекションをサポートしません。これらのデバイスは暗号化されたトラフィックを検査できないため、記録される接続イベントには暗号化された接続に関する情報は含まれていません。

### トラフィックの特性

システムは、ネットワークトラフィック内に存在する（および検出可能な）情報だけを報告します。たとえば、イニシエータホストに関連付けられているユーザがない、またはプロトコルが DNS、HTTP、または HTTPS ではない接続で検出される参照先ホストがない可能性があります。

### 発信元/検出方法：トラフィック ベースの検出と NetFlow

NetFlow 専用フィールドを除き、NetFlow レコードで利用可能な情報は、トラフィック ベースの検出によって生成される情報よりも限定されます。[NetFlow データと管理対象デバイスデータの違い（2028 ページ）](#)を参照してください。

### 評価ステージ

各タイプのトラフィックのインспекションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。

たとえば、システムは、さらなるリソース集中型評価を行う前に、セキュリティインテリジェンスを強制します。接続がセキュリティインテリジェンスによってブロックされた場合、結果として生成されるイベントには、その後の評価によってシステムで収集されることになっていた情報（ユーザ ID など）が含まれません。

### ロギング方法：接続の開始または終了

システムが接続の検出時にその接続の開始または終了（またはその両方）をログに記録できるかどうかは、システムがその接続をどのように検出して処理するように設定されているかによって異なります。

接続開始イベントには、セッション期間にわたってトラフィックを調査して判別しなければならない情報が伴ってません（送信されたデータの合計量や、接続の最終パケットのタイムスタンプなど）。また、接続開始イベントにセッションのアプリケーションや URL トラフィックに関する情報が伴っている保証もなく、セッションの暗号化に関する詳細は含まれていません。通常、ブロックされる接続については、接続開始イベントのログへの記録が唯一のオプションになります。

### 接続イベントタイプ：個々またはサマリー

接続サマリーには、集約された接続に関連付けられたすべての情報が含まれているわけではありません。たとえば、接続の概要に集約される接続にはクライアント情報が使用されないため、概要にはクライアント情報は含まれません。

接続グラフは、接続終了ログのみを使用する接続サマリーのデータに基づいていることに注意してください。接続開始データだけをロギングするようにシステムが設定されている場合、接続グラフと接続サマリーのイベント ビューにはデータが表示されません。

## その他の設定

接続のロギングに影響するその他の設定には以下のものが含まれますが、これらに限定されるわけではありません。

- Active Directory ドメインコントローラで認証するユーザに関連付けられている接続では、ISE が設定されている場合にのみ、ISE 関連のフィールドにデータが入力されます。接続イベントには、LDAP、RADIUS、RSA ドメインコントローラで認証するユーザの ISE データは含まれません。
- [セキュリティ グループ タグ (Security Group Tag) ] フィールドにデータが入力されるのは、ISE をアイデンティティ ソースとして設定した場合、またはカスタム SGT ルール条件を追加した場合のみです。
- プレフィルタ関連のフィールド (セキュリティ ゾーン フィールドのトンネル ゾーン情報を含む) には、プレフィルタ ポリシーで処理される接続の場合にのみ、データが入力されます。
- SSL 関連のフィールドには、SSL ポリシーで処理される暗号化接続の場合にのみ、データが入力されます。
- ファイル情報フィールドには、ファイル ポリシーと関連付けられたアクセス コントロールルールによってログに記録される接続の場合にのみ、データが入力されます。
- 侵入情報フィールドには、侵入ポリシーに関連付けられているアクセスコントロールルールあるいはデフォルトアクションによってログに記録される接続の場合にのみ、データが入力されます。
- QoS 関連のフィールドには、レート制限が適用される接続の場合にのみ、データが入力されます。
- [理由 (Reason) ] フィールドには、特定の場合にのみデータが入力されます (ユーザがインタラクティブ ブロック設定をバイパスしている場合など)。
- [ドメイン (Domain) ] フィールドが表示されるのは、マルチテナンシー用に Firepower Management Center を設定した場合のみです。
- アクセスコントロールポリシーの詳細設定では、HTTP セッションのモニタ対象ホストによって要求された URL ごとにシステムが接続ログに保存する文字数を制御できます。この設定を使用して URL のロギングを無効化する場合、システムは接続ログで個々の URL を表示しませんが、カテゴリとレピュテーションデータは参照できます (存在する場合)。

## 関連トピック

[NetFlow データと管理対象デバイス データの違い](#) (2028 ページ)

# 接続イベント フィールドで利用可能な情報

このトピックの表に、システムが接続およびセキュリティインテリジェンスのフィールドに値を読み込むことができるタイミングを示します。表の列は、次のイベントタイプを示しています。

- [発信元：直接 (Origin: Direct) ] : Firepower システムの管理対象デバイスで検出および処理される接続を表すイベント。
- [発信元：NetFlow (Origin: NetFlow) ] : NetFlow エクスポートでエクスポートされる接続を表すイベント。
- [ロギング：開始 (Logging: Start) ] : 開始時にログに記録される接続を表すイベント。
- [ロギング：終了 (Logging: End) ] : 終了時にログに記録される接続を表すイベント。

表内の「はい (yes) 」は、システムが接続イベント フィールドに値を読み込む必要があることを意味するのではなく、読み込むことができることを意味します。システムは、ネットワーク トラフィック内に存在する (および検出可能な) 情報だけを報告します。たとえば、SSL 関連のフィールドには、SSL ポリシーによって処理される暗号化された接続の記録についてのみ値が読み込まれます。

接続イベント フィールド	[発信元：直接 (Origin: Direct) ]	[発信元：NetFlow (Origin: NetFlow) ]	[ロギング：開始 (Logging: Start) ]	[ロギング：終了 (Logging: End) ]
アクセス コントロール ポリシー (Access Control Policy)	Yes	No	Yes	Yes
アクセス コントロール ルール (Access Control Rule)	Yes	No	Yes	Yes
操作	Yes	No	Yes	Yes
アプリケーション プロトコル	Yes	Yes	利用可能な場合	Yes
アプリケーション プロトコル カテゴリとタグ (Application Protocol Category & Tag)	Yes	No	利用可能な場合	Yes
アプリケーションのリスク (Application Risk)	Yes	No	利用可能な場合	Yes
ビジネスとの関連性 (Business Relevance)	Yes	No	利用可能な場合	Yes
クライアント	Yes	No	利用可能な場合	Yes
クライアント カテゴリとタグ (Client Category & Tag)	Yes	No	利用可能な場合	Yes
クライアント バージョン (Client Version)	Yes	No	利用可能な場合	Yes

接続イベント フィールド	[発信元：直接 (Origin: Direct) ]	[発信元：NetFlow (Origin: NetFlow) ]	[ロギング：開 始 (Logging: Start) ]	[ロギング：終 了 (Logging: End) ]
接続 (Connections)	Yes	Yes	No	Yes
メンバー数 (Count)	Yes	Yes	Yes	Yes
宛先ポート/ICMP タイプ (Destination Port/ICMP Type)	Yes	Yes	Yes	Yes
Device	Yes	Yes	Yes	Yes
ドメイン (Domain)	Yes	Yes	Yes	Yes
DNS クエリ (DNS Query)	Yes	No	Yes	Yes
DNS レコード タイプ (DNS Record Type)	Yes	No	Yes	Yes
DNS レスポンス (DNS Response)	Yes	No	Yes	Yes
DNS シンクホール名 (DNS Sinkhole Name)	Yes	No	Yes	Yes
DNS TTL	Yes	No	Yes	Yes
出力インターフェイス (Egress Interface)	Yes	No	Yes	Yes
出力セキュリティゾーン (Egress Security Zone)	Yes	No	Yes	Yes
エンドポイント ロケーション (Endpoint Location)	Yes	No	Yes	Yes
エンドポイント プロファイル (Endpoint Profile)	Yes	No	Yes	Yes
ファイル	Yes	No	No	Yes
最初のパケット (First Packet)	Yes	Yes	Yes	Yes
HTTP リファラ (HTTP Referrer)	Yes	No	No	Yes
HTTP 応答コード (HTTP Response Code)	Yes	No	Yes	Yes

接続イベント フィールド	[発信元：直接 (Origin: Direct) ]	[発信元： NetFlow (Origin: NetFlow) ]	[ロギング：開 始 (Logging: Start) ]	[ロギング：終 了 (Logging: End) ]
入力インターフェイス (Ingress Interface)	Yes	No	Yes	Yes
入力セキュリティゾーン (Ingress Security Zone)	Yes	No	Yes	Yes
イニシエータ バイト数 (Initiator Bytes)	Yes	Yes	有用でない	Yes
イニシエータの国 (Initiator Country)	Yes	No	Yes	Yes
イニシエータ IP (Initiator IP)	Yes	Yes	Yes	Yes
イニシエータ パケット (Initiator Packets)	Yes	Yes	有用でない	Yes
イニシエータ ユーザ (Initiator User)	Yes	Yes	Yes	Yes
侵入イベント	Yes	No	No	Yes
侵入ポリシー (Intrusion Policy)	Yes	No	Yes	Yes
IOC (侵害の兆候) (IOC (Indication of Compromise))	Yes	No	Yes	Yes
最後のパケット (Last Packet)	Yes	Yes	No	Yes
NetBIOS ドメイン (NetBIOS Domain)	Yes	No	Yes	Yes
NetFlow 送信元/宛先の自律システム (NetFlow Source/Destination Autonomous System)	No	Yes	No	Yes
NetFlow 送信元/宛先のプレフィックス (NetFlow Source/Destination Prefix)	No	Yes	No	Yes
NetFlow 送信元/宛先 TOS (NetFlow Source/Destination TOS)	No	Yes	No	Yes

接続イベント フィールド	[発信元 : 直接 (Origin: Direct) ]	[発信元 : NetFlow (Origin: NetFlow) ]	[ロギング : 開 始 (Logging: Start) ]	[ロギング : 終 了 (Logging: End) ]
NetFlow SNMP 入出力 (NetFlow SNMP Input/Output)	No	Yes	No	Yes
ネットワーク分析ポリシー (Network Analysis Policy)	Yes	No	Yes	Yes
クライアントのオリジナル国 (Original Client Country)	Yes	No	Yes	Yes
クライアントのオリジナル IP (Original Client IP)	Yes	No	Yes	Yes
プレフィルタ ポリシー (Prefilter Policy)	Yes	No	Yes	Yes
QoS が適用されたインター フェイス (QoS-Applied Interface)	Yes	No	No	Yes
QoS がドロップされたイニシ エータのバイト数 (QoS-Dropped Initiator Bytes)	Yes	No	No	Yes
QoS がドロップされたイニシ エータのパケット数 (QoS-Dropped Initiator Packets)	Yes	No	No	Yes
QoS がドロップされたレスポ ンダのバイト数 (QoS-Dropped Responder Bytes)	Yes	No	No	Yes
QoS がドロップされたレスポ ンダのパケット数 (QoS-Dropped Responder Packets)	Yes	No	No	Yes
QoS ポリシー	Yes	No	No	Yes
QoS ルール (QoS Rule)	Yes	No	No	Yes
理由 (Reason)	Yes	No	Yes	Yes
参照ホスト (Referenced Host)	Yes	No	No	Yes

接続イベント フィールド	[発信元：直接 (Origin: Direct) ]	[発信元： NetFlow (Origin: NetFlow) ]	[ロギング：開 始 (Logging: Start) ]	[ロギング：終 了 (Logging: End) ]
レスポнда バイト数 (Responder Bytes)	Yes	Yes	有用でない	Yes
レスポндаの国 (Responder Country)	Yes	No	Yes	Yes
レスポнда IP (Responder IP)	Yes	Yes	Yes	Yes
レスポнда パケット (Responder Packets)	Yes	Yes	有用でない	Yes
セキュリティ コンテキスト (ASA のみ) (Security Context (ASA only))	Yes	No	Yes	Yes
セキュリティ グループ タグ (SGT) (Security Group Tag (SGT))	Yes	No	Yes	Yes
セキュリティ インテリジェン スのカテゴリ (Security Intelligence Category)	Yes	No	Yes	Yes
送信元デバイス (Source Device)	Yes	Yes	Yes	Yes
送信元ポート/ICMP タイプ (Source Port/ICMP Type)	Yes	Yes	Yes	Yes
SSL 証明書ステータス (SSL Certificate Status)	Yes	No	No	Yes
SSL 暗号スイート (SSL Cipher Suite)	Yes	No	No	Yes
SSL フロー エラー (SSL Flow Error)	Yes	No	No	Yes
SSL フロー フラグ (SSL Flow Flags)	Yes	No	No	Yes
SSL フロー メッセージ (SSL Flow Messages)	Yes	No	No	Yes



接続イベント フィールド	[発信元 : 直接 (Origin: Direct) ]	[発信元 : NetFlow (Origin: NetFlow) ]	[ロギング : 開 始 (Logging: Start) ]	[ロギング : 終 了 (Logging: End) ]
SSL ポリシー (SSL Policy)	Yes	No	No	Yes
SSL ルール (SSL Rule)	Yes	No	No	Yes
SSL セッション ID (SSL Session ID)	Yes	No	No	Yes
SSL ステータス (SSL Status)	Yes	No	No	Yes
SSL バージョン (SSL Version)	Yes	No	No	Yes
TCP フラグ (TCP Flags)	No	Yes	No	Yes
時刻 (Time)	Yes	Yes	No	Yes
トンネル/プレフィルタールール (Tunnel/Prefilter Rule)	Yes	No	Yes	Yes
URL	Yes	No	利用可能な場合	Yes
URL Category	Yes	No	利用可能な場合	Yes
URLレピュテーション (URL Reputation)	Yes	No	利用可能な場合	Yes
ユーザ エージェント (User Agent)	Yes	No	No	Yes
VLAN ID (Admin. VLAN ID)	Yes	No	Yes	Yes
Web アプリケーション (Web Application)	Yes	No	利用可能な場合	Yes
Web アプリケーションのカテゴリとタグ (Web Application Category & Tag)	Yes	No	利用可能な場合	Yes

## 接続およびセキュリティインテリジェンス イベント テーブルの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

Firepower Management Center を使用して、接続イベントまたはセキュリティインテリジェンス イベントのテーブルを表示することができます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

接続グラフにアクセスしたときに表示されるページは、使用するワークフローによって異なります。イベントのテーブル ビューで終わる事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

接続またはセキュリティインテリジェンス ワークフロー テーブルを使用すると、たくさんの一般的なアクションを実行できます。

ドリルダウンページで接続イベントを制約する場合、同一のイベントからのパケット数とバイト数が合計されることに注意してください。ただし、カスタムワークフローを使用しており、ドリルダウン ページに [カウント (Count) ] カラムを追加していない場合、イベントは個別に表示され、パケット数とバイト数は合計されません。

システムが生成した接続イベントが 25 個を超えると、[接続イベント (Connection Events) ] テーブルビューに、使用可能なイベントのページ数ではなく、「1 of Many」と表示されます。

### 手順

**ステップ 1** 次のいずれかを選択します。

- [分析 (Analysis) ] > [接続 (Connections) ] > [イベント (Events) ] (接続イベントの場合)
- [分析 (Analysis) ] > [接続 (Connections) ] > [セキュリティインテリジェンス イベント (Security Intelligence Events) ]






(注) テーブルの代わりに接続グラフが表示された場合、ワークフロータイトルで[(ワークフローの切り替え) ((switch workflow)) ]をクリックし、事前定義された [接続イベント (Connection Events) ] ワークフローまたはカスタムワークフローを選択します。事前定義されたすべての接続イベント (接続グラフを含む) は、接続のテーブルビューで終了することに注意してください。

**ステップ 2** 次の選択肢があります。


- 時間範囲：時間範囲を調整（イベントが表示されない場合に役立ちます）する方法については、[時間枠の変更（2455 ページ）](#)を参照してください。

- フィールド名：テーブルのカラムの内容について詳しく調べるには、[接続およびセキュリティインテリジェンス イベント フィールド（2523 ページ）](#)を参照してください。

**ヒント** イベントのテーブル ビューでは、各アプリケーション タイプの [カテゴリ (Category)] および [タグ (Tag)] フィールド、NetFlow 関連のフィールド、SSL 関連のフィールドなど、いくつかのフィールドがデフォルトで非表示です。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム (Disabled Columns)] の下のフィールド名をクリックします。

- ホスト プロファイル：IP アドレスのホスト プロファイルを表示するには、ホスト プロファイルのアイコン () をクリックします。アクティブな侵害の兆候 (IOC) タグのあるホストの場合は、IP アドレスの横に表示される侵害されたホストのアイコン () をクリックします。
- ユーザ プロファイル：ユーザ ID 情報を表示するには、ユーザ ID の横に表示されるユーザアイコン () をクリックします。
- ファイルおよびマルウェア：接続で検出されたまたはブロックされたマルウェアを含むファイルを表示するには、ファイルの表示アイコン () をクリックし、[接続で検出されたファイルとマルウェアの表示（2550 ページ）](#)の説明に従って続行します。
- 侵入イベント：接続に関連付けられている侵入イベントを優先順位や影響とともに表示するには、[侵入イベント (Intrusion Events)] カラムの侵入イベントアイコン () をクリックして、[接続に関連付けられた侵入イベントの表示（2552 ページ）](#)の説明に従って続行します。

**ヒント** 1つまたは複数の接続に関連付けられた侵入、ファイル、マルウェア イベントをすばやく表示するには、イベント ビューアのチェック ボックスを使用して接続を選択し、[ジャンプ (Jump to)] ドロップダウン リストから該当するオプションを選択します。セキュリティインテリジェンスによりブラックリストに載せられている接続に関連するファイルまたは侵入が、アクセス コントロール ルールの評価の前にブロックされることによって、1つも存在しない可能性があることに注意してください。ブラックリストではなく、接続をモニタするようにセキュリティインテリジェンスを設定した場合に限り、セキュリティインテリジェンス イベントに関するこの情報が表示されます。

- 証明書：接続を暗号化するために使用される利用可能な証明書についての詳細を表示するには、[SSL ステータス (SSL Status)] カラムの有効なロックアイコン () をクリックします。

- 制約：表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン（✕）をクリックします。表示されるポップアップウィンドウで、[適用（Apply）] をクリックします。

**ヒント** 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェックボックスをオンまたはオフにします。無効になったカラムをビューに再び追加するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- イベントの削除：現在の制約されたビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。
- ドリルダウン：[ドリルダウン ページの使用（2439 ページ）](#) を参照してください。

**ヒント** ログイングされた接続に一致した複数のモニター ルールのうち 1 つにドリルダウンするには、[N モニター ルール（N Monitor Rules）] の値をクリックします。表示されるポップアップウィンドウで、接続イベントを抑制するために使用するモニター ルールをクリックします。

- このページに移動する：[ワークフロー ページのトラバーサル ツール（2436 ページ）](#) を参照してください。
- ページ間で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページリンクをクリックします。
- イベントビュー間で移動する：関連するイベントを表示するためその他のイベントビューに移動するには、[ジャンプ（Jump to）] をクリックし、ドロップダウン リストからイベント ビューを選択します。
- ソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。


#### 関連トピック

[概要：ワークフロー（2417 ページ）](#)

[イベント ビュー設定の設定（37 ページ）](#)

## 接続で検出されたファイルとマルウェアの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威またはマルウェア	保護またはマルウェア	任意 (Any)	任意 (Any)	Admin/Any Security Analyst


1つまたは複数のアクセスコントロールルールにファイルポリシーを関連付けると、システムは一致するトラフィックのファイル（マルウェアを含む）を検出できます。これらのルールによってログされた接続に関連付けられたファイルイベントがある場合は、イベントビューアを使用して確認できます。ファイルリストの代わりに、Firepower Management Centerはファイル表示アイコン（）を [ファイル (Files) ] カラムに表示します。アイコンの数字は、その接続で検出またはブロックされたファイル数（マルウェアファイルを含む）を示します。

すべてのファイルおよびマルウェアイベントが接続に関連付けられるわけではありません。具体的には次のとおりです。




- エンドポイントベースのマルウェアイベントは、接続に関連付けられていません。これらのイベントは AMP for Endpoints 展開からインポートされます。
- IMAP に対応した電子メールクライアントの多くは単一 IMAP セッションを使用し、それはユーザがアプリケーションを終了したときに終了します。長時間接続はシステムによってログされますが、セッションでダウンロードされたファイルは、そのセッションが終了するまで接続に関連付けられません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

## 手順

**ステップ 1** 接続イベントテーブルを使用している場合、ファイル表示アイコン（）をクリックします。ポップアップウィンドウが表示され、接続で検出されたファイルのリストとともに、そのタイプと、該当する場合はマルウェア処理が示されます。

**ステップ 2** 次の選択肢があります。

- 表示：ファイルイベントのテーブルビューを表示するには、ファイルの表示アイコン（）をクリックします。
- 表示：マルウェア イベントのテーブルビューに詳細を表示するには、マルウェア ファイルの表示アイコン（）をクリックします。
- 追跡：ネットワークを経由するファイルの伝送を追跡するには、ファイルのトラジェクトリアイコン（）をクリックします。
- 表示：接続で検出されたファイルまたはネットワーク ベースのマルウェア イベントすべての詳細を表示するには、[ファイルイベントの表示 (View File Events) ] または [マルウェア イベントの表示 (View Malware Events) ] をクリックします。

## 接続に関連付けられた侵入イベントの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

アクセス コントロールルールまたはデフォルト アクションに侵入ポリシーを関連付けると、システムは一致するトラフィックのエクスプロイトを検出できます。イベントビューアを使用して、ロギングされた接続に関連付けられた侵入イベント（ある場合）と、その優先順位や影響について確認できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

**ステップ 1** 接続イベントテーブルを使用する場合、[侵入イベント (Intrusion Events)] カラムの侵入イベントアイコン (🔍) をクリックします。

**ステップ 2** 表示されるポップアップ ウィンドウで、以下のオプションを選択できます。

- パケット ビューで詳細を表示するには、リストされたイベントの表示アイコン (🔍) をクリックします。
- [侵入イベントの表示 (View Intrusion Events)] をクリックして、接続に関連付けられた侵入イベントすべての詳細を表示します。

## 暗号化接続の証明書の詳細

イベントビューアを使用して、システムで処理される接続を暗号化するために使用される公開キー証明書（使用可能な場合）を表示できます。証明書には次の情報が含まれています。

表 291: 暗号化接続の証明書の詳細

属性 (Attribute)	説明
サブジェクト/発行元共通名 (Subject/Issuer Common Name)	証明書のサブジェクトまたは証明書発行元のホストおよびドメイン名。
サブジェクト/発行元組織 (Subject/Issuer Organization)	証明書のサブジェクトまたは証明書発行元の組織。
サブジェクト/発行元組織単位 (Subject/Issuer Organization Unit)	証明書のサブジェクトまたは証明書発行元の組織単位。

属性 (Attribute)	説明
有効期間 (Not Valid Before/After)	証明書の有効期間。
シリアル番号 (Serial Number)	発行元 CA によって割り当てられたシリアル番号。
証明書フィンガープリント (Certificate Fingerprint)	証明書の認証に使用する SHA ハッシュ値。
公開キー フィンガープリント (Public Key Fingerprint)	証明書に含まれる公開キーの認証に使用する SHA ハッシュ値。

## デバイス サマリー ページの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	カスタム (Custom)

[接続サマリー (Connection Summary) ] ページは、接続イベントの検索によって制限されたカスタム ロールを持ち、[接続サマリー (Connection Summary) ] ページへのメニューベースの明示的なアクセスを許可されたユーザにのみ表示されます。このページは、監視対象ネットワーク上のアクティビティをさまざまな条件で整理したグラフを表示します。たとえば [一定期間の接続数 (Connections over Time) ] グラフでは、選択した間隔における監視対象ネットワーク上の接続の合計数が表示されます。

接続グラフでできる操作と同じことが、接続サマリーのグラフでも、ほぼすべてできます。ただし、[接続サマリー (Connection Summary) ] ページのグラフは集約データに基づいているため、グラフの基になっている個々の接続イベントを調べることはできません。つまり、接続サマリーのグラフから接続データのテーブル ビューにドリルダウンすることはできません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

- ステップ 1 [概要 (Overview) ] > [概要 (Summary) ] > [接続の概要 (Connection Summary) ] を選択します。
- ステップ 2 [デバイスの選択 (Select Device) ] リストから、サマリーを表示したいデバイスを選択するか、もしくはすべてのデバイスのサマリーを表示するために [すべて (All) ] を選択します。
- ステップ 3 グラフ接続の操作および分析を行うには、[接続イベント グラフの使用方法 \(2443 ページ\)](#) の説明に従って続行します。

ヒント デフォルトの時間範囲に影響を与えずにさらに分析を行えるように接続グラフ分離するには、[表示 (View)] をクリックします。

---

#### 関連トピック

[ユーザ ロールのエスカレーション \(82 ページ\)](#)





## 第 107 章

# 侵入イベントの操作

以下のトピックでは、侵入イベントを操作する方法について説明します。

- [侵入イベントについて \(2555 ページ\)](#)
- [侵入イベントの表示 \(2556 ページ\)](#)
- [侵入イベントのワークフロー ページ \(2576 ページ\)](#)
- [侵入イベントのクリップボード \(2599 ページ\)](#)
- [侵入イベントの統計情報の表示 \(2601 ページ\)](#)
- [侵入イベントのパフォーマンス グラフの表示 \(2604 ページ\)](#)
- [侵入イベント グラフの表示 \(2610 ページ\)](#)

## 侵入イベントについて

Firepower システムは、ホストとそのデータの可用性、整合性、および機密性に影響する可能性のあるトラフィックがないかどうか、ネットワークをモニタするのに役立ちます。主要なネットワークセグメントに管理対象デバイスを配置すると、悪意のあるアクティビティを目的としてネットワークを通過するパケットを検査できます。このシステムには、攻撃者が開発したさまざまな 익스プロイトを検索するのに使用できるいくつかのメカニズムがあります。

システムは、潜在的な侵入を特定すると侵入イベントを生成します。これは、 익스プロイトの日付、時間、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報のデータです。パケットベースのイベントの場合、イベントをトリガーとして使用したパケットのコピーも記録されます。管理対象デバイスは、Firepower Management Center にイベントを送信します。ここで、集約データを確認し、ネットワーク アセットに対する攻撃を的確に把握できます。

管理対象デバイスをインライン、スイッチド、またはルーテッドの侵入システムとして展開することもできます。これにより、危険だと認識したパケットをドロップまたは置換するようデバイスを設定できます。

Firepower システムは、ユーザが侵入イベントを確認し、ネットワーク環境とセキュリティポリシーのコンテキストでそのイベントが重要であるかどうかを評価するために必要なツールも提供します。これらのツールは次のとおりです。

- [管理対象デバイスでの現在のアクティビティの概要について説明するイベント要約ページ](#)

- 選択した任意の期間に生成できるテキストベースおよびグラフィカルなレポート。独自のレポートを設計し、スケジュールされた間隔で実行されるよう設定することもできます
- 攻撃に関連したイベントデータの収集に使用できるインシデント処理ツール。調査や応答のトラッキングに役立つ注記を追加することもできます
- SNMP、電子メール、および syslog で設定できる自動アラート
- 特定の侵入イベントに対する応答や修復に使用できる自動化された関連ポリシー
- データをドリルダウンして、さらに調査したいイベントを特定するのに使用できる定義済みカスタム ワークフロー

## 侵入イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入イベントは、ネットワークセキュリティに対する脅威があるかどうかを判断するために表示します。

初期の侵入イベントビューは、ページにアクセスするために使用するワークフローによって異なります。1つ以上のドリルダウンページ、侵入イベントのテーブルビュー、および終了パケットビューを含む、定義済みワークフローの1つを使用するか、独自のワークフローを作成できます。カスタムテーブルに基づいてワークフローを表示することもできます。これには、侵入イベントを含めることができます。

大量のIPアドレスが含まれている状態で、[IPアドレスの解決 (Resolve IP Addresses)] イベントビュー設定が有効になっていると、イベントビューの表示が遅くなる場合があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

**ステップ 1** [分析 (Analysis)] > [侵入 (Intrusions)] > [イベント (Events)] を選択します。

**ステップ 2** 次の選択肢があります。

- 時間範囲の調整： [時間枠の変更 \(2455ページ\)](#) の説明に従って、イベントビューの時間範囲を調整します。
- ワークフローの変更：侵入イベントのテーブルビューが含まれないカスタムワークフローを使用している場合、ワークフローのタイトルの横にある [(ワークフローの切り替え) (switch workflow)] をクリックして、システム提供のワークフローのいずれかを選択します。

- 制約：表示する対象を分析において重要な侵入イベントに狭めるには、[侵入イベントワークフローの使用 \(2577 ページ\)](#) を参照してください。
- イベントの削除：データベースからイベントを削除するには、[削除 (Delete) ] をクリックして表示しているパケットのイベントを削除するか、[すべて削除 (Delete All) ] をクリックして以前に選択したパケットのすべてのイベントを削除します。
- 確認済みのマークを付ける：侵入イベントに確認済みのマークを付けるには、[侵入イベントを確認済みとしてマーク \(2570 ページ\)](#) を参照してください。
- 接続データの表示：侵入イベントに関連付けられた接続データを表示するには、[侵入イベントと関連付けられた接続データの表示 \(2570 ページ\)](#) を参照してください。
- 内容の表示：[侵入イベントフィールド \(2557 ページ\)](#) の説明に従ってテーブルのカラムの内容を表示します。

---

### 関連トピック

[侵入イベント パケット ビューの使用 \(2581 ページ\)](#)

## 侵入イベント フィールド

システムは、潜在的な侵入を特定すると侵入イベントを生成します。これは、エクスプロイトの日付、時間、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報のデータです。パケットベースのイベントの場合、イベントをトリガーとして使用したパケットのコピーも記録されます。

侵入イベントを検索するときは、個別のイベントで利用可能な情報は、システムがいつ、なぜ、どのようにしてイベントを記録したかによって異なることに注意してください。たとえば、復号化されたトラフィックでトリガーされた侵入イベントだけが SSL 情報を含んでいません。



- (注) デフォルトでは、侵入イベントのテーブル ビューにいくつかのフィールドが表示されます。セッション中にフィールドを有効にするには、検索制約を拡張してから、[無効の列 (Disabled Columns) ] の下の列名をクリックします。

---

### アクセス コントロール ポリシー (Access Control Policy)

イベントを生成した侵入ルール、プリプロセッサルール、またはデコーダルールが有効になっている侵入ポリシーに関連付けられているアクセス コントロール ポリシー。

### アクセス コントロール ルール (Access Control Rule)

イベントを生成した侵入ルールを呼び出したアクセス コントロール ルール。[デフォルトアクション (Default Action) ] は、ルールが有効化されている侵入ポリシーが特定のアクセス コントロール ルールに関連付けられておらず、代わりに、アクセス コントロール ポリシーのデフォルト アクションとして設定されていることを示しています。

侵入インスペクションがアクセス コントロール ルールにもデフォルト アクションにも関連付けられていない場合、このフィールドは空欄になります。たとえば、パケットがデフォルトの侵入ポリシーによって検査された場合などです。

### アプリケーション プロトコル (Application Protocol)

(使用可能な場合) 侵入イベントをトリガーとして使用したトラフィックで検出されたホスト間の通信を表す、アプリケーション プロトコル。

### アプリケーション プロトコル カテゴリおよびタグ (Application Protocol Category and Tag)

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

### アプリケーションのリスク (Application Risk)

侵入イベントをトリガーしたトラフィックで検出されたアプリケーションに関連付けられているリスク。[非常に高い (Very High) ]、[高 (High) ]、[中 (Medium) ]、[低 (Low) ]、および [非常に低い (Very Low) ]。接続で検出されるアプリケーションのタイプごとに関連するリスクがあります。このフィールドは、それらのうち最も高いリスクを表示します。

### ビジネスとの関連性 (Business Relevance)

侵入イベントをトリガーしたトラフィックで検出されたアプリケーションに関連付けられているビジネスとの関連性。[非常に高い (Very High) ]、[高 (High) ]、[中 (Medium) ]、[低 (Low) ]、および [非常に低い (Very Low) ]。接続で検出されるアプリケーションのタイプごとに関連するビジネスとの関連性があります。このフィールドは、それらのうち最も低い (関連性が最も低い) ものを表示します。

### 分類 (Classification)

イベントを生成したルールが属する分類。

このフィールドを検索するときは、表示するイベントを生成したルールの分類番号を入力するか、分類名または説明のすべてまたは一部を入力します。また、番号、名前、または説明のコンマ区切りリストを入力することもできます。最後に、カスタム分類を追加した場合、その名前または説明のすべてまたは一部を使用して検索することもできます。

### クライアント (Client)

(使用可能な場合) 侵入イベントをトリガーとして使用したトラフィックで検出されたモニタ対象のホストで実行されているソフトウェアを表す、クライアント アプリケーション。

### クライアント カテゴリおよびタグ (Client Category and Tag)

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

**メンバー数 (Count)**

各行に表示される情報と一致するイベントの数。[カウント (Count)] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

**送信先の大陸 (Destination Continent)**

侵入イベントに関連する受信ホストの大陸。

**送信先の国 (Destination Country)**

侵入イベントに関連する受信ホストの国。

**宛先 IP (Destination IP)**

侵入イベントに関連する受信ホストが使用する IP アドレス。

**送信先ポートまたは ICMP コード (Destination Port / ICMP Code)**

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、このフィールドには ICMP コードが表示されます。

**宛先ユーザ (Destination User)**

宛先ホストにログインしている既知のユーザのユーザ ID。

**Device**

アクセス コントロール ポリシーが展開された管理対象デバイス。

スタック構成設定では、プライマリ デバイスとセカンダリ デバイスは、別々のデバイスであるかのように侵入イベントをレポートすることに注意してください。

**ドメイン**

侵入を検出したデバイスのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

**出力インターフェイス (Egress Interface)**

イベントをトリガーとして使用したパケットの出力インターフェイス。パッシブインターフェイスの場合、このインターフェイスの列には入力されません。

**出力セキュリティゾーン (Egress Security Zone)**

イベントをトリガーとして使用したパケットの出力セキュリティゾーン。パッシブ展開環境では、このセキュリティゾーンのフィールドには入力されません。

### 電子メールの添付ファイル (Email Attachments)

[MIME コンテンツ - 傾向 (MIME Content-Disposition)] 見出しから取得された MIME 添付ファイル名。添付ファイルの名前を表示するには、SMTP プリプロセッサの [MIME 添付ファイル名のログ (Log MIME Attachment Names)] オプションを有効にする必要があります。複数の添付ファイル名がサポートされます。

### 電子メール ヘッダー (Email Headers) (検索のみ)

電子メールのヘッダーから取得したデータ。

電子メールのヘッダーを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [ヘッダーのログ (Log Headers)] オプションを有効にする必要があります。

### メール受信者 (Email Recipient)

SMTPRCPTTO コマンドから取得された電子メール受信者のアドレス。このフィールドの値を表示するには、SMTP プリプロセッサの [受信者アドレスのログ (Log To Addresses)] オプションを有効にする必要があります。複数の受信者アドレスがサポートされます。

### メール送信者 (Email Sender)

SMTP MAIL FROM コマンドから取得された電子メール送信者のアドレス。このフィールドの値を表示するには、SMTP プリプロセッサの [送信者アドレスのログ (Log From Address)] オプションを有効にする必要があります。複数の送信者アドレスがサポートされます。

### ジェネレータ (Generator)

イベントを生成したコンポーネント。

### HTTP ホスト名 (HTTP Hostname)

HTTP 要求のホストヘッダーから取得されたホスト名 (存在する場合)。要求パケットにホスト名が常に含まれているわけではないことに注意してください。

ホスト名を HTTP クライアント トラフィックの侵入イベントと関連付けるには、HTTP 検査プリプロセッサの [ホスト名のログ (Log Headers)] オプションを有効にする必要があります。

テーブル ビューで、この列には、取得されたホスト名の最初の 50 文字が表示されます。ホストの省略名の表示部分にポインタを合わせると、最大 256 バイトまでの完全な名前を表示することができます。また、最大 256 バイトまでの完全なホスト名をパケットビューに表示することもできます。

### HTTP 応答コード (HTTP Response Code)

イベントをトリガーした接続を介してクライアントの HTTP 要求に応答して送信される HTTP ステータス コード。

## HTTP URI

(存在する場合) 侵入イベントをトリガーしたHTTP要求パケットに関連付けられたraw URI。要求パケットにURIが常に含まれているわけではないことに注意してください。

URIをHTTPクライアントトラフィックの侵入イベントと関連付けるには、HTTP検査プリプロセッサの[URIのログ(Log URI)]オプションを有効にする必要があります。

HTTP応答によってトリガーとして使用された侵入イベントの関連HTTPURIを参照するには、[両方のポートでのストリーム再構成の実行(Perform Stream Reassembly on Both Ports)]オプションにHTTPサーバのポートを設定する必要があります。ただし、これにより、トラフィックのリアセンブル用のリソース要求が増加することに注意してください。

この列には、取得されたURIの最初の50文字が表示されます。省略URIの表示部分にポインタを合わせると、最大2048バイトまでの完全なURIを表示することができます。また、最大2048バイトまでの完全なURIをパケットビューに表示することもできます。

## 影響 (Impact)

このフィールドの影響レベルは、侵入データ、ネットワーク検出データ、脆弱性情報との関係を示します。

このフィールドを検索するときは、影響アイコンの色または一部の文字列を指定しないでください。たとえば、**blue**、**level 1**、または**0**を使用しないでください。有効な大文字と小文字を区別しない値は次のとおりです。

- Impact 0、Impact Level 0
- Impact 1、Impact Level 1
- Impact 2、Impact Level 2
- Impact 3、Impact Level 3
- Impact 4、Impact Level 4

NetFlowデータからネットワークマップに追加されたホストに使用可能なオペレーティングシステムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な(インパクトレベル1:赤)インパクトレベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティングシステムIDを手動で設定します。

## 入力インターフェイス (Ingress Interface)

イベントをトリガーしたパケットの入力インターフェイス。パッシブインターフェイスの場合、このインターフェイスの列だけに入力されます。

## 入力セキュリティゾーン (Ingress Security Zone)

イベントをトリガーとして使用したパケットの入力セキュリティゾーンまたはトンネルゾーン。パッシブ展開環境では、このセキュリティゾーンフィールドだけに入力されます。

### インライン結果 (Inline Result)

ワークフローとテーブルビューでは、このフィールドには次のいずれかが表示されます。

- 黒い下矢印：ルールをトリガーとして使用したパケットをシステムがドロップしたことを示します
- 灰色の下矢印：[インライン時にドロップ (Drop when Inline)] 侵入ポリシー オプション (インライン展開環境) を有効にした場合、またはシステムがブルーニングしている間に [ドロップしてイベントを生成する (Drop and Generate)] ルールがイベントを生成した場合、IPS がパケットをドロップしたことを示します
- 空白：トリガーとして使用されたルールが [ドロップしてイベントを生成する (Drop and Generate Events)] に設定されていないことを示します

侵入ポリシーのルールの状態またはインライン ドロップ動作にかかわらず、インラインインターフェイスがタップ モードになっている場合を含め、パッシブ展開環境ではシステムはパケットをドロップしません。

このフィールドを検索するときは、次のいずれかを入力します。

- **dropped** : パケットがインライン展開環境でパケットをドロップするかどうかを指定します
- **would have dropped** : インライン展開環境でパケットをドロップするように侵入ポリシーが設定されている場合に、パケットをドロップするかどうかを指定します

### 侵入ポリシー (Intrusion Policy)

イベントを生成した侵入ルール、プリプロセッサルール、またはデコーダルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルトアクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。

### IOC

侵入イベントをトリガーとして使用したトラフィックが、接続に関係するホストに対する侵入の痕跡 (IOC) もトリガーとして使用したかどうか。このフィールドを検索するときは、**triggered** または **n/a** を指定します。

### メッセージ (Message)

イベントを説明するテキスト。ルールベースの侵入イベントの場合、イベントメッセージはルールから取得されます。デコーダベースおよびプリプロセッサベースのイベントの場合は、イベントメッセージはハードコーディングされています。

### MPLSラベル (MPLS Label)

侵入イベントをトリガーしたパケットと関連付けられているマルチプロトコル ラベル スイッチング ラベル。



### ネットワーク分析ポリシー (Network Analysis Policy)

イベントの生成に関連付けられているネットワーク分析ポリシー (ある場合)。

この列には、取得された URI の最初の 50 文字が表示されます。省略 URI の表示部分にポインタを合わせると、最大 2048 バイトまでの完全な URI を表示することができます。また、最大 2048 バイトまでの完全な URI をパケット ビューに表示することもできます。

### クライアントのオリジナル IP (Original Client IP)

X-Forwarded-For (XFF)、True-Client-IP、またはカスタム定義の HTTP ヘッダーから取得された、元のクライアント IP アドレス。

このフィールドの値を表示するには、ネットワーク解析ポリシーで HTTP プリプロセッサ [元のクライアント IP アドレスの抽出 (Extract Original Client IP Address)] オプションを有効にする必要があります。オプションで、ネットワーク解析ポリシーの同じエリアで、最大 6 つのカスタム クライアント IP 見出しを指定し、システムが [クライアントのオリジナル IP (Original Client IP)] イベント フィールドの値を選択する優先順位を設定します。

### [プライオリティ (Priority)]

Cisco Talos Security Intelligence and Research Group (Talos) で指定されたイベントの優先度。優先度は、`priority` キーワードの値または `classtype` キーワードの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。有効な値は、[高 (high)]、[中 (medium)]、および [低 (low)] です。

### プロトコル (Protocol) (検索のみ)

<http://www.iana.org/assignments/protocol-numbers> に一覧表示されている、接続で使用するトランスポートプロトコルの名前または番号。これは、送信元および宛先ポート/ICMP の列と関連付けられたプロトコルです。

### 確認者 (Reviewed By)

イベントを確認したユーザの名前。このフィールドを検索するときは、`unreviewed` と入力すると、まだ確認されていないイベントを検索できます。

### セキュリティ コンテキスト (Security Context)

トラフィックが通過した仮想ファイアウォールグループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチ コンテキスト モードの ASA FirePOWER だけです。

### Snort ID (Snort ID) (検索のみ)

イベントを生成したルールの Snort ID (SID) を指定するか、オプションで、ルールの複合ジェネレータ ID (GID) および SID を指定します。ここで、GID および SID は、コロン (:) で区切られ、GID:SID の形式になります。次の表の任意の値を指定できます。

表 292: Snort ID 検索値

値	例
単一の SID	10000
SID の範囲	10000 ~ 11000
SID より大きい	>10000
SID 以上	>=10000
SID 未満	<10000
SID 以下	<=10000
SID のカンマ区切りリスト	10000,11000,12000
単一の GID:SID の組み合わせ	1:10000
GID:SID の組み合わせのカンマ区切りリスト	1:10000,1:11000,1:12000
SID および GID:SID の組み合わせのカンマ区切りリスト	10000,1:11000,12000

表示しているイベントの SID が [メッセージ (Message) ] 列に表示されます。

#### ソースの大陸 (Source Continent)

侵入イベントに関連する送信ホストのある大陸。

#### ソースの国 (Source Country)

侵入イベントに関連する送信ホストのある国。

#### ソース IP

侵入イベントに関連する送信ホストが使用する IP アドレス。

#### 送信元ポート/ICMP タイプ (Source Port / ICMP Type)

送信元ホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、このフィールドには ICMP タイプが表示されます。

#### 送信元ユーザ (Source User)

送信元ホストにログインしている既知のユーザのユーザ ID。

#### SSL の実際のアクション (SSL Actual Action) (検索のみ)

システムが暗号化トラフィックに適用したアクション。

**ブロック (Block) /リセットしてブロック (Block With Reset)**

ブロックされた暗号化接続を表します。

**複合 (再署名) (Decrypt (Resign))**

再署名サーバ証明書を使用して復号された発信接続を表します。

**復号 (キーの置き換え) (Decrypt (Replace Key))**

置き換えられた公開キーと自己署名サーバ証明書を使用して復号された発信接続を表します。

**復号 (既知のキー) (Decrypt (Known Key))**

既知の秘密キーを使用して復号された着信接続を表します。

**デフォルト アクション (Default Action)**

接続がデフォルト アクションによって処理されたことを示しています。

**復号しない (Do Not Decrypt)**

システムが復号しなかった接続を表します。

フィールド値は、検索ワークフロー ページの [SSL ステータス (SSL Status) ] フィールドに表示されます。

**SSL 証明書情報 (SSL Certificate Information) (検索のみ)**

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- 件名/発行元共通名 (Subject/Issuer Common Name)
- 件名/発行元組織 (Subject/Issuer Organization)
- 件名/発行元組織ユニット (Subject/Issuer Organization Unit)
- 有効期間の開始/終了 (Not Valid Before/After)
- シリアル番号 (Serial Number)
- 証明書フィンガープリント (Certificate Fingerprint)
- 公開キー フィンガープリント (Public Key Fingerprint)

**SSL 失敗理由 (SSL Failure Reason) (検索のみ)**

システムが暗号化されたトラフィックの復号に失敗した理由：

- 不明
- 不一致 (No Match)
- Success
- キャッシュされていないセッション (Uncached Session)

- 不明な暗号スイート (Unknown Cipher Suite)
- サポートされていない暗号スイート (Unsupported Cipher Suite)
- サポートされていない SSL バージョン (Unsupported SSL Version)
- SSL 圧縮の使用 (SSL Compression Used)
- パッシブ モードで復号できないセッション (Session Undecryptable in Passive Mode)
- ハンドシェイク エラー (Handshake Error)
- 復号エラー (Decryption Error)
- 保留サーバ名カテゴリ ルックアップ (Pending Server Name Category Lookup)
- 保留共通名カテゴリ ルックアップ (Pending Common Name Category Lookup)
- 内部エラー (Internal Error)
- ネットワーク パラメータを使用できません (Network Parameters Unavailable)
- 無効なサーバ証明書の処理 (Invalid Server Certificate Handle)
- サーバ証明書フィンガープリントを使用できません (Server Certificate Fingerprint Unavailable)
- サブジェクト DN をキャッシュできません (Cannot Cache Subject DN)
- 発行元 DN をキャッシュできません (Cannot Cache Issuer DN)
- 不明の SSL バージョン (Unknown SSL Version)
- 外部証明書リストを使用できません (External Certificate List Unavailable)
- 外部証明書フィンガープリントを使用できません (External Certificate Fingerprint Unavailable)
- 内部証明書リストが無効です (Internal Certificate List Invalid)
- 内部証明書リストを使用できません (Internal Certificate List Unavailable)
- 内部証明書を使用できません (Internal Certificate Unavailable)
- 内部証明書フィンガープリントを使用できません (Internal Certificate Fingerprint Unavailable)
- サーバ証明書検証を使用できません (Server Certificate Fingerprint Unavailable)
- サーバ証明書検証エラー (Server Certificate Validation Failure)
- 無効なアクション (Invalid Action)

フィールド値は、検索ワークフロー ページの [SSL ステータス (SSL Status) ] フィールドに表示されます。

### SSL ステータス (SSL Status)

暗号化接続をログに記録した [SSL の実際のアクション (SSL Actual Action)] (SSL ルール、デフォルトのアクション、または復号化できないトラフィックアクション) に関連付けられているアクション。

システムが暗号化された接続の復号化に失敗した場合、実行された [SSL の実際のアクション (SSL Actual Action)] (復号化できないトラフィックアクション) と [SSL 障害の理由 (SSL Failure Reason)] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [復号しない (不明な暗号スイート) (Do Not Decrypt (Unknown Cipher Suite))] が表示されます。

証明書の詳細を表示するにはロックアイコン (🔒) をクリックします。

このフィールドを検索するときは、[SSL の実際のアクション (SSL Actual Action)] および [SSL 障害の理由 (SSL Failure Reason)] の値を 1 つ以上を入力して、システムが処理した暗号化されたトラフィック、または復号化に失敗したトラフィックを表示します。

### SSL 件名/発行元国 (SSL Subject/Issuer Country) (検索のみ)

暗号化証明書に関連付けられている件名または発行者の国に関する 2 文字の ISO 3166-1 アルファ 2 国コード。

### 時刻 (Time)

イベントの日付と時刻。このフィールドは検索できません。

### VLAN ID (Admin. VLAN ID)

侵入イベントをトリガーとして使用したパケットと関連付けられた最内部 VLAN ID。

### Web アプリケーション (Web Application)

侵入イベントをトリガーとして使用したトラフィックで検出された HTTP トラフィックの内容または要求された URL を表す、Web アプリケーション。

システムが HTTP のアプリケーションプロトコルを検出し、特定の Web アプリケーションを検出できなかった場合、システムはここで一般的な Web ブラウジング指定を提供します。

### Web アプリケーションカテゴリおよびタグ (Web Application Category and Tag)

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

### 関連トピック

[イベントの検索](#) (2467 ページ)

## 侵入イベント影響レベル

イベントがネットワークに与える影響を評価するために、Firepower Management Center は侵入イベントのテーブルビューに影響レベルを表示します。イベントごとに、システムは影響レベ

ルアイコンを追加し、侵入データ、ネットワーク検出データ、脆弱性情報との関係を色で示します。



- (注) NetFlow データからネットワーク マップに追加されたホストに使用可能なオペレーティング システムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な (インパクトレベル1: 赤) インパクトレベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティング システム ID を手動で設定します。

次の表に、影響レベルで使用可能な値を示します。

表 293: 影響レベル

影響レベル	脆弱性	カラー	説明
0	不明	グレー	送信元ホストと宛先ホストは両方ともネットワーク検出によってモニタされているネットワーク上に存在しません。
1	脆弱	赤色	次のいずれかを行います。 <ul style="list-style-type: none"> <li>送信元ホストまたは宛先ホストはネットワークマップ内にあり、脆弱性はホストにマッピングされます</li> <li>送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵害される可能性があります。</li> </ul>

影響レベル	脆弱性	カラー	説明
2	潜在的に脆弱	オレンジ	<p>送信元ホストまたは宛先ホストはネットワーク マップ内にあり、次のいずれかに当てはまります。</p> <ul style="list-style-type: none"> <li>• ポート指向のトラフィックの場合、ポートはサーバアプリケーションプロトコルを実行しています</li> <li>• ポート指向ではないトラフィックの場合、ホストはプロトコルを使用しません</li> </ul>
3	現在は脆弱ではない	黄色	<p>送信元ホストまたは宛先ホストはネットワーク マップ内にあり、次のいずれかに当てはまります。</p> <ul style="list-style-type: none"> <li>• ポート指向のトラフィック（たとえば、TCP または UDP）の場合、ポートが開いていません</li> <li>• ポート指向ではないトラフィック（たとえば、ICMP）の場合、ホストはプロトコルを使用しません</li> </ul>
4	ターゲット不明	青	送信元ホストまたは宛先ホストがモニタ対象のネットワークにありますが、ネットワーク マップ内にそのホストのエントリがありません。

## 侵入イベントと関連付けられた接続データの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

システムは、侵入イベントが検出された接続を記録できます。このロギングは、アクセスコントロールルールに関連付けられている侵入ポリシーに対して自動的に行われますが、デフォルトアクションに関連する接続データを参照するには、接続ロギングを手動で有効にする必要があります。

関連データの表示は、イベントのテーブルビュー間を移動する場合に非常に役立ちます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

**ステップ 1** [分析 (Analysis)] > [侵入 (Intrusions)] > [イベント (Events)] を選択します。

**ステップ 2** イベントビューアのチェックボックスを使用して侵入イベントを選択してから、[ジャンプ (Jump to)] ドロップダウンリストから [接続 (Connections)] を選択します。

**ヒント** 同じ方法で、特定の接続に関連した侵入イベントを表示できます。詳細については、[ワークフロー間のナビゲーション \(2463 ページ\)](#) を参照してください。

### 関連トピック

[許可された接続のロギング \(2512 ページ\)](#)

[侵入イベント ワークフローの使用 \(2577 ページ\)](#)

[接続およびセキュリティ インテリジェンス イベント テーブルの使用 \(2548 ページ\)](#)

## 侵入イベントを確認済みとしてマーク

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入イベントが悪意のあるものではないことがわかったら、そのイベントを確認済みとしてマークできます。

侵入イベントを調べて、そのイベントがネットワークセキュリティに対して脅威ではないことがわかったら（たとえば、ネットワーク上のどのホストも検出されたエクスプロイトに対して



脆弱でないことがわかっているなど)、そのイベントを確認済みとしてマークできます。確認済みのイベントはイベント データベースに保存され、イベント要約統計に含まれますが、デフォルトの侵入イベントページには表示されなくなります。自分の名前がレビューアとして表示されます。

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

バックアップを実行してから確認済みの侵入イベントビューを削除した場合、バックアップを復元すると、削除された侵入イベントビューは復元されますが、確認済みのステータスは復元されません。こうして復元された侵入イベントは、[確認済みイベント (Reviewed Events)] の下ではなく [侵入イベント (Intrusion Events)] の下に表示されます。

### 手順

侵入イベントが表示されるページで、次の2つの方法を選択できます。

- イベントのリストから1つまたは複数の侵入イベントにマークを付けるには、イベントの横にあるチェックボックスをオンにして、[レビュー (Review)] をクリックします。
- イベントのリストからすべての侵入イベントにマークを付けるには、[すべて確認 (Review All)] をクリックします。

### 関連トピック

[侵入イベント ワークフローの使用 \(2577 ページ\)](#)

## 以前に確認された侵入イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

### 手順

**ステップ 1** [分析 (Analysis)] > [侵入 (Intrusions)] > [見直されたイベント (Reviewed Events)] を選択します。

**ステップ 2** 次の選択肢があります。

- [時間枠の変更 \(2455 ページ\)](#) の説明に従って、時間範囲を調整します。

- 侵入イベントのテーブルビューが含まれないカスタムワークフローを使用している場合、ワークフローのタイトルの横にある [(ワークフローの切り替え) ((switch workflow))] をクリックして、システム提供のワークフローのいずれかを選択します。
- 表示されるイベントの詳細については、[侵入イベントフィールド \(2557 ページ\)](#) を参照してください。

#### 関連トピック

[侵入イベント ワークフローの使用 \(2577 ページ\)](#)

## 侵入イベントへの未確認としてマーク

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

イベントに未確認のマークを付けることで、確認済みイベントをデフォルトの侵入イベントビューに戻すことができます。

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

#### 手順

確認済みイベントが表示されるページで、次の 2 つの方法を選択できます。

- 確認済みイベントリストから個別の侵入イベントを削除するには、特定のイベントの横にあるチェックボックスをオンにして、[未確認 (Unreview)] をクリックします。
- 確認済みイベント リストからすべての侵入イベントを削除するには、[すべて未確認 (Unreview All)] をクリックします。

## プリプロセッサ イベント

プリプロセッサが提供する機能は 2 つあります。1 つは、パケットに対して指定されたアクション (HTTP トラフィックを復号して正規化するなど) を実行する機能、もう 1 つは、パケットが特定のプリプロセッサ オプションをトリガーしたときに関連するプリプロセッサルールが有効にされている場合は常にイベントを生成することで、指定のプリプロセッサオプションの実行を報告するという機能です。たとえば、プリプロセッサが IIS の二重にエンコードされたトラフィックを検出した場合にイベントが生成されるようにするには、HTTP Inspect の [二重エンコード (Double Encoding)] オプションと、HTTP Inspect Generator (GID) 119 および Snort ID (SID) 2 が設定された関連するプリプロセッサルールを有効にします。

プリプロセッサの実行を報告するイベントを生成すると、異常なプロトコルエクスプロイトを検出するのに役立ちます。たとえば、攻撃者は重複している IP フラグメントを作成して、ホスト上で DoS 攻撃を引き起こす可能性があります。IP 最適化プリプロセッサはこのタイプの攻撃を検出し、それに関する侵入イベントを生成できます。

プリプロセッサ イベントは、パケット ディスプレイにイベントの詳細なルールの説明が表示されないという点で、ルール イベントとは異なります。代わりに、パケット ディスプレイには、イベント メッセージ、GID、SID、パケット ヘッダー データおよびパケット ペイロードが表示されます。これにより、パケットのヘッダー情報を分析し、そのヘッダーオプションが使用中であるかをどうか判断して、それがシステムをエクスプロイトする可能性がある場合は、パケットペイロードを検査できます。プリプロセッサによる各パケットの分析が完了すると、ルールエンジンは、その結果に応じて適切なルールを実行し（プリプロセッサが各パケットを最適化し、有効なセッションの一部として確立できた場合）、潜在的なコンテンツレベルの脅威についてさらに分析を行い、それらのパケットについて報告します。

## プリプロセッサのジェネレータ ID

各プリプロセッサには、独自のジェネレータ ID 番号 (GID) があり、これはパケットによってトリガーとして使用されたプリプロセッサを示します。一部のプリプロセッサは関連した SID もあり、これは潜在的攻撃を分類する ID 番号です。ルールの Snort ID (SID) が、ルールをトリガーとして使用するパケットのコンテキストを提供できる方法とほぼ同じで、この ID 番号によりイベントのタイプを分類することによって、イベントをより効率的に分析するのに役立ちます。侵入ポリシー ルールのページのプリプロセッサ フィルター グループのプリプロセッサごとにプリプロセッサルールをリストできます。また、プリプロセッサのプリプロセッサルールとカテゴリ フィルター グループのパケット デコーダ サブグループをリストできます。



(注) 標準テキスト ルールによって生成されるイベントのジェネレータ ID は 1 です。共有オブジェクトルールの場合、イベントのジェネレータ ID は 3 です。どちらの場合も、トリガーした特定のルールがイベントの SID に示されます。

次の表では、各 GID を生成するイベントのタイプについて説明します。

表 294: ジェネレータ ID

ID	コンポーネント	説明
1	標準的なテキストルール	パケットが標準テキストルールをトリガーとして使用したときにイベントが生成されました。
2	タグ付きパケット	タグ付きセッションからパケットを生成するタグジェネレータによって、イベントが生成されました。これは、tag ルールオプションが使用される場合に発生します。

ID	コンポーネント	説明
3	共有オブジェクトルール	パケットが共有オブジェクトルールをトリガーとして使用したときにイベントが生成されました。
102	HTTP デコーダ	デコーダ エンジンが、パケット内の HTTP データを復号化しました。
105	Back Orifice ディテクタ	Back Orifice ディテクタが、パケットに関連付けられた Back Orifice 攻撃を特定しました。
106	RPC デコーダ	RPC デコーダがパケットを復号化しました。
116	パケット デコーダ	パケットデコーダによってイベントが生成されました。
119、120	HTTP Inspect プリプロセッサ	HTTP Inspect プリプロセッサによってイベントが生成されました。GID 120 ルールは、サーバ固有の HTTP トラフィックに関するルールです。
122	ポートスキャン ディテクタ	ポートスキャンフロー ディテクタによってイベントが生成されました。
123	IP デフラグメンタ	断片化された IP データグラムを適切に再構成できなかったときに、イベントが生成されました。
124	SMTP デコーダ	SMTP プリプロセッサが SMTP バーブに対するエクスプロイトを検出したときに、イベントが生成されました。
125	FTP デコーダ	FTP/Telnet デコーダが FTP トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。
126	Telnet デコーダ	FTP/Telnet デコーダが Telnet トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。
128	SSH プリプロセッサ	SSH プリプロセッサが SSH トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。

ID	コンポーネント	説明
129	ストリーム プリプロセッサ	ストリームプリプロセッサによるストリームの前処理中に、イベントが生成されました。
131	DNSプリプロセッサ	DNSプリプロセッサによってイベントが生成されました。
133	DCE/RPC プリプロセッサ	このイベントは、DCE/RPC プリプロセッサにより生成されました。
134	ルール遅延 パケット遅延	ルール遅延によって侵入ルールのグループが中断された (134:1) または再有効化された (134:2) とき、あるいはパケット遅延しきい値が超過したために、システムがパケットの検査を停止したとき (134:3) に、イベントが生成されました。
135	レートベースの攻撃ディテクタ	レートベースの攻撃ディテクタがネットワークのホストに対する過度の識別したときに、イベントが生成されました。
137	SSL プリプロセッサ	このイベントは、SSL プリプロセッサによって生成されました。
138、139	機密データ プリプロセッサ	機密データプリプロセッサによってイベントが生成されました。
140	SIP プリプロセッサ	SIP プリプロセッサによってイベントが生成されました。
141	IMAP プリプロセッサ	IMAP プリプロセッサによってイベントが生成されました。
142	POP プリプロセッサ	POPプリプロセッサによってイベントが生成されました。
143	GTP プリプロセッサ	GTPプリプロセッサによってイベントが生成されました。
144	Modbus プリプロセッサ	Modbus SCADA プリプロセッサによってイベントが生成されました。
145	DNP3 プリプロセッサ	DNP3 SCADA プリプロセッサによってイベントが生成されました。

## 侵入イベントのワークフロー ページ

現在の侵入ポリシーで有効になっているプリプロセッサ、デコーダ、および侵入ルールは、モニタしているトラフィックがポリシーに違反するたびに、侵入イベントを生成します。

Firepower システムは、侵入イベントの表示および分析に使用できる、イベント データが入力された定義済みワークフローのセットを提供します。これらのワークフローは、評価する侵入イベントの特定に役立つ一連のページを表示して手順を示します。

定義済みの侵入イベントのワークフローには、次の3種類のページまたはイベントビューがあります。

- 1つ以上のドリルダウン ページ
- 侵入イベントのテーブル ビュー
- パケット ビュー

ドリルダウン ページには通常、1つの特定の種類の情報を表示できるように1つのテーブル（一部のドリルダウン ビューでは複数のテーブル）に2つ以上の列が含まれます。

「ドリルダウン」して1つ以上の宛先ポートの詳細情報を検索すると、これらのイベントは自動的に選択され、ワークフローの次のページが表示されます。このように、ドリルダウンテーブルを使用すると、一度に分析するイベントの数を減らすことができます。

侵入イベントの最初のテーブル ビューでは、各侵入イベントが独自の行にリストされます。テーブルの列には、時間、発信元 IP アドレスおよびポート、宛先 IP アドレスおよびポート、イベントの優先度、イベント メッセージなどの情報が示されます。

イベントを選択してワークフローの次のページを表示する代わりに、テーブルビューでイベントを選択した場合、イベントはいわゆる制約に追加されます。制約とは、分析するイベントの種類に加える制限のことです。

たとえば、任意の列で列のクローズ アイコン (✖) をクリックして、ドロップダウン リストから [時間 (Time)] をクリアすると、[時間 (Time)] を列の1つとして削除できます。分析内でイベントのリストを絞り込むには、テーブルビューの行のいずれかの値のリンクをクリックします。たとえば、分析を送信元 IP アドレスの1つ（おそらく、潜在的な攻撃者）から生成されたイベントに制限するには、[送信元 IP アドレス (Source IP Address)] 列の IP アドレスをクリックします。

テーブル ビューの1つまたは複数の行を選択し、[表示 (View)] をクリックすると、パケット ビューが表示されます。パケット ビューは、ルールをトリガーとして使用したパケットまたはイベントを生成したプリプロセッサに関する情報を提供します。パケット ビューの各セクションには、パケット内の特定の層についての情報が含まれます。折りたたまれたセクションを展開すると、より多くの情報を参照できます。



- (注) それぞれのポートスキャンイベントは複数のパケットによってトリガーとして使用されるため、ポートスキャンイベントは特別なバージョンのパケットビューを使用します。

事前定義済みのワークフローが特定のニーズに合致しない場合は、必要な情報だけを表示するカスタムワークフローを作成できます。カスタム侵入イベントのワークフローには、ドリルダウン ページ、イベントのテーブルビュー、またはその両方を含めることができます。システムはパケットビューを最後のページとして自動的に組み込みます。イベントを調査する方法に応じて、定義済みワークフローと独自のカスタムワークフローを簡単に切り替えることができます。

## 侵入イベントワークフローの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

イベントのドリルダウンビューとテーブルビューは、イベントのリストを絞り込み、関連するイベントのグループに分析を集中するために使用できる共通機能を共有します。

別のワークフローページで同じ侵入イベントを表示しないようにするため、ページの下部にあるリンクをクリックして別のページのイベントを表示すると時間範囲は一時停止し、クリックして後続のページでその他のアクションを実行すると再開します。



- ヒント** プロセスの任意の時点で、制約を検索条件のセットとして保存できます。たとえば、ネットワークが数日にわたり単一の IP アドレスから攻撃者によって探られていることに気付いた場合、調査中に制約をいったん保存し、後で使用することができます。ただし、複合制約を検索条件のセットとして保存することはできません。

### 手順

- ステップ 1** [分析 (Analysis)] > [侵入 (Intrusions)] > [イベント (Events)] を使用して侵入イベントワークフローにアクセスします。
- ステップ 2** オプションで、[侵入イベントドリルダウンページの制約 \(2579 ページ\)](#) または [侵入イベントテーブルビューの制約 \(2580 ページ\)](#) の説明に従って、イベントビューに表示される侵入イベントの数を制限します。
- ステップ 3** 次の選択肢があります。
  - 表示されるカラムの詳細については、[侵入イベントフィールド \(2557 ページ\)](#) を参照してください。

- ホストのプロファイルを表示するには、ホスト IP アドレスの横に表示されるホスト プロファイルアイコン (📄) をクリックします。
- 地理位置情報の詳細を表示するには、[送信元の国 (Source Country)] または [宛先の国 (Destination Country)] カラムに表示されるフラグアイコンをクリックします。
- 表示されたイベントの時刻と日付の範囲を変更するには、[時間枠の変更 \(2455 ページ\)](#) を参照してください。

**ヒント** 侵入イベントがイベントビューに表示されない場合、指定した時間範囲を調整すると、結果が返される場合があります。古い時間範囲を指定した場合、その時間範囲内のイベントが削除されることがあります。ルールのしきい値の設定を調整すると、イベントが生成される場合があります。

(注) イベントビューを時間によって制約している場合は、(グローバルかイベント固有かに関係なく) アプライアンスに設定されている時間枠の外で生成されたイベントがイベントビューに表示されます。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

- 現在のワークフロー ページのイベントをソートする、または現在のワークフロー ページ内で移動するには、[ワークフローの使用 \(2429 ページ\)](#) を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページリンクをクリックします。
- 後でインシデントにイベントを転送できるように、クリップボードにイベントを追加するには、[コピー (Copy)] または [すべてコピー (Copy All)] をクリックします。
- イベントデータベースからイベントを削除するには、削除するイベントの横にあるチェックボックスをオンにし、[削除 (Delete)] または [すべて削除 (Delete All)] をクリックします。
- イベントに確認済みのマークを付けて、侵入イベントのページからそれらを削除し、イベントデータベースからは削除しないようにするには、[侵入イベントを確認済みとしてマーク \(2570 ページ\)](#) を参照してください。
- 選択したイベントをトリガーしたパケットのローカルコピー (libpcap 形式のパケットキャプチャファイル) をダウンロードするには、ダウンロードするパケットによってトリガーされたイベントの横にあるチェックボックスをオンにして、[パケットのダウンロード (Download Packets)] または [すべてのパケットのダウンロード (Download All Packets)] をクリックします。キャプチャされたパケットは libpcap 形式で保存されます。この形式は、複数の一般的なプロトコルアナライザで使用されます。
- 他のイベントビューに移動して関連イベントを表示するには、[ワークフロー間のナビゲーション \(2463 ページ\)](#) を参照してください。
- 別のワークフローを一時的に使用するには、[(ワークフローの切り替え) ((switch workflow))] をクリックします。



- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク (Bookmark This Page)] をクリックします。
- [サマリー ダッシュボード (Summary Dashboard)] の [侵入イベント (Intrusion Events)] セクションを表示するには、[ダッシュボード (Dashboards)] をクリックします。
- ブックマークの管理ページに移動するには、[ブックマークの表示 (View Bookmarks)] をクリックします。
- 現在のビューのデータに基づいてレポートを生成するには、[イベントビューからのレポート テンプレートの作成 \(2312 ページ\)](#) を参照してください。

#### 関連トピック

[イベントの検索 \(2467 ページ\)](#)

[ブックマーク \(2464 ページ\)](#)

## 侵入イベント ドリルダウン ページの制約

次の表では、ドリルダウン ページの使用方法について説明します。

表 295: ドリルダウン ページでのイベントの制約

目的	操作
次のワークフロー ページのドリルダウンを特定の値に制約する	<p>値をクリックします。</p> <p>たとえば、[宛先ポート (Destination Port)] ワークフローで、イベントを宛先ポートが 80 であるものに制約するには、[DST ポート/ICMP コード (DST Port/ICMP Code)] 列で [80/tcp (80/tcp)] をクリックします。ワークフローの次のページ [イベント (Events)] が表示され、ポート 80/tcp のイベントだけが含まれます。</p>

目的	操作
次のワークフロー ページのドリルダウンを選択したイベントに制約する	<p>次のワークフロー ページで表示するイベントの横にあるチェックボックスを選択し、[表示 (View)] をクリックします。</p> <p>たとえば、[宛先ポート (Destination Port)] ワークフローで、イベントを宛先がポート 20/tcp および 21/tcp であるものに制約するには、それらのポートの行の横にあるチェックボックスを選択し、[表示 (View)] をクリックします。ワークフローの次のページ [イベント (Events)] が表示され、ポート 20/tcp および 21/tcp のイベントだけが含まれます。</p> <p>複数の行を制約し、テーブルに複数の列が存在する場合 ([数 (Count)] 列を含まない) は、複合制約と呼ばれるものが作成されることに注意してください。複合制約により、必要以上のイベントを制約に含めないようにすることができます。たとえば、[イベント (Event)] と [宛先 (Destination)] のワークフローを使用する場合は、最初のドリルダウン ページで選択した各行により、複合制約が作成されます。宛先 IP アドレス 10.10.10.100 のイベント 1:100 を選択し、宛先 IP アドレス 192.168.10.100 のイベント 1:200 も選択した場合、複合制約により、イベントタイプとして 1:100 を含むイベントや宛先 IP アドレスとして 192.168.10.100 を含むイベント、またはイベントタイプとして 1:200 を含むイベントや宛先 IP アドレスとして 10.10.10.100 を含むイベントが選択されなくなります。</p>
現在の制約を保持しながら、次のワークフロー ページをドリルダウンする	[すべて表示 (View All)] をクリックします。

## 侵入イベント テーブル ビューの制約

次の表では、テーブル ビューの使用方法について説明します。

表 296: イベントのテーブル ビューでのイベントの制約

目的	操作
1 つの属性を持つイベントにビューを制約する	<p>属性をクリックします。</p> <p>たとえば、宛先がポート 80 であるイベントにビューを制約するには、[DST ポート/ICMP コード (DST Port/ICMP Code)] 列で [80/tcp (80/tcp)] をクリックします。</p>

目的	操作
テーブルから列を削除する	<p>非表示にする列見出しのクローズアイコン (✕) をクリックします。表示されるポップアップ ウィンドウで、[適用 (Apply)] をクリックします。</p> <p>他のカラムを表示または非表示にするには、[適用 (Apply)] をクリックする前に、該当するチェックボックスをオンまたはオフにします。無効になった列をビューに再追加するには、展開矢印 (▶) をクリックして検索制約を拡張し、[無効の列 (Disabled Columns)] の下の列名をクリックします。</p>
1つ以上のイベントに関連付けられたパケットを表示する	<p>次のいずれかを行います。</p> <ul style="list-style-type: none"> <li>• パケットを表示するイベントの横にある下矢印アイコン (↓) をクリックします。</li> <li>• パケットを表示する 1つ以上のイベントを選択し、ページの下部にある [表示 (View)] をクリックします。</li> <li>• ページの下部で、[すべて表示 (View All)] をクリックして、現在の制約に一致するすべてのイベントのパケットを表示します。</li> </ul>

## 侵入イベントパケットビューの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

パケットビューは、侵入イベントを生成したルールをトリガーとして使用したパケットに関する情報を表示します。



**ヒント** イベントを検出するデバイスで [パケットの転送 (Transfer Packet)] オプションが無効になっている場合、Firepower Management Center でのパケットビューにはパケット情報は含まれません。

パケットビューは、パケットがトリガーとして使用した侵入イベントに関する情報を提供することによって、イベントのタイムスタンプ、メッセージ、分類、優先度、イベントを生成したルール (イベントが標準テキストルールによって生成された場合) など、特定のパケットが

キャプチャされた理由を示します。パケットビューは、パケットのサイズなど、パケットに関する一般情報も表示します。

さらに、パケットビューにはパケット内の各層（データリンク、ネットワーク、およびトランスポート）について説明したセクションと、パケットを構成するバイトについて説明したセクションがあります。システムがパケットを復号化した場合は、復号化されたバイトを表示できます。折りたたまれたセクションを展開すると、詳細情報を参照できます。



- (注) それぞれのポートスキャンイベントは複数のパケットによってトリガーとして使用されるため、ポートスキャンイベントは特別なバージョンのパケットビューを使用します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができません。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

**ステップ 1** [侵入イベントテーブルビューの制約 \(2580 ページ\)](#) の説明に従って、侵入イベントのテーブルビューで、表示するパケットを選択します。

**ステップ 2** 複数のイベントを選択した場合は、オプションで、ページの下部にあるページ番号を使用することによって、パケットビューでパケットのページを切り替えることができます。

**ステップ 3** 次のオプションもあります。

- 調整：パケットビューで日時範囲を変更するには、[時間枠の変更 \(2455 ページ\)](#) を参照してください。
- クリップボード：後でイベントをインシデントに転送するためクリップボードにそのイベントを追加するには、[コピー (Copy)] をクリックして表示しているパケットのイベントをコピーするか、[すべてコピー (Copy All)] をクリックして以前に選択したパケットのすべてのイベントをコピーします。
- 設定：イベントをトリガした侵入ルールを設定するには、[アクション (Actions)] の横にある矢印をクリックし、[パケットビュー内での侵入ルールの設定 \(2587 ページ\)](#) の説明に従って操作を続けます。
- 削除：データベースからイベントを削除するには、[削除 (Delete)] をクリックして表示しているパケットのイベントを削除するか、[すべて削除 (Delete All)] をクリックして以前に選択したパケットのすべてのイベントを削除します。
- ダウンロード：イベントをトリガーしたパケットのローカルコピー (libpcap 形式のパケットキャプチャファイル) をダウンロードするには、[パケットのダウンロード (Download Packet)] をクリックして表示しているイベントに関するキャプチャしたパケットのコピーを保存するか、[すべてのパケットをダウンロード (Download All Packets)] をクリックして以前に選択したパケットのすべてのイベントのキャプチャしたパケットのコピーを保存します。キャプチャされたパケットは libpcap 形式で保存されます。この形式は、複数の一般的なプロトコルアナライザで使用されます。

(注) 単一のポートスキャンイベントは複数のパケットに基づいているため、ポートスキャンパケットをダウンロードできません。ただし、ポートスキャンビューは使用可能なすべてのパケット情報を提供します。ダウンロードするには少なくとも 15% の使用可能なディスク領域が必要です。

- 確認済みのマークを付ける：イベントデータベースからは削除せずに、イベントビューから削除するため確認済みのイベントにマークを付けるには、[確認 (Review)] をクリックして表示しているパケットのイベントにマークを付けるか、[すべて確認 (Review All)] をクリックして以前に選択したパケットのすべてのイベントにマーク付けます。詳細については、[侵入イベントを確認済みとしてマーク \(2570 ページ\)](#) を参照してください。
- 追加情報の表示：ページセクションを展開したり、折りたたんだりするには、セクションの横にある矢印をクリックします。詳細については、[イベント情報のフィールド \(2583 ページ\)](#)、[フレーム情報のフィールド \(2591 ページ\)](#)、[データリンク層情報フィールド \(2592 ページ\)](#) を参照してください。
- ネットワーク層の情報の表示：[ネットワーク層情報の表示 \(2593 ページ\)](#) を参照してください。
- パケットバイト情報の表示：[パケットバイト情報の表示 \(2599 ページ\)](#) を参照してください。
- トランスポート層の情報の表示：次を参照してください。[トランスポート層情報の表示 \(2596 ページ\)](#)

---

#### 関連トピック

[ポートスキャン検出 \(1991 ページ\)](#)

[侵入イベントのクリップボード \(2599 ページ\)](#)

## イベント情報のフィールド

パケットビューで、[イベント情報 (Event Information)] セクションのパケットに関する情報を表示できます。

### イベント

イベントのメッセージ。ルールベースのイベントの場合、これはルールメッセージに対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

イベントの ID は、(GID:SID:Rev) の形式でメッセージに付加されます。GID は、ルールエンジン、デコーダ、またはイベントを生成したプリプロセッサのジェネレータ ID です。SID は、ルール、デコーダメッセージ、またはプリプロセッサメッセージの ID です。Rev はルールのリビジョン番号です。

### Timestamp

パケットがキャプチャされた時間。

### 分類 (Classification)

イベントの分類。ルールベースのイベントの場合、これはルールの分類に対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

### [プライオリティ (Priority)]

イベントの優先度。ルールベースのイベントの場合、これは `priority` キーワードの値または `classtype` キーワードの値に対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

### 入力セキュリティ ゾーン (Ingress Security Zone)

イベントをトリガーしたパケットの入力セキュリティゾーン。パッシブ展開環境では、このセキュリティゾーンフィールドだけに入力されます。

### 出力セキュリティ ゾーン (Egress Security Zone)

イベントをトリガーとして使用したパケットの出力セキュリティゾーン。パッシブ展開では、このフィールドには入力されません。

### ドメイン

管理対象デバイスが属するドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

### Device

アクセス コントロール ポリシーが展開された管理対象デバイス。

スタック構成設定では、プライマリ デバイスとセカンダリ デバイスは、別々のデバイスであるかのように侵入イベントをレポートすることに注意してください。

### セキュリティ コンテキスト (Security Context)

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。マルチ コンテキストモードの ASA FirePOWER の場合に、システムがこのフィールドにデータを設定することに注意してください。

### 入力インターフェイス (Ingress Interface)

イベントをトリガーしたパケットの入力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列だけに入力されます。

### 出力インターフェイス (Egress Interface)

インラインセットの場合、イベントをトリガーとして使用したパケットの出力インターフェイス。

### 送信元/宛先 IP (Source/Destination IP)

イベントをトリガーとして使用したパケットの発生元 (送信元) であるホスト IP アドレスまたはドメイン名、またはイベントをトリガーとして使用したトラフィックのターゲット (宛先) ホスト。

### 送信元ポート/ICMP タイプ (Source Port/ICMP Type)

イベントをトリガーしたパケットの送信元ポート。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP タイプを表示します。

### 宛先ポート/ICMP コード (Destination Port/ICMP Code)

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP コードを表示します。

### 電子メールのヘッダー (Email Headers)

電子メールヘッダーから取得したデータ。電子メールヘッダーは侵入イベントのテーブルビューには表示されませんが、電子メールヘッダー データは検索条件として使用できることに注意してください。

電子メールのヘッダーを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [ヘッダーのログ (Log Headers) ] オプションを有効にする必要があります。ルールベースのイベントの場合、この行は電子メールデータが取得されたときに表示されます。

### HTTP ホスト名 (HTTP Hostname)

(存在する場合) HTTP 要求のホストヘッダーから取得されたホスト名。この行には、最大 256 バイトの完全なホスト名が表示されます。ホスト名が 1 行より長い場合は、完全なホスト名を展開できます。

ホスト名を表示するには、HTTP 検査プリプロセッサ [ホスト名のログ (Log Hostname) ] オプションを有効にする必要があります。

HTTP 要求パケットにホスト名が常に含まれているわけではないことに注意してください。ルールベースのイベントの場合、この行はパケットに HTTP ホスト名または HTTP URI が含まれる場合に表示されます。

### HTTP URI

(存在する場合) 侵入イベントをトリガーした HTTP 要求パケットに関連付けられた raw URI。この行には、最大 2048 バイトの完全な URI が表示されます。URI が 1 行より長い場合は、完全な URI を展開できます。

URI を表示するには、HTTP 検査プリプロセッサ [URI のログ (Log URI) ] オプションを有効にする必要があります。

HTTP 要求パケットに URI が常に含まれているわけではないことに注意してください。ルールベースのイベントの場合、この行はパケットに HTTP ホスト名または HTTP URI が含まれる場合に表示されます。

HTTP 応答によってトリガーとして使用された侵入イベントの関連 HTTP URI を参照するには、[両方のポートでのストリーム再構成の実行 (Perform Stream Reassembly on Both Ports)] オプションに HTTP サーバのポートを設定する必要があります。ただし、これにより、トラフィックのリアセンブル用のリソース要求が増加することに注意してください。

### 侵入ポリシー (Intrusion Policy)

(存在する場合) 侵入イベントを生成した侵入、プリプロセッサ、デコーダのルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルトアクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。

### アクセス コントロール ポリシー (Access Control Policy)

イベントを生成した侵入ルール、プリプロセッサルール、またはデコーダルールが有効にされた侵入ポリシーが含まれるアクセス コントロール ポリシー。

### アクセス コントロール ルール (Access Control Rule)

イベントを生成した侵入ルールと関連付けられたアクセス コントロール ルール。[デフォルトアクション (Default Action)] は、ルールが有効にされた侵入ポリシーがアクセス コントロール ルールに関連付けられていないことと、代わりにアクセス コントロール ポリシーのデフォルトアクションとして設定されていることを示します。

### ルール (Rule)

標準テキストルール イベントの場合、イベントを生成したルール。

イベントが、共有オブジェクトルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

ルールデータにはネットワークに関する機密情報が含まれるため、管理者はユーザがローカルルールの表示権限を使用してパケット ビューでルール情報を表示できる機能を、ユーザ ロール エディタで切り替えることができます。

### アクション (Actions)

標準テキストルール イベントの場合は、[アクション (Actions)] を展開して、イベントをトリガーとして使用したルールに対して次の操作のいずれかを実行します。

- ルールを編集する
- ルールのリビジョンのドキュメンテーションを表示する
- ルールにコメントを追加する
- ルールの状態を変更する
- ルールのしきい値を設定する
- ルールを抑制する



イベントが、共有オブジェクトルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

### パケットビュー内での侵入ルールの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入イベントのパケットビュー内で、イベントをトリガーとして使用したルールに対して複数のアクションを実行できます。イベントが、共有オブジェクトルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

### 手順

**ステップ 1** 侵入ルールによって生成された侵入イベントのパケットビュー内で、[イベント情報 (Event Information)] セクションの [アクション (Actions)] を展開します。

**ステップ 2** 次の選択肢があります。

- **コメント** : 標準テキストルールイベントの場合、[ルールコメント (Rule Comment)] をクリックして、イベントを生成したルールにテキストコメントを追加します。これにより、ルールや、特定されたエクスプロイトまたはポリシー違反に関するコンテキストおよび情報を提供できます。さらに、侵入ルールエディタでルールのコメントの追加および表示を行うこともできます。
- **無効化** : [このルールを無効にする... (Disable this rule...)] をクリックして、ルールを無効にします。

このイベントが標準テキストルールによって生成された場合は、必要に応じてルールを無効にできます。ローカルで編集できるすべてのポリシーにルールを設定できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー (つまり、イベントを生成したポリシー) のみにルールを設定することもできます。

現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーを編集できますが、システムが提供するデフォルトポリシーは編集できません。

(注) パケットビューから共有オブジェクトルールを無効にしたり、デフォルトのポリシーでルールを無効にしたりすることは**できません**。

- **パケットのドロップ** : [このルールを設定してトリガーパケットをドロップ... (Set this rule to drop the triggering packet...)] をクリックして、トリガーするパケットをドロップするルールを設定します。

管理対象デバイスがネットワーク上でインライン展開されている場合、イベントをトリガーとして使用したルールを設定して、ローカルで編集できるすべてのポリシーでルールをトリガーするパケットをドロップできます。または、現在のポリシーをローカルで編集

できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーを編集できますが、システムが提供するデフォルトポリシーは編集できません。このオプションは[インラインの場合ドロップ (Drop when Inline)]が現在のポリシーで有効になっている場合のみ表示されることに注意してください。

- **編集**：標準テキストルールイベントの場合、[編集 (Edit)]をクリックして、イベントを生成したルールを編集します。イベントが、共有オブジェクトルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できません。

(注) システムによって提供された（カスタム標準テキストルールではない）ルールを編集する場合、実際には新規のローカルルールを作成していることになります。ローカルルールを設定して、イベントを生成し、現在の侵入ポリシーで元のルールを無効にしていることを確認してください。ただし、デフォルトのポリシーのローカルルールは有効に**できない**ことに注意してください。

- **イベントの生成**：[このルールを設定してイベントを生成... (Set this rule to generate events...)]をクリックして、イベントを生成するルールを設定します。

このイベントが標準テキストルールによって生成された場合は、ルールを設定して、ローカルで編集できるすべてのポリシーでイベントを生成できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーを編集できますが、システムが提供するデフォルトポリシーは編集できません。

(注) 共有オブジェクトルールでパケットビューからイベントを生成したり、デフォルトポリシーでルールを無効にしたりすることは**できません**。

- **抑制オプションの設定**：[パケットビュー内での抑制オプションの設定 \(2590ページ\)](#)の説明に従って、[抑制オプションの設定 (Set Suppression Options)]を展開し、続行します。

このオプションを使用して、ローカルで編集できるすべてのポリシーで、このイベントをトリガーとして使用したルールを抑制できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみでルールを制約することもできます。

現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーを編集できますが、シスコが提供するデフォルトポリシーは編集できません。

- **しきい値オプションの設定**：[パケットビュー内でのしきい値オプションの設定 \(2589ページ\)](#)の説明に従って、[しきい値オプションの設定 (Set Thresholding Options)]を展開し、続行します。

このオプションを使用して、ローカルで編集できるすべてのポリシーでも、これをトリガーとして使用したルールやしきい値を作成できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）でのみしきい値を作成することもできます。

現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーは編集できますが、システムが提供するデフォルトの侵入ポリシーは編集できません。

- ドキュメントの表示：標準テキストルールイベントの場合、[ドキュメントの表示 (View Documentation)] をクリックして、イベントを生成したルールリビジョンの説明を確認します。

### パケットビュー内でのしきい値オプションの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入イベントのパケットビューでしきい値オプションを設定することによって、ルールごとに時間の経過とともに生成されるイベントの数を制御できます。ローカルで編集できるすべてのポリシーに、またはローカルで編集できる場合は現在のポリシー（つまり、イベントを生成したポリシー）のみに、しきい値オプションを設定できます。

#### 手順

- ステップ 1** 侵入ルールによって生成された侵入イベントのパケットビュー内で、[イベント情報 (Event Information)] セクションの [アクション (Actions)] を展開します。
- ステップ 2** [しきい値オプションの設定 (Set Thresholding Options)] を展開し、次の2つの有効なオプションから1つを選択します。
  - 現在のポリシー (in the current policy)
  - ローカルで作成されたすべてのポリシー (in all locally created policies)
    - (注) 現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されます。たとえば、カスタムポリシーは編集できますが、システムが提供するデフォルトポリシーは編集できません。
- ステップ 3** 設定するしきい値のタイプを選択します。
  - 通知を期間ごとに指定したイベントインスタンスの数の数に制限する場合は、[制限 (limit)] をクリックします。

- 期間ごとに指定したイベント インスタンス数に達するたびに通知を行う場合は、[しきい値 (threshold) ]をクリックします。
- 指定されたイベント インスタンス数に達した後で、期間あたり 1 回ずつ通知を行う場合は、[両方 (Both) ]をクリックします。

- ステップ 4** 該当するオプション ボタンをクリックして、イベント インスタンスを [送信元 (Source) ] IP アドレスと [宛先 (Destination) ] IP アドレスのどちらかで追跡するかを指定します。
- ステップ 5** [カウント (Count) ] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。
- ステップ 6** [秒 (Seconds) ] フィールドに、イベント インスタンスを追跡する期間を指定する数 (1 ~ 86400) を入力します。
- ステップ 7** 既存の侵入ポリシーでこのルール現在のしきい値をオーバーライドする場合は、[このルールの既存の設定をオーバーライドする (Override any existing settings for this rule) ] チェックボックスをオンにします。
- ステップ 8** [しきい値の保存 (Save Thresholding) ] をクリックします。

## パケット ビュー内での抑制オプションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

抑制オプションを使用して、侵入イベントをまとめて、または送信元 IP アドレスまたは宛先 IP アドレスに基づいて抑制できます。ローカルで編集できるすべてのポリシーで抑制オプションを設定できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー (つまり、イベントを生成したポリシー) のみに抑制オプションを設定することもできます。

### 手順

- ステップ 1** 侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報 (Event Information) ] セクションの [アクション (Actions) ] を展開します。
- ステップ 2** [抑制オプションの設定 (Set Suppression Options) ] を展開し、次の 2 つの有効なオプションから 1 つを選択します。
- 現在のポリシー (in the current policy)
  - ローカルで作成されたすべてのポリシー (in all locally created policies)

(注) 現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されます。たとえば、カスタム ポリシーを編集できますが、シスコが提供するデフォルトポリシーは編集できません。

**ステップ 3** 次のいずれかの [追跡対象 (Track By)] オプションを選択します。

- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元 (Source)] をクリックします。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先 (Destination)] をクリックします。
- このイベントをトリガーしたルールのイベントを完全に抑制する場合は、[ルール (Rule)] をクリックします。

**ステップ 4** [IP アドレス (IP address)] または [CIDR ブロック (CIDR block)] フィールドに、送信元または宛先 IP アドレスとして指定する IP アドレスまたは CIDR ブロック/プレフィクス長を入力します。

**ステップ 5** [抑制の保存 (Save Suppression)] をクリックします。

---

#### 関連トピック

[Firepower システムの IP アドレス表記法 \(14 ページ\)](#)

## フレーム情報のフィールド

パケット ビューで、[フレーム (Frame)] の横にある矢印をクリックして、キャプチャされたフレームに関する情報を表示します。パケットビューには単一フレームまたは複数フレームを表示できます。各フレームには、個々のネットワークパケットに関する情報が表示されます。たとえば、タグ付きパケットまたは再構成された TCP ストリーム内のパケットの場合、複数のフレームが表示されます。

#### フレーム $n$ (Frame $n$ )

キャプチャされたフレーム。 $n$  は単一フレームパケットの場合は 1、複数フレームパケットの場合は差分フレーム番号です。フレーム内のキャプチャされたバイト数はフレーム番号に追加されます。

#### 到着時間 (Arrival Time)

フレームがキャプチャされた日時。

#### キャプチャ済みのフレームの時間デルタ (Time delta from previous captured frame)

複数フレームパケットの場合、前のフレームがキャプチャされてからの経過時間。

#### 表示済みのフレームの時間デルタ (Time delta from previous displayed frame)

複数フレームパケットの場合、前のフレームが表示されてからの経過時間。

#### 参照以降または先頭フレームからの時間 (Time since reference or first frame)

複数フレームパケットの場合、最初のフレームがキャプチャされてからの経過時間。

**フレーム番号 (Frame Number)**

増分フレーム番号。

**フレーム長 (Frame Length)**

フレームの長さ (バイト単位)。

**キャプチャ長 (Capture Length)**

キャプチャされたフレームの長さ (バイト単位)。

**フレームのマーク付け (Frame is marked)**

フレームがマークされているかどうか (true または false)。

**フレームのプロトコル (Protocols in frame)**

フレームに含まれるプロトコル。

**関連トピック**

[tag キーワード \(1801 ページ\)](#)

[TCP ストリームの再構成 \(1973 ページ\)](#)

## データリンク層情報フィールド

パケットビューで、データリンク層プロトコル (たとえば、[イーサネット II (Ethernet II)] ) の横にある矢印をクリックして、パケットに関するデータリンク層情報を表示します。これには、送信元ホストおよび宛先ホストの 48 ビットの Media Access Control (MAC) アドレスが含まれます。ハードウェアプロトコルに応じて、パケットに関する他の情報も表示されることがあります。



(注) この例では、イーサネットリンク層情報について説明していることに注意してください。他のプロトコルも表示されることがあります。

パケットビューはデータリンク層で使用されるプロトコルを反映します。次のリストでは、パケットビューでイーサネット II または IEEE 802.3 イーサネット パケットについて参照できる情報について説明します。

**【接続先 (Destination)】**

宛先ホストの MAC アドレス。



(注) イーサネットは、宛先アドレスとしてマルチキャストおよびブロードキャストアドレスを使用することもできます。

**ソース (Source)**

送信元ホストの MAC アドレス。

**タイプ (Type)**

イーサネット II パケットの場合、イーサネットフレームでカプセル化されるパケットの種類。たとえば、IPv6 または ARP データグラム。この項目はイーサネット II パケットの場合にのみ表示されることに注意してください。

**長さ (Length)**

IEEE 802.3 イーサネットパケットの場合、チェックサムを含まないパケットのトータル長 (バイト単位)。この項目は IEEE 802.3 イーサネットパケットの場合にのみ表示されることに注意してください。

**ネットワーク層情報の表示**

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

**手順**

パケットビューで、パケットにネットワーク層プロトコル (たとえば、[インターネットプロトコル (Internet Protocol) ]) の横にある矢印をクリックして、パケットに関連したネットワーク層の情報の詳細情報を表示します。

(注) この例では、IP パケットについて説明していることに注意してください。他のプロトコルも表示されることがあります。

**IPv4 ネットワーク層の情報フィールド**

以下のリストは、IPv4 パケットで表示される可能性があるプロトコル固有の情報の説明です。

**バージョン (Version)**

インターネットプロトコルのバージョン番号。

**ヘッダー長 (Header Length)**

すべての IP オプションを含む、ヘッダーのバイト数。オプションのない IP ヘッダーの長さは 20 バイトです。

### 差別化サービス (Differentiated Services) フィールド

送信元ホストが明示的輻輳通知 (ECN) サポートする方法を示す次の差別化サービスの値。

- 0x0 : ECN-Capable Transport (ECT) をサポートしません
- 0x1 および 0x2 : ECT をサポートします
- 0x3 : Congestion Experienced (CE)

### トータル長 (Total Length)

IP ヘッダーを差し引いた IP パケットの長さ (バイト単位)。

### ID

送信元ホストから送信される IP データグラムを一意に識別する値。この値は同じデータグラムフラグメントをトレースするために使用されます。

### フラグ (Flags)

IP フラグメンテーションを制御する値。

[最終フラグメント (Last Fragment) ] フラグの値は、データグラムに関連付けられた追加のフラグメントが存在するかどうかを次のように示します。

- 0 : データグラムに関連付けられた追加のフラグメントは存在しない
- 1 : データグラムに関連付けられた追加のフラグメントが存在する

[フラグメント化しない (Don't Fragment) ] フラグの値は、データグラムをフラグメント化できるかどうかを次のように制御します。

- 0 : データグラムをフラグメント化できる
- 1 : データグラムをフラグメント化してはならない

### フラグメントオフセット (Fragment Offset)

データグラムの先頭からのフラグメント オフセットの値。

### 存続時間 (ttl) (Time to Live (ttl))

データグラムが期限切れになる前にデータグラムがルータ間で作成できるホップの残数。

### プロトコル

IP データグラムにカプセル化されるトランスポート プロトコル。たとえば、ICMP、IGMP、TCP、または UDP。



### ヘッダー チェックサム (Header Checksum)

IP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損したか、侵入回避の試行において使用中である可能性があります。

### 送信元/宛先 (Source/Destination)

送信元 (または宛先) ホストの IP アドレスまたはドメイン名。

ドメイン名を表示するには、IP アドレス解決を有効にする必要があることに注意してください。

アドレスまたはドメイン名をクリックしてコンテキストメニューを表示してから、whois 検索を実行する場合は [Whois] を、ホスト情報を表示する場合は [ホストプロファイルの表示 (View Host Profile)] を、アドレスをグローバルブラックリストまたはホワイトリストに追加する場合は [今すぐブラックリスト化する (Blacklist Now)] または [今すぐホワイトリスト化する (Whitelist Now)] を選択します。

## IPv6 ネットワーク層の情報フィールド

以下のリストは、IPv6 パケットで表示される可能性があるプロトコル固有の情報の説明です。

### トラフィック クラス (Traffic Class)

IPv4 で提供される差別化サービス機能と同じように、IPv6 パケット クラスまたは優先度を特定する IPv6 見出し内の Experimental 8 ビットのフィールド。未使用の場合、このフィールドはゼロに設定されます。

### フロー ラベル (Flow Label)

非デフォルトの QoS またはリアルタイム サービスなどの特別なフローを特定する、1 から FFFF までの、オプションの 20 ビットの IPv6 16 進数値。未使用の場合、このフィールドはゼロに設定されます。

### ペイロード長 (Payload Length)

IPv6 ペイロードのオクテットの数を特定する 16 ビット フィールド。これは、任意の拡張子見出しを含む、IPv6 見出しに続くすべてのパケットで構成されます。

### 次ヘッダー (Next Header)

IPv4 プロトコル フィールドと同じ値を使用して、IPv6 見出しのすぐ後に続く、見出しの種類を特定する 8 ビットのフィールド。

### ホップ リミット (Hop Limit)

パケットを転送するノードごとに 1 つずつデクリメントする 8 ビットの 10 進整数。デクリメントした値がゼロになると、パケットは破棄されます。

**ソース (Source)**

送信元ホストの 128 ビットの IPv6 アドレス。

**【接続先 (Destination)】**

宛先ホストの 128 ビットの IPv6 アドレス。

## トランスポート層情報の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

## 手順

- 
- ステップ 1** パケットビューで、トランスポート層プロトコル (たとえば[TCP]、[UDP]、または[ICMP]) の横にある矢印をクリックします。
- ステップ 2** オプションで、存在する場合、[データ (Data)] をクリックして、パケットビューの [パケット情報 (Packet Information)] セクションで、プロトコルのすぐ上にあるペイロードの最初の 24 バイトを表示します。
- ステップ 3** [TCP パケットビューのフィールド \(2596 ページ\)](#)、[UDP パケットビューのフィールド \(2597 ページ\)](#)、または[ICMP パケットビューフィールド \(2598 ページ\)](#) の説明に従って、TCP、UDP、ICMP プロトコルのトランスポート層の内容を表示します。

(注) これらの例では、TCP、UDP、ICMP パケットについて説明していますが、他のプロトコルも表示されることがあることに注意してください。

---

## TCP パケットビューのフィールド

ここでは、TCP パケットのプロトコル固有の情報について説明します。

**ソースポート**

発信元のアプリケーションプロトコルを識別する番号。

**接続先ポート (Destination port)**

受信側のアプリケーションプロトコルを識別する番号。

**シーケンス番号 (Sequence number)**

TCP ストリームの初期シーケンス番号と連動する、現在の TCP セグメントの最初のバイトの値。

**次のシーケンス番号 (Next sequence number)**

応答パケットにおける、送信する次のパケットのシーケンス番号。

**確認応答番号 (Acknowledgement number)**

以前に受信されたデータのシーケンス番号に連動した TCP 確認応答。

**ヘッダー長 (Header Length)**

ヘッダーのバイト数。

**フラグ (Flags)**

TCP セグメントの伝送状態を示す 6 ビット。

- U: 緊急ポインタが有効
- A: 確認応答番号が有効
- P: 受信者はデータをプッシュする必要がある
- R: 接続をリセットする
- S: シーケンス番号を同期して新しい接続を開始する
- F: 送信者はデータ送信を終了した

**ウィンドウ サイズ (Window size)**

受信ホストが受け入れる、確認応答されていないデータの量 (バイト単位)。

**チェックサム (Checksum)**

TCP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損したか、回避の試行において使用中である可能性があります。

**緊急ポインタ (Urgent Pointer)**

緊急データが終了する TCP セグメントの位置 (存在する場合)。U フラグとともに使用します。

**オプション (Options)**

TCP オプションの値 (存在する場合)。

**UDP パケット ビューのフィールド**

ここでは、UDP パケットのプロトコル固有の情報について説明します。

**ソース ポート**

発信元のアプリケーションプロトコルを識別する番号。

**接続先ポート (Destination port)**

受信側のアプリケーション プロトコルを識別する番号。

**長さ (Length)**

UDP ヘッダーとデータを組み合わせた長さ。

**チェックサム (Checksum)**

UDP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損した可能性があります。

**ICMP パケット ビュー フィールド**

ここでは、ICMP パケットのプロトコル固有の情報について説明します。

**タイプ (Type)**

ICMP メッセージのタイプ。

- 0 : エコー応答
- 3 : 宛先到達不能
- 4 : ソース クエンチ (始点抑制要求)
- 5 : リダイレクト
- 8 : エコー要求
- 9 : ルータ アドバタイズメント
- 10 : ルータ送信要求
- 11 : 時間超過
- 12 : パラメータの問題
- 13 : タイムスタンプ要求
- 14 : タイムスタンプ応答
- 15 : 情報要求 (廃止)
- 16 : 情報応答 (廃止)
- 17 : アドレス マスク要求
- 18 : アドレス マスク応答

**コード (Code)**

ICMP メッセージタイプに付随するコード。ICMP メッセージタイプ 3、5、11、および 12 には、RFC 792 で説明されている対応コードがあります。

### チェックサム (Checksum)

ICMP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損した可能性があります。

## パケットバイト情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

### 手順

パケットビューで、[パケットバイト (Packet Bytes)] の横にある矢印をクリックして、パケットを構成するバイトの 16 進数および ASCII バージョンを表示します。システムがトラフィックを復号化した場合は、復号化されたパケットバイトを表示できます。

## 侵入イベントのクリップボード

クリップボードは、任意の侵入イベントビューから侵入イベントをコピーできる保存エリアです。

クリップボードの内容は、イベントが生成された日特別にソートされます。クリップボードに侵入イベントを追加した後、クリップボードからそれらを削除することも、クリップボードの内容のレポートを生成することもできます。

クリップボードの侵入イベントをインシデントに追加することもできます。インシデントとは、セキュリティポリシーの違反の可能性に関係していると思われるイベントのコンパイルです。

### 関連トピック

[侵入イベント ワークフローの使用 \(2577 ページ\)](#)

[侵入イベント パケット ビューの使用 \(2581 ページ\)](#)

[インシデントの作成 \(2410 ページ\)](#)

## クリップボードのレポートの生成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

任意のイベントビューで行うのと同じように、クリップボードのイベントに関するレポートを生成できます。

#### 始める前に

- クリップボードに1つ以上のイベントを追加します。詳細については、[侵入イベントワークフローの使用 \(2577ページ\)](#) または [侵入イベントパケットビューの使用 \(2581ページ\)](#) を参照してください。

#### 手順

**ステップ 1** [分析 (Analysis)] > [侵入 (Intrusions)] > [クリップボード (Clipboard)] を選択します。

**ステップ 2** 次の選択肢があります。

- クリップボード上のページの特定のイベントを含めるには、そのページに移動し、イベントの横にあるチェックボックスをオンにして、[レポートの生成 (Generate Report)] をクリックします。
- クリップボードのすべてのイベントを含めるには、[すべてのレポートの生成 (Generate Report All)] をクリックします。

**ステップ 3** レポートの表示方法を指定して、[生成 (Generate)] をクリックします。

**ステップ 4** 1つ以上の出力形式を選択し、オプションで、他の設定を変更します。

**ステップ 5** [生成 (Generate)] をクリックしてから、[はい (Yes)] をクリックします。

**ステップ 6** 次の選択肢があります。

- レポートリンクをクリックして、新しいウィンドウにレポートを表示します。
- [OK] をクリックして、レポートのデザインを変更できる [レポートテンプレート (Report Templates)] ページに戻ります。

#### 関連トピック

[レポートテンプレート \(2307 ページ\)](#)

## クリップボードからのイベントの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

インシデントに追加したくない侵入イベントがクリップボード上にある場合は、そのイベントを削除できます。



- (注) クリップボードからイベントを削除しても、イベントデータベースからイベントは削除されません。ただし、イベントデータベースからイベントを削除すると、イベントはクリップボードから削除されます。

#### 手順

**ステップ 1** [分析 (Analysis)] > [侵入 (Intrusions)] > [クリップボード (Clipboard)] を選択します。

**ステップ 2** 次の選択肢があります。

- クリップボードのページの特定の侵入イベントを削除するには、そのページに移動し、イベントの横にあるチェックボックスを選択し、[削除 (Delete)] をクリックします。
- クリップボードからすべての侵入イベントを削除するには、[すべて削除 (Delete All)] をクリックします。[イベント設定 (Event Preferences)] で [全てのアクションを確認 (Confirm All Actions)] オプションを選択した場合、最初にすべてのイベントを削除するかどうかを確認するプロンプトが出されることに注意してください。

## 侵入イベントの統計情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

[侵入イベントの統計情報 (Intrusion Event Statistics)] ページは、アプライアンスの現在の状態の概要と、ネットワークで生成されたすべての侵入イベントを表示します。

このページに表示される IP アドレス、ポート、プロトコル、イベントメッセージなどはそれぞれリンクになっています。関連イベントの情報を表示するには、任意のリンクをクリックします。たとえば、上位 10 個の宛先ポートのいずれかが 80 (http) /tcp である場合、そのリンクをクリックすると、デフォルトの侵入イベントワークフローの最初のページが表示され、そのポートをターゲットとするイベントがリストされます。現在の時刻範囲で表示されるのはイベント (およびイベントを生成する管理対象デバイス) のみであることに注意してください。さらに、確認済みマークを付けた侵入イベントも統計に引き続き表示されます。たとえば、現在の時刻範囲が過去 1 時間であり、最初のイベントが 5 時間前に生成された場合、[最初のイベント (First Event)] リンクをクリックすると、そのイベントは時刻範囲を変更するまでイベント ページには表示されません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

## 手順

- ステップ1 [概要 (Overview)] > [概要 (Summary)] > [侵入イベント統計 (Intrusion Event Statistics)] を選択します。
- ステップ2 ページの上部にある2つの選択ボックスから、統計を表示するゾーンおよびデバイスを選択するか、[すべてのセキュリティゾーン (All Security Zones)] および [すべてのデバイス (All Devices)] を選択して、侵入イベントを収集するすべてのデバイスの統計を表示します。
- ステップ3 [統計の取得 (Get Statistics)] をクリックします。

ヒント カスタム時刻範囲からデータを表示するには、右上のページエリアのリンクをクリックし、[時間枠の変更 \(2455 ページ\)](#) にある指示に従います。

## ホスト統計情報

[侵入イベント統計情報 (Intrusion Event Statistics)] ページの [ホスト統計情報 (Host Statistics)] セクションは、アプライアンス自体に関する情報を提供します。Firepower Management Center では、このセクションはすべての管理対象デバイスに関する情報も提供します。

この情報には、次の内容が含まれます。

### 時刻 (Time)

アプライアンスの現在の時刻。

### アップタイム (Uptime)

アプライアンス自体が再起動してから経過した日数、時間、および分数。Firepower Management Center では、[アップタイム (Uptime)] に各管理対象デバイスの最終起動時刻、ログインしたユーザの数、および負荷平均も示されます。

### ディスク使用率 (Disk Usage)

使用中のディスクの割合。

### メモリ使用率 (Memory Usage)

使用中のシステムメモリの割合。

### 負荷平均 (Load Average)

直前の1分間、5分間、15分間のCPUキュー内の平均プロセス数。

## イベントの概要

[侵入イベント統計 (Intrusion Event Statistics)] ページの [イベントの概要 (Event Overview)] セクションは、侵入イベントデータベースにある情報の概要を示します。

これらの統計には、次の情報が含まれています。



## イベント

侵入イベント データベースのイベントの数。

### 時間範囲内のイベント (Events in Time Range)

現在選択されている時間範囲と、時間範囲内に収まるデータベースのイベントの割合。

### 最初のイベント (First Event)

イベント データベース内の最初のイベントのイベント メッセージ。

### 最後のイベント (Last Event)

イベント データベース内の最後のイベントのイベント メッセージ。



(注) Firepower Management Center で侵入イベントデータを表示中に管理対象デバイスを選択した場合は、そのデバイスの [イベントの概要 (Event Overview)] セクションが代わりに表示されます。

## イベント統計

[侵入イベント統計 (Intrusion Event Statistics)] ページの [イベント統計 (Event Statistics)] セクションでは、侵入イベント データベース内の情報に関する具体的な情報が表示されます。

この情報には、次に関する詳細が含まれます。

- 上位 10 個のイベント タイプ
- 上位 10 個の送信元 IP アドレス
- 上位 10 個の宛先 IP アドレス
- 上位 10 個の宛先ポート
- イベント数が最大であるプロトコル、イングレスとイーグレスのセキュリティゾーン、およびデバイス



(注) マルチドメイン展開では、システムは、各リーフ ドメインに個別のネットワーク マップを作成します。その結果、リーフ ドメインには、ネットワーク内で一意である IP アドレスを含めることができますが、別のリーフ ドメイン内の IP アドレスと同じにすることができます。先祖ドメインでイベントの統計情報を表示すると、システムで、その IP アドレスの複数のインスタンスが繰り返し表示される場合があります。一見すると、エントリが重複しているように見えることがあります。ただし、各 IP アドレスのホストプロファイル情報までドリルダウンすると、それらが異なるリーフ ドメインに属していることがわかります。

## 侵入イベントのパフォーマンス グラフの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

[侵入イベントのパフォーマンス (Intrusion Event Performance) ] ページでは、Firepower Management Center または管理対象デバイスの指定された期間の侵入イベントのパフォーマンス統計情報を示すグラフを生成できます。グラフを生成することにより、1秒あたりの侵入イベントの数、1秒あたりのメガビット数、1パケットあたりの平均バイト数、Snort によって検査されていないパケットの割合、および TCP 正規化の結果としてブロックされたパケットの数を反映できます。これらのグラフは、過去1時間、前日、先週、または先月の操作の統計を表示できます。



(注) 新しいデータは5分ごとに統計グラフに蓄積されます。したがって、グラフをすばやくリロードしても、次の5分の差分更新が実行されるまでデータは変更されていない場合があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

- ステップ 1 [概要 (Overview) ] > [概要 (Summary) ] > [侵入イベント パフォーマンス (Intrusion Event Performance) ] を選択します。
- ステップ 2 [デバイスの選択 (Select Device) ] リストから、データを表示するデバイスを選択します。
- ステップ 3 [侵入イベントのパフォーマンス統計情報グラフの種類 \(2604 ページ\)](#) で説明されているように、[グラフの選択 (Select Graph(s)) ] リストから、作成するグラフの種類を選択します。
- ステップ 4 [時間範囲の選択 (Select Time Range) ] リストから、グラフに使用する時間範囲を選択します。
- ステップ 5 [グラフ (Graph) ] をクリックします。
- ステップ 6 グラフを保存するには、グラフを右クリックし、ブラウザでイメージを保存する手順に従います。

## 侵入イベントのパフォーマンス統計情報グラフの種類

次の表に、表示可能なグラフの種類を示します。ネットワーク分析ポリシーの [インラインモード (Inline Mode) ] 設定の影響を受けるデータを含むグラフ タイプでは、表示が異なるので注意してください。[インラインモード (Inline Mode) ] が無効になっている場合、Web イン

ターフェイスでアスタリスク (\*) が付いているグラフタイプ (下記の表では列に[はい (yes)] と記載) には、[インライン モード (Inline Mode)] が有効になっている場合に変更またはドロップされるトラフィックに関するデータが含まれています。

表 297: 侵入イベントのパフォーマンス グラフの種類

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
平均バイト/パケット	適用対象外	各パケットに含まれる平均バイト数。	No
TCP トラフィックまたはパケットで正規化された ECN フラグ	[明示的輻輳通知 (Explicit Congestion Notification)] を有効にして、[パケット (Packet)] を選択します。	ネゴシエーションに関係なく、パケット単位で ECN フラグがクリアされたパケットの数。	Yes
TCP トラフィックまたはセッションで正規化された ECN フラグ	[明示的輻輳通知 (Explicit Congestion Notification)] を有効にして、[ストリーム (Stream)] を選択します。	ECN の使用がネゴシエーションされなかった場合にストリーム単位で ECN フラグがクリアされた回数。	Yes
イベント/秒	適用対象外	デバイスで生成された 1 秒あたりのイベント数。	No
ICMPv4 エコーの正規化	[ICMPv4 の正規化 (Normalize ICMPv4)] を有効にします。	エコー (要求) またはエコー応答メッセージの 8 ビットコードフィールドがクリアされた ICMPv4 パケットの数。	Yes
ICMPv6 エコーの正規化	[ICMPv6 の正規化 (Normalize ICMPv6)] を有効にします。	エコー (要求) またはエコー応答メッセージの 8 ビットコードフィールドがクリアされた ICMPv6 パケットの数。	Yes
IPv4 DF フラグの正規化	[IPv4 の正規化 (Normalize IPv4)] と [DF ビットの正規化 (Normalize Don't Fragment Bit)] を有効にします。	[IPv4 フラグ (IPv4 Flags)] ヘッダー フィールドのシングルビット [フラグメント禁止 (Don't Fragment)] サブフィールドがクリアされた IPv4 パケットの数。	Yes
IPv4 オプションの正規化	[IPv4 の正規化 (Normalize IPv4)] を有効にします。	オプション オクテットが 1 (No Operation) に設定された IPv4 パケットの数。	Yes

## 侵入イベントのパフォーマンス統計情報グラフの種類

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
IPv4 予約済みフラグの正規化	[IPv4 の正規化 (Normalize IPv4) ]と [予約済みビットの正規化 (Normalize Reserved Bit) ]を有効にします。	[IPv4 フラグ (IPv4 Flags) ]ヘッダー フィールドのシングルビット [予約済み (Reserved) ]サブフィールドがクリアされた IPv4 パケットの数。	Yes
IPv4 サイズ変更の正規化	[IPv4 の正規化 (Normalize IPv4) ]を有効にします。	超過ペイロードが IP ヘッダーで指定されたデータグラム長に切り詰められた IPv4 パケットの数。	Yes
IPv4 TOS の正規化	[IPv4 の正規化 (Normalize IPv4) ]と [TOS ビットの正規化 (Normalize TOS Bit) ]を有効にします。	1 バイトの [差別化サービス (DS) (Differentiated Services (DS)) ]フィールド (旧 [タイプ オブ サービス (ToS) (Type of Service (TOS)) ]フィールド) がクリアされた IPv4 パケットの数。	Yes
IPv4 TTL の正規化	[IPv4 の正規化 (Normalize IPv4) ]、[最大 TTL (Maximum TTL) ]、および [TTLのリセット (Reset TTL) ]を有効にします。	IPv4 存続時間 (TTL) 正規化の数。	Yes
IPv6 オプションの正規化	[IPv6 の正規化 (Normalize IPv6) ]を有効にします。	[ホップバイホップオプション (Hop-by-Hop Options) ]または [宛先オプション (Destination Options) ]拡張ヘッダーの [オプションタイプ (Option Type) ]フィールドが、00 (スキップして処理を続行) に設定された IPv6 パケットの数。	Yes
IPv6 TTL の正規化	[IPv6 の正規化 (Normalize IPv6) ]、[最小 TTL (Minimum TTL) ]、および [TTLのリセット (Reset TTL) ]を有効にします。	IPv6 ホップリミット (TTL) 正規化の数。	Yes

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
メガビット/秒	適用対象外	デバイスをパススルーするトラフィックの1秒あたりのメガビット数。	No
MSS に合わせてサイズ変更されたパケットの正規化	[データを MSS にトリミング (Trim Data to MSS) ] を有効にします。	ペイロードが TCP データフィールドよりも長かったために、ペイロードが最大セグメントサイズに切り詰められたパケットの数。	Yes
TCP ウィンドウに合わせてサイズ変更されたパケットの正規化	[データをウィンドウにトリミング (Trim Data to Window) ] を有効にします。	受信側ホストの TCP ウィンドウに合わせて TCP データフィールドが切り詰められたパケットの数。	Yes
ドロップされたパケットの割合	適用対象外	選択されたすべてのデバイスにおける未検査のパケットの平均パーセンテージ。たとえば、2つのデバイスを選択した場合、平均が 50% であるというのは、1つのデバイスのドロップ率が 90% であり、もう1つのデバイスのドロップ率が 10% であることを示している可能性があります。また、両方のデバイスのドロップ率が 50% である可能性もあります。グラフは、1つのデバイスを選択した場合にのみ合計ドロップ率を表します。	No
データストリップが適用された RST パケットの正規化	[RST に関するデータを削除 (Remove Data on RST) ] を有効にします。	TCP リセット (RST) パケットからデータが削除されたパケットの数。	Yes
データストリップが適用された SYN パケットの正規化	[SYN に関するデータを削除 (Remove Data on SYN) ] を有効にします。	TCP オペレーティングシステムが Mac OS でない場合に、SYN パケットからデータが削除されたパケットの数。	Yes

■ 侵入イベントのパフォーマンス統計情報グラフの種類

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
TCP ヘッダーパディングの正規化	[オプションパディングバイトの正規化またはクリア (Normalize/Clear Option Padding Bytes)] を有効にします。	オプションのパディングバイトが 0 に設定された TCP パケットの数。	Yes
TCP オプションなしの正規化	[これらの TCP オプションを許可 (Allow These TCP Options)] を有効にして、[任意 (any)] 以外のオプションに設定します。	タイムスタンプオプションがストリップされたパケットの数。	Yes
TCP NS フラグの正規化	[明示的輻輳通知 (Explicit Congestion Notification)] を有効にして、[パケット (Packet)] を選択します。	ECN Nonce Sum (NS) オプション正規化の数。	Yes
TCP オプションの正規化	[これらの TCP オプションを許可 (Allow These TCP Options)] を有効にして、[任意 (any)] 以外のオプションに設定します。	オプションフィールドが No Operation (TCP オプション 1) に設定されているオプションの数 (MSS、ウィンドウスケール、タイムスタンプ、および明示的に許可されたオプションを除く)。	Yes
正規化によってブロックされた TCP パケット	[TCP ペイロードの正規化 (Normalize TCP Payload)] を有効にします (セグメントのリアセンブリは失敗します)。	TCP セグメントを正常にリアセンブルできなかったためにドロップされたパケットの数。	Yes
TCP 予約済みフラグの正規化	[予約済みビットの正規化またはクリア (Normalize/Clear Reserved Bits)] を有効にします。	予約済みビットがクリアされた TCP パケットの数。	Yes
TCP セグメントリアセンブルの正規化	[TCP ペイロードの正規化 (Normalize TCP Payload)] を有効にします (セグメントのリアセンブリは成功します)。	再送信データの一貫性を確保するために TCP データフィールドが正規化されたパケットの数 (正しくリアセンブルできないセグメントはすべてドロップされます)。	Yes

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
TCP SYN オプションの正規化	[これらの TCP オプションを許可 (Allow These TCP Options) ]を有効にして、[任意 (any) ] 以外のオプションに設定します。	SYN 制御ビットが設定されていないため、最大セグメントサイズまたはウィンドウスケール オプションが No Operation (TCP オプション 1) に設定されたオプションの数。	Yes
TCP タイムスタンプ ECR の正規化	[これらの TCP オプションを許可 (Allow These TCP Options) ]を有効にして、[任意 (any) ] 以外のオプションに設定します。	確認応答 (ACK) 制御ビットが設定されていないために、タイムスタンプ エコー応答 (TSectr) オプションフィールドがクリアされたパケットの数。	Yes
TCP 緊急ポインタの正規化	[緊急ポインタの正規化 (Normalize Urgent Pointer) ]を有効にします。	TCP ヘッダーの [緊急ポインタ (Urgent Pointer) ]フィールド (2バイト) がペイロード長を超えていたため、ペイロード長に合わせて設定されたパケットの数。	Yes
ブロックされたパケットの総数	[インラインモード (Inline Mode) ]または [インライン時にドロップ (Drop when Inline) ]を設定します。	ルール、デコーダ、およびプリプロセッサのドロップを含む、ドロップされたパケットの総数。	No
インジェクトされたパケットの総数	[インラインモード (Inline Mode) ]を設定します。	再送信前にサイズ変更されたパケットの数。	No
TCP フィルタ適用パケットの総数	TCP ストリームの前処理を設定します。	TCP ポートフィルタリングのためにストリームによってスキップされたパケットの数。	No
UDP フィルタ適用パケットの総数	UDP ストリームの前処理を設定します。	UDP ポートフィルタリングのためにストリームによってスキップされたパケットの数。	No

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
緊急フラグ クリア済みの正規化	[緊急ポインタが設定されていない場合 URG をクリア (Clear URG if Urgent Pointer is Not Set) ] を有効にします。	緊急ポインタが設定されていないために、TCP ヘッダーの URG 制御ビットがクリアされたパケットの数。	Yes
緊急ポインタおよび緊急フラグ クリア済みの正規化	[空のペイロードに設定された緊急ポインタまたは URG をクリア (Clear Urgent Pointer/URG on Empty Payload) ] を有効にします。	ペイロードがなかったために、TCP ヘッダーの緊急ポインタフィールドと URG 制御ビットがクリアされたパケットの数。	Yes
緊急ポインタ クリア済みの正規化	[URG=0 の場合に緊急ポインタをクリア (Clear Urgent Pointer if URG=0) ] を有効にします。	緊急 (URG) 制御ビットが設定されていないために、TCP ヘッダーの [緊急ポインタ (Urgent Pointer) ] フィールド (16 ビット) がクリアされたパケットの数。	Yes

#### 関連トピック

[インライン正規化プリプロセッサ \(1951 ページ\)](#)

[インライン導入でのプリプロセッサによるトラフィックの変更 \(1852 ページ\)](#)

[インライン展開でのドロップ動作 \(1615 ページ\)](#)

## 侵入イベントグラフの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

Firepower System は、経時的な侵入イベントの傾向を示すグラフを表示します。1 つまたはすべての管理対象デバイスについて、過去 1 時間から先月までの範囲の経時的な侵入イベントグラフを生成できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。



## 手順

---

- ステップ 1** [概要 (Overview) ] > [概要 (Summary) ] > [侵入イベントグラフ (Intrusion Event Graphs) ] を選択します。
- ステップ 2** [デバイスの選択 (Select Device) ] で、[すべて (all) ] を選択してすべてのデバイスを含めるか、グラフに含める特定のデバイスを選択します。
- ステップ 3** [グラフの選択 (Select Graph(s) ) ] で、生成するグラフの種類を選択します。
- 上位 10 個の宛先ポート
  - 上位 10 個の送信元 IP アドレス
  - 上位 10 個のイベント メッセージ
- ステップ 4** [時間範囲の選択 (Select Time Range) ] で、グラフの時間範囲を選択します。
- 直近の 1 時間 (Last Hour)
  - 前日 (Last Day)
  - 先週 (Last Week)
  - 先月 (Last Month)
- ステップ 5** [グラフ (Graph) ] をクリックします。
-





## 第 108 章

# ファイル/マルウェア イベントとネットワーク ファイル トラジェクトリ

次のトピックでは、ファイル/マルウェア イベント、ローカル マルウェア分析、動的分析、キャプチャされたファイル、およびネットワーク ファイル トラジェクトリの概要を示します。

- [ファイル イベント/マルウェア イベントとネットワーク ファイル トラジェクトリについて \(2613 ページ\)](#)
- [ファイルおよびマルウェア イベント \(2614 ページ\)](#)
- [ローカル マルウェア分析 \(Local Malware Analysis\) \(2632 ページ\)](#)
- [動的分析 \(Dynamic Analysis\) \(2633 ページ\)](#)
- [ファイル分析評価 \(2636 ページ\)](#)
- [キャプチャ ファイルとファイル ストレージ \(2639 ページ\)](#)
- [ネットワーク ファイル トラジェクトリ \(2648 ページ\)](#)

## ファイル イベント/マルウェア イベントとネットワーク ファイル トラジェクトリについて

マルウェアの影響を特定して軽減しやすくするため、Firepower システムのファイル制御、ネットワーク ファイル トラジェクトリ、および *AMP for Firepower* の各コンポーネントによって、アーカイブ ファイルの内のマルウェア ファイルとネストされたファイルを含むファイルの伝送を検出、追跡、キャプチャ、分析、ログ記録、および必要に応じてブロックできます。

また、システムを組織の *AMP for Endpoints* の展開に統合して、スキャン、マルウェア検出、および検疫のレコードと侵害の兆候 (IOC) をインポートできます。

コンテキスト エクスプローラ、およびレポート機能を使用すると、検出/キャプチャ/ブロックされたファイルとマルウェアについてより詳しく理解できます。また、イベントを使用して相関ポリシー違反をトリガーしたり、電子メール、SMTP、または syslog によるアラートを発行したりすることもできます。



- (注) Firepower システムでは、Unicode (UTF-8) 文字を使用するファイル名の表示および入力がサポートされます。ただし、Unicode のファイル名は PDF レポートに変換された形式で表示されます。また、SMB プロトコルによって、ファイル名の印刷不能な文字がピリオドに置き換えられます。

## ファイルおよびマルウェア イベント

Firepower Management Center は、さまざまなタイプのファイルおよびマルウェア イベントをログに記録できます。個々のイベントに関する情報は、イベントの生成方法と生成理由に応じて異なります。

- ファイル イベントとは、AMP for Firepower によって検出されたマルウェアを含むファイルを意味します。ファイル イベントには、AMP for Endpoints 関連のフィールドは含まれません。
- マルウェア イベントとは、AMP for Firepower または AMP for Endpoints によって検出されたマルウェアを意味します。また、マルウェア イベントは、スキャンや検疫など、AMP for Endpoints の導入からの脅威以外のデータを記録できます。
- レトロスペクティブ マルウェア イベントとは、性質（ファイルがマルウェアかどうか）が変更された、AMP for Firepower によって検出されたファイルを意味します。



- (注) AMP for Firepower によってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。エンドポイントベースのマルウェア イベントには、対応するファイル イベントはありません。

## ファイル イベントおよびマルウェア イベントの種類

### ファイル イベント

システムは、現在展開されているファイル ポリシーのルールに従って、管理対象デバイスがネットワークトラフィック内のファイルを検出またはブロックしたときに生成されたファイル イベントを記録します。

システムがファイル イベントを生成する際に、呼び出しを行うアクセス コントロール ルールのログ設定に関係なく、システムは Firepower Management Center データベースへの関連する接続の終わりも記録します。

## ネットワーク ベースのマルウェア イベント (AMP for Firepower)

システムは、全体的なアクセス コントロール設定の一環として、ネットワーク トラフィックのマルウェアを検出できます。AMP for Firepower は、結果として生じたイベントの性質や、いつどこでどのようにしてマルウェアが検出されたかに関するコンテキスト データを含むマルウェア イベントを生成できます。

表 298: AMP for Firepower でのマルウェア イベントの生成シナリオ

AMP for Firepower によるファイル検出時の動作	性質
AMPクラウドにファイルの性質についてクエリを行い (マルウェア クラウドルックアップを実行)、クエリに成功した場合	マルウェア、クリーン、または不明
AMP クラウドにクエリを行ったものの、接続を確立できないか、他の理由でクラウドが利用可能でない場合	応対不可 この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。
ファイルに関連付けられている脅威スコアが、ファイルを検出したファイル ポリシーで定義されたマルウェアしきい値の脅威スコアを超えた場合、またはローカルマルウェア分析でマルウェアが識別された場合	マルウェア
ファイルがカスタム検出リストに設定されている場合 (手動でマルウェアとしてマークされている場合)	カスタム検出
ファイルがクリーン リストに設定されている場合 (手動でクリーンとしてマークされている場合)	クリーン

## 遡及的マルウェア イベント (AMP for Firepower)

ネットワーク トラフィックで検出されたマルウェアの場合、性質が変わることがあります。たとえば、AMPクラウドによる判定の結果、以前はクリーンであると考えられていたファイルが今はマルウェアとして識別されるようになり、その逆、つまりマルウェアと識別されたファイルが実際にはクリーンであったりする可能性があります。先週クエリしたファイルの性質が変わると、AMPクラウドがシステムに通知します。その場合、以下の2つが行われます。

- Firepower Management Center が新しい遡及的マルウェア イベントを生成します。

この新しい遡及的マルウェア イベントは、前の週に検出された、同じ SHA-256 ハッシュ値を持つすべてのファイルの性質変更を表します。そのため、これらのイベントに含まれる情報は、Firepower Management Center に性質変更が通知された日時、新しい性質、ファイルの SHA-256 ハッシュ値、脅威名に限定されています。IP アドレスや他のコンテキスト情報は含まれません。

- Firepower Management Center は遡及的イベントに関連付けられた SHA-256 ハッシュ値を持つ、検出済みのファイルのファイル性質を変更します。

ファイルの性質が[マルウェア (Malware)]に変更されると、Firepower Management Center は新しいマルウェア イベントをデータベースに記録します。新しい性質を除き、この新しいマルウェア イベントの情報は、ファイルが最初に検出されたときに生成されたファイル イベントのものと同じです。

ファイルの性質が[クリーン (Clean)]に変更された場合、Firepower Management Center はそのマルウェア イベントを削除しません。代わりに、イベントに性質の変更が反映されます。つまり、マルウェア テーブルには性質が[クリーン (Clean)]のファイルが含まれることがあります。それはそのファイルが最初マルウェアと識別されていた場合だけです。マルウェアとして識別されたことのないファイルは、ファイルのテーブルにのみ含まれます。

## エンドポイントベースのマルウェア イベント (AMP for Endpoints)

組織で AMP for Endpoints を使用している場合は、個々のユーザがエンドポイントに軽量コネクタ (コンピュータおよびモバイルデバイス) を取り付けます。コネクタは、ファイルのアップロード、ダウンロード、実行、開く、コピー、移動などの操作を行う際にファイルを検査します。コネクタは AMP クラウドと通信して、検査対象のファイルにマルウェアが含まれるかどうかを判断します。

ファイルがマルウェアとして特定された場合、AMPクラウドは特定した脅威の情報を Firepower Management Center に送ります。さらに AMP クラウドは、スキャン、検疫、実行のブロッキング、クラウドリコールなど、他の種類のデータを Firepower Management Center に送信することもできます。Firepower Management Center はこれらの情報をマルウェア イベントとしてログに記録します。



- (注) エンドポイントベースのマルウェア イベントで報告される IP アドレスは、ネットワーク マップに (そして、モニタ対象ネットワークにも) 含まれない場合もあります。展開、コンプライアンスのレベル、およびその他の要因によっては、AMP for Endpoints によってモニタされる組織内のエンドポイントが、AMP for Firepower によってモニタされているものと同じホストではない可能性があります。

## ファイルおよびマルウェア イベントのワークフローの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

イベントビューアでは、テーブルにファイル イベントとマルウェア イベントを表示できます。分析に関連する情報に応じてイベントビューアを操作することができます。イベントにアクセスしたときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページで

す。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

## 手順

次のいずれかを実行します。

- [分析 (Analysis)] > [ファイル (Files)] > [ファイル イベント (File Events)]
- [分析 (Analysis)] > [ファイル (Files)] > [マルウェア イベント (Malware Events)]

**ヒント** イベントのテーブルビューでは、一部のフィールドがデフォルトで非表示にされています。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム (Disabled Columns)] の下のフィールド名をクリックします。

**ヒント** 特定のファイルが検出された接続をすぐに表示するには、イベントビューアーでチェック ボックスを使用してファイルを選択してから、[ジャンプ (Jump to)] ドロップダウンリストで [接続イベント (Connections Events)] を選択します。

## 関連トピック

- [ファイルおよびマルウェア イベント フィールド \(2617 ページ\)](#)
- [定義済みファイルのワークフロー \(2420 ページ\)](#)
- [定義済みマルウェアのワークフロー \(2420 ページ\)](#)
- [イベント ビュー設定の設定 \(37 ページ\)](#)

# ファイルおよびマルウェア イベント フィールド

ワークフローを使用して表示および検索できるマルウェア イベントには、このセクションにリストするフィールドがあります。個別のイベントで利用可能な情報は、いつ、どのように生成されたかによって異なることに注意してください。



- (注) AMP for Firepower によってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。エンドポイントベースのマルウェア イベントには、対応するファイル イベントはありません。また、ファイル イベントには AMP for Endpoints 関連のフィールドはありません。

## アクション (Action)

ファイルを検出したファイル ポリシー ルールに関連したアクション、および関連するファイル アクション オプション。

**AMP クラウド (AMP Cloud)**

AMP for Endpoints イベントが発信された AMP クラウドの名前。

**アプリケーション ファイル名 (Application File Name)**

AMP for Endpoints 検出が行われたときに、マルウェア ファイルにアクセスしていたクライアントアプリケーション。これらのアプリケーションはネットワーク検出またはアプリケーション制御とは関係ありません。

**アプリケーション ファイル SHA256 (Application File SHA256)**

検出が行われたときに、AMP for Endpoints で検出された、または隔離されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。

**アプリケーション プロトコル (Application Protocol)**

管理対象デバイスがファイルを検出したトラフィックで使用されるアプリケーションプロトコル。

**アプリケーション プロトコル カテゴリまたはタグ (Application Protocol Category or Tag)**

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

**アプリケーションのリスク (Application Risk)**

接続で検出されたアプリケーショントラフィックに関連付けられたリスク。「非常に高い (Very High)」、「高 (High)」、「中 (Medium)」、「低 (Low)」、「非常に低い (Very Low)」のいずれかとなります。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

**アーカイブ深度 (Archive Depth)**

アーカイブ ファイル内でファイルがネストされたレベル (存在する場合)。

**アーカイブ名 (Archive Name)**

マルウェアファイルが関連付けられているアーカイブファイル (存在する場合) の名前。アーカイブファイルの内容を表示するには、アーカイブファイルのイベントビューア行を右クリックしてコンテキストメニューを開き、[アーカイブコンテンツの表示 (View Archive Contents)] をクリックします。

**アーカイブ SHA256 (Archive SHA256)**

マルウェア ファイルが関連付けられているアーカイブ ファイル (存在する場合) の SHA-256 ハッシュ値。アーカイブ ファイルの内容を表示するには、アーカイブ ファイルのイベントビューア行を右クリックしてコンテキストメニューを開き、[アーカイブコンテンツの表示 (View Archive Contents)] をクリックします。



### ビジネスとの関連性 (Business Relevance)

接続で検出されたアプリケーショントラフィックに関連するビジネス関連性：Very High、High、Medium、Low、またはVery Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネス関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

### カテゴリ (Category) / ファイルタイプカテゴリ (File Type Category)

ファイルタイプの一般的なカテゴリ (Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコードファイル、グラフィック、システムファイルなど)。

### クライアント (Client)

1つのホストで実行され、ファイルを送信するためにサーバに依存するクライアントアプリケーション。

### クライアント カテゴリまたはタグ (Client Category or Tag)

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

### メンバー数 (Count)

複数の同じ行を作成する制約を適用した後の、各行の情報に一致するイベントの数。

### 検出名 (Detection Name)

検出されたマルウェアの名前。

### ディテクタ (Detector)

マルウェアを識別した AMP for Endpoints ディテクタ (ClamAV、Spero、SHA など)。

### Device

ファイル イベントおよびネットワークベースのマルウェア イベントの場合、ファイルを検出したデバイスの名前。

エンドポイントベースのマルウェア イベントおよび AMP クラウドによって生成される遡及的マルウェア イベントの場合、Firepower Management Center の名前。

### 傾向 (Disposition) / ファイル性質 (File Disposition)

ファイルの性質：

### マルウェア (Malware)

AMP クラウドでそのファイルがマルウェアとして分類された、ローカルマルウェア分析でマルウェアとして識別された、またはファイルポリシーで定義されたマルウェアしきい値をファイルの脅威スコアが超えたことを示します。

### クリーン (Clean)

AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。クリーンのファイルがマルウェア テーブルに含められるのは、そのファイルがクリーンに変更された場合だけです。

### 不明

システムが AMP クラウドに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、AMPクラウドがファイルを正しく分類していませんでした。

### カスタム検出 (Custom Detection)

ユーザがカスタム検出リストにファイルを追加したことを示します。

### 対応不可 (Unavailable)

システムがAMPクラウドに問い合わせできなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。

### 該当なし

[ファイル検出 (Detect Files) ] または [ファイルブロック (Block Files) ] ルールがファイルを処理し、Firepower Management Center が AMP クラウドに問い合わせなかったことを示します。

ファイル性質は、システムが AMP クラウドに問い合わせたファイルでのみ表示されます。

### ドメイン (Domain)

ファイル イベント および ネットワークベースのマルウェア イベントの場合、ファイルを検出したデバイスのドメイン。エンドポイントベースのマルウェア イベント および AMP クラウドによって生成される遡及的マルウェア イベントの場合、イベントを報告した AMP クラウド接続に関連付けられたドメイン。

このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

### イベント サブタイプ (Event Subtype)

マルウェア検出につながった AMP for Endpoints アクション ([作成 (Create) ]、[実行 (Execute) ]、[移動 (Move) ]、[スキャン (Scan) ] など)。

### イベント タイプ (Event Type)

マルウェア イベントのサブタイプ。

### ファイル名 (File Name)

マルウェア ファイルの名前。

**ファイルパス (File Path)**

AMP for Endpoints によって検出されたマルウェア ファイルのファイルパス (ファイル名を含まない)。

**ファイルポリシー (File Policy)**

ファイルを検出したファイルポリシー。

**ファイルストレージ (File Storage) /保存 (Stored) (検索のみ)**

イベントに関連付けられたファイルのストレージステータス:

**保存 (Stored)**

関連するファイルが現在保存されているすべてのイベントを返します。

**関連保存 (Stored in connection)**

関連するファイルが現在保存されているかどうかに関係なく、関連するファイルをシステムがキャプチャおよび保存したすべてのイベントを返します。

**失敗しました (Failed)**

関連するファイルをシステムが保存できなかったすべてのイベントを返します。

**ファイルのタイムスタンプ (File Timestamp)**

AMP for Endpoints が検出したマルウェア ファイルが作成された日時。

**HTTP 応答コード (HTTP Response Code)**

ファイルの転送時にクライアントの HTTP 要求に応じて送信される HTTP ステータスコード。

**IOC**

マルウェア イベントが、接続に関与したホストに対する侵入の痕跡 (IOC) をトリガーしたかどうか。AMP for Endpoints データが IOC ルールをトリガーした場合、タイプ AMP IOC で、完全なマルウェア イベントが生成されます。

**メッセージ (Message)**

マルウェア イベントに関連付けられる追加情報。ファイル イベントおよびネットワーク ベースのマルウェア イベントでは、このフィールドは、性質が変更された、つまり関連付けられた遡及的イベントがあるファイルに対してのみ入力されます。

**受信側の大陸 (Receiving Continent)**

ファイルを受信するホストの大陸。

**受信側の国 (Receiving Country)**

ファイルを受信するホストの国。

**受信側 IP (Receiving IP)**

ファイル イベントおよびネットワークベースのマルウェア イベントの場合、ファイルを受信するホストの IP アドレス。エンドポイント ベースのマルウェアのイベントの場合、コネクタがイベントを報告したエンドポイントの IP アドレス。

**受信側のポート (Receiving Port)**

ファイルが検出されたトラフィックによって使用される宛先ポート。

**セキュリティ コンテキスト (Security Context)**

トラフィックが通過した仮想ファイアウォールグループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチコンテキストモードの ASA FirePOWER だけです。

**送信側の大陸 (Sending Continent)**

ファイルを送信するホストの大陸。

**送信側の国 (Sending Country)**

ファイルを送信するホストの国。

**送信側 IP (Sending IP)**

ファイルを送信するホストの IP アドレス。

**送信側のポート (Sending Port)**

ファイルが検出されたトラフィックによって使用される送信元ポート。

**SHA256/ファイル SHA256 (File SHA256)**

ファイルの SHA-256 ハッシュ値と、最後に検出されたファイル イベントおよびファイル性質を表すネットワーク ファイル トラジェクトリ アイコン、およびネットワーク ファイル トラジェクトリにリンクするネットワーク ファイル トラジェクトリ アイコン。SHA256 値を得るには、ファイルが次のいずれかによって処理されている必要があります。

- [ファイルの保存 (Store files) ] が有効になっているファイル検出ファイルルール。
- [ファイルの保存 (Store files) ] が有効になっているファイルブロック ファイルルール。
- マルウェア クラウドルックアップ ファイルルール
- マルウェア ブロック ファイルルール
- AMP for Endpoints

**サイズ (KB) (Size (KB)) / ファイル サイズ (KB) (File Size (KB))**

ファイルのサイズ (KB 単位)。ファイルが完全に受信される前にシステムがファイルのタイプを判別すると、ファイルサイズが計算されずに、このフィールドがブランクになる場合がありますので注意してください。

**SSL の実際の動作 (SSL Actual Action) (検索のみ)**

システムが暗号化トラフィックに適用したアクション。

**ブロック (Block) / リセットしてブロック (Block With Reset)**

ブロックされた暗号化接続を表します。

**複合 (再署名) (Decrypt (Resign))**

再署名サーバ証明書を使用して復号された発信接続を表します。

**復号 (キーの置き換え) (Decrypt (Replace Key))**

置き換えられた公開キーと自己署名サーバ証明書を使用して復号された発信接続を表します。

**復号 (既知のキー) (Decrypt (Known Key))**

既知の秘密キーを使用して復号された着信接続を表します。

**デフォルト アクション (Default Action)**

接続がデフォルトアクションによって処理されたことを示しています。

**復号しない (Do Not Decrypt)**

システムが復号しなかった接続を表します。

フィールド値は、検索ワークフロー ページの [SSL ステータス (SSL Status)] フィールドに表示されます。

**SSL 証明書情報 (SSL Certificate Information) (検索のみ)**

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- 件名/発行元共通名 (Subject/Issuer Common Name)
- 件名/発行元組織 (Subject/Issuer Organization)
- 件名/発行元組織ユニット (Subject/Issuer Organization Unit)
- 有効期間の開始/終了 (Not Valid Before/After)
- シリアル番号 (Serial Number)、証明書フィンガープリント (Certificate Fingerprint)
- 公開キー フィンガープリント (Public Key Fingerprint)

**SSL 失敗理由 (SSL Failure Reason) (検索のみ)**

システムが暗号化されたトラフィックの復号に失敗した理由：

- 不明
- 不一致 (No Match)
- Success
- キャッシュされていないセッション (Uncached Session)
- 不明な暗号スイート (Unknown Cipher Suite)
- サポートされていない暗号スイート (Unsupported Cipher Suite)
- サポートされていない SSL バージョン (Unsupported SSL Version)
- SSL 圧縮の使用 (SSL Compression Used)
- パッシブ モードで復号できないセッション (Session Undecryptable in Passive Mode)
- ハンドシェイク エラー (Handshake Error)
- 復号エラー (Decryption Error)
- 保留サーバ名カテゴリ ルックアップ (Pending Server Name Category Lookup)
- 保留共通名カテゴリ ルックアップ (Pending Common Name Category Lookup)
- 内部エラー (Internal Error)
- ネットワーク パラメータを使用できません (Network Parameters Unavailable)
- 無効なサーバ証明書の処理 (Invalid Server Certificate Handle)
- サーバ証明書フィンガープリントを使用できません (Server Certificate Fingerprint Unavailable)
- サブジェクト DN をキャッシュできません (Cannot Cache Subject DN)
- 発行元 DN をキャッシュできません (Cannot Cache Issuer DN)
- 不明の SSL バージョン (Unknown SSL Version)
- 外部証明書リストを使用できません (External Certificate List Unavailable)
- 外部証明書フィンガープリントを使用できません (External Certificate Fingerprint Unavailable)
- 内部証明書リストが無効です (Internal Certificate List Invalid)
- 内部証明書リストを使用できません (Internal Certificate List Unavailable)
- 内部証明書を使用できません (Internal Certificate Unavailable)
- 内部証明書フィンガープリントを使用できません (Internal Certificate Fingerprint Unavailable)
- サーバ証明書検証を使用できません (Server Certificate Fingerprint Unavailable)
- サーバ証明書検証エラー (Server Certificate Validation Failure)
- 無効なアクション (Invalid Action)

フィールド値は、検索ワークフロー ページの [SSL ステータス (SSL Status) ] フィールドに表示されます。

### SSL ステータス (SSL Status)

暗号化された接続を記録した、[SSL の実際の動作 (SSL Actual Action) ] (SSL ルール、デフォルトアクション、または復号できないトラフィックアクション) に関連したアクション。ロックアイコン (🔒) は、SSL 証明書の詳細にリンクしています。証明書を利用できない場合 (たとえば、SSL ハンドシェイク エラーにより接続がブロックされる場合)、ロックアイコンはグレー表示になります。

システムが暗号化接続を復号できなかった場合は、[SSL の実際の動作 (SSL Actual Action) ] (実行された復号不能のトラフィック アクション) と、[SSL 失敗理由 (SSL Failure Reason) ] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [Do Not Decrypt (Unknown Cipher Suite)] が表示されます。

このフィールドを検索する場合は、[SSL の実際の動作 (SSL Actual Action) ] と [SSL 失敗理由 (SSL Failure Reason) ] の 1 つ以上の値を入力し、システムが処理した、または復号に失敗した暗号化トラフィックを表示します。

### SSL 件名/発行元国 (SSL Subject/Issuer Country) (検索のみ)

暗号化証明書に関連付けられた件名または発行元国の 2 文字の ISO 3166-1 alpha-2 国番号。

### 脅威名 (Threat Name)

検出されたマルウェアの名前。

### 脅威スコア (Threat Score)

そのファイルに関連する最新の脅威スコア。脅威スコアアイコンは、[動的分析要約 (Dynamic Analysis Summary) ] レポートにリンクされています。

### 時刻 (Time)

イベントが生成された日時。このフィールドは検索できません。

### タイプ (Type) /ファイルタイプ (File Type)

ファイルのタイプ (HTML や MSEXE など)。

### URI (URI) /ファイル URI (File URI)

ファイルの送信元の URI (ファイルをダウンロードした URL など)。

### ユーザ (User)

イベントが発生したホスト (受信 IP) のユーザ

ファイルイベントおよびネットワークベースのマルウェア イベントの場合、このユーザはネットワーク検出によって判別されます。ユーザは宛先ホストに関連付けられているため、ユーザがマルウェア ファイルをアップロードしたマルウェア イベントに、ユーザは関連付けられていません。

エンドポイントベースのマルウェア イベントの場合、AMP for Endpoints がユーザ名を判別します。これらのユーザをユーザ検出または制御に関連付けることはできません。それらは[ユーザ (Users) ]テーブルに含まれず、それらのユーザの詳細を表示することもできません。

### Web アプリケーション (Web Application)

接続で検出された HTTP トラフィックについて、内容を表すまたは URL を要求したアプリケーション。

### Web アプリケーションのカテゴリまたはタグ (Web Application Category or Tag)

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

## マルウェア イベントのサブタイプ

次の表に、マルウェア イベントのサブタイプと、ネットワークベースまたはエンドポイントベースのマルウェア イベントにそのサブタイプを指定できるかどうか、そのサブタイプを使用してネットワーク ファイル トラジェクトリが構築されるかどうかを一覧で示します。

表 299: マルウェア イベントのタイプ

マルウェア イベントのサブタイプ/検索値	AMP for Firepower	エンドポイント向け AMP	ファイル トラジェクトリ
ネットワーク ファイル転送時に検出された脅威 (Threat Detected in Network File Transfer)	Yes	No	Yes
ネットワーク ファイル転送時に検出された脅威 (遡及的) (Threat Detected in Network File Transfer (retrospective))	Yes	No	Yes
検出された脅威 (Threat Detected)	No	Yes	Yes
除外項目内で検出された脅威 (Threat Detected in Exclusion)	No	Yes	Yes
検疫された脅威 (Threat Quarantined)	No	Yes	Yes



マルウェア イベントのサブタイプ/検索値	AMP for Firepower	エンドポイント向け AMP	ファイルトラジェクトリ
AMP IOC (侵害の兆候) (AMP IOC (Indications of compromise))	No	Yes	No
ブロックされた実行 (Blocked Execution)	No	Yes	No
隔離のクラウドリコール (Cloud Recall Quarantine)	No	Yes	No
隔離のクラウドリコールの試 行に失敗 (Cloud Recall Quarantine Attempt Failed)	No	Yes	No
隔離のクラウドリコールの 開始 (Cloud Recall Quarantine Started)	No	Yes	No
隔離からのクラウドリコール の復元 (Cloud Recall Restore from Quarantine)	No	Yes	No
隔離からのクラウドリコール の復元に失敗 (Cloud Recall Restore from Quarantine Failed)	No	Yes	No
隔離からのクラウドリコール の復元の開始 (Cloud Recall Restore from Quarantine Started)	No	Yes	No
隔離エラー (Quarantine Failure)	No	Yes	No
隔離されたアイテムの復元 (Quarantined Item Restored)	No	Yes	No
隔離の復元に失敗 (Quarantine Restore Failed)	No	Yes	No
隔離の復元の開始 (Quarantine Restore Started)	No	Yes	No

マルウェア イベントのサブタイプ/検索値	AMP for Firepower	エンドポイント向け AMP	ファイル トラジェクトリ
スキャン完了、検出なし (Scan Completed, No Detections)	No	Yes	No
スキャンが検出ありで完了 (Scan Completed With Detections)	No	Yes	No
スキャンに失敗 (Scan Failed)	No	Yes	No
スキャン開始 (Scan Started)	No	Yes	No

## ファイルおよびマルウェア イベント フィールドで利用可能な情報

次の表に、システムが各ファイルおよびマルウェア イベント フィールドの情報を表示するかどうかを示します。すべてのフィールドがすべてのイベントに読み込まれるわけではないことに留意してください。次に例を示します。

- AMP for Firepower はネットワーク トラフィックでマルウェア ファイルを検出することから、ファイル イベントおよびネットワーク ベースのマルウェア イベントには、ファイルの送信に使用された接続に関する、ポート、アプリケーションプロトコル、および送信元 IP アドレスの情報が含まれます。
- エンドポイント向け AMP の展開からインポートされたマルウェア イベントと侵害の兆候 (IOC) には、コンテキスト接続情報は含まれていませんが、ダウンロード時または実行時に取得された情報 (ファイルパス、呼び出し元クライアント アプリケーションなど) が含まれています。
- ファイル イベント テーブル ビューには、エンドポイント向け AMP 関連のフィールドは表示されません。

表 300: ファイルおよびマルウェア イベント フィールドで利用可能な情報

フィールド	ファイル イベント	AMP for Firepower マルウェア イベント	AMP for Firepower レトロスペクティブ イベント	エンドポイント向け AMP マルウェア イベント
操作 (Action)	Yes	Yes	Yes	No
AMP クラウド (AMP Cloud)	No	No	No	Yes

フィールド	ファイル イベント	AMP for Firepower マルウェア イベント	AMP for Firepower レトロスペクティブ イベント	エンドポイント向け AMP マルウェア イベント
アプリケーションファイル名 (Application File Name)	No	No	No	Yes
アプリケーションファイル SHA256 (Application File SHA256)	No	No	No	Yes
アプリケーションプロトコル	Yes	Yes	No	No
アプリケーションプロトコルカテゴリまたはタグ (Application Protocol Category or Tag)	Yes	Yes	Yes	No
アプリケーションのリスク (Application Risk)	Yes	Yes	Yes	No
アーカイブ深度 (Archive Depth)	Yes	Yes	No	Yes
アーカイブ名 (Archive Name)	Yes	Yes	No	Yes
アーカイブ SHA256 (Archive SHA256)	Yes	Yes	No	Yes
ビジネスとの関連性 (Business Relevance)	Yes	Yes	Yes	No
カテゴリ/ファイルタイプカテゴリ (Category / File Type Category)	Yes	Yes	No	Yes
クライアント	Yes	Yes	Yes	No
クライアントカテゴリまたはタグ (Client Category or Tag)	Yes	Yes	Yes	No

フィールド	ファイル イベント	AMP for Firepower マルウェア イベント	AMP for Firepower レトロスペクティブ イベント	エンドポイント向け AMP マルウェア イベント
メンバー数 (Count)	Yes	Yes	Yes	Yes
検出名 (Detection Name)	No	Yes	No	No
ディテクタ (Detector)	No	No	No	Yes
Device	Yes	Yes	Yes	Yes
処理/ファイルの処理 (Disposition / File Disposition)	Yes	Yes	Yes	No
ドメイン (Domain)	Yes	Yes	Yes	Yes
イベント サブタイプ (Event Subtype)	No	No	No	Yes
イベント タイプ (Event Type)	No	Yes	Yes	Yes
ファイル名 (File Name)	Yes	Yes	No	Yes
ファイルパス (File Path)	No	No	No	Yes
ファイル ポリシー (File Policy)	Yes	No	No	No
ファイルのタイムスタンプ (File Timestamp)	No	No	No	Yes
HTTP 応答コード (HTTP Response Code)	Yes	Yes	No	No
IOC (侵害の兆候) (IOC (Indication of Compromise))	No	Yes	Yes	Yes
メッセージ (Message)	Yes	Yes	No	Yes

フィールド	ファイル イベント	AMP for Firepower マルウェア イベント	AMP for Firepower レトロスペクティブ イベント	エンドポイント向け AMP マルウェア イベント
受信側の大陸 (Receiving Continent)	Yes	Yes	Yes	No
受信側の国 (Receiving Country)	Yes	Yes	No	No
受信側 IP (Receiving IP)	Yes	Yes	No	Yes
受信側のポート (Receiving Port)	Yes	Yes	No	No
セキュリティ コンテキスト (Security Context)	Yes	Yes	Yes	Yes
送信側の大陸 (Sending Continent)	Yes	Yes	Yes	No
送信側の国 (Sending Country)	Yes	Yes	No	No
送信側 IP (Sending IP)	Yes	Yes	No	No
送信側のポート (Sending Port)	Yes	Yes	No	No
SHA256/ファイル SHA256 (SHA256/File SHA256)	Yes	Yes	Yes	Yes
サイズ (KB) / ファイルサイズ (KB) (Size (KB) / File Size (KB))	Yes	Yes	No	Yes
SSL の実際のアクション (SSL Actual Action) (検索のみ)	Yes	Yes	No	No
SSL 証明書情報 (SSL Certificate Information) (検索のみ)	Yes	Yes	No	No

フィールド	ファイル イベント	AMP for Firepower マルウェア イベント	AMP for Firepower レトロスペクティブ イベント	エンドポイント向け AMP マルウェア イベント
SSL 障害の理由 (SSL Failure Reason) (検索のみ)	Yes	Yes	No	No
SSL ステータス (SSL Status)	Yes	Yes	No	No
SSL 件名/発行者の国 (SSL Subject/Issuer Country) (検索のみ)	Yes	Yes	No	No
ファイル ストレージ/保存済み (File Storage / Stored) (検索のみ)	Yes	Yes	No	No
脅威名 (Threat Name)	No	Yes	Yes	Yes
脅威スコア (Threat Score)	Yes	Yes	No	No
時刻 (Time)	Yes	Yes	Yes	Yes
タイプ/ファイル タイプ (Type / File Type)	Yes	Yes	No	Yes
URI/ファイル URI (URI / File URI)	Yes	Yes	No	No
ユーザ (User)	Yes	Yes	No	Yes
Web アプリケーション (Web Application)	Yes	Yes	Yes	No
Web アプリケーション カテゴリまたはタグ (Web Application Category or Tag)	Yes	Yes	Yes	No

## ローカル マルウェア分析 (Local Malware Analysis)

ローカルマルウェア分析では、管理対象デバイスで Cisco Talos Security Intelligence and Research Group (Talos) から提供される検出ルールを使用して、実行可能ファイル、PDF、Office 文書、

およびその他のタイプのファイルで最も一般的なタイプのマルウェアの有無をローカルで検査することができます。ローカルマルウェア分析ではファイルを AMP クラウドに送信する必要はなく、ファイルを実行することもしないの、時間とシステム リソースを節約できます。

システムはローカルマルウェアによってマルウェアを識別すると、その既存のファイルの性質を [不明 (Unknown)] から [マルウェア (Malware)] に更新します。その上で、システムは新しいマルウェア イベントを生成します。システムはマルウェアを識別しなかったとしても、ファイルの性質を [不明 (Unknown)] から [正常 (Clean)] に更新することはありません。ローカルマルウェア分析を実行した後、システムはファイル情報 (SHA-256 ハッシュ値、タイムスタンプ、ファイルの性質など) をキャッシュに入れて、特定の期間内にそのファイルを再度検出した場合に再び分析を行わなくてもマルウェアを識別できるようにします。

イベント ビューアで、コンテキスト メニューを使用してローカルマルウェア分析用にファイルを 1 つずつ手動で送信することも、最大 25 個のキャプチャ済みファイルを同時に送信することもできます。システムはローカル分析を実行してから、それらのファイルをダイナミック分析対象としてクラウドに送信します。

ローカルマルウェア分析では、AMP Threat Grid クラウドとの通信を確立する必要はありません。ただし、マルウェアとして事前に分類したファイルをダイナミック分析用にクラウドに送信するため、また、アップデートをローカルマルウェア分析ルールセットにダウンロードするために、クラウドとの通信を設定する必要があります。

## ファイル構成

ローカルマルウェアの分析または動的分析を設定すると、ファイルの分析後にファイル構成レポートが生成されます。このレポートを使用して、ファイルをさらに分析し、ファイルにマルウェアが組み込まれているかどうかを判断することができます。

ファイル構成レポートでは、ファイルのプロパティ、ファイルに組み込まれているオブジェクト、および検出されたウイルスが示されます。また、ファイル構成レポートでは、そのファイルタイプに固有の追加情報が示される場合があります。保存されているファイルのプルーニング時に、関連ファイル構成レポートもプルーニングされます。

## 動的分析 (Dynamic Analysis)

AMPクラウドの精度を改善し、追加のマルウェア分析および脅威の特定を提供するには、AMP Threat Grid クラウドまたはオンプレミスの AMP Threat Grid アプライアンスに、キャプチャされた適格なファイルを動的分析用に送信します。AMPクラウドでは、ファイルがサンドボックス環境で実行され、ファイルにマルウェアが含まれているかどうか判別されます。

動的分析用にファイルを送信できるかどうかは、次によって異なります。

- ファイルタイプ
- ファイルサイズ
- ファイルルールのアクション

- 自動送信用にマルウェアとしてシステムで事前に分類されたファイル

マルウェアをブロックするか、マルウェア クラウドルックアップを実行するようにルールが設定されている場合は、不明または使用不可の性質を持つ一致するファイルのみが送信されます。

AMP Threat Grid クラウドでは、動的分析用にファイルがキューに登録され、各ファイルがサンドボックス環境で実行されます。クラウドは、ファイルにマルウェアが含まれている確率の詳細を示す脅威スコアを返します。脅威スコアが定義されているしきい値を超えるファイルを自動的にブロックできます。

イベント ビューア、キャプチャされたファイル ビュー、またはネットワーク ファイル トラジェクトリから、ファイルが動的分析用に送信されたかどうかの特定、ローカルマルウェアおよびファイルの動的分析用の手動送信、またはクラウドに脅威スコアが割り当てられている理由のサマリーの表示を行うことができます。また、動的分析のサマリーレポートも取得できます。これには、全体的な脅威スコアを構成する各種評価、およびクラウドによるファイル実行の試行時に開始されたその他のプロセスが示されます。

## 自動ダイナミック分析と Spero 分析

ファイルポリシーは、マルウェアとして事前分類されたファイルを自動的にダイナミック分析に提出するように設定できます。

クエリ対象にするファイルを自動的に Spero 分析に提出することで、ダイナミック分析を補足することができます。Spero 分析は SHA-256 ハッシュ値の分析を補うもので、実行可能ファイル内のマルウェアをより正確に識別できます。

Spero 分析では、ファイル構造の特性（メタデータやヘッダー情報など）を調べます。この情報に基づいて Spero シグネチャを生成した後、デバイスはそれを AMP クラウド内の Spero ヒューリスティック エンジンに送信します。Spero シグネチャに基づいて、そのファイルがマルウェアかどうかを Spero エンジンが返します。現時点のファイル処理が [不明 (Unknown)] であれば、システムは [マルウェア (Malware)] のファイル処理を割り当てます。

Spero 分析のために実行可能ファイルを送信できるのは、検出時だけなので注意してください。後から手動で送信することはできません。ダイナミック分析にはファイルを送信せずに、Spero 分析にのみファイルを送信することもできます。

## 手動によるダイナミック分析

イベント ビューア、コンテキスト メニュー、ネットワーク ファイル トラジェクトリから、保管されたファイルをダイナミック分析の対象として手動で送信できます。キャプチャファイル ビューからは、一度に最大 25 個の保存済みファイルを手動で送信できます。

実行可能ファイルの他に、自動送信に適格ではないファイル タイプ (.swf、.jar など) も送信できます。これにより、ファイルの性質に関わらず、さまざまなファイルをより迅速に分析し、問題の正確な原因を突き止めることができます。





- (注) 動的分析に適切なファイルタイプのリストと送信可能な最小および最大のファイルサイズに関して更新がないか、システムは AMP クラウドを検査します（この検査は、一日に 1 回だけ行われます）。

## 動的分析とキャパシティ処理

容量処理によって、現在、ファイルを動的分析のためにクラウドに送信できない場合に一時的にデバイスでファイルを保存できます。デバイスでは、そのハードドライブまたはマルウェアストレージパックにファイルが保存されます。

システムでは、動的分析を有効にして、マルウェアクラウドルックアップを実行する任意のファイルを一時的に保存できます。ファイルがマルウェアとして事前に分類されており、デバイスがクラウドへの最大送信数に到達したか、クラウドと通信できない場合に、システムはこのファイルを保存します。

デバイスでは、次のいずれかの場合に保存されているファイルがクラウドに再送信されます。

- デバイスがクラウドと通信できず、クラウドコミュニケーションを再確立する場合
- デバイスがクラウドへの最大送信数に到達し、十分な時間が経過した場合

## 脅威スコアと動的分析のサマリ レポート

### 脅威スコア

表 301: 脅威スコア レーティング

脅威スコア	アイコン
Low	
Medium	
High	
Very High	

Firepower Management Center は、ファイルの性質と同じ期間だけ、ファイルの脅威スコアをキャッシュに入れます。これらのファイルが後から検出されると、AMP Threat Grid クラウドまたは AMP Threat Grid オンプレミス アプライアンスが再クエリされる代わりに、キャッシュされた脅威スコアが表示されます。ファイルの脅威スコアが、定義済みのマルウェアしきい値の脅威スコアを超える場合は、そのファイルにマルウェアの性質を自動的に割り当てることができます。

### 動的分析のサマリ

動的分析のサマリが生成可能な場合、脅威スコアアイコンをクリックすると、サマリが表示されます。複数のレポートが存在する場合、このサマリは、脅威スコアと完全に一致する最新のレポートに基づいて生成されます。完全に一致する脅威スコアがない場合、最も高い脅威スコアに関するレポートが表示されます。複数のレポートがある場合は、脅威スコアを選択して、それぞれのレポートを表示することができます。

サマリには、脅威スコアを構成する各コンポーネントの脅威がリストされます。各コンポーネントの脅威を展開すると、そのコンポーネントの脅威に関連するプロセスだけでなく、AMPクラウドの調査結果もリストされます。

プロセス ツリーには、AMP Threat Grid クラウドがファイルを実行しようとしたときに開始されたプロセスが示されています。これは、マルウェアを含むファイルが、想定外のプロセスやシステム リソースへアクセスしようとしているかどうか（たとえば、Word ドキュメントを実行すると、Microsoft Word が開き、次に Internet Explorer が起動し、さらに Java Runtime Environment が実行されるなど）を識別するのに役立ちます。

リストされる各プロセスには、実際のプロセスを検査するのに使用できるプロセス ID が含まれます。プロセス ツリー内の子ノードは、親プロセスの結果として開始されたプロセスを表します。

動的分析のサマリから [完全なレポートを表示 (View Full Report)] をクリックすることにより、AMPクラウドの完全な分析を詳述する完全版分析レポートを表示できます。レポートには、ファイルの一般情報、検出されたすべてのプロセスの詳細な説明、ファイル分析の概要、およびその他の関連情報が含まれます。

## ファイル分析評価

Spero 分析とローカル マルウェア分析、動的分析、またはこれらの組み合わせの結果に基づいて、システムはファイルの性質を更新することがあります。

システムは、ファイルに対して最初に Spero 分析、次にローカルマルウェア分析、動的分析の順に実行します。システムがマルウェアを特定した場合でも、ファイルがマルウェアとして事前分類されていれば、ファイルは AMP Threat Grid クラウドに送信されます。

ファイル ルールでローカル マルウェア分析または動的分析を設定すると、システムによってルールに一致するファイルが事前分類され、ファイル構成レポートが生成されます。事前分類の結果としてファイルの性質が変更されることはありません。

次の表に、ファイル分析の各タイプの利点と欠点、および分析に基づいたファイルの性質の変更方法について説明します。

表 302: ファイル分析のタイプの比較

分析タイプ	利点	制限事項	マルウェアの特定
Spero 分析	実行可能ファイルの構造分析。Spero シグネチャを分析のために AMP クラウドに送信します。	ローカルマルウェア分析または動的分析よりも詳細度が低くなります。実行可能ファイル専用です。	マルウェアの特定がポジティブの場合にのみ、性質が [不明 (Unknown) ] から [マルウェア (Malware) ] に変更されます。
ローカルマルウェア分析	動的分析より消費するリソースが少なく、特に検出されたマルウェアが一般的な場合は結果がより迅速に返されます。	動的分析よりも結果の詳細度が低くなります。	マルウェアの特定がポジティブの場合にのみ、性質が [不明 (Unknown) ] から [マルウェア (Malware) ] に変更されます。
動的分析	AMP Threat Grid クラウドを使用してサンドボックス環境でファイルを実行することで、結果の詳細度がより高くなります。	ローカルマルウェア分析単独の場合よりも消費するリソースが多くなります。	マルウェアの可能性があると事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ファイルポリシーに設定されている脅威スコアしきい値に基づいて性質が変更されます。
Spero 分析とローカルマルウェア分析	AMP クラウドのリソースを使用してマルウェアを特定しながら、ローカルマルウェア分析と動的分析を設定するよりも少ないリソースを消費します。	動的分析、Spero 分析よりも詳細度が低くなります。実行可能ファイル専用です。	マルウェアの特定がポジティブの場合にのみ、性質が [不明 (Unknown) ] から [マルウェア (Malware) ] に変更されます。

分析タイプ	利点	制限事項	マルウェアの特定
Spero 分析と動的分析	ファイルおよび Spero シグネチャの送信時に AMP クラウドの全機能を使用します。	ローカルマルウェア分析を使用する場合よりも結果の取得に時間がかかります。	マルウェアの可能性があると事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ファイルポリシーで設定されている脅威スコアしきい値に基づいて、および Spero 分析でマルウェアが特定された場合は、性質が [不明 (Unknown)] から [マルウェア (Malware)] に変更されます。
ローカルマルウェア分析と動的分析	両方のタイプのファイル分析を使用することで詳細な結果が得られます。	どちらか一方の場合よりも消費するリソースが多くなります。	マルウェアの可能性があると事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ローカルマルウェア分析でマルウェアが特定された場合、またはファイルポリシーで設定されている脅威スコアしきい値に基づいて、性質が [不明 (Unknown)] から [マルウェア (Malware)] に変更されます。
Spero 分析、ローカルマルウェア分析、および動的分析	最も詳細な結果になります。	3 つすべてのタイプのファイル分析を実行するため消費するリソースが最も多くなります。	マルウェアの可能性があると事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。Spero 分析またはローカルマルウェア分析でマルウェアが特定された場合、またはファイルポリシーで設定されている脅威スコアしきい値に基づいて、性質が [不明 (Unknown)] から [マルウェア (Malware)] に変更されます。

## キャプチャファイルとファイルストレージ

ファイルポリシーの設定に基づき、ファイル制御機能を使用して、ファイルの検出およびブロックを行えます。ただし、疑わしいホストまたはネットワークからのファイルや、ネットワーク上の監視対象ホストに送信された大量のファイルについては、さらに分析が必要になる場合があります。ファイルストレージ機能を使用することにより、選択したファイル（トラフィックで検出された）をキャプチャして、それらをデバイスのハードドライブかマルウェアストレージバック（インストールされている場合）に自動的に保存できます。

デバイスがトラフィックでファイルを検出すると、そのファイルをキャプチャできます。このようにして作成されたコピーは、ダイナミック分析のために、システムが保存したり送信したりできます。デバイスがファイルをキャプチャした後に、以下の選択肢があります。

- 後で分析するために、キャプチャしたファイルをデバイスのハードドライブに保存する。
- さらに手動で分析したりアーカイブしたりするために、保存したファイルをローカルコンピュータにダウンロードする。
- ダイナミック分析用に、AMPクラウドにファイルを送信します。

注意すべき点として、デバイスがファイルを保存した後は、以後それを検出しても、デバイスが引き続きそれを保存していれば、そのファイルを再度キャプチャすることはありません。



- (注) ファイルがネットワーク上で初めて検出された際には、ファイルの検出を表すファイルイベントを生成できます。ただし、ファイルルールがマルウェアクラウドルックアップを行う場合は、システムがAMPクラウドにクエリを行い、判定結果が返るまで、より多く時間を要します。この遅延により、システムはネットワークでこのファイルが2回目に検出され、ファイルの判定結果を即座に判断できるまでは、このファイルを保存できません。

システムがファイルをキャプチャするか保存するかに関わらず、以下が可能です。

- イベントビューアからのキャプチャされたファイルに関する情報（ダイナミック分析のためにファイルが保存されたのか送信されたかどうか、ファイル判定結果、脅威スコアなど）を確認することにより、ネットワーク上で検出されたマルウェアの潜在的な脅威について迅速に検討する。
- ファイルのトラジェクトリを表示して、ネットワークのトラバースの仕方およびコピーを保持しているホストを判別する。
- ファイルをクリーンリストまたはカスタム検出リストに追加することで、以後の検出時には常に、クリーンまたはマルウェアの判定結果を持つファイルとして扱う。

ファイルポリシーでファイルルールを設定して、特定のタイプまたは特定のファイル判定結果（使用できる場合）のファイルをキャプチャして保存します。ファイルポリシーをアクセスコントロールポリシーと関連付けて、それをデバイスに展開した後、トラフィック内の一致

ファイルが検出され、保存されます。また、保存するファイルサイズの最小値と最大値を設定できます。保存したファイルは、システムバックアップファイルには含まれません。

## マルウェアストレージパック

ファイルポリシー構成によっては、デバイスがハードドライブにかなりの量のファイルデータを保存することがあります。デバイスにマルウェアストレージパックを設置すると、システムはファイルをマルウェアストレージパックに保存して、プライマリハードドライブでイベントおよび設定ファイルの保存用スペースをより多く確保できます。システムは定期的に古いファイルを削除します。デバイスのプライマリハードドライブに使用可能な領域が十分でなく、マルウェアストレージパックも設置されていない場合、ファイルを保存することはできません。



**注意** Cisco から供給されたハードドライブ以外はデバイスに取り付けしないでください。サポートされていないハードドライブを取り付けると、デバイスが破損する可能性があります。マルウェアストレージパックキットは、シスコからのみ購入でき、8000 シリーズデバイスでのみ使用できます。マルウェアストレージパックのサポートが必要な場合は、サポートにお問い合わせください。詳細については、*Firepower System Malware Storage Pack Guide*を参照してください。

マルウェアストレージパックが設置されていない場合、ファイルを保存するデバイスを設定すると、プライマリハードドライブのスペースの特定の部分がキャプチャファイルストレージに割り当てられます。ダイナミック分析用に一時的にファイルに保存するよう容量処理を設定すると、システムはファイルをクラウドに再送信できるようになるまで、同じハードドライブ割り当てを使用してそれらのファイルを保存します。

デバイスにマルウェアストレージパックを設置してファイルストレージまたは容量処理を設定すると、デバイスはマルウェアストレージパック全体をこれらのファイルの保存用として割り当てます。デバイスは、マルウェアストレージパックに他の情報を保存することはできません。

キャプチャファイルストレージに割り当てられたスペースがいっぱいになると、システムは割り当てられたスペースがシステム定義しきい値に達するまで、保管されている古いファイルを削除します。保存されていたファイルの数によっては、システムがファイルを削除した後、ディスク使用率がかなり減る場合があります。

マルウェアストレージパックを設置する時点で、デバイスがすでにファイルを保存している場合、次にデバイスを再起動したときに、プライマリハードドライブに保存されていたキャプチャファイルまたは容量処理ファイルはすべて、マルウェアストレージパックに移動します。それ以降デバイスが保存するファイルはすべて、マルウェアストレージパックに保存されます。

## 保存されているファイルのダウンロード

デバイスによって保存されたファイルは、Firepower Management Center がそのデバイスと通信可能であり、ファイルが削除されていない限り、長期間保存し分析するためにローカルホストにダウンロードし、手動でファイルを分析できます。関連ファイルイベント、マルウェアイベント、キャプチャファイルビュー、またはファイルのトラジェクトリからファイルをダウンロードできます。

マルウェアによる被害を防ぐため、デフォルトでは、ファイルのダウンロードのたびに確認を行う必要があります。ただし、この確認は[ユーザ設定 (User Preferences)]で無効にすることもできます。

性質が使用不可のファイルにはマルウェアが含まれている可能性があるため、ファイルをダウンロードすると、システムはまずそのファイルを .zip パッケージにアーカイブします。 .zip ファイル名には、ファイルの性質とファイルタイプ (存在する場合) さらに SHA-256 ハッシュ値が含まれます。誤って解凍してしまわないように、.zip ファイルをパスワードで保護できます。 .zip ファイルのデフォルトパスワードは、[ユーザ設定 (User Preferences)]で編集または削除できます。



### 注意

有害な結果が発生することがあるため、マルウェアをダウンロードしないように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先をセキュアにするために必要な予防措置を行っていることを確認します。

## キャプチャされたファイルワークフローの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
機能に応じて異なる	機能に応じて異なる	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

管理対象デバイスは、ネットワークトラフィックで検出されたファイルをキャプチャすると、イベントをログに記録します。



### (注)

デバイスがマルウェアを含むファイルをキャプチャすると、デバイスは、ファイルを検出した場合はファイルイベント、マルウェアを識別した場合はマルウェアイベントの2種類のイベントを生成します。

イベントビューアでは、テーブルにキャプチャファイルを表示できます。また、分析に関連する情報に応じてイベントビューアを操作することができます。キャプチャファイルにアクセスしたときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページ

です。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

ファイルポリシーの更新など設定を変更した後に、システムがファイルを再キャプチャする場合、そのファイルの既存の情報が更新されます。

たとえば、[マルウェアクラウドルックアップ (Malware Cloud Lookup) ]アクションを使用してファイルをキャプチャするようにファイルポリシーを設定した場合、システムはそのファイルと一緒にファイル処理と脅威スコアを保存します。その後、ファイルポリシーを更新し、新しい[ファイルの検出 (Detect Files) ]アクションのためにシステムが同じファイルを再キャプチャすると、システムはファイルの [最終変更時刻 (Last Changed) ] の値を更新します。ただし、別のマルウェアクラウドルックアップを実行しなかったとしても、システムは既存の処理や脅威スコアを削除しません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

## 手順

---

[分析 (Analysis) ] > [ファイル (Files) ] > [キャプチャ ファイル (Captured Files) ] を選択します。

**ヒント** イベントのテーブルビューでは、一部のフィールドがデフォルトで非表示にされています。イベントビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム (Disabled Columns) ] の下のフィールド名をクリックします。

---

## 関連トピック

[キャプチャされたファイルのフィールド](#) (2642 ページ)

[定義済みキャプチャ ファイルのワークフロー](#) (2421 ページ)

[イベントビュー設定の設定](#) (37 ページ)

# キャプチャされたファイルのフィールド

キャプチャされたファイルのテーブルビューは、定義済みファイル イベントのワークフローの最後のページであり、カスタムワークフローに追加できます。このテーブルビューには、ファイルテーブルの各フィールドの列が含まれます。

このテーブルを検索する場合、検索結果は、検索対象のイベントで使用可能なデータによって決まることに留意してください。使用可能なデータによって、検索の制約が適用されないことがあります。たとえば、ダイナミック分析のためにファイルが送信されていない場合は、関連する脅威スコアがない可能性があります。



表 303: キャプチャされたファイルのフィールド

フィールド	説明
アーカイブ検査ステータス (Archive Inspection Status)	<p>アーカイブファイルのアーカイブ検査ステータスであり、次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• [保留中 (Pending)] は、システムがアーカイブファイルとその内容をまだ検査していることを示します。ファイルが再びシステムを通過すると、完全な情報が使用可能になります。</li> <li>• [抽出済み (Extracted)] は、アーカイブの内容を抽出し、検査できたことを示します。</li> <li>• [失敗 (Failed)] は、まれなケースですが、システムが抽出を処理できない場合に発生します。</li> <li>• [深さ超過 (Depth Exceeded)] は、許可されている最大深さを超えるネストされたアーカイブファイルがアーカイブに含まれていることを示します。</li> <li>• [暗号化 (Encrypted)] は、アーカイブファイルの内容が暗号化されていて、検査できなかったことを示します。</li> <li>• [検査不可 (Not Inspectable)] は、システムがアーカイブの内容を抽出して検査しなかったことを示しています。このステータスの主な理由としては、ポリシールールアクション、ポリシー設定、破損ファイルの3つがあります。</li> </ul> <p>アーカイブファイルの内容を表示するには、イベントビューアで該当の行を右クリックしてコンテキストメニューを開いてから、[アーカイブの内容の表示 (View Archive Contents)] を選択します。</p>
カテゴリ (Category)	<p>ファイルタイプの一般的なカテゴリ (Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコードファイル、グラフィック、システムファイルなど)。</p>
検出名 (Detection Name)	<p>検出されたマルウェアの名前。</p>

フィールド	説明
傾向 (Disposition)	<p>Firepowerの傾向に関するファイルのAMPであり、次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• [マルウェア (Malware)] は、ファイルがローカルのマルウェア分析でマルウェアとして認識され、クラウドでマルウェアとして分類されていること、または、ファイルの脅威スコアが、ファイルポリシーで定義されたマルウェアしきい値を超えていることを示します。</li> <li>• [クリーン (Clean)] は、ファイルがAMPクラウドでクリーンとして分類されていること、または、ファイルをユーザがクリーンリストに追加したことを示します。</li> <li>• [不明 (Unknown)] は、システムがAMPクラウドに問い合わせましたが、ファイルの傾向が割り当てられていないこと、つまり、ファイルがAMPクラウドで正しく分類されていないことを示します。</li> <li>• [カスタム検出 (Custom Detection)] は、ファイルをユーザがカスタム検出リストに追加したことを示します。</li> <li>• [使用不可 (Unavailable)] は、システムがAMPクラウドに問い合わせできなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。</li> <li>• [N/A] は、[ファイルを検出する (Detect Files)] または [ファイルをブロックする (Block Files)] ルールによってファイルが処理され、Firepower Management CenterがAMPクラウドに問い合わせなかったことを示します。</li> </ul>
ドメイン	<p>キャプチャされたファイルが検出されたドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。</p>

フィールド	説明
ダイナミック分析ステータス (Dynamic Analysis Status)	

フィールド	説明
	<p>ファイルが AMP for Firepower によるダイナミック分析のために送信されたかどうかを示すものであり、次のうちの1つ以上が表示されます。</p> <ul style="list-style-type: none"> <li>• [分析完了 (Analysis Complete) ] : ファイルがダイナミック分析のために送信され、脅威スコアおよびダイナミック分析のサマリーレポートを受け取りました。</li> <li>• [処理予定の容量 (Capacity Handled) ] : 送信できなかったため、ファイルが保存されました。</li> <li>• [処理予定の容量 (ネットワークの問題) (Capacity Handled (Network Issue)) ] : ネットワーク接続の問題が原因で送信できなかったため、ファイルが保存されました。</li> <li>• [処理予定の容量 (レート制限) (Capacity Handled (Rate Limit)) ] : 最大数に達したことが原因で送信できなかったため、ファイルが保存されました。</li> <li>• [非アクティブなデバイス (Device Not Activated) ] : デバイスがオンプレミスの AMP Threat Grid アプリケーションでアクティブになっていないため、ファイルが送信されません。このステータスが表示された場合は、サポート担当に連絡してください。</li> <li>• [失敗 (分析タイムアウト) (Failure (Analysis Timeout)) ] : ファイルが送信されましたが、まだAMPから結果が返されていません。</li> <li>• [失敗 (ファイル実行不可) (Failure (Cannot Run File)) ] : ファイルが送信されましたが、AMP クラウドがテスト環境でファイルを実行できませんでした。</li> <li>• [失敗 (ネットワークの問題) (Failure (Network Issue)) ] : ネットワーク接続の問題のため、ファイルが送信されませんでした。</li> <li>• [分析のための送信なし (Not Sent for Analysis) ] : ファイルが送信されませんでした。</li> <li>• [疑わしくないファイル (分析のための送信なし) (Not Suspicious (Not Sent For Analysis)) ] : ファイルがマルウェアではないものとして事前に分類されています。</li> <li>• [以前に分析済み (Previously Analyzed) ] : キャッシュされた脅威スコアがあるファイルをユーザが再び送信しようとした。</li> </ul>

フィールド	説明
	<ul style="list-style-type: none"> <li>• [分析のために送信 (Sent for Analysis)] : ファイルがマルウェアとして事前に分類されており、ダイナミック分析のためにキューに入れられました。</li> </ul>
ダイナミック分析ステータスの変更 (Dynamic Analysis Status Changed)	前回、ファイルのダイナミック分析のステータスが変更された日時。
ファイル名	ファイルの SHA-256 ハッシュ値に関連付けられているものとして最後に検出されたファイル名。
前回の変更 (Last Changed)	このファイルに関連する情報が最後に更新された時刻。
最終送信日時 (Last Sent)	ファイルがダイナミック分析のために AMP for Firepower によって AMP クラウドに最後に送信された日時。
ローカル マルウェア分析ステータス (Local Malware Analysis Status)	<p>ローカル マルウェア分析が実行されたかどうかを示すものであり、次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• [分析完了 (Analysis Complete)] : ローカル マルウェア分析を使用してファイルが検査され、事前に分類されました。</li> <li>• [分析失敗 (Analysis Failed)] : ローカルマルウェア分析を使用してファイルを検査しようとし、失敗しました。</li> <li>• [手動による要求の送信 (Manual Request Submitted)] : ユーがローカル マルウェア分析のためにファイルを送信しました。</li> <li>• [分析なし (Not Analyzed)] : システムでローカル マルウェア分析を使用してファイルが検査されませんでした。</li> </ul>
SHA256	ファイルの SHA-256 ハッシュ値と、最後に検出されたファイル イベントおよびファイルの性質を表すネットワーク ファイル トラジェクトリ アイコン。ネットワーク ファイル トラジェクトリを表示するには、トラジェクトリ アイコンをクリックします。
ストレージステータス (Storage Status)	<p>ファイルが管理対象デバイスに保存されているかどうかを示し、次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• ファイル保存済み (File Stored)</li> <li>• 保存なし (性質分析の保留) (Not Stored (Disposition Was Pending))</li> </ul>

フィールド	説明
脅威スコア (Threat Score)	このファイルに関連付けられている最新の脅威スコア。 ダイナミック分析のサマリー レポートを表示するには、 脅威スコア アイコンをクリックします。
タイプ (Type)	ファイルのタイプ (HTML や MSEXE など)。

## ネットワーク ファイルトラジェクトリ

ネットワーク ファイルのトラジェクトリ機能は、ネットワーク全体でホストがどのようにファイル (マルウェア ファイルを含む) を転送したかをマッピングします。トラジェクトリは、ファイル転送データ、ファイルの性質、ファイル転送がブロックされたかどうか、ファイルが隔離されたかどうかをグラフに示します。これにより、マルウェアを転送したおそれのあるホストやリスクがあるホストがどれであるかを判定したり、ファイル転送の傾向を観測したりできます。

AMP クラウドで性質が割り当てられているファイルであれば、どのファイルの送信でも追跡できます。システムは、AMP for Firepower と AMP for Endpoints の両方によるマルウェアの検出およびブロック情報を使用して、トラジェクトリを作成します。

## 最近検出されたマルウェアおよび分析済みトラジェクトリ

[ネットワーク ファイルトラジェクトリ リスト (Network File Trajectory List)] ページには、ネットワークで最近検出されたマルウェアと最後に表示したトラジェクトリマップのファイルが表示されます。これらのリストから、ネットワークで各ファイルが最後に発見されたのはいつか、ファイルの SHA-256 のハッシュ値、名前、タイプ、現在のファイルの性質、内容 (アーカイブ ファイルの場合)、ファイルに関連付けられたイベント数を確認できます。

また、このページに含まれる検索ボックスを使用して、SHA-256 ハッシュ値またはファイル名を基準に、あるいはファイルを送信または受信するホストの IP アドレスによってファイルを見つけることができます。ファイルを見つけた後、[ファイル SHA256 (File SHA256)] 値をクリックすると詳細なトラジェクトリ マップが表示されます。

## ネットワーク ファイルトラジェクトリの詳細ビュー

詳細なネットワーク ファイルトラジェクトリを表示して、ネットワーク全体でファイルを追跡できます。ファイルの SHA 256 値を検索するか、[ネットワーク ファイルトラジェクトリ (Network File Trajectory)] リスト内の [ファイルの SHA 256 (File SHA 256)] リンクをクリックして、そのファイルに関する詳細を表示します。

ネットワーク ファイルトラジェクトリの詳細ページには、3 つの部分があります。

- サマリー情報：ファイルのトラジェクトリ ページには、ファイルに関するサマリー情報（ファイル識別情報、ネットワーク上でファイルが最初に表示された時間および最後に表示された時間、ファイルに関連したイベントおよびホストの数、ファイルの現在の性質など）が表示されます。このセクションから、管理対象デバイスがファイルを保存した場合に、そのファイルをローカルにダウンロードしたり、ファイルを動的分析用に送信したり、ファイルをファイル リストに追加したりできます。
- トラジェクトリー マップ：ファイルのトラジェクトリ マップは、ネットワークで最初に検出された時点から直近までファイルを視覚的に追跡します。このマップは、ホストがファイルを転送または受信した時点、ファイルを転送した頻度、ファイルがブロックまたは隔離された時点を示します。データポイント間の縦線は、ホスト間のファイル転送を表します。データポイントをつなぐ横棒は、時間の経過に応じたホストのファイルアクティビティを示します。  
また、そのファイルでファイルイベントが発生した頻度や、システムがファイルに性質または適応的性質を割り当てた時点についても示します。マップでデータポイントを選択し、ホストがそのファイルを転送した最初のインスタンスに遡るパスを強調表示できます。また、このパスは、ファイルの送信側または受信側としてホストが関与する各オカレンスと交差します。
- 関連イベント：[イベント (Events)] テーブルに、マップ内の各データポイントに関するイベント情報がリストされます。テーブルおよびマップを使用して、特定のファイルイベント、このファイルを転送または受信したネットワーク上のホスト、マップ内の関連するイベント、選択した値で制限されたテーブル内の他の関連するイベントを特定することができます。

## ネットワーク ファイル トラジェクトリのサマリー情報

次の概要情報は、ネットワーク ファイル トラジェクトリのリストに表示されるファイルの詳細ページの上部に表示されます。



**ヒント** 関連するファイルイベントを表示するには、フィールド値のリンクをクリックします。ファイルイベントのデフォルトのワークフローの最初のページが新しいウィンドウで開き、選択した値を含むすべてのファイル イベントも表示されます。

表 304: ネットワーク ファイル トラジェクトリのサマリー情報フィールド

[名前 (Name)]	説明
コンテンツのアーカイブ (Archive Contents)	検査されたアーカイブ ファイルで、アーカイブに含まれているファイルの数。

[名前 (Name) ]	説明
現在の傾向 (Current Disposition)	<p>次のいずれかの AMP for Firepower ファイルの性質です。</p> <ul style="list-style-type: none"> <li>• マルウェア (Malware) : ファイルが AMP クラウドでマルウェアと分類されていること、ローカル マルウェア分析でマルウェアとして識別されたこと、またはファイルの脅威スコアがファイル ポリシーに定義されたマルウェアのしきい値を超えたこと示します。</li> <li>• [クリーン (Clean) ] : AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。</li> <li>• [不明 (Unknown) ] : システムが AMP クラウドに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、AMPクラウドがファイルを正しく分類していませんでした。</li> <li>• カスタム検出 (Custom Detection) : ユーザがカスタム検出リストにファイルを追加したことを示します。</li> <li>• 利用不可 (Unavailable) : システムが AMP クラウドでクエリを行えなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。</li> <li>• [該当なし (N/A) ] : [ファイル検出 (Detect Files) ] または [ファイルブロック (Block Files) ] ルールがファイル进行处理し、Firepower Management Center が AMPクラウドに問い合わせなかったことを示します。</li> </ul>
検出名 (Detection Name)	ローカル マルウェア分析によって検出されたマルウェアの名前。
イベント カウント (Event Count)	ファイルに関連付けられたネットワークで発見されたイベントの数、検出されたイベントの数が 250 を超える場合は、マップに表示されるイベントの数。
ファイル カテゴリ (File Category)	ファイル タイプの一般的なカテゴリ (Office Documents や System Files など) 。
ファイル名 (File Names)	<p>ネットワーク上で発見された、イベントに関連したファイルの名前。</p> <p>複数のファイル名が SHA-256 ハッシュ値に関連付けられている場合、最後に検出されたファイル名がリストされます。[詳細 (more) ] をクリックすると、これが展開されて、残りのファイル名が表示されます。</p>



[名前 (Name) ]	説明
ファイル SHA256 (File SHA256)	ファイルの SHA-256 ハッシュ値。  デフォルトで、ハッシュは簡略化された形式で表示されず。完全なハッシュ値を表示するには、その上にポインタを移動させます。複数の SHA-256 ハッシュ値がファイル名に関連付けられている場合、リンクの上にポインタを移動されると、すべてのハッシュ値が表示されます。
ファイル サイズ (File Size) (KB)	ファイルのサイズ (KB 単位)。
ファイル タイプ (File Type)	ファイルのタイプ (HTML や MSEXEC など)。
最初の確認日時 (First Seen)	AMP for Firepower またはエンドポイント向け AMP による初めてのファイル検出に加えて、ファイルを初めてアップロードしたホストの IP アドレス、。
前回の検出 (Last Seen)	AMP for Firepower またはエンドポイント向け AMP による最新のファイル検出に加えて、ファイルを最後にダウンロードしたホストの IP アドレス、。
親アプリケーション (Parent Application)	エンドポイント向け AMP による検出が行われたときに、マルウェア ファイルにアクセスしていたクライアントアプリケーション。これらのアプリケーションはネットワーク検出またはアプリケーション制御とは関係ありません。
表示日 (Seen On)	ファイルを送信または受信したホストの数。1つのホストが1つのファイルのアップロードおよびダウンロードを時を異にして行う場合があるため、ホストの合計数が、[明細の表示日 (Seen On Breakdown) ] フィールドの送信側の総数と受信側の総数の合計と一致しないことがあります。
分析 (Seen On Breakdown)	ファイルを送信したホストの数とファイルを受信したホストの数。
脅威名 (Threat Name)	エンドポイント向け AMP によって検出されたマルウェアに関連付けられている脅威の名前。
脅威スコア (Threat Score)	ファイルの脅威スコア。

## ネットワーク ファイルトラジェクトリマップと関連イベントリスト

ファイルトラジェクトリマップの Y 軸には、ファイルと対話したすべてのホストの IP アドレスがリストされます。IP アドレスは、システムがそのホストでファイルを最初に検出した時点に基づいて降順でリストされます。各行には、その IP アドレスに関連付けられたすべてのイベント (単一のファイルイベント、ファイル転送、遡及的イベント) が含まれます。X 軸には、システムが各イベントを検出した日時が含まれます。タイムスタンプは時間順にリストさ

れます。複数のイベントが1分以内に発生する場合、すべてが同じ列内にリストされます。マップを左右および上下にスクロールして、イベントおよびIPアドレスをさらに表示できます。

マップには、ファイルのSHA-256ハッシュに関連した最大250のイベントが表示されます。イベントが250を超える場合、マップには最初の10個が表示され、余分のイベントは省略されて矢印アイコン (◀▶) が示されます。その後ろに、マップは残りの240個のイベントを表示します。

デフォルトの [File Events (ファイルイベント)] ワークフローの最初のページが新しいウィンドウで開き、ファイルタイプに基づいて制限されて、すべての余分のイベントが表示されません。エンドポイントベースのマルウェア イベントが表示されない場合、[マルウェア イベント (Malware Events)] テーブルに切り替えて、それらを表示する必要があります。

各データポイントは、イベントの他にファイル性質を表しています。マップの下の凡例を参照してください。たとえば、[マルウェア ブロック (Malware Block)] イベントアイコンは、[悪意のある性質 (Malicious Disposition)] アイコンと [ブロック イベント (Block Event)] アイコンを結合したものです。

エンドポイントベースのマルウェア イベントには1つアイコンが含まれます。遡及的イベントでは、ファイルで検出された各ホストのコラムにアイコンが表示されます。ファイル転送イベントでは、縦線をつながれた2つのアイコン (ファイル送信アイコンとファイル受信アイコン) が常に含まれます。矢印は、送信側から受信側へのファイル転送方向を示します。

ネットワークを介したファイルの進行状況を追跡するために、データポイントをクリックして、選択したデータポイントに関連するすべてのデータポイントを含むパスを強調表示できます。これには、次のタイプのイベントに関連付けられたデータポイントが含まれます。

- 関連付けられている IP アドレスが送信側または受信側だったファイル転送
- 関連付けられている IP アドレスが関係するエンドポイントベースのマルウェア イベント
- 別の IP アドレスが関係する場合、その関連する IP アドレスが送信側または受信側であったすべてのファイル転送
- 別の IP アドレスが関係する場合、その他方の IP アドレスが関係するエンドポイントベースのマルウェア イベント

強調表示されたデータポイントに関連付けられたすべての IP アドレスとタイムスタンプも強調表示されます。[イベント (Events)] テーブルの対応するイベントも強調表示されます。省略されたイベントがパスに含まれている場合、そのパス自体が点線で強調表示されます。省略されたイベントがパスを交差している場合がありますが、マップに表示されません。

## ネットワーク ファイルトラジェクトリの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア (AMP for Firepower) 任意 (AMP for Endpoints)	マルウェア (AMP for Firepower) 任意 (AMP for Endpoints)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができません。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

**ステップ 1** [分析 (Analysis)] > [ファイル (Files)] > [ネットワーク ファイルトラジェクトリ (Network File Trajectory)] を選択します。

**ヒント** また、ファイル情報を使用して、コンテキストエクスプローラ、ダッシュボード、またはイベント ビューからファイルのトラジェクトリにアクセスできます。

**ステップ 2** リストの [ファイル SHA 256 (File SHA 256)] リンクをクリックします。

**ステップ 3** オプションで、追跡するファイルの完全な SHA-256 ハッシュ値、ホスト IP アドレス、またはファイル名を検索フィールドに入力して、Enter を押します。

**ヒント** 1つの結果だけが一致する場合、そのファイルの [ネットワーク ファイルトラジェクトリ (Network File Trajectory)] ページが表示されます。

**ステップ 4** [サマリー情報 (Summary Information)] セクションでは、以下を実行できます。

- ファイルリストにファイルを追加する：クリーンリストまたはカスタム検出リストにファイルを追加したり、ファイルを削除したりするには、編集アイコン (✎) をクリックします。
- ファイルをダウンロードする：ファイルをダウンロードするには、ファイルのダウンロードアイコン (↓) をクリックし、プロンプトが表示されたら、ファイルをダウンロードすることを確認します。ファイルをダウンロードできない場合、このアイコンは淡色表示されます。
- レポートする：脅威スコア アイコンをクリックすると、動的分析サマリー レポートが表示されます。
- 動的分析のために送信する：AMP クラウドアイコン (☁) をクリックすると、動的分析のためにファイルを送信できます。ファイルを送信できない場合、または AMP クラウドに接続できない場合は、このアイコンは淡色表示されます。

- アーカイブの内容を表示する：アーカイブファイルの内容に関する情報を表示するには、表示アイコン (🔍) をクリックします。
- ファイル構成を表示する：ファイルの構成を表示するには、ファイル リスト アイコン (📁) をクリックします。システムがファイル構成レポートを生成していなければ、このアイコンは淡色表示されます。
- 同じ脅威スコアでキャプチャされたファイルを表示する：脅威スコアリンクをクリックすると、その脅威スコアでキャプチャされたすべてのファイルが表示されます。

(注) シスコでは、有害な結果が発生することがあるため、マルウェアをダウンロードしないように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先を保護するために必要な予防措置を行っていることを確認します。

**ステップ 5** トラジェクトリ マップでは、以下を実行できます。

- 最初のインスタンスを見つける：IP アドレスをクリックして、IP アドレスが含まれる、最初に発生したファイル イベントを見つけます。これにより、そのデータ ポイントへのパスが強調表示され、その最初のファイル イベントに関連した仲介ファイル イベントと IP アドレスがあればそれも強調表示されます。[イベント (Events)] テーブルの対応するイベントも強調表示されます。そのデータ ポイントが現在表示されていない場合、表示されるまでマップがスクロールされます。
- 追跡する：データ ポイントをクリックすると、選択したデータ ポイントに関連するすべてのデータ ポイントが含まれるパスが強調表示されます。これにより、ネットワークを介してファイルの進捗を追跡できます。
- 非表示のイベントを表示する：矢印アイコンをクリックすると、[ファイルサマリー (File Summary)] イベント ビューに表示されていないすべてのイベントが表示されます。
- ファイルの一致イベントを表示する：イベント アイコン (🔍) の上にポインタを合わせると、イベントのサマリー情報が表示されます。いずれかのイベントサマリー情報リンクをクリックすると、デフォルトの [ファイル イベント (File Events)] ワークフローの最初のページが新しいウィンドウで開き、そのファイルタイプのすべての余分のイベントが表示されます。[ファイルサマリー (File Summary)] イベント ビューが新しいウィンドウで表示され、クリックした条件値に一致するすべてのファイル イベントが表示されます。

**ステップ 6** [イベント (Events)] テーブルでは、以下を実行できます。

- 強調表示：テーブル行を選択すると、マップ上のデータ ポイントが強調表示されます。選択したファイル イベントが現在表示されていない場合、表示されるまでマップがスクロールされます。
- ソート：カラム見出しをクリックすると、昇順または降順で情報をソートできます。



## 第 109 章

# ホスト プロファイルの使用

ここでは、ホスト プロファイルの使用方法について説明します。

- [ホスト プロファイル \(2655 ページ\)](#)
- [ホスト プロファイルの基本ホスト情報 \(2657 ページ\)](#)
- [ホスト プロファイルのオペレーティング システム \(2660 ページ\)](#)
- [ホスト プロファイルのサーバ \(2666 ページ\)](#)
- [ホスト プロファイルの Web アプリケーション \(2672 ページ\)](#)
- [ホスト プロファイルのホスト プロトコル \(2674 ページ\)](#)
- [ホスト プロファイル内の侵害の兆候 \(2675 ページ\)](#)
- [ホスト プロファイルの VLAN タグ \(2675 ページ\)](#)
- [ホスト プロファイル内のユーザ履歴 \(2676 ページ\)](#)
- [ホスト プロファイル内のホスト属性 \(2676 ページ\)](#)
- [ホスト プロファイル内のホワイト リスト違反 \(2681 ページ\)](#)
- [ホスト プロファイルでのマルウェア検出 \(2683 ページ\)](#)
- [ホスト プロファイルの脆弱性 \(2684 ページ\)](#)
- [ホスト プロファイルのスキャン結果 \(2687 ページ\)](#)

## ホスト プロファイル

ホスト プロファイルは、システムが1つのホストについて収集したすべての情報の完全なビューを提供します。ホスト プロファイルにアクセスするには、以下のいずれかを実行します。

- 任意のネットワーク マップ ビューから選択します。
- モニタ対象ネットワークでホストの IP アドレスを含む任意のイベント ビューから選択します。

ホスト プロファイルは、ホスト名やMACアドレスなど、検出されたホストやデバイスに関する基本的な情報を提供します。ライセンスやシステム設定によっては、ホスト プロファイルは次の情報を提供することもできます。

- ホスト上で実行中のオペレーティング システム

- ホスト上で実行中のサーバ
- ホスト上で実行中のクライアントと Web アプリケーション
- ホスト上で実行中のプロトコル
- ホスト上の侵害の兆候 (IOC) タグ
- ホスト上の VLAN タグ
- ネットワーク上で過去の 24 時間のユーザ アクティビティ
- ホストに関連付けられているホワイトリスト違反
- ホストの最新のマルウェア イベント
- ホストに関連付けられている脆弱性
- ホストの Nmap スキャン結果

プロファイルには、ホスト属性もリストされます。ホスト属性を使用して、ネットワーク環境にとって重要な方法でホストを分類することができます。例えば、以下を行うことができます。

- ホストが存在する建物を示すホスト属性を割り当てる
- ホストの重要度の属性を使用して、特定のホストのビジネス重要度を指定し、ホストの重要度に基づいて関連ポリシーとアラートを作成する

ホストプロファイルで、そのホストに適用されている既存のホスト属性を表示し、そのホスト属性値を変更できます。

パッシブ侵入防御展開の一部としてアダプティブプロファイルの更新を使用している場合、ホスト上のオペレーティングシステム、およびホストが実行しているサーバとクライアントのタイプに最も適合するように、システムがトラフィックを処理する方法を調整することができます。

オプションで、ホストプロファイルから Nmap スキャンを実行し、ホストプロファイルのサーバ情報とオペレーティングシステムの情報を増やすことができます。Nmap スキャナはホストをアクティブに調査し、ホストを実行しているオペレーティングシステムおよびサーバの情報を取得します。スキャンの結果は、ホストのオペレーティングシステムおよびサーバアイデンティティのリストに追加されます。

ホストプロファイルには、次の制限事項があります。

#### 利用できないホスト

ホストプロファイルは、ネットワーク上のすべてのホストでは使用できない可能性があります。考えられる原因は次のとおりです。

- タイムアウトしたため、ネットワーク マップからホストが削除された。
- ホスト ライセンスの制限に達した。

- ネットワーク検出ポリシーでモニタリングされないネットワークセグメントに、ホストが存在している。

#### 利用できない情報

ホストプロファイルに表示される情報は、ホストのタイプ、および利用可能なホストの情報によって異なる可能性があります。

次に例を示します。

- 非 IP ベースのプロトコル（STP、SNAP、IPX など）を使用してシステムでホストを検出した場合、そのホストは MAC ホストとしてネットワーク マップに追加され、IP ホストに比べて使用できる情報はかなり少なくなります。
- システムは、ホストをエクスポートされた NetFlow レコードからネットワーク マップに追加できますが、これらのホストに使用できる情報は限られます（[NetFlow データと管理対象デバイス データの違い（2028 ページ）](#) を参照）。

#### 関連トピック



[ホストプロファイルの表示（2657 ページ）](#)

## ホストプロファイルの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

#### 手順

次の 2 つの選択肢があります。

- ネットワーク マップで、プロファイルを表示するホストの IP アドレスをドリル ダウンします。
- 任意のイベントビューで、ホストプロファイルアイコン () をクリックするか、またはプロファイルを表示するホストの IP アドレスの隣にある、侵害されたホストアイコン () をクリックします。

## ホストプロファイルの基本ホスト情報

各ホストプロファイルは、検出されたホストまたは他のデバイスに関する基本情報を提供します。

次に、基本的なホストプロファイルのフィールドについて説明します。

### ドメイン (Domain)

ホストに関連付けられているドメイン。

### IP アドレス

ホストに関連付けられているすべての IP アドレス (IPv4 と IPv6 の両方)。システムは、ホストに関連付けられている IP アドレスを検出し、サポートされている場合は、同じホストで使用される複数の IP アドレスをグループ化します。多くの場合、IPv6 ホストには、少なくとも 2 つの IPv6 アドレス (ローカルのみでルーティング可能なものと、グローバルにルーティング可能なもの) があり、その他に IPv4 アドレスを持っていることがあります。IPv4 専用ホストは、複数の IPv4 アドレスを持っていることがあります。

ホストプロファイルは、そのホストに関連付けられている、検出されたすべての IP アドレスを一覧で示します。可能な場合は、ルーティング可能なホスト IP アドレスに、フラグアイコン、およびアドレスに関連付けられている地理情報データを表す国コードも含まれています。

デフォルトでは最初の 3 つのアドレスだけが表示されることに注意してください。[すべて表示 (Show All)] をクリックすると、ホストのすべてのアドレスが表示されます。

### ホストネーム

ホストの完全修飾ドメイン名 (わかる場合)。

### NetBIOS 名 (NetBIOS Name)

ホストの NetBIOS 名 (使用できる場合)。Microsoft Windows ホストだけでなく、Macintosh、Linux、または NetBIOS を使用するように設定されているその他のプラットフォームに NetBIOS 名を指定できます。たとえば、Samba サーバとして設定されている Linux ホストに NetBIOS 名を指定します。

### デバイス (ホップ数) (Device (Hops))

次のいずれかを行います。

- ホストが存在しているネットワークの報告元のデバイス (ネットワーク検出ポリシーで定義)、または
- ホストをネットワーク マップへ追加する NetFlow データを処理したデバイス

デバイス名の後に、ホストを検出したデバイスとホスト自身の間のネットワークホップの数が丸括弧で囲まれて表示されます。複数のデバイスで対象のホストを参照できる場合は、報告元のデバイスが太字で表示されます。

このフィールドが空白の場合は、次のいずれかです。

- ホストがデバイスによってネットワークマップに追加されたが、このデバイスは、ホストが存在しているネットワークに対してネットワーク検出ポリシーに定義されているとおりに明示的に監視していない。または、



- ホストの入力機能を使用してホストが追加されたが、Firepower システムによって検出されていない。

### MAC アドレス (TTL) (MAC Addresses (TTL))

ホストについて検出された1つ以上のMACアドレスおよび関連付けられているNICベンダー。NICのハードウェアベンダーと現在の存続可能時間(TTL)値が括弧で囲まれて表示されます。MACアドレスが太字で表示されている場合、そのMACアドレスは、ARPおよびDHCPトラフィックで検出されたホストの実際のMACアドレスです。複数のデバイスが同じホストを検出した場合、Firepower Management Centerには、どのデバイスがホストを報告したかに関係なく、ホストに関連付けられているすべてのMACアドレスとTTL値が表示されます。

ルータのホストプロファイルは、通常、このリスト内でルーティングしているネットワークセグメント内のホスト(IPアドレス)を示します。モニタリング対象のルータのIPアドレスは、多くの場合、モニタリングされるワークステーションとサーバのリストに表示されます。MACアドレスの実際のIPアドレスは太字で表示されます。

### ホストタイプ (Host Type)

システムで検出されたデバイスのタイプ(ホスト、モバイルデバイス、ジェイルブレイクされたモバイルデバイス、ルータ、ブリッジ、NATデバイス、またはロードバランサ)。

ネットワークデバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol (CDP) メッセージの分析。ネットワークのデバイスおよびそれらのタイプ(シスコデバイスのみ)を特定できます。
- スパニングツリープロトコル(STP)の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じMACアドレスを使用している複数のホストの検出。MACアドレスを、ルータに属しているものとして識別します。
- クライアント側からのTTL値の変更、または通常のブート時間よりも頻繁に変更されているTTL値の検出。この検出では、NATデバイスとロードバランサを識別します。
- モバイルデバイスを区別するためにシステムでは次の方法を使用します。
- モバイルデバイスのモバイルブラウザからのHTTPトラフィックのユーザエージェント文字列の分析
- 特定のモバイルアプリケーションのHTTPトラフィックのモニタリング

デバイスがネットワークデバイスまたはモバイルデバイスとして識別されない場合は、ホストとして分類されます。

### 前回の検出 (Last Seen)

ホストのいずれかのIPアドレスが最後に検出された日時。

### 現在のユーザ (Current User)

このホストに最後にログインしたユーザ。

既存の現在のユーザが権限のあるユーザでない場合、ホストにログインしている権限を持たないユーザは、現在のユーザとして登録されるだけであることに注意してください。

### 表示 (View)

接続、検出、マルウェア、および侵入イベントデータのビューへのリンク。このリンクは、そのイベントタイプのデフォルトワークフローを使用し、ホストに関連するイベントを表示するように制限されています。可能な場合は、これらのイベントには、ホストに関連付けられているすべての IP アドレスが含まれます。

## ホストプロファイルのオペレーティングシステム

システムは、ホストで生成されたトラフィック内のネットワークおよびアプリケーションスタックを分析したり、**User Agent** でレポートされたホストデータを分析することによって、ホスト上で稼動しているオペレーティングシステムのアイデンティティをパッシブに検出します。システムでは、他のソース (Nmap スキャナ、ホストの入力機能によりインポートされたアプリケーションデータ) のオペレーティングシステムの情報も照合します。どのアイデンティティを使用するかを判断する場合、システムは、各アイデンティティのソース (発生源) に割り当てられている優先度を考慮します。デフォルトでは、ユーザ入力が高最も高い優先度を持ち、以降は高い順にアプリケーションまたはスキャナソース、検出されたアイデンティティ、となります。

システムでは、オペレーティングシステムの具体的な定義ではなく、全般的な定義を提供することがあります。これは、トラフィックおよび他のアイデンティティソースで、対象のアイデンティティを詳しく調べるための十分な情報が提供されないためです。システムは、できるだけ詳しい定義を使用するために、ソースの情報を照合します。

オペレーティングシステムは、ホストの脆弱性リスト、およびホストを対象とするイベントの影響の相関関係に影響するため、オペレーティングシステムの特定の情報を手動で入力することもできます。また、オペレーティングシステムに対して、サービスパックやアップデートなどの修正ファイルが適用されたことを示すことも、修正ファイルによって対処された脆弱性を無効にすることもできます。

たとえば、システムでホストのオペレーティングシステムが **Microsoft Windows 2003** であると特定されたが、実際にはホストが **Microsoft Windows XP Professional** および **Service Pack 2** を実行していることがわかっている場合、オペレーティングシステムのアイデンティティを実際のおりに設定することができます。より具体的なオペレーティングシステムのアイデンティティを設定すると、ホストの脆弱性のリストの精度が向上するため、対象のホストに対する影響の相関関係が、より限定的かつ正確になります。

システムでホストに対するオペレーティングシステム情報が検出され、その情報が、アクティブなソースによって提供されている現行のオペレーティングシステムのアイデンティティと競合している場合、アイデンティティの競合が発生します。実際にアイデンティティの競合が発

生している場合、システムは脆弱性と影響の相関関係の両方のアイデンティティを使用します。

ネットワーク検出ポリシーを設定して、NetFlow エクスポートによってモニタされるホストのネットワーク マップに検出データを追加することができます。ただし、オペレーティング システムの ID を設定するためにホスト入力機能の使用を設定しない限り、これらのホストで使用可能なオペレーティング システム データはありません。

オペレーティングシステムを実行しているホストが、有効なネットワーク検出ポリシーのコンプライアンスのホワイトリストに違反している場合、Firepower Management Center はオペレーティングシステムの情報にホワイトリストの違反アイコン (❗) のマークを付けます。また、ジェイルブレイクされたモバイルデバイスが有効なホワイトリストに違反している場合、そのデバイスのオペレーティング システムの隣にアイコンが表示されます。

ホストのオペレーティングシステムのアイデンティティに対して、カスタム表示文字列を設定できます。この表示文字列は、ホスト プロファイルで使用されます。



(注) あるホストについてオペレーティングシステムの情報を変更すると、ホストのコンプライアンス、およびコンプライアンスのホワイト リストが変わる可能性があります。

ネットワーク デバイスに対するホスト プロファイルでは、[オペレーティング システム (Operating Systems)] セクションのラベルが [システム (Systems)] に変わり、[ハードウェア (Hardware)] カラムが新しく表示されます。[システム (Systems)] の下にハードウェアプラットフォームの値が表示され場合、システムは、ネットワークデバイスの背後で1つ以上のモバイルデバイスが検出されたことを示しています。モバイルデバイスはハードウェアプラットフォームの情報を持っていることも、持っていないこともあります。モバイルデバイスではないシステムではハードウェアプラットフォーム情報は検出されないことに注意してください。

次に、ホスト プロファイルで表示されるオペレーティング システムの情報フィールドについて説明します。

#### ハードウェア (Hardware)

モバイルデバイスのハードウェア プラットフォーム。

#### OS ベンダー/ベンダー (OS Vendor/Vendor)

オペレーティング システムのベンダー。

#### OS 製品/製品 (OS Product/Product)

次の値のいずれかを指定します。

- すべてのソースから収集されたアイデンティティデータに基づいて、実行されている可能性が最も高いと判断されたオペレーティング システム。

- [Pending] : システムがオペレーティングシステムをまだ識別しておらず、他に使用可能なアイデンティティ データがない場合。
- [unknown] : システムがオペレーティングシステムを識別できず、オペレーティングシステムに関して他に使用可能なアイデンティティ データがない場合。



(注) ホストのオペレーティングシステムをシステムで検出できない場合には、[ホストオペレーティングシステムの識別 \(2040 ページ\)](#) を参照してください。

### OS バージョン/バージョン (OS Version/Version)

オペレーティングシステムのバージョン。ホストがジェイルブレイクされたモバイル デバイスの場合、バージョンの後に括弧で囲まれて Jailbroken と示されます。

### ソース (Source)

次の値のいずれかを指定します。

- [ユーザ (User) ] : user\_name
- [アプリケーション (Application) ] : app\_name
- [スキャナ (Scanner) ] : scanner\_type (Nmap またはその他のスキャナ)
- Firepower

システムでは、オペレーティングシステムのアイデンティティを判断するために、複数のソースのデータを統合することができます。

## オペレーティングシステムアイデンティティの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

検出された、またはホストに追加された特定のオペレーティングシステムのアイデンティティを表示することができます。システムはソースの優先度を使用して、ホストに対する現行のアイデンティティを判断します。アイデンティティのリストでは、現行のアイデンティティが太字で強調されます。

1つのホストに対して複数のオペレーティングシステムのアイデンティティが存在している場合のみ、[表示 (View) ] ボタンが有効になっていることに注意してください。

手順

- ステップ 1 ホスト プロファイルの [オペレーティング システム (Operating System) ] または [オペレーティング システムの競合 (Operating System Conflicts) ] セクションで [表示 (View) ] をクリックします。
- ステップ 2 [ホスト プロファイルのオペレーティング システム \(2660 ページ\)](#) の説明に従って情報を入力します。
- ステップ 3 必要に応じて、オペレーティング システムのアイデンティティの横にある削除アイコン (🗑️) をクリックします。

(注) シスコが検出したオペレーティング システムのアイデンティティは削除できません。

該当する場合は、このシステムは [オペレーティング システムのアイデンティティ情報 (Operating System Identity Information) ] ポップアップ ウィンドウからアイデンティティを削除し、ホスト プロファイルのオペレーティング システムの現在のアイデンティティを更新します。

## 現在のオペレーティング システムのアイデンティティの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

Firepower システム Web インターフェイスを使用して、ホストに対する現行のオペレーティング システムのアイデンティティを設定できます。Web インターフェイスを介してアイデンティティを設定すると、他のすべてのアイデンティティソースが上書きされるため、このアイデンティティが、脆弱性の評価および影響の相関関係で使用されます。ただし、オペレーティング システムを編集した後で、ホストに対するオペレーティング システムのアイデンティティの競合がシステムで検出されると、オペレーティング システムの競合が発生します。競合が解決されるまで、両方のオペレーティング システムが現行のものであるとみなされます。

手順

- ステップ 1 ホスト プロファイルの [オペレーティング システム (Operating System) ] セクションで [編集 (Edit) ] をクリックします。
- ステップ 2 ここでは次のオプションがあります。
  - [OS 定義 (OS Definition) ] ドロップダウンリストから [現在の定義 (Current Definition) ] を選択して、ホスト入力によって現行のオペレーティング システムのアイデンティティを確認して、手順 6 に進みます。

- [OS 定義 (OS Definition)] ドロップダウン リストから現行のオペレーティングシステム のアイデンティティのバリエーションを選択し、手順 6 に進みます。
- [OS 定義 (OS Definition)] ドロップダウンリストから [ユーザ定義 (User-Defined)] を選択して、手順 3 に進みます。

**ステップ 3** 必要に応じて、[カスタム表示文字列を使用する (Use Custom Display String)] を選択し、[ベンダー文字列 (Vendor String)]、[製品文字列 (Product String)]、および [バージョン文字列 (Version String)] フィールドに表示するカスタム文字列を変更します。

**ステップ 4** 必要に応じて、別のベンダーからのオペレーティングシステムに変更するには、[ベンダー (Vendor)] と [製品 (Product)] のドロップダウンリストから選択します。

**ステップ 5** 必要に応じて、オペレーティングシステムの製品リリース レベルを設定するには、[メジャー (Major)]、[マイナー (Minor)]、[リビジョン (Revision)]、[ビルド (Build)]、[パッチ (Patch)]、および [拡張 (Extension)] ドロップダウンリストから選択します。

**ステップ 6** 必要に応じて、オペレーティングシステムに対して修正ファイルが適用されたことを示す場合は、[修正の設定 (Configure Fixes)] をクリックします。

**ステップ 7** ドロップダウン リストから適用可能な修正を選択し、[追加 (Add)] をクリックします。

**ステップ 8** 必要に応じて、[パッチ (Patch)] および [拡張 (Extension)] ドロップダウン リストを使用して、対象のパッチと拡張機能を追加します。

**ステップ 9** [終了 (Finish)] をクリックします。

---

#### 関連トピック

[オペレーティングシステムのアイデンティティの競合](#) (2664 ページ)

## オペレーティングシステムのアイデンティティの競合

システムで検出された新しいアイデンティティと現行のアイデンティティが競合しており、そのアイデンティティが、スキャナやアプリケーション、ユーザなどのアクティブなソースによって提供されていた場合、オペレーティングシステムのアイデンティティで競合が発生します。

ホスト プロファイルでは、競合状態のオペレーティングシステムのアイデンティティのリストは太字で表示されます。

システムの Web インターフェイスを介して、アイデンティティの競合を解決し、ホストに対する現行のオペレーティングシステムのアイデンティティを設定することができます。Web インターフェイスを介してアイデンティティを設定すると、他のすべてのアイデンティティソースが上書きされるため、このアイデンティティが、脆弱性の評価および影響の相関関係で使用されます。

#### 関連トピック

[ネットワーク検出アイデンティティ競合の解決の設定](#) (2165 ページ)

## 競合しているオペレーティングシステムのアイデンティティの現行化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

## 手順

**ステップ 1** ホスト プロファイルの [オペレーティング システム (Operating System)] セクションに移動します。

**ステップ 2** 次の 2 つの選択肢があります。

- ホストのオペレーティング システムとして設定するオペレーティング システムのアイデンティティの隣にある、[現行にする (Make Current)] をクリックします。
- アクティブなソースで、現行のアイデンティティとして使用しないアイデンティティが表示された場合は、使用しないアイデンティティを削除します。

## オペレーティングシステムのアイデンティティ競合の解決

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

## 手順

**ステップ 1** ホスト プロファイルの [オペレーティング システムの競合 (Operating System Conflicts)] セクションにある [解決 (Resolve)] をクリックします。

**ステップ 2** 次の選択肢があります。

- [OS 定義 (OS Definition)] ドロップダウンリストから [現在の定義 (Current Definition)] を選択して、ホスト入力によって現行のオペレーティングシステムのアイデンティティを確認して、手順 6 に進みます。
- [OS 定義 (OS Definition)] ドロップダウンリストから、競合しているオペレーティングシステムのアイデンティティのいずれかのバリエーションを選択して、手順 6 に進みます。
- [OS 定義 (OS Definition)] ドロップダウンリストから [ユーザ定義 (User-Defined)] を選択して、手順 3 に進みます。

- ステップ 3** 必要に応じて、[カスタム表示文字列の使用 (Use Custom Display String)] を選択して、表示するカスタム文字列を [ベンダー文字列 (Vendor String)]、[製品文字列 (Product String)]、および [バージョン文字列 (Version String)] フィールドに入力します。
- ステップ 4** 必要に応じて、別のベンダーからのオペレーティングシステムに変更するには、[ベンダー (Vendor)] と [製品 (Product)] のドロップダウンリストから選択します。
- ステップ 5** 必要に応じて、オペレーティングシステムの製品リリースレベルを設定するには、[メジャー (Major)]、[マイナー (Minor)]、[リビジョン (Revision)]、[ビルド (Build)]、[パッチ (Patch)] および [拡張 (Extension)] ドロップダウンリストから選択します。
- ステップ 6** 必要に応じて、オペレーティングシステムに対して修正ファイルが適用されたことを示す場合は、[修正の設定 (Configure Fixes)] をクリックします。
- ステップ 7** 適用した修正ファイルを、修正ファイルリストに追加します。
- ステップ 8** [終了 (Finish)] をクリックします。

---

### 関連トピック

[ネットワーク検出アイデンティティ競合の解決の設定 \(2165 ページ\)](#)

## ホストプロファイルのサーバ

ホストプロファイルのサーバセクションでは、監視対象ネットワーク上のホストで検出されるか、エクスポートされた NetFlow レコードから追加されるか、スキャナまたはホスト入力機能のようなアクティブなソースを介して追加されるサーバを列挙します。

リストは 1 つのホストにつき最大 100 台のサーバを表示します。100 個の制限に達すると、ホストからサーバを削除するか、またはサーバがタイムアウトになるまで、いずれかのソースの新しいサーバ情報は、アクティブであってもパッシブであっても廃棄されます。

Nmap を使用してホストをスキャンすると、オープンな TCP ポート上で稼動している、以前に検出されなかったサーバの結果が Nmap によって Servers リストに追加されます。Nmap スキャンを実行した場合、または Nmap の結果をインポートした場合、ホストプロファイルに拡張可能な [スキャン結果 (Scan Results)] セクションも表示され、Nmap スキャンによってホスト上で検出されたサーバ情報が示されます。さらに、ネットワークマップからホストが削除されると、ホストのそのサーバに対する Nmap スキャンの結果は廃棄されます。





- (注) システムは、ホストをエクスポートされた NetFlow レコードからネットワークマップに追加できますが、これらのホストに使用できる情報は限られます ([NetFlow データと管理対象デバイスデータの違い \(2028 ページ\)](#) を参照)。

ホストプロファイルでサーバを使用するためのプロセスは、ユーザがプロファイルにアクセスする方法によって異なります。

- ネットワークマップを介したドリルダウンによりホストプロファイルにアクセスする場合は、サーバの名前が太字で強調されて、サーバの詳細が表示されます。ホストの他の



サーバについて詳細を表示する場合は、対象のサーバ名の隣にある表示アイコン ([) をクリックします。

- 他の方法でホストプロファイルにアクセスする場合は、[サーバ (Servers) ]セクションを展開し、詳細を表示するサーバの隣にある表示アイコン ([) をクリックします。



- (注) ホストが、有効な相関ポリシーにおけるコンプライアンスのホワイトリストに違反しているサーバを実行している場合、Firepower Management Center は非準拠サーバに、ホワイトリストの違反アイコン ([) のマークを付けます。

次に、[Servers リスト (Servers list) ] の列について説明します。

### プロトコル

サーバが使用するプロトコルの名前。

### [ポート (Port) ]

サーバが実行されているポート。

### アプリケーション プロトコル (Application Protocol)

次のいずれかになります。

- アプリケーション プロトコルの名前
- [保留中 (pending) ]: システムで、いずれかの理由でアプリケーション プロトコルをポジティブまたはネガティブに識別できない場合
- [未知 (unknown) ]: 既知のアプリケーション プロトコルのフィンガープリントに基づいてシステムでアプリケーションプロトコルを識別できない場合、または (対応するサーバは追加せずに、ポート情報での脆弱性を追加することにより) ホストの入力を介してサーバが追加された場合

アプリケーションプロトコルの名前にマウスを重ねると、タグが表示されます。

### ベンダーおよびバージョン (Vendor and Version)

Firepower システム、Nmap、または他のアクティブなソースで識別されたベンダーとバージョン、またはホストの入力機能を介して取得したベンダーとバージョン。有効なソースで識別が行われなかった場合、フィールドは空白になります。

### 関連トピック

[ホスト制限と検出イベント ロギング](#) (2102 ページ)

[NetFlow データと管理対象デバイス データの違い](#) (2028 ページ)

[アプリケーションディテクタの基本](#) (2098 ページ)

## ホストプロファイルのサーバの詳細

Firepower Management Center は、1つのサーバについてパッシブに検出されるアイデンティティを最大16個表示します。パッシブな検出ソースには、ネットワーク検出データおよびNetFlowレコードが含まれます。システムで、このサーバの複数のベンダーまたはバージョンを検出した場合、サーバは複数のパッシブなアイデンティティを持つことができます。たとえば、Webサーバが、サーバソフトウェアと同じバージョンを実行していない場合、管理対象デバイスとWebサーバファーム間にロードバランサがあると、HTTPに対してシステムが複数のパッシブアイデンティティを識別することがあります。Firepower Management Center は、ユーザ入力、スキャナ、その他のアプリケーションなど、アクティブなソースからのサーバアイデンティティの数を制限することはありません。

Firepower Management Center は現行のアイデンティティを太字で表示します。システムでは、1つのホストに対する脆弱性の割り当て、影響の評価、ホストプロファイルの証明書およびコンプライアンスホワイトリストに対して記載された関連ルールの評価など、いくつかの目的のためにサーバの現行のアイデンティティを使用します。

サーバの詳細には、選択されたサーバについて知られている、更新済みのサブサーバ情報が表示されることもあります。

サーバの詳細にサーバのバナーが表示されることもあります。これは、ホストプロファイルからサーバを表示したときに、サーバの詳細の下に表示されます。サーバのバナーは、サーバを識別するのに役立つサーバに関する追加情報を提供します。攻撃者がサーバのバナー文字列を意図的に変更した場合、システムは誤ったアイデンティティが示されたサーバを識別または検出できません。サーバのバナーには、そのサーバについて検出された最初のパケットの最初の256文字が表示されます。この情報は、サーバがシステムによって最初に検出されたときに一度だけ収集されます。バナーの内容は2列で表示されます。左側の列は16進表記で示され、右側の列は対応するASCII表記で示されます。



- (注) サーバのバナーを表示するには、ネットワーク検出ポリシーで[バナーのキャプチャ (Capture Banners)]チェックボックスを有効にする必要があります。このオプションはデフォルトでは無効になっています。

ホストプロファイルのサーバの詳細セクションには、次の情報が含まれています。

### プロトコル

サーバが使用するプロトコルの名前。

### [ポート (Port)]

サーバが実行されているポート。

### ヒット数 (Hits)

Firepower システムの管理対象デバイスまたはNmapスキャナによってサーバが検出された回数。ホストの入力によってインポートされたサーバについては、システムがそのサーバについてトラフィックを検出しない場合、検出回数は0になります。

### 前回の使用 (Last Used)

サーバが最後に検出された日時。システムで対象のサーバについて新しいトラフィックを検出しない場合、ホスト入力のデータが最後に使用された時間は、データの最初のインポート時間を反映しています。ホストの入力機能を介してインポートされたスキャナおよびアプリケーションのデータは、Firepower Management Center の設定に応じてタイムアウトしますが、Management Center の Web インターフェイスを介したユーザ入力の場合はタイムアウトしません。

### アプリケーション プロトコル (Application Protocol)

既知の場合、サーバが使用するアプリケーション プロトコルの名前。

### ベンダー (Vendor)

サーバのベンダー。ベンダーがわからない場合、このフィールドは表示されません。

### バージョン (Version)

サーバのバージョン。バージョンがわからない場合、このフィールドは表示されません。

### ソース (Source)

次の値のいずれかを指定します。

- [ユーザ (User) ] : user\_name
- [アプリケーション (Application) ] : app\_name
- [スキャナ (Scanner) ] : scanner\_type (Nmap またはその他のスキャナ)
- Firepower システムで検出されたアプリケーションの場合、Firepower、Firepower Port Match、または Firepower Pattern Match
- NetFlow レコードからネットワーク マップに追加されたサーバの場合、NetFlow

システムでは、サーバのアイデンティティを判断するために、複数のソースのデータを統合することができます。

### 関連トピック

[アプリケーションおよびオペレーティング システムの現在の ID](#) (2024 ページ)

## サーバに関する詳細情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

## 手順

ホストプロファイルの [サーバ (Servers) ] セクションで、サーバの横にある表示アイコン (🔍) をクリックします。

## サーバのアイデンティティの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

ホスト上のサーバのアイデンティティ設定を手動で更新し、修正ファイルによって対処された脆弱性を削除するために、ホストに適用した何らかの修正ファイルを設定することができます。サーバのアイデンティティを削除することもできます。

アイデンティティを削除した場合、削除したアイデンティティが唯一のアイデンティティであっても、サーバは削除されません。アイデンティティを削除すると、[サーバの詳細 (Server Detail) ] ポップアップ ウィンドウからアイデンティティが削除されます。可能な場合は、ホストプロファイルでそのサーバの現行のアイデンティティを更新します。

シスコ管理対象デバイスによって追加されたサーバのアイデンティティは、編集または削除できません。

## 手順

- ステップ 1** ホストプロファイルの [サーバ (Servers) ] セクションに移動します。
- ステップ 2** [表示 (View) ] をクリックし、[サーバの詳細 (Server Detail) ] ポップアップ ウィンドウを開きます。
- ステップ 3** サーバのアイデンティティを削除するには、削除するサーバのアイデンティティの横にある削除アイコン (🗑️) をクリックします。
- ステップ 4** サーバのアイデンティティを変更するには、サーバリストでサーバの横にある編集アイコン (✏️) をクリックします。
- ステップ 5** 次の 2 つの選択肢があります。
  - [サーバタイプの選択 (Select Server Type) ] ドロップダウンリストから現行の定義を選択します。
  - [サーバタイプの選択 (Select Server Type) ] ドロップダウンリストからサーバのタイプを選択します。

- ステップ6** オプションで対象のサーバタイプのベンダーと製品のみを表示するには、[サーバタイプで制限 (Restrict by Server Type)] チェックボックスをオンにします。
- ステップ7** オプションでサーバの名前とバージョンをカスタマイズするには、[カスタム表示文字列の使用 (Use Custom Display String)] を選択し、[ベンダー文字列 (Vendor String)] と [バージョン文字列 (Version String)] に入力します。
- ステップ8** [製品マッピング (Product Mappings)] セクションで、使用するオペレーティング システム、製品、およびバージョンを選択します。
- 例：
- たとえば、サーバを Red Hat Linux 9 にマップする場合は、ベンダーとして [Redhat, Inc.] を、製品として [Redhat Linux] を選択し、バージョンとして [9] を選択します。
- ステップ9** サーバの修正が適用されていることを示す場合は、[修正の設定 (Configure Fixes)] をクリックして、そのサーバに適用するパッチを修正リストに追加します。
- ステップ10** [終了 (Finish)] をクリックします。

## サーバアイデンティティの競合の解決

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

アプリケーションやスキャナなどのアクティブなソースが、サーバのアイデンティティデータをホストへ追加したときに、サーバアイデンティティの競合が発生します。その後で、システムはサーバアイデンティティの競合を示しているポートのトラフィックを検出します。

### 手順

- ステップ1** ホスト プロファイルで、[サーバ (Servers)] セクションに移動します。
- ステップ2** サーバの横にある解決アイコンをクリックします。
- ステップ3** [サーバタイプの選択 (Select Server Type)] ドロップダウンリストからサーバのタイプを選択します。
- ステップ4** 必要に応じて、対象のサーバタイプのベンダーと製品のみを表示する場合は、[サーバタイプ別に制限 (Restrict by Server Type)] チェックボックスをオンにします。
- ステップ5** 必要に応じて、サーバの名前とバージョンをカスタマイズする場合は、[カスタム表示文字列の使用 (Use Custom Display String)] を選択して、[ベンダー文字列 (Vendor String)] と [バージョン文字列 (Version String)] を入力します。
- ステップ6** [製品マッピング (Product Mappings)] セクションで、使用するオペレーティング システム、製品、およびバージョンを選択します。

例：

たとえば、サーバを Red Hat Linux 9 にマップする場合は、ベンダーとして [Redhat, Inc.] を、製品として [Redhat Linux] を選択し、バージョンとして [9] を選択します。

**ステップ 7** サーバの修正が適用されていることを示す場合は、[修正の設定 (Configure Fixes)] をクリックして、そのサーバに適用するパッチを修正リストに追加します。

**ステップ 8** [終了 (Finish)] をクリックします。

---

#### 関連トピック

[ネットワーク検出アイデンティティ競合の解決の設定](#) (2165 ページ)

## ホスト プロファイルの Web アプリケーション

ホストプロファイルの [Web アプリケーション (Web Application)] セクションには、ネットワーク内のホスト上で動作していることをシステムが識別したクライアントと Web アプリケーションが表示されます。システムでは、パッシブ検出ソースとアクティブ検出ソースの両方から取得されるクライアントと Web アプリケーションの情報を識別できます。ただし、NetFlow レコードから追加されたホストに関する情報は一部しか取得することができません。

このセクションには、ホスト上で検出されたアプリケーションの製品とバージョン、使用できるクライアントまたは Web アプリケーションの情報、アプリケーションが最後に使用中であると検出された時間などの詳細情報が表示されます。

ホスト上で稼動している最大 16 個のクライアントが、このセクションに表示されます。16 個の制限に達すると、ユーザがホストからクライアントアプリケーションを削除するか、または非アクティブである (クライアントがタイムアウトしている) ためにシステムによってホストプロファイルからクライアントが削除されるまで、新しいクライアント情報は、どのソースのものであるか、アクティブかパッシブかにかかわらず、廃棄されます。

また、検出されたそれぞれの Web ブラウザについては、アクセスされた最初の 100 個の Web アプリケーションが表示されます。この制限に達すると、ブラウザに関連付けられている新しい Web アプリケーションは、どのソースのものであるか、アクティブかパッシブかにかかわらず、次の条件を満たすまで廃棄されます。

- Web ブラウザのクライアントアプリケーションがタイムアウトになる、または
- ユーザが、Web アプリケーションに関連付けられているアプリケーション情報をホストプロファイルから削除する

ホストが、有効な相関ポリシーにおけるコンプライアンスのホワイトリストに違反しているアプリケーションを実行している場合、Firepower Management Center は非標準アプリケーションに、ホワイトリストの違反アイコン (🚫) のマークを付けます。



**ヒント** ホスト上の特定のアプリケーションに関連付けられている接続イベントを分析するには、アプリケーションの隣にあるイベントアイコン (🔍) をクリックします。接続イベントに対する優先ワークフロー最初のページが表示され、ホストの IP アドレスの他、アプリケーションのタイプ、プロトコル、およびバージョンで制約されて接続イベントが示されます。接続イベントに対する優先ワークフローがない場合、ワークフローを選択する必要があります。

次に、ホストプロファイルに表示されるアプリケーション情報について説明します。

#### アプリケーション プロトコル

アプリケーション (HTTP ブラウザ、DNS クライアントなど) で使用されるアプリケーション プロトコルを表示します。

#### クライアント (Client)

ペイロードから派生したクライアント情報。この情報は、Firepower システムが識別するか、Nmap がキャプチャするか、またはホスト入力機能によって取得されます。有効なソースで識別が行われなかった場合、フィールドは空白になります。

#### バージョン (Version)

クライアントのバージョンが表示されます。

#### Web アプリケーション

Web ブラウザの場合は、http トラフィックでシステムによって検出されたコンテンツ。Web アプリケーションの情報は、Firepower システムによって識別された、Nmap によってキャプチャされた、他のアクティブなソースによって取得された、またはホストの入力機能を介して取得された特定のタイプのコンテンツ (WMV や QuickTime など) を表します。有効なソースで識別が行われなかった場合、フィールドは空白になります。

## ホストプロファイルからの Web アプリケーションの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

ホストプロファイルからアプリケーションを削除して、ホスト上で稼動していないことがわかっているアプリケーションを削除することができます。ホストからアプリケーションを削除すると、そのホストにホワイトリストのコンプライアンスが適用されることがあります。



(注) システムでアプリケーションが再検出されると、アプリケーションはネットワークマップおよびホストプロファイルに再度追加されます。

#### 手順

**ステップ1** ホストプロファイルで、[アプリケーション (Applications)] セクションに移動します。

**ステップ2** 削除するアプリケーションの横にある削除アイコン (🗑️) をクリックします。

## ホストプロファイルのホストプロトコル

各ホストプロファイルには、ホストに関連付けられているネットワークトラフィックで検出されたプロトコルに関する情報が含まれています。この情報には次のものが含まれます。

#### プロトコル

ホストが使用するプロトコルの名前。

#### 層 (Layer)

プロトコルを実行しているネットワーク層 (ネットワークまたはトランスポート)。

ホストプロファイルに表示されているプロトコルが、有効な関連ポリシーのコンプライアンスホワイトリストに違反する場合、Firepower Management Center は非準拠プロトコルに、ホワイトリストの違反アイコン (🚫) のマークを付けます。

ホストプロファイルに、ホスト上で実行していないことがわかっているプロトコルがリストされている場合は、これらのプロトコルを削除できます。ホストからプロトコルを削除すると、ホストがコンプライアンスホワイトリストに準拠する可能性があります。



(注) システムでプロトコルが再検出されると、プロトコルはネットワークマップおよびホストプロファイルに再度追加されます。

## ホストプロファイルからのプロトコルの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst



## 手順

**ステップ1** ホスト プロファイルの [プロトコル (Protocols) ] セクションに移動します。

**ステップ2** 削除するプロトコルの横にある削除アイコン (🗑️) をクリックします。

# ホスト プロファイル内の侵害の兆候

Firepower システムは、さまざまなタイプのデータ (侵入イベント、セキュリティインテリジェンス、接続イベントおよびファイルまたはマルウェア イベント) を関連付け、モニタ対象ネットワーク上のホストが悪意のある手段によって侵害された可能性があるかどうかを判断します。イベントデータの特定の組み合わせと頻度が、影響を受けるホストの侵害の兆候 (IOC) タグをトリガーします。

ホスト プロファイルの [侵害の兆候 (Indications of Compromise) ] セクションには、ホストのすべての侵害の兆候のタグが表示されます。

侵害の兆候にタグを付けるようにシステムを構成するには、[侵害の兆候ルールの有効化 \(2168 ページ\)](#) を参照してください。

侵害の兆候についての作業の詳細については、[侵害の兆候データ \(2717 ページ\)](#) とそのトピックのサブトピックを参照してください。

### 関連トピック

[侵害の兆候 \(2167 ページ\)](#)

# ホスト プロファイルの VLAN タグ

ホストが仮想 LAN (VLAN) のメンバである場合、ホスト プロファイルの [VLAN タグ (VLAN Tag) ] セクションが表示されます。

物理ネットワーク機器は、多くの場合に VLAN を使用して、さまざまなネットワーク ブロックから論理ネットワーク セグメントを作成します。システムは 802.1q VLAN タグを検出し、それぞれに対して以下の情報を表示します。

- [VLANID] は、ホストがメンバである VLAN を表します。これは、802.1q VLAN の場合、0 ~ 4095 の任意の整数となります。
- [タイプ (Type) ] は、VLAN タグが含まれている、カプセル化されたパケットを表します。値は [イーサネット (Ethernet) ] または [トークンリング (Token Ring) ] となります。
- [優先順位 (Priority) ] は、VLAN タグの優先度を表します。これは 0 ~ 7 の任意の整数で、7 が最も高い優先度です。

VLAN タグがパケット内でネスト構造になっている場合、システムは最も内側の VLAN タグを処理し、Firepower Management Center は最も内側の VLAN タグを表示します。システムは、ARP および DHCP トラフィックを通じて識別される MAC アドレスのみの VLAN タグ情報を収集し、これらのタグを表示します。

たとえば全体がプリンタで構成されている VLAN があり、システムがこの VLAN で Microsoft Windows 2000 のオペレーティング システムを検出した場合などは、VLAN タグ情報が有用です。VLAN 情報により、システムは正確性の高いネットワーク マップを生成できるようになります。

## ホスト プロファイル内のユーザ履歴

ホスト プロファイルのユーザ履歴の部分には、過去 24 時間のユーザ アクティビティがグラフィック表示されます。一般的なユーザは夕方にログオフし、また他のユーザとホストのリソースを共有することがあります。電子メールのチェックなどの目的で行われる定期的なログインの要求は、短い標準の棒で示されます。ユーザのアイデンティティリストは棒グラフで提示され、ユーザログインが検出されたタイミングを示します。権限のないログインの場合は、棒グラフがグレーになっていることに注意してください。

システムは、ホストに対する権限のないユーザ ログインを、そのホストの IP アドレスに関連付けるため、そのユーザはそのホストのユーザ履歴に表示されます。ただし、権限のあるユーザ ログインが同じホストで検出された場合、その権限のあるユーザ ログインに関連付けられているユーザが、そのホストの IP アドレスとの関連付けを引き継ぐため、新しい権限のないユーザ ログインがそのホストの IP アドレスとのそのユーザの関連付けを壊すことはありません。ネットワーク検出ポリシーで、失敗したログインのキャプチャを設定した場合、リストにはこのホストへのログインに失敗したユーザが含まれます。

## ホスト プロファイル内のホスト属性

ホスト属性を使用して、ネットワーク環境にとって重要な方法でホストを分類することができます。Firepower システムには以下の 3 つのタイプの属性があります。

- 定義済みホスト属性
- ホワイトリスト ホスト属性
- ユーザ定義ホスト属性

定義済みホスト属性を設定後、またはユーザ定義ホスト属性を作成後は、ホスト属性の値を割り当てる必要があります。



(注) ホスト属性は、どのドメインレベルでも定義できます。現在のドメインと先祖ドメインで作成されたホスト属性を割り当てることができます。

## 定義済みホスト属性

Firepower Management Center には、2 つの定義済みホスト変数が用意されています。

### ホストの重要度 (Host Criticality)

特定のホストの業務の重要性を指定し、ホストの重要性に応じて関連ポリシーの応答を調整するには、この属性を使用します。たとえば、業務にとって組織のメールサーバが一般的なユーザワークステーションよりも重要であるとみなしている場合は、メールサーバと業務に重要なその他のデバイスに [高 (High)] の値を割り当て、他のホストには [中 (Medium)] または [低 (Low)] の値を割り当てることができます。その上で、影響を受けるホストの重要度に基づいて異なるアラートを起動する関連ポリシーを作成できます。

### 注記 (Notes)

他のアナリストに確認してもらいたいホストに関する情報を記録するには、このホスト固有の属性を使用します。たとえば、ネットワーク上のコンピュータに、パッチが適用されていない古いバージョンのテスト用オペレーティングシステムが搭載されている場合、[注記 (Notes)] 属性を使用して、システムは意図的にパッチを適用していないことを明示できます。

## ホワイトリストのホスト属性

ユーザが作成するそれぞれのコンプライアンス ホワイトリストによって、そのホワイトリストと同じ名前でホスト属性が自動的に作成されます。ホワイトリストのホスト属性に設定可能な値は、次のとおりです。

- 準拠 (Compliant) : ホワイトリストに準拠しているホストを識別します。
- 非準拠 (Non-Compliant) : ホワイトリストに違反しているホストを識別します。
- 未評価 (Not Evaluated) : ホワイトリストの有効な対象ではないホスト、または何らかの理由で評価されていないホストを識別します。

ホワイトリストのホスト属性の値を編集したり、ホワイトリストのホスト属性を削除したりすることはできません。

## ユーザ定義のホスト属性

定義済みのホスト属性またはホワイトリストのホスト属性で使用されている基準と異なる基準を使用してホストを識別する場合、ユーザ定義のホスト属性を作成することができます。例えば、以下を行うことができます。

- ホストに対してファシリティ コード、市町村、部屋番号などの物理的なロケーション ID を割り当てます。
- 特定のホストを担当するシステム管理者を示す担当者 ID を割り当てます。ホストに関連する問題が検出された場合、関連ルールとポリシーを作成して、適切なシステム管理者にアラートを送信することができます。

- ホストの IP アドレスに基づいて、事前定義されたリストからホストへ自動的に値を割り当てます。この機能は、ネットワーク上にホストが初めて表示されたときに、その新しいホストへ値を割り当てるために役立ちます。

ユーザ定義のホスト属性は、ホストプロファイルのページに表示されます。ここでホストごとに値を割り当てることができます。次のことも実行できます。

- 関連ポリシーと検索でホスト属性を使用します。
- イベントのホスト属性テーブルビューで属性を表示して、それに基づいてレポートを生成します。

ユーザ定義のホスト属性として、次のタイプのいずれか 1 つを使用できます。

### テキスト (Text)

ホストに対してテキスト文字列を手動で割り当てることができます。

### 整数 (Integer)

正の整数の範囲の最初の数と最後の数を指定してから、ホストに対してこれらの数の 1 つを手動で割り当てることができます。

### リスト (List)

文字列値のリストを作成してから、ホストに対してこの値のいずれかを割り当てることができます。また、ホストの IP アドレスに基づいて、ホストに対して値を自動的に割り当てることもできます。

複数の IP アドレスを持つホストの 1 つの IP アドレスに基づいて値を自動的に割り当てると、これらの値は、ホストに関連付けられているすべてのアドレスに適用されます。[ホスト属性 (Host Attributes)] テーブルを表示する場合は、このことに留意してください。

リストの値を自動的に割り当てる場合は、リテラルの IP アドレスではなくネットワークオブジェクトの使用を検討してください。このアプローチによって保守容易性を向上でき、特にマルチドメイン展開で有効です。これは、マルチドメイン展開でオーバーライドが有効になったオブジェクトを使用すると、子孫ドメインの管理者が先祖ドメインの設定を自分のローカル環境に合わせて調整できるためです。マルチドメイン展開では、子孫ドメインで重複した IP アドレスを使用している場合に意図しないホストに一致するのを避けるために、先祖ドメインレベルで自動割り当てリストを定義する場合は注意してください。

### URL

ホストに対して手動で URL の値を割り当てることができます。

ユーザ定義のホスト属性を削除すると、その属性が使用されているすべてのホストプロファイルから削除されます。

## テキストまたは URL ベースのホスト属性の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

### 手順

- ステップ 1 [分析 (Analysis)] > [ホスト (Hosts)] > [ホスト属性 (Host Attributes)] を選択します。
- ステップ 2 [ホスト属性管理 (Host Attribute Management)] をクリックします。
- ステップ 3 [属性の作成 (Create Attribute)] をクリックします。
- ステップ 4 名前を入力します。
- ステップ 5 作成する属性の [タイプ (Type)] を選択します。 [ユーザ定義のホスト属性 \(2677 ページ\)](#)
- ステップ 6 [保存 (Save)] をクリックします。

## 整数ベースのホスト属性の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

整数ベースのホスト属性を定義する場合は、その属性が受け入れる数値の範囲を指定する必要があります。

### 手順

- ステップ 1 [分析 (Analysis)] > [ホスト (Hosts)] > [ホスト属性 (Host Attributes)] を選択します。
- ステップ 2 [ホスト属性管理 (Host Attribute Management)] をクリックします。
- ステップ 3 [属性の作成 (Create Attribute)] をクリックします。
- ステップ 4 名前を入力します。
- ステップ 5 [ユーザ定義のホスト属性 \(2677 ページ\)](#) の説明に従って、作成する属性の [タイプ (Type)] を選択します。
- ステップ 6 [最小 (Min)] フィールドに、ホストに対して割り当てることができる範囲の最小の整数値を入力します。

**ステップ 7** [最大 (Max) ] フィールドに、ホストに対して割り当てることができる範囲の最大の整数値を入力します。

**ステップ 8** [保存 (Save) ] をクリックします。

## リストベースのホスト属性の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

リストベースのホストの属性を定義する場合は、リストに対してそれぞれの値を提供する必要があります。これらの値には、英数字、スペース、および記号を含めることができます。

### 手順

- ステップ 1** [分析 (Analysis) ] > [ホスト (Hosts) ] > [ホスト属性 (Host Attributes) ] を選択します。
- ステップ 2** [ホスト属性管理 (Host Attribute Management) ] をクリックします。
- ステップ 3** [属性の作成 (Create Attribute) ] をクリックします。
- ステップ 4** 名前を入力します。
- ステップ 5** [ユーザ定義のホスト属性 \(2677 ページ\)](#) の説明に従って、作成する属性の [タイプ (Type) ] を選択します。
- ステップ 6** リストに値を追加するには、[値の追加 (Add Value) ] をクリックします。
- ステップ 7** [名前 (Name) ] フィールドに、追加する最初の値を入力します。
- ステップ 8** オプションで、ホストに追加した属性値を自動で割り当てるには、[ネットワークを追加 (Add Networks) ] をクリックします。
- ステップ 9** [値 (Value) ] ドロップダウン リストから、追加した値を選択します。
- ステップ 10** [IP アドレス (IP Address) ] および [ネットマスク (Netmask) ] フィールドに、この値を自動的に割り当てる IP アドレスのブロックを表す IP アドレスとネットワーク マスク (IPv4) を入力します。
- ステップ 11** リストにさらに値を追加して、IP アドレス ブロックの範囲内の新しいホストにこれらの値を自動的に割り当てるには、手順 6 ~ 10 を繰り返します。
- ステップ 12** [保存 (Save) ] をクリックします。

## ホスト属性値の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

事前定義またはユーザ定義のホスト属性に値を設定できます。システムによって生成されたホワイトリストのホスト属性値は設定できません。

### 手順

- ステップ 1 変更するホストプロファイルを開きます。
- ステップ 2 [属性 (Attributes) ] セクションで、[属性の編集 (Edit Attributes) ] をクリックします。
- ステップ 3 必要に応じて、属性を更新します。
- ステップ 4 [保存 (Save) ] をクリックします。

## ホスト プロファイル内のホワイト リスト違反

コンプライアンス ホワイトリスト (またはホワイト リスト) は一連の基準であり、ユーザはこれを使用して、特定のサブネット上での実行が許可されるオペレーティングシステム、アプリケーションプロトコル、クライアント、Web アプリケーション、およびプロトコルを指定することができます。

ホワイト リストをアクティブな相関ポリシーに追加した場合に、システムでホワイト リストに違反しているホストが検出されると、Firepower Management Center はホワイト リストのイベント (相関イベントの特別な種類) をデータベースに記録します。これらのホワイト リスト イベントはそれぞれホワイト リスト違反に関連付けられます。これには、特定のホストがどのようにホワイト リストに違反しているか、および違反している理由が含まれています。あるホストが1つ以上のホワイト リストに違反している場合、ホストプロファイルにおいて、2つの方法でこれらの違反を参照することができます。

最初に、ホストに関連付けられている個々のホワイト リストのすべての違反が、ホストプロファイルに一覧表示されます。

ホストプロファイルに一覧表示されるホワイト リストの違反に関する情報は、次のとおりです。

### タイプ (Type)

違反のタイプ (つまり、違反がオペレーティングシステム、アプリケーション、サーバ、またはプロトコルの非準拠の結果として生じたかどうか)。

**理由 (Reason)**

違反についての特別な理由。たとえば、Microsoft Windows のホストのみを許可するホワイトリストがある場合、ホストプロファイルには、ホストで稼動している現行のオペレーティングシステム (Linux Linux 2.4、2.6 など) が表示されます。

**ホワイトリスト (White List)**

違反に関連付けられているホワイトリストの名前。

次に、オペレーティングシステム、アプリケーション、プロトコル、およびサーバに関連付けられているセクションで、Firepower Management Center が、非準拠の要素にホワイトリスト違反のアイコン (🚫) のマークを付けます。たとえば、Microsoft Windows ホストのみを許可するホワイトリストでは、ホストプロファイルで、ホストのオペレーティングシステム情報の隣にホワイトリスト違反のアイコンが表示されます。



(注) ホストのプロファイルを使用すると、コンプライアンスホワイトリストの共有ホストプロファイルを作成することができます。

## 共有ホワイトリスト ホスト プロファイルの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

コンプライアンス ホワイトリストに対する共有ホストプロファイルは、複数のホワイトリストをまたがるターゲットホスト上で実行を許可されるオペレーティングシステム、アプリケーションプロトコル、クライアント、Webアプリケーション、およびプロトコルを指定します。つまり、複数のホワイトリストを作成するが、同じホストプロファイルを使用して複数のホワイトリストで特定のオペレーティングシステムを実行するホストを評価する場合は、共有のホストプロファイルを使用します。

既知の IP アドレスを持つ任意のホストのホストプロファイルを使用して、コンプライアンス ホワイトリストで使用できる共有ホストプロファイルを作成することができます。ただし、システムでホストのオペレーティングシステムをまだ特定していない場合は、個々のホストのホストプロファイルに基づいて共有ホストプロファイルを作成することはできないことに注意してください。

**手順**

**ステップ 1** ホストプロファイルで、[ホワイトリスト プロファイルの生成 (Generate White List Profile) ] をクリックします。



**ステップ2** 特別なニーズに応じて、共有ホストプロファイルを変更し、保存します。


#### 関連トピック

[ホワイトリストホストプロファイルの作成](#) (2213 ページ)

## ホストプロファイルでのマルウェア検出

[最後に検出されたマルウェア (Most Recent Malware Detections)] セクションには、ホストがマルウェア ファイルを送信または受信した、最近のマルウェア イベントが最大 100 個表示されます。ホストプロファイルは、ネットワークベース (AMP for Firepower) とエンドポイントベース (エンドポイント向け AMP) のマルウェア イベントを一覧で示します。

ファイルが遡ってマルウェアと識別されたファイル イベントにホストが関係している場合、ファイルが送信された元のイベントは、マルウェアの特定が行われた後で、マルウェアの検出リストに表示されます。マルウェアとして識別されたファイルが、マルウェアではないと遡って判断された場合、そのファイルに関連するマルウェア イベントはリストには表示されなくなります。たとえば、ファイルに Malware の性質が含まれており、その処理が clean に変わった場合、そのファイルのイベントは、ホストプロファイル上のマルウェア検出リストから削除されます。

ホストプロファイルでマルウェアの検出を表示する場合は、イベントビューアで、そのホストのマルウェア イベントを表示できます。イベントを表示するには、マルウェアのアイコン () をクリックします。

次に、ホストプロファイルの [最後に検出されたマルウェア (Most Recent Malware Detections)] セクションのカラムについて説明します。

#### 時刻 (Time)

イベントが生成された日時。

ファイルがマルウェアであると遡って特定されたイベントでは、これはマルウェアが特定された時刻ではなく、元のイベントの時刻であることに注意してください。

#### ホストの役割 (Host Role)

検出されたマルウェアの伝送におけるホストの役割 (送信者または受信者)。エンドポイントベースのマルウェア イベントの場合は、ホストは常に受信者であることに注意してください。

#### 脅威名 (Threat Name)

検出されたマルウェアの名前。

#### ファイル名 (File Name)

マルウェア ファイルの名前。

### ファイルタイプ (File Type)

ファイルのタイプ (PDF や MSEXEC など)。

## ホストプロファイルの脆弱性

ホストプロファイルの [脆弱性 (Vulnerabilities)] セクションには、ホストに影響を与える脆弱性が示されます。これらの脆弱性は、システムがホスト上で検出したオペレーティングシステム、サーバ、およびアプリケーションに基づきます。

ホストのオペレーティングシステムのアイデンティティ、またはホスト上のアプリケーションプロトコルのアイデンティティのいずれかで、アイデンティティの競合が発生している場合、システムは、競合が解決するまで両方のアイデンティティに対して脆弱性を表示します。

NetFlow データからネットワーク マップに追加されたホストに使用可能なオペレーティングシステムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な (インパクトレベル1: 赤) インパクトレベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティングシステム ID を手動で設定します。

サーバのベンダーおよびバージョンの情報は、ほとんどの場合はトラフィックに含まれていません。デフォルトでは、システムはこのようなトラフィックの送信側および受信側に対して、関連付けられている脆弱性をマップしません。ただし、ベンダーまたはバージョンの情報を持たない特定のアプリケーションプロトコルに対して脆弱性をマップするよう、システムを設定することができます。

ホストの入力機能を使用して、ネットワーク上のホストにサードパーティの脆弱性情報を追加すると、追加の [脆弱性 (Vulnerabilities)] セクションが表示されます。たとえば QualysGuard Scanner から脆弱性をインポートすると、ホストプロファイルには [QualysGuard 脆弱性 (QualysGuard Vulnerabilities)] セクションが含まれます。サードパーティの脆弱性の場合、ホストプロファイルの対応する [脆弱性 (Vulnerabilities)] セクションの情報は、ホストの入力機能を使用して脆弱性データをインポートしたときに提供した情報に制限されます。

サードパーティの脆弱性をオペレーティングシステムおよびアプリケーションプロトコルと関連付けることはできますが、クライアントに関連付けることはできません。サードパーティの脆弱性のインポートについては、『*Firepower System Host Input API Guide*』を参照してください。

次に、ホストプロファイルの [脆弱性 (Vulnerabilities)] セクションのカラムについて説明します。

### [名前 (Name)]

脆弱性の名前。

### [リモート (Remote)]

脆弱性がリモートで不正利用される可能性があるかどうかを示します。この列が空白の場合、脆弱性の定義にはこの情報は含まれていません。

### コンポーネント

脆弱性に関連付けられているオペレーティング システム、アプリケーション プロトコル、またはクライアントの名前。

### [ポート (Port) ]

ポート番号（脆弱性が、特定のポート上で実行されているアプリケーションプロトコルに関連付けられている場合）。

### 関連トピック

[脆弱性データのフィールド](#) (2733 ページ)

[脆弱性の非アクティブ化](#) (2735 ページ)

## 脆弱性に対するパッチのダウンロード

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

ネットワーク上のホストで検出された脆弱性を軽減するためのパッチをダウンロードできます。

### 手順

- ステップ 1 パッチをダウンロードするホストのホスト プロファイルにアクセスします。
- ステップ 2 [脆弱性 (Vulnerabilities) ] セクションを展開します。
- ステップ 3 パッチを適用する脆弱性の名前をクリックします。
- ステップ 4 [修正 (Fixes) ] セクションを展開して、脆弱性に対するパッチの一覧を表示します。
- ステップ 5 ダウンロードするパッチの隣の [ダウンロード (Download) ] をクリックします。
- ステップ 6 パッチをダウンロードして、影響を受けるシステムに適用します。

## 個々のホストに対する脆弱性の非アクティブ化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

ホストの脆弱性エディタを使用して、ホストごとに脆弱性を非アクティブにすることができます。ホストの脆弱性を非アクティブにしても、そのホストの影響の相関に対して脆弱性は使用されますが、影響レベルは自動的に1レベル減少します。

### 手順

- 
- ステップ 1** ホストプロファイルの [脆弱性 (Vulnerabilities) ] セクションに移動します。
- ステップ 2** [脆弱性の編集 (Edit Vulnerabilities) ] をクリックします。
- ステップ 3** [有効な脆弱性 (Valid Vulnerabilities) ] リストから脆弱性を選択し、下矢印をクリックして [無効な脆弱性 (Invalid Vulnerabilities) ] リストに移動します。
- ヒント 隣接している複数の脆弱性を選択するには、クリックおよびドラッグを使用します。脆弱性をダブルクリックして、リスト間を移動することもできます。
- ステップ 4** [保存 (Save) ] をクリックします。
- 

### 次のタスク

- 必要に応じて、ホストの脆弱性を [無効な脆弱性 (Invalid Vulnerabilities) ] リストから [有効な脆弱性 (Valid Vulnerabilities) ] リストに移動して、脆弱性をアクティブ化します。

### 関連トピック

- [個々の脆弱性の非アクティブ化](#) (2686 ページ)
- [複数の脆弱性の非アクティブ化](#) (2738 ページ)

## 個々の脆弱性の非アクティブ化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

ホストプロファイルで脆弱性を非アクティブ化すると、ネットワーク マップにあるすべてのホストに対して脆弱性が非アクティブ化されます。ただし、いつでもその脆弱性を再アクティブ化することができます。

マルチドメイン展開では、先祖ドメインの脆弱性を非アクティブ化すると、すべての子孫ドメインでその脆弱性が非アクティブ化されます。先祖ドメインで脆弱性をアクティブにした場合、リーフドメインでは、そのドメインにあるデバイスに対して脆弱性のアクティブ化または非アクティブ化を実行できます。

## 手順

**ステップ 1** 次のようにして、脆弱性の詳細にアクセスします。

- 影響を受けるホストプロファイルで、[脆弱性 (Vulnerabilities)] セクションを展開し、有効または無効にする脆弱性の名前をクリックします。
- 事前定義されたワークフローで、[分析 (Analysis)] > [脆弱性 (Vulnerabilities)] > [脆弱性 (Vulnerabilities)] を選択し、有効または無効にする脆弱性の横にある表示アイコン (🔍) をクリックします。

**ステップ 2** [影響を受ける条件 (Impact Qualification)] ドロップダウンリストから [無効 (Disabled)] を選択します。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**ステップ 3** ネットワーク マップ上のすべてのホストに対して、[影響を受ける条件 (Impact Qualification)] の値を変更することを確認します。

**ステップ 4** [完了 (Done)] をクリックします。

## 次のタスク

- オプションで、上記の手順を実行中に、[影響を受ける条件 (Impact Qualification)] ドロップダウンリストから [有効 (Enabled)] を選択することによって、脆弱性をアクティブにします。

## 関連トピック

[個々のホストに対する脆弱性の非アクティブ化](#) (2685 ページ)

[複数の脆弱性の非アクティブ化](#) (2738 ページ)

[オペレーティング システムのアイデンティティの競合](#) (2664 ページ)

# ホスト プロファイルのスキャン結果

Nmap を使用してホストをスキャンする場合、または Nmap のスキャンから結果をインポートする場合、これらの結果は、スキャンに含まれているすべてのホストのホストプロファイルに表示されます。

Nmap が、ホストのオペレーティングシステムについて、およびオープンでフィルタリングされていないポート上で稼動している任意のサーバについて収集した情報が、ホストプロファイルの [オペレーティング システム (Operating System)] と [サーバ (Servers)] セクションにそれぞれ追加されます。また、Nmap は、そのホストのスキャン結果のリストを [スキャン結果 (Scan Results)] セクションに追加します。プロファイルに [スキャン結果 (Scan Results)] セクションが表示されるのは、スキャンでホスト上のオープンポートが検出された場合のみであることに注意してください。

各結果には、情報のソース、スキャンしたポートの番号とタイプ、ポート上で稼動しているサーバの名前、Nmapで検出された任意の追加情報（ポートの状態やサーバのベンダー名など）が示されます。UDPポートをスキャンする場合、そのポートで検出されたサーバは[スキャン結果（Scan Results）]セクションにのみ表示されます。

ホストプロファイルからNmapスキャンを実行できることに注意してください。

## ホストプロファイルからのホストのスキャン

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ホストプロファイルから、ホストに対してNmapスキャンを実行できます。スキャンが完了すると、そのホストのサーバおよびオペレーティングシステムの情報がホストプロファイルで更新されます。追加のスキャン結果は、すべてホストプロファイルの[スキャン結果（Scan Results）]セクションに追加されます。



**注意** Nmap 提供のサーバおよびオペレーティングシステムのデータは、別のNmapスキャンを実行するか、より優先度の高いホスト入力の上書きするまでスタティックなままになります。Nmapを使用したホストのスキャンを計画している場合は、定期的にスキャンをスケジューリングします。

### 始める前に

- Nmap スキャンインスタンスを追加します。[Nmap スキャンインスタンスの追加（2082 ページ）](#)を参照してください。

### 手順

- ステップ 1** ホストプロファイルで、[ホストのスキャン（Scan Host）]をクリックします。
- ステップ 2** ホストのスキャンに使用するスキャン修復の横にある[スキャン（Scan）]をクリックします。システムによってホストがスキャンされ、ホストプロファイルに結果が追加されます。

### 関連トピック

[Nmap スキャンの自動化（225 ページ）](#)



## 第 110 章

# ディスカバリ イベントの操作

以下のトピックでは、ディスカバリ イベントを操作する方法について説明します。

- [検出イベントの検出データとアイデンティティ データ \(2689 ページ\)](#)
- [ディスカバリ イベントの統計情報の表示 \(2690 ページ\)](#)
- [ディスカバリ パフォーマンス グラフの表示 \(2694 ページ\)](#)
- [ディスカバリおよびアイデンティティ ワークフローの使用 \(2695 ページ\)](#)

## 検出イベントの検出データとアイデンティティ データ

システムは、モニタ対象のネットワークで検出された変更を表すイベントのテーブルを生成します。このテーブルを使用して、ネットワークのユーザアクティビティを確認し、応答方法を決定できます。ネットワーク検出およびアイデンティティ ポリシーは、収集するデータ、モニタするネットワークセグメント、およびそのために使用する特定のハードウェアインターフェイスの種類を指定します。

検出およびアイデンティティ イベント テーブルを使用して、ネットワークのホスト、アプリケーション、およびユーザに関連付けられている脅威を特定できます。システムには事前定義のワークフローセットが用意されており、これを使用して、システムで生成されるイベントを分析することができます。また、特定のニーズに合った情報のみを表示するカスタムワークフローを作成することもできます。

分析用にネットワーク検出およびアイデンティティ データを収集し、保存するには、ネットワーク検出およびアイデンティティ ポリシーを設定する必要があります。アイデンティティ ポリシーを設定した後、アクセス コントロール ポリシーで呼び出して、トラフィックのモニタに使用するデバイスに展開する必要があります。

ネットワーク検出ポリシーは、ホスト、アプリケーション、および権限のないユーザデータを提供します。アイデンティティ ポリシーは、権限のあるユーザ データを提供します。

次の検出イベント テーブルは、[分析 (Analysis)] > [ホスト (Hosts)]、[分析 (Analysis)] > [ユーザ (Users)]、および [分析 (Analysis)] > [脆弱性 (Vulnerabilities)] メニューにあります。

検出イベント テーブル	検出データが入力されますか。	アイデンティティ データが入力されますか。
ホスト (Hosts)	[はい (Yes) ]	[いいえ (No) ]
の侵害の兆候	[はい (Yes) ]	[いいえ (No) ]
アプリケーション	[はい (Yes) ]	[いいえ (No) ]
アプリケーション詳細 (Application Details)	[はい (Yes) ]	[いいえ (No) ]
サーバ	[はい (Yes) ]	[いいえ (No) ]
ホスト属性 (Host Attributes)	[はい (Yes) ]	[いいえ (No) ]
検出イベント (Discovery Events)	○	○
ユーザアクティビティ (User Activity)	○	○
Users	○	○
脆弱性 (Vulnerabilities)	[はい (Yes) ]	[いいえ (No) ]
サードパーティの脆弱性 (Third-Party Vulnerabilities)	[はい (Yes) ]	[いいえ (No) ]

## ディスカバリ イベントの統計情報の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

[ディスカバリ統計情報 (Discovery Statistics) ] ページには、システムで検出されたホスト、イベント、プロトコル、アプリケーションプロトコル、オペレーティングシステムの概要が表示されます。

ページには、最後の 1 時間の統計情報、および累計の統計情報が示されます。特定のデバイス、またはすべてのデバイスについての統計情報を表示することができます。サマリに示されているイベント、サーバ、オペレーティングシステム、またはオペレーティングシステムのベンダーをクリックして、ページ上のエントリに一致するイベントを表示することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。



## 手順

- ステップ 1** [概要 (Overview) ] > [概要 (Summary) ] > [検出統計 (Discovery Statistics) ] を選択します。
- ステップ 2** [デバイスの選択 (Select Device) ] リストから、統計情報を表示するデバイスを選択します。オプションで、Firepower Management Center で管理されるすべてのデバイスの統計情報を表示するには、[すべて (All) ] を選択します。
- ステップ 3** 次の選択肢があります。
- [統計情報サマリ (Statistics Summary) ]セクション (2691 ページ) で説明されているように、[統計サマリー (Statistics Summary) ] に一般的な統計情報を表示します。
  - [イベントの中断 (Event Breakdown) ] で、表示するイベントタイプをクリックします。イベントが1つも表示されない場合は、[時間枠の変更 \(2455 ページ\)](#) で説明されているように、時間範囲を調整する必要があるかもしれません。
  - [プロトコルの中断 (Protocol Breakdown) ] で、検出されたホストによって現在使用されているプロトコルを表示します。
  - [アプリケーションプロトコルの中断 (Application Protocol Breakdown) ] で、表示するアプリケーションプロトコルの名前をクリックします。
  - [OS の中断 (OS Breakdown) ] で、[OS 名 (OS Name) ] または [OS ベンダー (OS Vendor) ] をクリックします。

## 関連トピック

[\[イベント分類 \(Event Breakdown\) \]セクション \(2693 ページ\)](#)

[\[プロトコル分類 \(Protocol Breakdown\) \]セクション \(2693 ページ\)](#)

[\[アプリケーションプロトコル分類 \(Application Protocol Breakdown\) \]セクション \(2693 ページ\)](#)

[\[OS 分類 \(OS Breakdown\) \]セクション \(2693 ページ\)](#)

## [統計情報サマリ (Statistics Summary) ]セクション

[統計情報サマリ (Statistics Summary) ]セクションの行の説明は次のとおりです。

### 合計イベント数 (Total Events)

Firepower Management Center に格納されているディスカバリ イベントの合計数。

### 過去 1 時間のイベントの合計 (Total Events Last Hour)

最後の 1 時間に生成されたディスカバリ イベントの合計数。

### 過去 1 日のイベントの合計 (Total Events Last Day)

最後の 1 日に生成されたディスカバリ イベントの合計数。

**アプリケーションプロトコル合計数 (Total Application Protocols)**

検出されたホストで実行されているサーバのアプリケーションプロトコルの合計数。

**IP ホストの合計 (Total IP Hosts)**

一意の IP アドレスによって特定された検出済みホストの合計数。

**MAC ホストの合計 (Total MAC Hosts)**

IP アドレスで特定されない検出済みホストの合計数。

すべてのデバイス、または特定のデバイスのどちらについてのディスカバリ統計情報を参照している場合でも、[MAC ホストの合計 (Total MAC Hosts)] の統計情報は同じになることに注意してください。これは、管理対象デバイスが IP アドレスに基づいてホストを検出するためです。この統計情報は、他の方法によって識別され、特定の管理対象デバイスに依存しないすべてのホストの合計を表します。

**ルータの合計 (Total Routers)**

ルータとして識別された検出ノードの合計数。

**ブリッジの合計 (Total Bridges)**

ブリッジとして識別された検出ノードの合計数。

**ホスト制限の使用 (Host Limit Usage)**

使用中のホスト制限のパーセンテージ合計。ホストの制限は、Firepower Management Center のモデルによって定義されます。すべての管理対象デバイスについての統計情報を表示している場合は、ホストの使用制限のみが表示されることに注意してください。



---

(注) ホストの制限に達してホストが削除されると、ディスカバリ データを消去するネットワークマップ上にホストは表示されなくなります。

---

**最後に受け取ったイベント (Last Event Received)**

最後のディスカバリ イベントが行われた日付と時間。

**最後に受信した接続 (Last Connection Received)**

最後の接続が完了した日付と時間。

## [ イベント分類 (Event Breakdown) ] セクション

[ イベント分類 (Event Breakdown) ] セクションには、データベースに格納されている各イベントタイプの合計数のカウントの他に、ネットワーク検出の各タイプのカウント、および最後の1時間で発生したホスト入力イベントが示されます。

[ イベント分類 (Event Breakdown) ] セクションを使用して、ディスカバリ イベントおよびホスト入力イベントの詳細を表示することもできます。

### 関連トピック

[検出イベントおよびホスト入力イベント](#) (2697 ページ)

## [ プロトコル分類 (Protocol Breakdown) ] セクション

[ プロトコル分類 (Protocol Breakdown) ] セクションには、検出されたホストで使用されているプロトコルが示されます。このセクションには、検出されたそれぞれのプロトコル名、プロトコルスタックの「レイヤ」、およびプロトコルを使用して通信しているホストの合計数が表示されます。

## [ アプリケーションプロトコル分類 (Application Protocol Breakdown) ] セクション

[ アプリケーションプロトコル分類 (Application Protocol Breakdown) ] セクションには、検出されたホストで使用されているアプリケーションプロトコルが示されます。このセクションには、プロトコル名、最後の1時間にアプリケーションプロトコルを実行したホストの合計数、いずれかのポイントでプロトコルの実行が検出されたホストの合計数が表示されます。

[ アプリケーションプロトコル分類 (Application Protocol Breakdown) ] セクションではさらに、検出されたプロトコルを使用しているサーバの詳細を表示することもできます。

### 関連トピック

[サーバデータ](#) (2722 ページ)

## [ OS 分類 (OS Breakdown) ] セクション

[ OS 分類 (OS Breakdown) ] セクションには、監視対象ネットワーク上で稼動しているオペレーティングシステム、およびオペレーティングシステムのベンダー、各オペレーティングシステムを実行しているホストの合計数が示されます。

オペレーティングシステムの名前またはバージョンの値が `unknown` の場合は、オペレーティングシステムまたはそのバージョンが、システムのフィンガープリントの内容と一致しないことを意味します。値が `pending` の場合は、オペレーティングシステムまたはそのバージョンを識別するための十分な情報がシステムで収集されていないことを意味します。

[ OS 分類 (OS Breakdown) ] セクションを使用して、検出されたオペレーティングシステムの詳細を表示することができます。

## 関連トピック

[ホスト データ](#) (2707 ページ)

## ディスカバリ パフォーマンス グラフの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint

ディスカバリ イベントを使用して、管理対象デバイスのパフォーマンス統計情報を示すグラフを生成することができます。

新しいデータは5分ごとに統計グラフに蓄積されます。したがって、グラフをすばやくリロードしても、次の5分の差分更新が実行されるまでデータは変更されていない場合があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

## 手順

- 
- ステップ 1 **[概要 (Overview)] > [概要 (Summary)] > [検出パフォーマンス (Discovery Performance)]** を選択します。
  - ステップ 2 **[デバイスの選択 (Select Device)]** リストから、Firepower Management Center または対象とする管理対象デバイスを選択します。
  - ステップ 3 **[ディスカバリ パフォーマンス グラフ タイプ \(2694 ページ\)](#)** で説明されているように、**[グラフの選択 (Select Graph(s))]** リストから、作成するグラフの種類を選択します。
  - ステップ 4 **[時間範囲の選択 (Select Time Range)]** リストから、グラフに使用する時間範囲を選択します。
  - ステップ 5 **[グラフ (Graph)]** をクリックして、選択した統計情報をグラフ化します。
- 

## ディスカバリ パフォーマンス グラフ タイプ

次に、使用できるグラフのタイプについて説明します。

## 処理されたイベント数/秒

Data Correlator が 1 秒間に処理するイベントの数を表します。

## 処理された接続数/秒

Data Correlator が 1 秒間に処理する接続の数を表します。

**生成されたイベント数/秒**

システムが1秒間に生成するイベントの数を表します。

**メガビット/秒**

ディスカバリ プロセスによって1秒間に分析されたトラフィック数（メガビット）を表します。

**平均バイト/パケット**

ディスカバリ プロセスによって分析された各パケットに含まれるバイト数の平均を表します。

**キロパケット/秒**

ディスカバリ プロセスで1秒間に分析されるパケット数を1000単位で表します。

## ディスカバリおよびアイデンティティワークフローの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	タスクに依存

Firepower Management Center は、ネットワークで生成されるディスカバリおよびアイデンティティ データの分析で使用できるイベントワークフローセットを提供します。ワークフローはネットワーク マップとともに、ネットワーク資産に関する主要な情報源になります。

Firepower Management Center には、ディスカバリおよびアイデンティティ データ、検出されたホストとそのホストの属性、サーバ、アプリケーション、アプリケーションの詳細、脆弱性、ユーザ アクティビティ、ユーザに関する事前定義されたワークフローが用意されています。ユーザはカスタム ワークフローを作成することもできます。

**手順**

**ステップ 1** 事前定義されたワークフローにアクセスするには、以下を実行します。

- ディスカバリとホスト入力データ：[ディスカバリ イベントとホスト入力イベントの表示 \(2705 ページ\)](#) を参照してください。
- ホスト データ：[ホスト データの表示 \(2707 ページ\)](#) を参照してください。
- ホスト属性データ：[ホスト属性の表示 \(2715 ページ\)](#) を参照してください。
- ホストまたはユーザの侵害の兆候データ：[侵害の兆候データの表示 \(2719 ページ\)](#) を参照してください。

- サーバ データ : [サーバ データの表示 \(2723 ページ\)](#) を参照してください。
- アプリケーション データ : [アプリケーション データの表示 \(2727 ページ\)](#) を参照してください。
- アプリケーション 詳細 データ : [アプリケーション 詳細 データの表示 \(2730 ページ\)](#) を参照してください。
- ユーザ データ : [ユーザ データの表示 \(2748 ページ\)](#) を参照してください。
- ユーザ アクティビティ データ : [ユーザ アクティビティ データの表示 \(2751 ページ\)](#) を参照してください。
- ネットワーク マップ : [ネットワーク マップの表示 \(2398 ページ\)](#) を参照してください。

**ステップ 2** カスタム ワークフローにアクセスするには、**[分析 (Analysis)] > [カスタム (Custom)] > [カスタム ワークフロー (Custom Workflows)]** を選択します。

**ステップ 3** カスタム テーブルに基づいたワークフローにアクセスするには、**[分析 (Analysis)] > [カスタム (Custom)] > [カスタム テーブル (Custom Tables)]** を選択します。

**ステップ 4** 以下のいずれかのアクションを実行します。これらは、ネットワーク検出ワークフローでアクセスするすべてのページに共通です。

- カラムの制約 : 表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン (✖) をクリックします。表示されるポップアップ ウィンドウで、**[適用 (Apply)]** をクリックします。




**ヒント** 他のカラムを表示または非表示にするには、**[適用 (Apply)]** をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効にしたカラムをビューに戻すには、展開の矢印をクリックして検索制約を展開し、**[無効にされたカラム (Disabled Columns)]** の下のカラム名をクリックします。

- 削除 : 現在の制約されたビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、**[削除 (Delete)]** または **[すべて削除 (Delete All)]** をクリックします。これらのアイテムが再検出されても、システムのディスカバリ機能が再開されるまで、これらのアイテムは削除されたままになります。

**注意** **[分析 (Analysis)] > [ユーザ (Users)] > [ユーザ (Users)]** ページでセッションを削除する前に、セッションが実際に閉じられていることを確認します。アクティブなセッションを削除すると、該当するポリシーはデバイス上のセッションを検出できなくなります。そのため、モニタしたり、ブロックしたりするようポリシーが設定されていたとしても、セッションはそれらのアクションを実行しません。

(注) サードパーティの場合とは異なり、シスコの脆弱性は削除できません。ただし、確認済みとしてマークすることはできます。

- ドリル ダウン : ワークフローの次のページにドリルダウンするには、[ドリルダウン ページの使用 \(2439 ページ\)](#) を参照してください。

- 現在のページを移動する：現在のワークフロー ページ内を移動するには、[ワークフロー ページのナビゲーション ツール \(2436 ページ\)](#) を参照してください。
- ワークフロー内で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページリンクをクリックします。
- 他のワークフローに移動する：関連するイベントを調べるために、その他のイベントビューに移動するには、[ワークフロー間のナビゲーション \(2463 ページ\)](#) を参照してください。
- データのソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- ホスト プロファイルの表示：IP アドレスのホスト プロファイルを表示するには、ホスト プロファイルのアイコン () をクリックします。アクティブな侵害の兆候 (IOC) タグのあるホストの場合は、IPアドレスの横に表示される侵害されたホストのアイコン () をクリックします。
- ユーザ プロファイル：ユーザ ID 情報を表示するには、ユーザ ID の横に表示されるユーザ アイコン () をクリックします。 の表示

---

#### 関連トピック

[ワークフローの使用 \(2429 ページ\)](#)

[Management Center データベースからのデータの消去 \(243 ページ\)](#)

## 検出イベントおよびホスト入カイベント

システムは検出イベントを生成します。このイベントは、監視対象ネットワークセグメントにおける変更の詳細をやり取りします。新しく検出されたネットワーク機能に対しては、新しいイベントが生成され、以前に認識されたネットワークアセットにおける何らかの変更に対しては、変更のイベントが生成されます。

最初のネットワーク検出のフェーズ中に、システムは各ホスト、および各ホスト上での稼働が検出された TCP または UDP サーバについて、新しいイベントを生成します。必要に応じて、エクスポートされた NetFlow レコードを使用してこれらの新しいホストおよびサーバのイベントを生成するよう、システムを設定することができます。

またシステムは、検出された各ホスト上で稼働しているネットワーク、トランスポート、およびアプリケーションプロトコルのそれぞれに対して新しいイベントを生成します。設定されている検出ルールでアプリケーションプロトコルの検出を無効にして、NetFlow エクスポートをモニタできますが、Firepower システムの管理対象デバイスをモニタするよう設定された検出ルールではできません。NetFlow 以外の検出ルールでホストまたはユーザの検出を有効にすると、アプリケーションが自動的に検出されます。

最初のネットワークマッピングが完了すると、続けてシステムは変更イベントを生成し、ネットワークの変更を記録します。変更イベントは、以前に検出されたアセットの設定が変更されるたびに生成されます。

検出イベントが生成されると、データベースに記録されます。Firepower Management Center の Web インターフェイスを使用して、検出イベントを表示、検索、および削除できます。また、関連ルールで検出イベントを使用することもできます。ユーザが指定する他の基準だけでなく、生成される検出イベントのタイプに基づいて、関連ルールを作成することができます。関連ルールは関連ポリシーで使用され、ネットワークトラフィックが基準を満たしたときに、修復、syslog、SNMP、および電子メールアラートの応答を起動します。

ホスト入力機能を使用して、ネットワークマップにデータを追加することができます。オペレーティングシステムの情報を追加、修正、または削除することができますが、この場合、システムは対象のホストに対する情報の更新を停止します。アプリケーションプロトコル、クライアント、サーバ、およびホストの属性を手動で追加、変更、または削除することも、脆弱性の情報を変更することもできます。この処理を行う場合、システムはホスト入力機能を生成します。

## ディスカバリ イベントタイプ

ネットワーク検出ポリシーにシステムが記録するディスカバリ イベントのタイプを設定できます。ディスカバリ イベントのテーブルを表示すると、[イベント (Event)] カラムにイベントタイプが表示されます。次に、ディスカバリ イベントタイプについて説明します。

### ホストの追加 MAC の検出

このイベントは、以前に検出したホストに対してシステムが新しい MAC アドレスを検出したときに生成されます。

このイベントは多くの場合、ルータを通じてトラフィックを渡すホストをシステムが検出したときに生成されます。各ホストにはそれぞれ異なる IP アドレスがありますが、これらの IP アドレスはすべて、ルータに関連付けられている MAC アドレスを持っているように見えます。システムは IP アドレスに関連付けられている実際の MAC アドレスを検出すると、ホストプロファイル内でその MAC アドレスを太字で表示し、イベントビューのイベント説明に「ARP/DHCP detected」のメッセージを表示します。

### クライアントタイムアウト

このイベントは、非アクティブであるという理由で、システムがデータベースからクライアントをドロップしたときに生成されます。

### クライアント更新

このイベントは、HTTP トラフィック内でシステムがペイロード（つまり音声やビデオ、Web メールなどの特別なタイプのコンテンツ）を検出したときに生成されます。



### DHCP : IP アドレスの変更

このイベントは、DHCP アドレスの割り当てによってホスト IP アドレスが変わったことがシステムで検出された場合に生成されます。

### DHCP : IP アドレスの再割り当て

このイベントは、ホストが IP アドレスを再利用するとき、つまり他の物理ホストが以前に使用した IP アドレスを、別のホストが DHCP の IP アドレス割り当てによって取得した場合に生成されます。

### ホップ数の変更

このイベントは、ホストと、そのホストを検出するデバイス間でシステムがネットワーク ホップ数の変更を検出した場合に生成されます。これは次のような場合に発生します。

- デバイスがさまざまなルータを介してホストのトラフィックを監視しており、ホストの場所についてより適切な決定ができる場合。
- デバイスがホストから ARP 送信を検出し、ホストがローカル セグメント上にあることを示している場合。

### ホスト削除 : ホスト制限に到達

このイベントは、Firepower Management Center 上でホストの制限を超えて、のネットワーク マップから監視対象のホストが削除されたときに生成されます。

### ホスト ドロップ : ホスト制限に到達

このイベントは、Firepower Management Center 上でホストの制限に達して新しいホストがドロップされたときに生成されます。このイベントとの相違点として、前述のイベントでは、ホストの制限に達したときに古いホストがネットワーク マップから削除されます。

ホストの制限に達したときに新しいホストをドロップするには、[ポリシー (Policies)] > [ネットワーク検出 (Network Discovery)] > [詳細 (Advanced)] を選択し、[ホストの制限に達した場合 (When Host Limit Reached)] を [ホストをドロップ (Drop hosts)] に設定します。

### ホストの IOC セット

このイベントは、ホストに対して IOC (侵害の痕跡) が設定され、アラートが生成されたときに生成されます。

### ホスト タイムアウト

このイベントは、ネットワーク検出ポリシーで定義された間隔内でホストがトラフィックを生成しなかったために、ネットワークマップからホストがドロップされたときに生成されます。個々のホストの IP アドレスと MAC アドレスはそれぞれタイムアウトになることに注意してください。関連付けられているアドレスがすべてタイムアウトになるまで、ホストはネットワーク マップから消えません。

ネットワーク検出ポリシーで監視するネットワークを変更する場合は、ネットワークマップから古いホストを手動で削除して、それらのホストがホストの制限に不利に作用しないようにします。

### ネットワーク デバイスへのホスト タイプの変更

このイベントは、システムが、検出されたホストが実際はネットワーク デバイスであったことを認識したときに生成されます。

### アイデンティティ競合

このイベントは、システムが、新しいサーバまたはオペレーティングシステムに対する現行のアクティブなアイデンティティと競合する、そのサーバまたはオペレーティングシステムのアイデンティティを検出したときに生成されます。

より新しいアクティブなアイデンティティデータを取得するためにホストを再スキャンして、アイデンティティの競合を解決する場合は、Identity Conflict イベントを使用して Nmap の修復をトリガーできます。

### アイデンティティ タイムアウト

このイベントは、アクティブなソースからのサーバまたはオペレーティング システムの ID データがタイムアウトしたときに生成されます。

より新しいアクティブなアイデンティティデータを取得するために、ホストを再スキャンしてアイデンティティデータをリフレッシュする場合は、Identity Conflict イベントを使用して Nmap の修復をトリガーできます。

### MAC 情報の変更

このイベントは、特定の MAC アドレスまたは TTL 値に関連付けられている情報で、システムが変更を検出したときに生成されます。

このイベントは多くの場合、ルータを通じてトラフィックを渡すホストをシステムが検出したときに発生します。各ホストにはそれぞれ異なる IP アドレスがありますが、これらの IP アドレスはすべて、ルータに関連付けられている MAC アドレスを持っているように見えます。システムは IP アドレスに関連付けられている実際の MAC アドレスを検出すると、ホストプロファイル内でその MAC アドレスを太字で表示し、イベント ビューのイベント説明に「ARP/DHCP detected」のメッセージを表示します。TTL は変わる可能性があります。これはトラフィックが複数のルータを通じて渡される可能性があるためです。また、システムがホストの実際の MAC アドレスを検出した場合も TTL が変わる可能性があります。

### NETBIOS 名の変更

このイベントは、システムがホストの NetBIOS 名に対する変更を検出したときに生成されます。このイベントは、NetBIOS プロトコルを使用するホストに対してのみ生成されます。

### 新しいクライアント

このイベントは、システムが新しいクライアントを検出したときに生成されます。



- (注) 分析用にクライアントデータを収集および格納するには、ネットワーク検出ポリシーのディスカバリ ルールでアプリケーションの検出が有効になっていることを確認します。

### 新しいホスト

このイベントは、システムがネットワーク上で稼動している新しいホストを検出したときに生成されます。

このイベントは、デバイスが新しいホストを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成するには、NetFlowデータを管理するネットワーク検出ルールでホストを検出するように設定します。

### 新しいネットワーク プロトコル

このイベントは、ホストが新しいネットワーク プロトコル (IP、ARP など) と通信していることをシステムが検出したときに生成されます。

### 新しい OS

このイベントは、システムがホストの新しいオペレーティングシステムを検出した、またはホストのオペレーティング システムで変更を検出したときに生成されます。

### 新しい TCP ポート

このイベントは、ホスト上でアクティブな新しい TCP サーバ ポート (SMTP または Web サービスで使用されているポートなど) をシステムが検出したときに生成されます。このイベントは、アプリケーションプロトコル、またはアプリケーションプロトコルに関連付けられているサーバの識別には使用されません。情報は、TCP Server Information Update イベントで伝送されます。

このイベントは、デバイスがネットワークマップにすでに存在しないモニタ対象ネットワーク上のサーバを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成するには、NetFlowデータを管理するネットワーク検出ルールでアプリケーションを検出するように設定します。

### 新しいトランスポート プロトコル

このイベントは、ホストが新しいトランスポート プロトコル (TCP、UDP など) と通信していることをシステムが検出したときに生成されます。

### 新しい UDP ポート

このイベントは、システムが、ホスト上で稼動している新しい UDP サーバ ポートを検出したときに生成されます。

このイベントは、デバイスがネットワークマップにすでに存在しないモニタ対象ネットワーク上のサーバを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成

するには、NetFlow データを管理するネットワーク検出ルールでアプリケーションを検出するように設定します。

### TCP ポート クローズ

このイベントは、システムが、ホスト上で TCP ポートがクローズしたことを検出したときに生成されます。

### TCP ポート タイムアウト

このイベントは、システムのネットワーク検出ポリシーに定義された間隔内で、システムが TCP ポートからアクティビティを検出しなかったときに生成されます。

### TCP サーバ情報の更新

このイベントは、ホスト上で稼動しており、すでに検出されている TCP サーバでシステムが変更を検出したときに生成されます。

このイベントは、TCP サーバが更新されたときに生成される場合があります。

### UDP ポート クローズ

このイベントは、システムが、ホスト上で UDP ポートがクローズしたことを検出したときに生成されます。

### UDP ポート タイムアウト

このイベントは、ネットワーク検出ポリシーに定義された間隔内で、システムが UDP ポートからアクティビティを検出しなかったときに生成されます。

### UDP サーバ情報の更新

このイベントは、ホスト上で稼動しており、すでに検出されている UDP サーバでシステムが変更を検出したときに生成されます。

このイベントは、UDP サーバが更新されたときに生成される場合があります。

### VLAN タグ情報の更新

このイベントは、システムが、VLAN タグ内でホストに起因する変更を検出したときに生成されます。

### 関連トピック

[ホスト入力イベント タイプ](#) (2703 ページ)

[ネットワーク検出のデータ ストレージ設定](#) (2170 ページ)

[アプリケーションおよびオペレーティング システムの ID の競合](#) (2026 ページ)

[ネットワーク検出アイデンティティ競合の設定](#) (2164 ページ)

## ホスト入力イベントタイプ

ディスカバリ イベントのテーブルを表示すると、[イベント (Event)] カラムにイベント タイプが表示されます。

ユーザが (手動でホストを追加するなどの) 特定のアクションを実行したときに生成されるホスト入力イベントとは異なり、ディスカバリ イベントは、システムが、監視対象ネットワークで変更を検出したとき (以前は検出されなかったホストでトラフィックを検出した場合など) に生成されます。

ネットワーク検出ポリシーを変更して、システムが記録するホスト入力イベントのタイプを設定できます。

さまざまなタイプのホスト入力イベントが提示する情報を理解すると、どのイベントを記録およびアラートの対象にするか、関連ポリシーでこれらのアラートをどのように使用するかを効率よく判断できるようになります。また、イベントタイプの名前がわかると、より効率のよいイベント検索を作成するうえで役に立ちます。次に、ホスト入力イベントのさまざまなタイプについて説明します。

### クライアントの追加 (Add Client)

このイベントは、ユーザがクライアントを追加したときに生成されます。

### ホストの追加 (Add Host)

このイベントは、ユーザがホストを追加したときに生成されます。

### プロトコルの追加 (Add Protocol)

このイベントは、ユーザがプロトコルを追加したときに生成されます。

### スキャン結果の追加 (Add Scan Result)

このイベントは、システムがNmap スキャンの結果をホストに追加したときに生成されます。

### ポートの追加 (Add Port)

このイベントは、ユーザがサーバ ポートを追加したときに生成されます。

### クライアントの削除 (Delete Client)

このイベントは、ユーザがシステムからクライアントを削除したときに生成されます。

### ホスト/ネットワークの削除 (Delete Host/Network)

このイベントは、ユーザがシステムから IP アドレスまたはサブネットを削除したときに生成されます。

### プロトコルの削除 (Delete Protocol)

このイベントは、ユーザがシステムからプロトコルを削除したときに生成されます。

**ポートの削除 (Delete Port)**

このイベントは、ユーザがシステムからサーバポートまたはサーバポートのグループを削除したときに生成されます。

**ホスト属性の追加 (Host Attribute Add)**

このイベントは、ユーザが新しいホスト属性を作成したときに生成されます。

**ホスト属性の削除 (Host Attribute Delete)**

このイベントは、ユーザが、ユーザ定義のホスト属性を削除したときに生成されます。

**ホスト属性値の削除 (Host Attribute Delete Value)**

このイベントは、ユーザが、ホスト属性に割り当てられている値を削除したときに生成されます。

**ホスト属性値の設定 (Host Attribute Set Value)**

このイベントは、ユーザがホストに対してホスト属性値を設定したときに生成されます。

**ホスト属性の更新 (Host Attribute Update)**

このイベントは、ユーザが、ユーザ定義のホスト属性の定義を変更したときに生成されます。

**ホスト重要度の設定 (Set Host Criticality)**

このイベントは、ユーザがホストに対してホストの重要度の値を設定した、または変更したときに生成されます。

**オペレーティングシステム定義の設定 (Set Operating System Definition)**

このイベントは、ユーザがホストに対してオペレーティングシステムを設定したときに生成されます。

**サーバ定義の設定 (Set Server Definition)**

このイベントは、ユーザがサーバに対してベンダーおよびバージョンの定義を設定したときに生成されます。

**脆弱性影響認定の設定 (Set Vulnerability Impact Qualification)**

このイベントは、脆弱性の影響の認定が設定されたときに生成されます。

脆弱性が、影響の認定に対する使用でグローバルレベルで無効になったとき、または脆弱性がグローバルレベルで有効になったときに、このイベントが生成されます。

**脆弱性を無効に設定 (Vulnerability Set Invalid)**

このイベントは、ユーザが1つ以上の脆弱性を無効にした（または確認した）ときに生成されます。

**脆弱性を有効に設定 (Vulnerability Set Valid)**

このイベントは、ユーザが、以前に無効であるとマークされた脆弱性を有効にしたときに生成されます。

**関連トピック**

[ディスカバリ イベントタイプ](#) (2698 ページ)

**ディスカバリ イベントとホスト入カイベントの表示**

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

ディスカバリ イベント ワークフローでは、ディスカバリ イベントとホスト入カイベント両方からのデータを表示できます。ユーザは検索する情報に応じてイベントビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがイベントにアクセスするときに表示されるページは、使用するワークフローによって異なります。ユーザは事前定義のワークフローを使用できますが、これにはディスカバリ イベントのテーブルビューと、ホスト ビューの最終ページが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

**手順**

**ステップ 1** [分析 (Analysis)] > [ホスト (Hosts)] > [検出イベント (Discovery Events)] を選択します。

**ステップ 2** 次の選択肢があります。

- [時間枠の変更 \(2455 ページ\)](#) の説明に従って、時間範囲を調整します。

(注) イベントビューを時間によって制約している場合は、(グローバルかイベント固有かに関係なく) アプライアンスに設定されている時間枠の外で生成されたイベントが、イベントビューに表示されます。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

- [(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタムワークフローを含む別のワークフローを使用します。

- 基本的なワークフロー操作を実行します（[ディスカバリおよびアイデンティティワークフローの使用 \(2695 ページ\)](#) を参照）。
- テーブルのカラムの内容について詳しく調べます（[ディスカバリ イベントのフィールド \(2706 ページ\)](#) を参照）。

---

### 関連トピック

[ディスカバリおよびアイデンティティ ワークフローの使用 \(2695 ページ\)](#)

## ディスカバリ イベントのフィールド

以下に、ディスカバリ イベント テーブルで表示および検索できるフィールドについて説明します。

### 時刻 (Time)

システムがイベントを生成した時間。

### イベント

ディスカバリ イベント タイプまたはホスト入力イベント タイプ。

### [IPアドレス (IP Address)]

イベントに関連するホストに関連付けられている IP アドレス。

### ユーザ (User)

イベントが生成される前に、イベントに関係するホストに最後にログインしたユーザ。権限のあるユーザの後に、権限のないユーザのみがログインした場合、権限のある別のユーザが次にログインするまで、権限のあるユーザがそのホストの現行ユーザとして保持されます。

### MAC アドレス (MAC Address)

ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックが使用する NIC の MAC アドレス。この MAC アドレスは、イベントに関連するホストの実際の MAC アドレスであるか、またはトラフィックが通過したネットワークデバイスの MAC アドレスになります。

### MAC ベンダー (MAC Vendor)

ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックが使用する NIC の MAC ハードウェア ベンダー。

このフィールドを検索する場合は、**virtual\_mac\_vendor** を入力して、仮想ホストに関するイベントを照合します。



**[ポート (Port) ]**

イベントをトリガーとして使用したトラフィックが使用するポート（該当する場合）。

**説明**

テキストによるイベントの説明。

**ドメイン**

ホストを検出したデバイスのドメイン。このフィールドは、マルチテナンシーのためにFirepower Management Center を設定したことがある場合に表示されます。

**Device**

イベントを生成した管理対象デバイスの名前。NetFlow データに基づいた新しいホストおよび新しいサーバのイベントの場合、これはそのデータを処理した管理対象デバイスになります。

**関連トピック**

[イベントの検索](#) (2467 ページ)

## ホスト データ

システムがホストを検出し、ホストプロファイルを作成するためにホストに関する情報を収集したときに、イベントが生成されます。Firepower Management Center Web インターフェイスを使用して、ホストを表示、検索、および削除できます。

ホストの表示中に、選択したホストに基づいてトラフィックのプロファイル、およびコンプライアンスのホワイトリストを作成できます。また、（ビジネスの重要度を設定する）ホストの重要度の値などのホスト属性をホストグループに割り当てることもできます。そのあとで、相関ルールおよびポリシーの中でこれらの重要度の値、ホワイトリスト、およびトラフィックプロファイルを使用できます。

システムは、ホストをエクスポートされたNetFlow レコードからネットワーク マップに追加できますが、これらのホストに使用できる情報は限られます（[NetFlow データと管理対象デバイスデータの違い](#) (2028 ページ) を参照）。

**関連トピック**

[NetFlow データと管理対象デバイスデータの違い](#) (2028 ページ)

## ホスト データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

Firepower Management Center を使用して、システムが検出したホストのテーブルを表示することができます。その後、探している情報に応じて表示方法を操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがホストにアクセスするときに表示されるページは、使用するワークフローによって異なります。両方の事前定義ワークフローが、制限を満たすすべてのホストのホストプロファイルを含むホストビューで終わります。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

## 手順

**ステップ 1** 次のように、ホストデータにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析 (Analysis)] > [ホスト (Hosts)] > [ホスト (Hosts)]** を選択します。
- ホストのテーブルビューが含まれないカスタムワークフローを使用している場合は、**[(ワークフローの切り替え) ((switch workflow))]** をクリックして**[ホスト (Hosts)]** を選択します。

**ステップ 2** 次の選択肢があります。

- **[(ワークフローの切り替え) ((switch workflow))]** をクリックしてカスタムワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(2695 ページ\)](#) を参照)。
- テーブルのカラムの内容について詳しく調べます ([ホストデータフィールド \(2708 ページ\)](#) を参照)。
- ホスト属性を特定のホストに割り当てます ([選択したホストのホスト属性の設定 \(2717 ページ\)](#) を参照)。
- 特定のホストのトラフィックプロファイルを作成します ([選択したホストのトラフィックプロファイルの作成 \(2713 ページ\)](#) を参照)。
- 特定のホストに基づいて、コンプライアンスのホワイトリストを作成します ([選択したホストに基づいたコンプライアンスのホワイトリストの作成 \(2714 ページ\)](#) を参照)。

## ホストデータ フィールド

システムはホストを検出したときに、そのホストに関するデータを収集します。そのデータには、ホストの IP アドレス、ホストが実行しているオペレーティングシステムなどが含まれることが可能です。ユーザは、ホストのテーブルビューでこれらの情報の一部を表示することができます。

ホストテーブルで表示および検索できるフィールドの説明が続きます。

### 前回の検出 (Last Seen)

システムによっていずれかのホストの IP アドレスが最後に検出された日付と時間。[前回の検出 (Last Seen)] の値は、ホストの IP アドレスに対してシステムが新しいホストイベントを生成したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

ホスト入力機能を使用して、オペレーティングシステムのデータを更新しているホストでは、[前回の検出 (Last Seen)] の値は、そのデータが最初に追加された日付と時間を表します。

### [IPアドレス (IP Address)]

ホストに関連付けられている IP アドレス。

### MAC アドレス (MAC Address)

ホストが検出した NIC の MAC アドレス。

[MAC アドレス (MAC Address)] フィールドは、[ホスト (Hosts)] ワークフローの [ホストのテーブル ビュー (Table View of Hosts)] に表示されます。以下のものに対して [MAC アドレス (MAC Address)] フィールドを追加できます。

- [ホスト (Hosts)] テーブルのフィールドが含まれているカスタム テーブル
- [ホスト (Hosts)] テーブルに基づいたカスタム ワークフローのドリルダウン ページ

### MAC ベンダー (MAC Vendor)

ホストが検出した NIC の MAC ハードウェア ベンダー。

[MAC ベンダー (MAC Vendor)] フィールドは、[ホスト (Hosts)] ワークフローの [ホストのテーブル ビュー (Table View of Hosts)] に表示されます。以下のものに対して [MAC ベンダー (MAC Vendor)] フィールドを追加できます。

- [ホスト (Hosts)] テーブルのフィールドが含まれているカスタム テーブル
- [ホスト (Hosts)] テーブルに基づいたカスタム ワークフローのドリルダウン ページ

このフィールドを検索する場合は、`virtual_mac_vendor` を入力して、仮想ホストに関するイベントを照合します。

### 現在のユーザ (Current User)

ホストに現在ログインしているユーザの ID (ユーザ名)。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

**ホストの重要度 (Host Criticality)**

ホストに割り当てられている、ユーザ指定の重要度の値。

**NetBIOS 名 (NetBIOS Name)**

ホストの NetBIOS 名。NetBIOS プロトコルを実行しているホストにのみ、NetBIOS 名があります。

**VLAN ID (Admin. VLAN ID)**

ホストが使用する VLAN ID。

**ホップ (Hops)**

ホストを検出したデバイスからホストへのネットワークのホップ数。

**ホストタイプ (Host Type)**

ホストのタイプ。ホスト、モバイルデバイス、**jailbroken** モバイルデバイス、ルータ、ブリッジ、NAT デバイス、ロードバランサのいずれかにできます。

ネットワーク デバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol (CDP) メッセージの分析。ネットワークのデバイスおよびそれらのタイプ (シスコ デバイスのみ) を特定できます。
- スパニングツリープロトコル (STP) の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロードバランサを識別します。

デバイスがネットワーク デバイスとして識別されない場合は、ホストとして分類されます。

このフィールドを検索するときは、!host と入力してすべてのネットワーク デバイスを検索します。

**ハードウェア (Hardware)**

モバイル デバイスのハードウェア プラットフォーム。

**OS**

次のいずれかです。

- ホスト上で検出されたオペレーティングシステム (名前、ベンダー、およびバージョン)、または Nmap がホスト入力機能を使用して更新されたオペレーティング システム。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は unknown

- オペレーティングシステムを識別するための十分な情報がシステムで収集されていない場合は `pending`

システムが複数のアイデンティティを検出した場合は、これらのアイデンティティはカンマ区切りリストで表示されます。

このフィールドは、ダッシュボード上で[カスタム分析 (Custom Analysis)] ウィジェットからホストイベントビューを起動したときに表示されます。また、これは[ホスト (Hosts)] テーブルに基づいたカスタム テーブルのフィールド オプションです。

このフィールドを検索するときは、`n/a` と入力して、オペレーティングシステムがまだ識別されていないホストを含めます。

### OS 競合 (OS Conflict)

このフィールドは検索専用です。

### OS ベンダー (OS Vendor)

次のいずれかです。

- ホストで検出されたオペレーティングシステムのベンダー、またはNmapがホスト入力機能を使用して更新されたオペレーティングシステムのベンダー。
- オペレーティングシステムが既知のフィンガープリントに一致しない場合は `unknown`
- オペレーティングシステムを識別するための十分な情報がシステムで収集されていない場合は `pending`

システムが複数のベンダーを検出した場合は、これらのベンダーはカンマ区切りリストで表示されます。

このフィールドを検索するときは、`n/a` と入力して、オペレーティングシステムがまだ識別されていないホストを含めます。

### OS 名 (OS Name)

次のいずれかです。

- ホスト上で検出されたオペレーティングシステム、またはNmapがホスト入力機能を使用して更新されたオペレーティングシステム。
- オペレーティングシステムが既知のフィンガープリントに一致しない場合は `unknown`
- オペレーティングシステムを識別するための十分な情報がシステムで収集されていない場合は `pending`

システムが複数の名前を検出した場合は、これらの名前はカンマ区切りリストで表示されます。

このフィールドを検索するときは、`n/a` と入力して、オペレーティングシステムがまだ識別されていないホストを含めます。

### OS バージョン (OS Version)

次のいずれかです。

- ホストで検出されたオペレーティングシステムのバージョン、またはNmapがホスト入力機能を使用して更新されたオペレーティングシステムのバージョン。
- オペレーティングシステムが既知のフィンガープリントに一致しない場合は unknown
- オペレーティングシステムを識別するための十分な情報がシステムで収集されていない場合は pending

システムが複数のバージョンを検出した場合は、これらのバージョンはカンマ区切りリストで表示されます。

このフィールドを検索するときは、n/a と入力して、オペレーティングシステムがまだ識別されていないホストを含めます。

### ソース タイプ (Source Type)

ホストのオペレーティングシステムのアイデンティティを確立するために使用されるソースのタイプは次のとおりです。

- [ユーザ (User) ] : user\_name
- [アプリケーション (Application) ] : app\_name
- スキャナ : scanner\_type (ネットワーク検出の設定を介して追加されたNmapまたはスキャナ)
- システムによって検出されたオペレーティングシステムの場合は Firepower

システムでは、オペレーティングシステムのアイデンティティを判断するために、複数のソースのデータを統合することができます。

### 信頼性 (Confidence)

次のいずれかです。

- システムで検出されたホストについて、ホスト上で稼動しているオペレーティングシステムのアイデンティティ内にシステムが保持している信頼度 (パーセンテージ) 。
- 100% (ホスト入力機能やNmap スキャナなどのアクティブなソースによって識別されたオペレーティングシステムの場合) 。
- unknown (システムがオペレーティングシステムのアイデンティティを特定できないホスト、およびNetFlow データに基づいてネットワーク マップに追加されたホストの場合) 。

このフィールドを検索するときは、n/a と入力して、NetFlow データに基づいてネットワーク マップに追加されたホストを含めます。

**注記 (Notes)**

[注記 (Notes) ] ホスト属性の、ユーザ定義のコンテンツ。

**ドメイン**

ホストに関連付けられているドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

**Device**

トラフィックを検出した管理対象デバイスか、NetFlow またはホスト入力データを処理したデバイスのいずれか。

このフィールドが空白の場合は、次のいずれかの条件を満たします。

- ホストがデバイスによってネットワーク マップに追加されたが、このデバイスは、ホストが存在しているネットワークに対してネットワーク検出ポリシーに定義されているとおりに明示的に監視していない。
- ホストの入力機能を使用してホストが追加されたが、システムによって検出されていない。

**メンバー数 (Count)**

各行に表示される情報と一致するイベントの数。このフィールドが表示されるのは、2 つ以上の同一の行を作成する制限を適用した後のみです。

**関連トピック**

[イベントの検索](#) (2467 ページ)

[オペレーティング システムのアイデンティティの競合](#) (2664 ページ)

**選択したホストのトラフィック プロファイルの作成**

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

トラフィック プロファイルは、指定した期間に収集された接続データに基づいた、ネットワーク上のトラフィックのプロファイルです。トラフィック プロファイルを作成した後、正常なネットワークトラフィックを表すと想定されるプロファイルに照らして新しいトラフィックを評価することにより、異常なネットワークトラフィックを検出できます。

[ホスト (Hosts) ] ページを使用して、指定するホスト グループのトラフィック プロファイルを作成できます。トラフィック プロファイルは、指定したホストのいずれかが発信元ホストである、検出された接続に基づいています。ソートおよび検索機能を使用して、プロファイルを作成するホストを分離することができます。

## 手順

- 
- ステップ 1** ホストワークフローのテーブルビューで、トラフィック プロファイルを作成するホストの隣にあるチェック ボックスをオンにします。
- ステップ 2** ページの下部で [トラフィック プロファイルの作成 (Create Traffic Profile) ] をクリックします。
- ステップ 3** 特別なニーズに応じて、トラフィック プロファイルを変更し、保存します。

## 関連トピック

[トラフィック プロファイルの概要](#) (2269 ページ)

## 選択したホストに基づいたコンプライアンスのホワイトリストの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

コンプライアンスのホワイトリストでは、ネットワーク上で許可されるオペレーティング システム、クライアント、ネットワーク、トランスポート、またはアプリケーションプロトコルを指定することができます。

[ホスト (Hosts) ] ページを使用して、ユーザが指定するホストグループのホストプロファイルに基づいて、コンプライアンスのホワイトリストを作成することができます。ソートおよび検索機能を使用して、ホワイトリストの作成に使用するホストを分離することができます。

## 手順

- 
- ステップ 1** ホストワークフローのテーブルビューで、ホワイトリストを作成するホストの隣にあるチェック ボックスをオンにします。
- ステップ 2** ページの下部で [ホワイトリストの作成 (Create White List) ] をクリックします。
- ステップ 3** 特別なニーズに応じて、ホワイトリストを変更し、保存します。

## 関連トピック

[コンプライアンス ホワイトリストの概要](#) (2203 ページ)

## ホスト属性データ

Firepower システムは、検出したホストに関する情報を収集し、その情報を使用してホストプロファイルを作成します。ただし、ネットワーク上のホストについて、アナリストに提供する追加情報が存在する場合があります。ユーザは、ホストプロファイルにメモを追加する、ホス



トのビジネス重要度を設定する、選択する他の情報を提供する、といったことが可能です。それぞれの情報は、ホスト属性と呼ばれます。

ホストプロファイルの認定でホスト属性を使用することができます。これにより、トラフィックプロファイルの作成中に収集するデータを制約し、関連ルールをトリガーする条件を制限することができます。関連ルールに応じて属性値を設定することもできます。

### 関連トピック

[ホスト属性の表示](#) (2715 ページ)

[セット属性修復の設定](#) (2296 ページ)

## ホスト属性の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

Firepower Management Center を使用して、システムで検出されたホストのテーブル、およびそのホスト属性を表示することができます。その後、探している情報に応じて表示方法を操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがホスト属性にアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフロー（検出されたすべてのホスト、およびそのホストの属性が記載されているホスト属性のテーブル ビューが含まれており、ホスト ビュー ページで終了するワークフロー）を使用することができます。このワークフローには、制約を満たすすべてのホストについて1つのホスト プロファイルが含まれています。

また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

### 手順

**ステップ 1** 次のように、ホスト属性データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析 (Analysis)] > [ホスト (Hosts)] > [ホスト属性 (Host Attributes)] を選択します。
- ホスト属性のテーブルビューが含まれないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして[属性 (Attributes)] を選択します。

**ステップ 2** 次の選択肢があります。

- [(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタムワークフローを含む別のワークフローを使用します。

- 基本的なワークフロー操作を実行します（[ディスカバリおよびアイデンティティワークフローの使用 \(2695 ページ\)](#) を参照）。
- テーブルのカラムの内容について詳しく調べます（[ホスト属性データ フィールド \(2716 ページ\)](#) を参照）。
- ホスト属性を特定のホストに割り当てます（[選択したホストのホスト属性の設定 \(2717 ページ\)](#) を参照）。

## ホスト属性データ フィールド

ホスト属性テーブルには、MAC アドレスでのみ識別されるホストは表示されないことに注意してください。

ホスト属性テーブルで表示および検索できるフィールドの説明が続きます。

### [IPアドレス (IP Address)]

ホストに関連付けられている IP アドレス。

### 現在のユーザ (Current User)

ホストに現在ログインしているユーザの ID (ユーザ名)。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

### ホストの重要度 (Host Criticality)

ユーザが割り当てた、企業にとってのホストの重要度。ホストの重要度を相関ルールおよびポリシーで使用して、イベントに関するホストの重要度に対して、ポリシー違反および違反の応答を作成することができます。ホストの重要度に [低 (Low) ]、[中 (Medium) ]、[高 (High) ]、または [なし (None) ] を割り当てることができます。

### 注記 (Notes)

他のアナリストに提示する、ホストに関する情報。

### コンプライアンス ホワイトリストの属性を含む、ユーザ定義のホスト属性 (Any user-defined host attribute, including those for compliance white lists)

ユーザ定義のホスト属性の値。ホスト属性テーブルには、ユーザ定義のそれぞれのホスト属性のフィールドが含まれています。

### ドメイン

ホストに関連付けられているドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

### メンバー数 (Count)

各行に表示される情報と一致するイベントの数。[カウント (Count)] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

### 関連トピック

[イベントの検索](#) (2467 ページ)

## 選択したホストのホスト属性の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

ホスト ワークフローから、事前定義済みのホスト属性とユーザ定義のホスト属性を設定できます。

### 手順

**ステップ 1** ホストワークフローで、ホスト属性を追加するホストの横にあるチェックボックスをオンにします。

**ヒント** ソート機能と検索機能を使用して、特別な属性を割り当てるホストを分離することができます。

**ステップ 2** ページの下部にある [属性の設定 (Set Attributes)] をクリックします。

**ステップ 3** 必要に応じて、選択したホストに対してホストの重要度を設定します。[なし (None)]、[低 (Low)]、[中 (Medium)]、または [高 (High)] を選択できます。


**ステップ 4** 必要に応じて、テキストボックスで、選択したホストのホスト プロファイルにメモを追加します。

**ステップ 5** 必要に応じて、自分で設定したユーザ定義のホストの属性を設定します。

**ステップ 6** [保存 (Save)] をクリックします。

## 侵害の兆候データ

Firepower システムは、さまざまなタイプのデータ (侵入イベント、セキュリティインテリジェンス、接続イベントおよびファイルまたはマルウェアイベント) を関連付け、モニタ対象ネッ

トワーク上のホストが悪意のある手段によって侵害された可能性があるかどうかを判断します。イベントデータの特定の組み合わせと頻度が、影響を受けるホストの侵害の兆候 (IOC) タグをトリガーします。このようなホストの IP アドレスは侵害を受けているホストの赤いアイコン (  ) でイベント ビューに表示されます。

IOC データは、Firepower システムの Web インターフェイスの数箇所に表示、操作を行えます。

- イベント ビューア：接続、セキュリティ インテリジェンス、侵入、マルウェアや IOC 検出のイベントビューでそのイベントが IOC をトリガーしたかどうかを表示します。IOC ルールをトリガーするエンドポイント ベースのマルウェア イベントは、イベント タイプが AMP IOC であり、侵害を指定するイベント サブタイプと一緒に表示されることに注意してください。イベント ビューは、[分析 (Analysis)] タブ内のさまざまなタブから使用できます。
- ダッシュボード：ダッシュボードでは、サマリー ダッシュボードの [脅威 (Threats)] タブに、ホスト別の IOC タグと一定期間にトリガーされた新しい IOC ルールがデフォルトで表示されます。カスタム分析ウィジェットは IOC データに基づくプリセットを提供します。
- コンテキスト エクスプローラ：コンテキスト エクスプローラの [侵害の兆候 (Indications of Compromise)] セクションに、IOC カテゴリ別のホストとホスト別の IOC カテゴリのグラフが表示されます。
- [ネットワーク マップ (Network Map)] ページ：[分析 (Analysis)] > [ホスト (Hosts)] > [ネットワーク マップ (Network Map)] にある [侵害の兆候 (Indications of Compromise)] タブには、侵害されている可能性があるネットワーク上のホストが侵害のタイプと IP アドレス別にグループ分けして示されます。
- [ネットワーク ファイル トラjectory (Network File Trajectory)] 詳細ページ：[分析 (Analysis)] > [ファイル (Files)] > [ネットワーク ファイル トラjectory (Network File Trajectory)] の下に一覧表示されているファイルの詳細ページでは、ネットワークの侵害の兆候を追跡できます。
- [侵害の兆候 (Host Indications of Compromise)] ページ：[分析 (Analysis)] > [ホスト (Hosts)] メニューの下の [侵害の兆候 (Host Indications of Compromise)] ページには、モニタ対象ホストの一覧が IOC タグ別にグループ分けされて表示されます。このページのワークフローを使ってデータをドリルダウンできます。
- ホスト プロファイル ページ：侵害されている可能性があるホストのホスト プロファイルには、そのホストに関連付けられているすべての IOC タグが表示され、IOC タグの解決と IOC ルール状態の設定ができます。

侵害の兆候としてイベントにタグを付けるように設定するには、[侵害の兆候ルールの有効化 \(2168 ページ\)](#) を参照してください。

## 関連トピック

[侵害の兆候ルールの有効化 \(2168 ページ\)](#)

## 侵害の兆候データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

Firepower Management Center を使用して、侵害の兆候 (IOC) を示すテーブルを表示できます。検索する情報に応じてイベント ビューを操作します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

表示されるページは、使用するワークフローによって異なります。事前定義の IOC ワークフローはプロファイル ビューで終了しますが、これには、制約を満たすすべてのホストまたはユーザのホストプロファイルまたはユーザプロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

### 始める前に


- システムで侵害の兆候 (IOC) を検出してタグを付けるには、ネットワーク検出ポリシーの IOC 機能をアクティブにして、少なくとも 1 つの IOC ルールを有効にする必要があります。[侵害の兆候ルールの有効化 \(2168 ページ\)](#) を参照してください。

### 手順

**ステップ 1** 事前定義されたワークフローを使用する場合、[分析 (Analysis)] > [ホスト (Hosts)] > [侵害の兆候 (Indications of Compromise)] を選択します。

ホスト IOC のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [侵害の兆候 (Indications of Compromise)] を選択します。

**ステップ 2** 次の選択肢があります。

- [(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(2695 ページ\)](#) を参照)。
- テーブルのカラムの内容について詳しく調べます ([侵害の兆候データ フィールド \(2720 ページ\)](#) を参照)。
- [ホストの侵害の兆候 (Host Indications of Compromise)] ページ: [IP アドレス (IP Address)] カラムにある侵害されたホストのアイコン (  ) をクリックして、侵害されたホストのホスト プロファイルを表示します。

- IOC イベントに解決済みとマークして、リストに表示されないようにします。これを実行するには、編集する IOC イベントの横にあるチェック ボックスをオンにして、[解決済みとマークを付ける (Mark Resolved)] をクリックします。
- [最初の確認日時 (First Seen)] または [前回の検出 (Last Seen)] カラムにある表示アイコン (🔍) をクリックして、IOC をトリガーしたイベントの詳細を表示します。

## 侵害の兆候データ フィールド

以下は、の IOC (侵害の兆候) テーブル内のフィールドです。すべての IOC 関連のテーブルにすべてのフィールドが含まれているわけではありません。

### IP アドレス (IP Address)

IOC をトリガーとして使用したホストに関連付けられている IP アドレス。

### カテゴリ (Category)

[マルウェアが実行されました (Malware Executed)] や [影響 1 の攻撃 (Impact 1 Attack)] など、示された侵害のタイプの簡単な説明。

### イベントタイプ (Event Type)

特定の IOC に関連付けられている識別子で、トリガーとして使用したイベントを参照します。

### 説明

侵害される可能性のあるホストへの影響の説明 ([このホストはリモート制御下にある可能性があります (This host may be under remote control)] や [このホスト上でマルウェアが実行されました (Malware has been executed on this host)] など)。

### 最初の確認日時/最新の確認日時 (First Seen/Last Seen)

IOC をトリガーとして使用したイベントが発生した最初 (または最新) の日付と時刻。

### ドメイン (Domain)

IOC をトリガーとして使用したホストのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合にのみ表示されます。

### 関連トピック

[イベントの検索](#) (2467 ページ)

## 単一ホストにおける侵害の兆候のルール状態の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst (読み取り専用を除く)

ネットワーク検出ポリシーで有効になっている場合、侵害の兆候ルールは監視対象ネットワーク内のすべてのホストに適用されます。個々のホストのルールを無効にして、無用なIOCタグを回避できません (たとえば、DNSサーバに対するIOCタグが表示されないようにできません)。適用可能なネットワーク検出ポリシーでルールを無効にすると、特定のホストに対して有効にすることができません。

### 手順

- ステップ 1** ホスト プロファイルの [侵害の兆候 (Indications of Compromise)] セクションに移動します。
- ステップ 2** [ルール状態の編集 (Edit Rule States)] をクリックします。
- ステップ 3** ルールの [有効 (Enabled)] 列で、スライダをクリックしてこれを有効または無効にします。
- ステップ 4** [保存 (Save)] をクリックします。

## 侵害の兆候のタグのソース イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

ホスト プロファイルの [侵害の兆候 (Indications of Compromise)] セクションを使用して、IOCタグをトリガーしたイベントにすばやく移動することができます。これらのイベントを分析すると、侵害される脅威に対処するのに必要なアクション、およびアクションが必要かどうかを判断するための情報が提供されます。

IOC タグのタイムスタンプの隣の表示アイコン (🔍) をクリックすると、関連するイベントタイプのイベントのテーブルビューにナビゲートします。ここでは、IOCタグをトリガーとして使用したイベントのみが表示されます。

### 手順

- ステップ 1** ホスト プロファイルで、[侵害の兆候 (Indications of Compromise)] セクションに移動します。

**ステップ 2** 調べたい IOC タグの [最初の痕跡 (First Seen)] または [最後の痕跡 (Last Seen)] カラムにある表示アイコン (🔍) をクリックします。

## 侵害の兆候タグの解決

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

侵害の兆候 (IOC) タグで示された脅威が分析および対処された後、または IOC タグが誤検出を示していると判断した場合、イベントに解決済みのマークを付けることができます。イベントに解決済みのマークを付けると、そのイベントはホストプロファイルから削除されます。プロファイル上のアクティブな IOC タグがすべて解決されると、侵害されたホストアイコン

(🔍) は表示されなくなります。解決した IOC についても、IOC のトリガー元であるイベントは引き続き表示できます。

IOC タグをトリガーしたイベントが繰り返された場合、ホストに対する IOC ルールが無効にされていない限り、このタグが再び設定されます。

### 手順

**ステップ 1** ホストプロファイルで、[侵害の兆候 (Indications of Compromise)] セクションに移動します。

**ステップ 2** 次の 2 つの選択肢があります。

- 個別の IOC タグに解決済みのマークを付けるには、解決するタグの右にある削除アイコン (🗑️) をクリックします。
- プロファイル上のすべての IOC タグに解決済みのマークを付けるには、[すべてに解決済みのマークを付ける (Mark All Resolved)] をクリックします。

## サーバデータ

Firepower システムは、モニタ対象ネットワーク セグメント上のホストで稼動しているすべてのサーバに関する情報を収集します。この情報には次のものが含まれます。

- サーバの名前
- サーバが使用するアプリケーションとネットワーク プロトコル
- サーバのベンダーとバージョン
- サーバを実行しているホストに関連付けられている IP アドレス



- サーバが通信するポート

システムはサーバを検出すると、関連するホストがまだサーバの最大数に達していない場合は、ディスカバリ イベントを生成します。Firepower Management Center の Web インターフェイスを使用して、サーバ イベントを表示、検索、削除できます。

また、サーバ イベントを相関ルールのベースにすることもできます。たとえばシステムが、いずれかのホスト上で稼動している ircd などのチャット サーバを検出したときに相関ルールをトリガーできます。

システムは、ホストをエクスポートされた NetFlow レコードからネットワーク マップに追加できますが、これらのホストに使用できる情報は限られます ([NetFlow データと管理対象デバイスデータの違い \(2028 ページ\)](#) を参照)。

#### 関連トピック

[ホスト制限と検出イベント ロギング \(2102 ページ\)](#)

[NetFlow データと管理対象デバイスデータの違い \(2028 ページ\)](#)

## サーバデータの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

Firepower Management Center を使用して、検出されたサーバのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがサーバにアクセスしたときに表示されるページは、使用するワークフローによって異なります。事前定義されたすべてのワークフローはホストビューで終了しますが、このホストビューには、制約を満たすすべてのホストに対して1つずつホストプロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

#### 手順

**ステップ 1** 次のように、サーバデータにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析 (Analysis)] > [ホスト (Hosts)] > [サーバ (Servers)] を選択します。
- サーバのテーブルビューが含まれていないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [サーバ (Servers)] を選択します。

**ステップ 2** 次の選択肢があります。

- [(ワークフローの切り替え) ((switch workflow)) ]をクリックしてカスタムワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(2695 ページ\)](#) を参照)。
- テーブルのカラムの内容について詳しく調べます ([サーバデータ フィールド \(2724 ページ\)](#) を参照)。
- 編集するサーバのイベントの横にあるチェック ボックスをオンにし、[サーバアイデンティティの設定 (Set Server Identity) ]をクリックすることによって、サーバのアイデンティティを編集します。

---

#### 関連トピック

[サーバのアイデンティティの編集 \(2670 ページ\)](#)

## サーバデータ フィールド

サーバテーブルで表示および検索できるフィールドの説明は次のとおりです。

#### 前回の使用 (Last Used)

ネットワーク上でサーバが最後に使用された日付と時間、またはホスト入力機能を使用してサーバが最初に更新された日付と時間。[前回の使用 (Last Used) ]の値は、システムがサーバ情報の更新を検出したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

#### [IPアドレス (IP Address) ]

サーバを実行しているホストに関連付けられている IP アドレス。

#### [ポート (Port) ]

サーバが稼動しているポート。

#### プロトコル

サーバが使用するネットワークまたはトランスポート プロトコル。

#### アプリケーション プロトコル (Application Protocol)

次のいずれかです。

- サーバのアプリケーション プロトコルの名前
- pending : システムで、いずれかの理由でサーバをポジティブまたはネガティブに識別できない場合

- unknown：既知のサーバフィンガープリントに基づいてシステムでサーバを識別できない場合、またはホストの入力を介してサーバが追加され、アプリケーションプロトコルが含まれていなかった場合

### アプリケーションプロトコルのカテゴリ、タグ、リスク、またはビジネスとの関連性 (Category, Tags, Risk, or Business Relevance for Application Protocols)

アプリケーションプロトコルに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネスとの関連性。これらのフィルタを使用して、特定のデータセットを対象にすることができます。

### ベンダー (Vendor)

次のいずれかです。

- サーバのベンダー：システム、Nmap、その他のアクティブなソースで識別された、またはホスト入力機能を使用して指定されたサーバのベンダー
- 空白：システムが既知のサーバフィンガープリントに基づいてベンダーを識別できなかった場合、またはNetFlowデータを使用してサーバがネットワークマップに追加された場合

### バージョン (Version)

次のいずれかです。

- サーバのバージョン：システム、Nmap、その他のアクティブなソースで識別された、またはホスト入力機能を使用して指定されたサーバのバージョン
- 空白：システムが既知のサーバフィンガープリントに基づいてバージョンを識別できなかった場合、またはNetFlowデータを使用してサーバがネットワークマップに追加された場合

### Web アプリケーション (Web Application)

HTTP トラフィックでシステムが検出したペイロードコンテンツに基づいた Web アプリケーション。システムが HTTP のアプリケーションプロトコルを検出したものの、特定の Web アプリケーションを検出できない場合は、一般的な Web ブラウジングの指定が提示されるので注意してください。

### Web アプリケーションのカテゴリ、タグ、リスク、またはビジネスとの関連性 (Category, Tags, Risk, or Business Relevance for Web Applications)

Web アプリケーションに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネスとの関連性。これらのフィルタを使用して、特定のデータセットを対象にすることができます。

### ヒット数 (Hits)

サーバがアクセスされた回数。ホスト入力機能を使用して追加されたサーバの場合、この値は必ず 0 になります。

### ソース タイプ (Source Type)

次の値のいずれかを指定します。

- [ユーザ (User) ] : user\_name
- [アプリケーション (Application) ] : app\_name
- スキャナ : scanner\_type (ネットワーク検出の設定を介して追加された Nmap または スキャナ)
- Firepower システムによって検出されたサーバの Firepower、Firepower Port Match、または Firepower Pattern Match
- NetFlow データを使用して追加されたサーバの NetFlow

### ドメイン

サーバを実行しているホストのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

### Device

トラフィックを検出した管理対象デバイスか、NetFlow またはホスト入力データを処理したデバイスのいずれか。

### 現在のユーザ (Current User)

ホストに現在ログインしているユーザの ID (ユーザ名)。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されます。権限のあるユーザがそのホストに関連付けられていない場合、権限のないユーザがそのホストの現行 (現在の) ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

### メンバー数 (Count)

各行に表示される情報と一致するイベントの数。このフィールドが表示されるのは、2 つ以上の同一の行を作成する制限を適用した後のみです。

### 関連トピック

[イベントの検索](#) (2467 ページ)

[ネットワーク検出のデータ ストレージ設定](#) (2170 ページ)

## アプリケーションデータとアプリケーション詳細データ

監視対象ホストが別のホストに接続すると、システムは多くの場合、どのアプリケーションが使用されたかを判断することができます。Firepower システムは、電子メール、インスタントメッセージ、ピアツーピア、Web アプリケーション、およびその他のタイプのアプリケーションが多用されると検出します。

検出されたそれぞれのアプリケーションに対してシステムは、アプリケーションを使用した IP アドレス、製品、バージョン、および使用が検出された回数を記録します。Web インターフェイスを使用して、アプリケーションイベントを表示、検索、および削除できます。ホスト入力機能を使用して、1つ以上のホスト上のアプリケーションデータを更新することもできます。

どのアプリケーションがどのホストで稼動しているかがわかっている場合は、その情報をもとにホスト プロファイルの認定を作成し、この認定によって、トラフィック プロファイルの作成中に収集するデータを制約することができます。また、関連ルールをトリガーする条件を制約することもできます。また、アプリケーションの検出を関連ルールのベースにすることもできます。たとえば、従業員に特定のメールクライアントを使用させたい場合は、システムが、いずれかの対象ホストで別のメールクライアントが稼動していることを検出したときに関連ルールをトリガーすることができます。

Firepower のアプリケーションディテクトに関する最新情報は、各 Firepower システム更新のリリースノート、各 VDB 更新のアドバイザリをよくご確認ください。

分析用にアプリケーションデータを収集および保存するには、ネットワーク検出ポリシーでアプリケーションの検出が有効になっていることを確認します。

### アプリケーションデータの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

Firepower Management Center を使用して、検出されたアプリケーションのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがアプリケーションにアクセスするときに表示されるページは、使用するワークフローによって異なります。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

#### 手順

**ステップ 1** 次のようにして、アプリケーションデータにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析 (Analysis)] > [ホスト (Hosts)] > [アプリケーション詳細 (Application Details)] を選択します。
- アプリケーションの詳細のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [クライアント (Clients)] を選択します。

**ステップ 2** 次の選択肢があります。

- [(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタムワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(2695 ページ\)](#) を参照)。
- テーブルのカラムの内容について詳しく調べます ([アプリケーション データ フィールド \(2728 ページ\)](#) を参照)。
- クライアント、アプリケーション プロトコル、Web アプリケーションの横にあるアプリケーション詳細ビューのアイコン (🔍) をクリックすることによって、特定のアプリケーションの [アプリケーション詳細ビュー (Application Detail View)] を開きます。

## アプリケーション データ フィールド

システムは、既知のクライアント、アプリケーションプロトコル、または Web アプリケーションについてトラフィックを検出すると、アプリケーションおよびそのアプリケーションを実行しているホストに関する情報をログに記録します。

次に、アプリケーション テーブルで表示および検索できるフィールドについて説明します。

### Application

検出されたアプリケーションの名前。

### [IPアドレス (IP Address)]

アプリケーションを使用しているホストに関連付けられている IP アドレス。

### タイプ (Type)

アプリケーションのタイプであり、次のものがあります。

### アプリケーション プロトコル (Application Protocols)

ホスト間の通信を意味します。

### クライアント アプリケーション

ホスト上で動作しているソフトウェアを意味します。

### Web アプリケーション (Web Applications)

HTTP トラフィックの内容や要求された URL を意味します。

### カテゴリ (Category)

アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも1つのカテゴリに属します。

### タグ

アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます (タグなしも可能)。

### リスク (Risk)

アプリケーションが組織のセキュリティポリシーに違反することがある目的で使用される可能性。アプリケーションのリスクの範囲は、[極めて低 (Very Low)] から [極めて高 (Very High)] までです。

侵入イベントをトリガーしたトラフィックで検出される Application Protocol Risk、Client Risk、Web Application Risk の3つ (存在する場合) の中で最も高いものとなります。

### ビジネスとの関連性 (Business Relevance)

アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。アプリケーションのビジネスとの関連性の範囲は、[極めて低 (Very Low)] から [極めて高 (Very High)] までです。

侵入イベントをトリガーしたトラフィックで検出される Application Protocol Business Relevance、Client Business Relevance、Web Application Business Relevance の3つ (存在する場合) の中で最も低いものとなります。

### 現在のユーザ (Current User)

ホストに現在ログインしているユーザの ID (ユーザ名)。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

### ドメイン

アプリケーションを使用しているホストのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

### メンバー数 (Count)

各行に表示される情報と一致するイベントの数。[カウント (Count)] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

## 関連トピック

[イベントの検索](#) (2467 ページ)

## アプリケーション詳細データの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

Firepower Management Center を使用して、検出されたアプリケーションの詳細テーブルを表示できます。ここでユーザは、検索する情報に応じてイベントビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。


ユーザがアプリケーションの詳細にアクセスするときに表示されるページは、使用するワークフローによって異なります。2つの事前定義されたワークフローがあります。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

## 手順

**ステップ 1** 次のようにして、アプリケーション詳細データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析 (Analysis)] > [ホスト (Hosts)] > [アプリケーション詳細 (Application Details)] を選択します。
- アプリケーションの詳細のテーブルビューが含まれないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [クライアント (Clients)] を選択します。

**ステップ 2** 次の選択肢があります。

- [(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタムワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(2695 ページ\)](#) を参照)。
- テーブルのカラムの内容について詳しく調べます ([アプリケーションの詳細データフィールド \(2731 ページ\)](#) を参照)。
- クライアントの横にあるアプリケーション詳細ビューのアイコン () をクリックして、特定のアプリケーションの [アプリケーション詳細ビュー (Application Detail View)] を開きます。



## アプリケーションの詳細データ フィールド

システムは、既知のクライアント、アプリケーションプロトコル、または Web アプリケーションについてトラフィックを検出すると、アプリケーションおよびそのアプリケーションを実行しているホストに関する情報をログに記録します。

次に、アプリケーションの詳細テーブルで表示および検索できるフィールドについて説明します。

### 前回の使用 (Last Used)

アプリケーションが前回使用された時間、またはホスト入力機能を使用してアプリケーションデータが更新された時間。[前回の使用 (Last Used)] の値は、システムがアプリケーション情報の更新を検出したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

### [IP アドレス (IP Address)]

アプリケーションを使用しているホストに関連付けられている IP アドレス。

### クライアント (Client)

アプリケーションの名前。ただし、システムがアプリケーションプロトコルを検出したにも関わらず特定のクライアントを検出できなかった場合は、アプリケーションプロトコル名に `client` が付加されて一般名が表示されます。

### バージョン (Version)

アプリケーションのバージョン。

### クライアント、アプリケーションプロトコル、および Web アプリケーションのカテゴリ、タグ、リスク、またはビジネスとの関係性 (Category, Tags, Risk, or Business Relevance for Clients, Application Protocols, and Web Applications)

アプリケーションに割り当てられているカテゴリ、タグ、リスクレベル、およびビジネスとの関連性。これらのフィルタを使用して、特定のデータセットを対象にすることができます。

### アプリケーションプロトコル (Application Protocol)

アプリケーションで使用されるアプリケーションプロトコル。ただし、システムがアプリケーションプロトコルを検出したにも関わらず特定のクライアントを検出できなかった場合は、アプリケーションプロトコル名に `client` が付加されて一般名が表示されます。

### Web アプリケーション (Web Application)

HTTP トラフィックでシステムが検出したペイロードコンテンツまたは URL に基づく Web アプリケーション。ただし、HTTP のアプリケーションプロトコルが検出されたにも関わらず特定の Web アプリケーションを検出できない場合、ここには、標準の Web 閲覧先が表示されます。

### ヒット数 (Hits)

システムが使用中のアプリケーションを検出した回数。ホスト入力機能を使用して追加されたアプリケーションの場合、この値は常に 0 になります。

### ドメイン

アプリケーションを使用しているホストのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

### Device

アプリケーションの詳細が含まれている検出イベントを生成したデバイス。

### 現在のユーザ (Current User)

ホストに現在ログインしているユーザの ID (ユーザ名)。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

### メンバー数 (Count)

各行に表示される情報と一致するイベントの数。[カウント (Count)] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

### 関連トピック

[イベントの検索 \(2467 ページ\)](#)

[ネットワーク検出のデータ ストレージ設定 \(2170 ページ\)](#)

## 脆弱性データ

Firepower システムには、それ独自の脆弱性追跡データベースが含まれています。そのデータベースは、このシステムのフィンガープリンティング機能と組み合わせて使用されて、ネットワーク上のホストに関連付けられている脆弱性が特定されます。ホストで稼動しているオペレーティングシステム、サーバ、およびクライアントには、関連付けられている異なる脆弱性一式があります。

Firepower Management Center を使用して次のことを行えます。

- ホストごとの脆弱性を追跡および確認できます。
- ホストにパッチを適用した後、またはホストが脆弱性に影響されないと判断した場合は、そのホストの脆弱性を非アクティブにすることができます。

サーバで使用されるアプリケーションプロトコルが Firepower Management Center 構成内でマップされない限り、ベンダーレスおよびバージョンレスのサーバの脆弱性はマップされません。ベンダーレスおよびバージョンレスのクライアントの脆弱性はマップできません。

### 関連トピック

[サーバの脆弱性のマッピング](#) (988 ページ)

## 脆弱性データのフィールド

以下に説明する脆弱性データのフィールドは、脆弱性のテーブルビューと脆弱性の詳細表示で次のように表示されます。

表 305: 表示場所別の脆弱性データ フィールド

フィールド	テーブルビュー	詳細の表示
その他の情報	No	Yes
使用可能なエクスプロイト (Available Exploits)	Yes	Yes
Bugtraq ID	Yes	Yes
CVE ID	No	Yes
メンバー数 (Count)	Yes	No
発行日 (Date Published)	Yes	Yes
説明	Yes	Yes
修正 (Fixes)	No	Yes
影響修飾子 (Impact Qualification)	No	Yes
[リモート (Remote) ]	Yes	Yes
Snort ID	Yes	Yes
ソリューション	Yes	Yes
SVID	Yes	Yes
技術的説明 (Technical Description)	Yes	Yes
役職 (Title)	Yes	Yes
脆弱性の影響 (Vulnerability Impact)	Yes	Yes

### その他の情報

既知の不正利用や可用性、不正利用のシナリオ、脆弱性を軽減する方針など、脆弱性に関する追加情報を（利用可能な場合に）表示するには、矢印をクリックします。

### 使用可能なエクスプロイト（Available Exploits）

脆弱性に対して既知の不正利用があるかどうかを示します（TRUE/FALSE）。

### Bugtraq ID

Bugtraq データベースにおいて脆弱性に関連付けられている識別番号。  
(<http://www.securityfocus.com/bid/>)

### メンバー数（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

### CVE ID

MITRE の Common Vulnerabilities and Exposures（CVE）データベースで、脆弱性に関連付けられている識別番号 (<http://www.cve.mitre.org/>) 。

### 発行日（Date Published）

脆弱性が公開された日付。

### 説明

脆弱性についての簡単な説明。

### 修正（Fixes）

選択した脆弱性に対して、ダウンロード可能なパッチへのリンクを提供します。



#### ヒント

修正ファイルまたはパッチのダウンロードに対する直接リンクが表示されている場合は、リンクを右クリックして、自分のローカルコンピュータへ保存します。

### 影響修飾子（Impact Qualification）

ドロップダウンリストを使用して、脆弱性を有効または無効にします。Firepower Management Center は、影響の相関関係において、無効な脆弱性を無視します。

ユーザがここで指定する設定によって、システム全体で脆弱性がどのように処理されるか、およびユーザが値を選択するホストプロファイルに脆弱性が限定されないかが決まります。

### [リモート (Remote)]

脆弱性がリモートで不正利用されるかどうかを示します (TRUE/FALSE)。

### Snort ID

Snort ID (SID) データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワークトラフィックを検出できる場合、その脆弱性は、侵入ルールの SID に関連付けられます。

脆弱性は複数の SID に関連付けることが可能 (または SID に関連付けないことも可能) であることに注意してください。脆弱性が複数の SID に関連付けられている場合、脆弱性テーブルには、各 SID に対して 1 つのローが含まれています。

### ソリューション

脆弱性の修復に関する情報。

### SVID

脆弱性を追跡するためにシステムで使用する Cisco の脆弱性識別番号。

SVID について脆弱性の詳細にアクセスするには、表示アイコン (🔍) をクリックします。

### 技術的説明 (Technical Description)

脆弱性に関する詳細な技術的説明。

### 役職 (Title)

脆弱性のタイトル。

### 脆弱性の影響 (Vulnerability Impact)

Bugtraq データベースにおいて脆弱性に割り当てられている重大度を示します。0～10 の値で、10 が最も重大です。脆弱性の影響は、Bugtraq エントリの作成者によって決定されます。この作成者は、自身の判断および SANS Critical Vulnerability Analysis (CVA) の基準に従って脆弱性の影響を決定します。

### 関連トピック

[イベントの検索](#) (2467 ページ)

## 脆弱性の非アクティブ化

脆弱性を非アクティブ化すると、システムでこの脆弱性を使用して侵入の影響の関連付けを評価することができなくなります。ネットワーク上のホストにパッチを適用した後、またはホストが脆弱性の影響を受けないと判断した後に、脆弱性を非アクティブ化できます。システムが、この脆弱性から影響を受けている新しいホストを検出すると、この脆弱性はこのホストに対して有効であると見なされます (自動的に非アクティブ化されません)。

IPアドレスによって制約されていない脆弱性ワークフロー内である1つの脆弱性を非アクティブ化すると、ネットワーク上の検出されたすべてのホストに対してその脆弱性が非アクティブ化されます。脆弱性ワークフロー内の脆弱性を非アクティブ化できるのは、次の各ページだけです。

- デフォルトの脆弱性ワークフローの2ページ目の[ネットワーク上の脆弱性 (Vulnerabilities on the Network)]。これには、ネットワーク上のホストに適用される脆弱性のみが表示されます。
- 脆弱性ワークフロー (カスタムまたは事前定義) のページ。このワークフローは、検索を使用して IP アドレスに基づいて制約されます。

1台のホストに対して1つの脆弱性を非アクティブ化できます。この非アクティブ化は、ネットワークマップの使用、ホストのホストプロファイルの使用、または脆弱性を非アクティブ化する対象の1つ以上のホストのIPアドレスに基づいて脆弱性ワークフローを制約することによって行えます。関連付けられた複数のIPアドレスを持つホストの場合、この機能はそのホストの選択された1つのIPアドレスのみに適用されます。

マルチドメイン展開では、先祖ドメインで脆弱性を非アクティブ化すると、すべての子孫ドメインでその脆弱性が非アクティブ化されます。先祖ドメインで脆弱性をアクティブにした場合、リーフドメインでは、そのドメインにあるデバイスに対して脆弱性のアクティブ化または非アクティブ化を実行できます。

#### 関連トピック

- [個々のホストに対する脆弱性の非アクティブ化 \(2685 ページ\)](#)
- [個々の脆弱性の非アクティブ化 \(2686 ページ\)](#)
- [複数の脆弱性の非アクティブ化 \(2738 ページ\)](#)

## 脆弱性データの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

Firepower Management Center を使用して、脆弱性のテーブルを表示できます。ここでユーザは、検索する情報に応じてイベントビューを操作することができます。

脆弱性にアクセスするときに表示されるページは、使用するワークフローによって異なります。ユーザは事前定義のワークフローを使用できますが、これには脆弱性のテーブルビューが含まれています。検出されたいずれかのホストが脆弱性を示しているかどうかに関係なく、テーブルビューにはデータベース内の各脆弱性に対して1つのローが含まれています。事前定義のワークフローの2ページ目には、ネットワーク上で検出されたホストに適用されるそれぞれの脆弱性 (まだユーザが非アクティブにしていないもの) に対して1つの行が含まれています。事前定義のワークフローは脆弱性の詳細ビューで終了しますが、このビューには、制約を満たすすべての脆弱性について詳細な説明が含まれています。



**ヒント** 単一のホストまたはホストのセットに適用される脆弱性を表示する場合は、ホストの IP アドレスまたは IP アドレスの範囲を指定して、脆弱性の検索を実行します。

また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

脆弱性のテーブルは、マルチドメイン展開のドメインによって制限されません。

### 手順

**ステップ 1** 次のように、脆弱性のテーブルにアクセスします。

- 事前定義された脆弱性ワークフローを使用する場合、[分析 (Analysis)] > [脆弱性 (Vulnerabilities)] > [脆弱性 (Vulnerabilities)] を選択します。
- 脆弱性テーブルビューが含まれないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [脆弱性 (Vulnerabilities)] を選択します。

**ステップ 2** 次の選択肢があります。

- 基本的なワークフロー操作を実行します (ディスカバリおよびアイデンティティワークフローの使用 (2695 ページ) を参照)。
- 脆弱性を非アクティブにして、現在脆弱な状態にあるホストについて、侵入の影響の相関に使用しないようにします (複数の脆弱性の非アクティブ化 (2738 ページ) を参照)。
- SVID カラムの表示アイコン (🔍) をクリックして、脆弱性に関する詳細を表示します。または、脆弱性 ID を制約して脆弱性の詳細ページへドリルダウンします。
- タイトルを右クリックして [フルテキストの表示 (Show Full Text)] を選択することによって、脆弱性タイトルのフルテキストを表示します。

## 脆弱性の詳細の表示

### 手順

脆弱性の詳細は、次の方法のいずれかで表示できます。

- [分析 (Analysis)] > [脆弱性 (Vulnerabilities)] > [脆弱性 (Vulnerabilities)] を選択し、SVID の横にある表示アイコン (🔍) をクリックします。
- [分析 (Analysis)] > [脆弱性 (Vulnerabilities)] > [サードパーティの脆弱性 (Third Party Vulnerabilities)] を選択し、SVID の横にある表示アイコン (🔍) をクリックします。
- [分析 (Analysis)] > [ホスト (Hosts)] > [ネットワーク マップ (Network Map)] を選択し、[脆弱性 (Vulnerabilities)] タブをクリックします。

- 脆弱性の影響を受けるホストのプロファイルを表示し、そのプロファイルの [脆弱性 (Vulnerabilities) ] セクションを展開します。

## 複数の脆弱性の非アクティブ化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

IPアドレスで制約されていない脆弱性ワークフロー内で脆弱性を非アクティブにすると、ネットワーク上で検出されたすべてのホストに対する脆弱性が非アクティブ化されます。

マルチドメイン導入では、先祖ドメインで脆弱性を非アクティブ化すると、すべての子孫ドメインでも脆弱性が非アクティブ化されます。リーフドメインは、先祖ドメインで脆弱性がアクティブ化されている場合は、自分のデバイスの脆弱性をアクティブ化または非アクティブ化できません。

### 手順

**ステップ 1** 次のように、脆弱性のテーブルにアクセスします。

- 事前定義された脆弱性ワークフローを使用する場合、[分析 (Analysis) ] > [脆弱性 (Vulnerabilities) ] > [脆弱性 (Vulnerabilities) ] を選択します。
- 脆弱性テーブルビューが含まれないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow)) ] をクリックして [脆弱性 (Vulnerabilities) ] を選択します。

**ステップ 2** [ネットワークの脆弱性 (Vulnerabilities on the Network) ] をクリックします。

**ステップ 3** 非アクティブにする脆弱性の横にあるチェックボックスをオンにします。

**ステップ 4** ページ下部の [レビュー (Review) ] をクリックします。

### 関連トピック

[個々のホストに対する脆弱性の非アクティブ化 \(2685 ページ\)](#)

[個々の脆弱性の非アクティブ化 \(2686 ページ\)](#)

## サードパーティの脆弱性データ

Firepower システムには、それ独自の脆弱性追跡データベースが含まれています。そのデータベースは、このシステムのフィンガープリンティング機能と組み合わせて使用されて、ネットワーク上のホストに関連付けられている脆弱性が特定されます。



システムの脆弱性データは、サードパーティ製のアプリケーションからインポートしたネットワーク マップ データで補完できます。これを行うには、組織で、このデータをインポートするためのスクリプトを記述できるか、コマンドラインでファイルのインポートを作成できなければなりません。詳細については、*Firepower System Host Input API Guide*を参照してください。

インポートしたデータを影響の相関に含めるには、サードパーティの脆弱性情報を、データベース内のオペレーティングシステムおよびアプリケーションの定義にマップする必要があります。サードパーティの脆弱性情報は、クライアントの定義にマップすることはできません。

## サードパーティの脆弱性データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

ホスト入力機能を使用してサードパーティの脆弱性データをインポートした後で、**Firepower Management Center**を使用してサードパーティの脆弱性のテーブルを表示することができます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

サードパーティの脆弱性にアクセスするときに表示されるページは、使用するワークフローによって異なります。2つの事前定義されたワークフローがあります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

### 手順

**ステップ 1** 次のようにして、サードパーティの脆弱性データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析 (Analysis)] > [脆弱性 (Vulnerabilities)] > [サードパーティの脆弱性 (Third Party Vulnerabilities)]** を選択します。
- サードパーティの脆弱性のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、**[(ワークフローの切り替え) ((switch workflow))]** をクリックして**[送信元別の脆弱性 (Vulnerabilities by Source)]** または **[IP アドレス別の脆弱性 (Vulnerabilities by IP Address)]** を選択します。

**ステップ 2** 次の選択肢があります。

- [(ワークフローの切り替え) ((switch workflow))]** をクリックしてカスタムワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します (**ディスカバリおよびアイデンティティワークフローの使用 (2695 ページ)** を参照)。
- テーブルのカラムの内容について詳しく調べます (**サードパーティの脆弱性データのフィールド (2740 ページ)** を参照)。

- SVID カラムの表示アイコン (🔍) をクリックして、サードパーティの脆弱性に関する詳細を表示します。または、脆弱性 ID を制約して脆弱性の詳細ページへドリルダウンします。

## サードパーティの脆弱性データのフィールド

サードパーティの脆弱性テーブルで表示および検索できるフィールドの詳細は以下のとおりです。

### 脆弱性ソース (Vulnerability Source)

サードパーティの脆弱性のソース (QualysGuard、NeXpose など)。

### 脆弱性 ID (Vulnerability ID)

ソースの脆弱性に関連付けられている ID 番号。

### [IPアドレス (IP Address)]

脆弱性の影響を受けるホストに関連付けられている IP アドレス。

### [ポート (Port)]

ポート番号 (脆弱性が、特定のポート上で実行されているサーバに関連付けられている場合)。

### Bugtraq ID

Bugtraq データベースにおいて脆弱性に関連付けられている識別番号。  
(<http://www.securityfocus.com/bid/>)

### CVE ID

MITRE の Common Vulnerabilities and Exposures (CVE) データベースで、脆弱性に関連付けられている識別番号 (<http://www.cve.mitre.org/>)。

### SVID

脆弱性を追跡するためにシステムで使用する従来の脆弱性識別番号。

SVID について脆弱性の詳細にアクセスするには、表示アイコン (🔍) をクリックします。

### Snort ID

Snort ID (SID) データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トラフィックを検出できる場合、その脆弱性は、侵入ルールの SID に関連付けられます。

脆弱性は複数のSIDに関連付けることが可能（またはSIDに関連付けられないことも可能）であることに注意してください。脆弱性が複数のSIDに関連付けられている場合、脆弱性テーブルには、各SIDに対して1つのローが含まれています。

#### 役職 (Title)

脆弱性のタイトル。

#### 説明

脆弱性についての簡単な説明。

#### ドメイン

この脆弱性を持つホストのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合にのみ表示されます。

#### メンバー数 (Count)

各行に表示される情報と一致するイベントの数。[カウント (Count)] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

#### 関連トピック

[イベントの検索](#) (2467 ページ)

## ユーザおよびユーザアクティビティ データ

ユーザおよびユーザアクティビティ データは、個々のユーザ関連のワークフローに表示されます。

- ユーザ：このワークフローは、ネットワークで認識されるすべてのユーザを表示します。この表では1ユーザが1つの行を占めます。詳細については、[ユーザデータ \(User Data\)](#) (2746 ページ) を参照してください。
- ユーザアクティビティ：このワークフローは、ネットワークで認識されるすべてのユーザアクティビティを表示します。この表では、複数のユーザアクティビティ インスタンスを持つ1ユーザが複数の行を占めます。詳細については、[ユーザアクティビティ データ](#) (2749 ページ) を参照してください。

これらのワークフローの入力元であるアイデンティティ ソースの詳細については、[ユーザアイデンティティ ソースについて](#) (2121 ページ) を参照してください。

### ユーザ関連フィールド

ユーザ関連データは、ユーザおよびユーザアクティビティのテーブルに表示されます。

表 306: ユーザおよびユーザ アクティビティのフィールドの説明

フィールド	説明	[ユーザテーブル (Users Table) ]	[ユーザアクティビティ (User Activity) ] テーブル
認証タイプ (Authentication Type)	認証のタイプ: [認証なし (No Authentication) ]、[パッシブ認証 (Passive Authentication) ]、[アクティブ認証 (Active Authentication) ]、[ゲスト認証 (Guest Authentication) ]、または [失敗した認証 (Failed Authentication) ]。	なし	○
メンバー数 (Count)	(注) [カウント (Count) ] フィールドは、制約を適用した結果、同じ行が複数作成された場合にのみ表示されます。  特定の行に表示される情報と一致するユーザまたはイベントの数。	○	○
現在の IP (Current IP)	ユーザがログインしたホストに関連付けられている IP アドレス。ユーザがログインした後で、権限を持っている他のユーザが同じ IP アドレスでホストにログインすると、このフィールドは空白になります。ただし、あるユーザが権限を持っており、新しいユーザが権限を持っていない場合は除きます。(システムは、IP アドレスと、最後にホストにログインした権限のあるユーザを関連付けます。)	[はい (Yes) ]	[いいえ (No) ]
部署名 (Department)	ユーザの部署 (レルムが取得)。サーバ上のユーザに明示的に関連付けられている部門がない場合、この部門は、サーバが割り当てられているいずれかのデフォルト グループとして示されます。たとえば、Active Directory では、これは Users (ad) となります。以下の場合、このフィールドは空白になります。  <ul style="list-style-type: none"> <li>レルムを設定していない。</li> <li>Firepower Management Center が、Management Center データベースのユーザと LDAP レコードを関連させていない (AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など)。</li> </ul>	[はい (Yes) ]	[いいえ (No) ]
説明	ユーザまたはユーザ アクティビティについての詳細情報 (利用可能な場合)。	なし	○
Device	トラフィックベースの検出によって検出されたユーザ アクティビティの場合、ユーザを検出したデバイスの名前。他のタイプのユーザ アクティビティの場合は、管理している側の Firepower Management Center になります。	なし	○

フィールド	説明	[ユーザテーブル (Users Table) ]	[ユーザアクティビティ (User Activity) ] テーブル
ドメイン	<p>[ユーザ (Users) ] テーブルでは、ユーザのレルムに関連付けられたドメイン。</p> <p>[ユーザアクティビティ (User Activity) ] テーブルでは、ユーザアクティビティが検出されたドメイン。</p> <p>このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。</p>	○	○
電子メール (E-Mail)	<p>ユーザのメールアドレス。以下の場合、このフィールドは空白になります。</p> <ul style="list-style-type: none"> <li>• AIM ログインによってユーザがデータベースに追加された。</li> <li>• LDAP ログインによってユーザがデータベースに追加されており、LDAP サーバ上にユーザと関連付けられている電子メールアドレスが存在しない。</li> </ul>	[はい (Yes) ]	[いいえ (No) ]
エンドポイントロケーション (Endpoint Location)	ISE で指定された、ユーザの認証に ISE を使用したネットワーク デバイスの IP アドレス。ISE を設定していない場合、このフィールドは空白です。	なし	○
エンドポイントプロファイル (Endpoint Profile)	Cisco ISE によって識別されるユーザのエンドポイントデバイスタイプ。ISE を設定していない場合、このフィールドは空白です。	なし	○
イベント	ユーザアクティビティのタイプ。	なし	○
名	<p>ユーザの名 (レルムが取得)。以下の場合、このフィールドは空白になります。</p> <ul style="list-style-type: none"> <li>• レルムを設定していない。</li> <li>• Firepower Management Center が、Management Center データベースのユーザと LDAP レコードを関連させていない (AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など)。</li> <li>• サーバに、対象のユーザと関連付けられている名がない。</li> </ul>	[はい (Yes) ]	[いいえ (No) ]

フィールド	説明	[ユーザテーブル (Users Table) ]	[ユーザアクティビティ (User Activity) ] テーブル
[IPアドレス (IP Address) ]	<p>「ユーザログイン (User Login) 」アクティビティの場合はログインに関連する IP アドレスです。ユーザのホストの IP アドレス (LDAP、POP3、IMAP、FTP、HTTP、MDNS、および AIM ログインの場合)、サーバの IP アドレス (SMTP および Oracle ログインの場合)、またはセッションの開始者の IP アドレス (SIP ログインの場合) のいずれかになります。</p> <p>関連付けられている IP アドレスは、そのユーザが IP アドレスの現行のユーザであることを意味するわけではないので注意してください。権限を持たないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されます。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることがあります。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。</p> <p>他のタイプのユーザ アクティビティの場合、このフィールドは空白です。</p>	なし	○
姓	<p>ユーザの姓 (レルムが取得)。以下の場合、このフィールドは空白になります。</p> <ul style="list-style-type: none"> <li>• レルムを設定していない。</li> <li>• Firepower Management Center が、Management Center データベースのユーザと LDAP レコードを相関させていない (AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など)。</li> <li>• サーバに、対象のユーザと関連付けられている姓がない。</li> </ul>	[はい (Yes) ]	[いいえ (No) ]

フィールド	説明	[ユーザテーブル (Users Table) ]	[ユーザアクティビティ (User Activity) ] テーブル
電話	<p>ユーザの電話番号 (レルムが取得)。以下の場合、このフィールドは空白になります。</p> <ul style="list-style-type: none"> <li>レルムを設定していない。</li> <li>Firepower Management Center が、Management Center データベースのユーザと LDAP レコードを関連させていない (AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など)。</li> <li>サーバに、対象のユーザと関連付けられている電話番号が存在しない。</li> </ul>	[はい (Yes) ]	[いいえ (No) ]
レルム	ユーザに関連付けられているアイデンティティ レルム。	○	○
セキュリティグループタグ (Security Group Tag)	パケットが信頼できる TrustSec ネットワークへ送信されたときに、Cisco TrustSec によって適用される [セキュリティグループタグ (Security Group Tag) ] (SGT) 属性。ISE を設定していない場合、このフィールドは空白です。	なし	○
時刻 (Time)	システムがユーザ アクティビティを検出した時間。	なし	○
タイプ (Type)	ユーザの検出に使用されるプロトコル。これは、ldap、pop3、imap、oracle、sip、http、ftp、mdns、aim のいずれかです。ユーザは SMTP ログインに基づいてデータベースに追加されることはないため、このフィールドには smtp は表示されません。	○	○
ユーザ (User)	<p>このフィールドには少なくとも、ユーザのレルムとユーザ名が表示されます。たとえば、Lobby\jsmith と表示された場合は、Lobby がレルム、jsmith がユーザ名です。</p> <p>レルムが LDAP サーバから追加のユーザ データをダウンロードし、システムがそれをユーザに関連付けた場合は、このフィールドにユーザの名、姓、タイプも表示されません。たとえば、John Smith (Lobby\jsmith, LDAP) と表示された場合は、John Smith がユーザの名前、LDAP がそのタイプです。</p> <p>(注) トラフィックベースの検出では失敗した AIM ログインが記録される可能性があるため (たとえば、ユーザが正しくないユーザ名を入力した場合など)、Firepower Management Center は無効な AIM ユーザを保存する可能性があります。</p>	[はい (Yes) ]	[いいえ (No) ]

フィールド	説明	[ユーザテーブル (Users Table) ]	[ユーザアクティビティ (User Activity) ] テーブル
[ユーザ名 (Username) ]	ユーザに関連付けられているユーザ名。	○	○

## ユーザデータ (User Data)

アイデンティティ ソースが、データベースに存在しないユーザのユーザ ログインを報告した場合、そのログインタイプが特に制限されていない限り、そのユーザはデータベースに追加されます。

次のいずれかが発生すると、システムはユーザ データベースを更新します。

- Firepower Management Center のユーザが、[ユーザ (Users) ] テーブルから権限のないユーザを手動で削除する。
- アイデンティティ ソースが、そのユーザによるログオフを報告する。
- レルムがレルムの [ユーザセッションのタイムアウト：認証されたユーザ (User Session Timeout: Authenticated Users) ] 設定、[ユーザセッションのタイムアウト：認証に失敗したユーザ (User Session Timeout: Failed Authentication Users) ] 設定、または [ユーザセッションのタイムアウト：ゲストユーザ (User Session Timeout: Guest Users) ] 設定で指定されているユーザセッションを終了した。



(注) ISEが設定されている場合は、ユーザテーブルにホストデータが表示されることがあります。ISEによるホスト検出は完全にはサポートされていないため、ISEが報告したホストデータを使用してユーザ制御を実行することはできません。

システムによって検出されたユーザログインのタイプに応じて、新しいユーザのどの情報が保存されるかが決まります。

ID ソース	ログインタイプ	格納されるユーザデータ
ISE	Active Directory LDAP RADIUS RSA	<ul style="list-style-type: none"> <li>• ユーザ名</li> <li>• 現行の IP アドレス</li> <li>• セキュリティグループ タグ (SGT)</li> <li>• エンドポイントのプロファイル/デバイス タイプ</li> <li>• エンドポイントの場所/場所 IP</li> <li>• タイプ (LDAP)</li> </ul>



ID ソース	ログインタイプ	格納されるユーザデータ
ユーザ エージェント	Active Directory	<ul style="list-style-type: none"> <li>ユーザ名</li> <li>現行の IP アドレス</li> <li>タイプ (LDAP)</li> </ul>
TS エージェント	Active Directory	<ul style="list-style-type: none"> <li>ユーザ名</li> <li>現行の IP アドレス</li> <li>開始ポート</li> <li>終了ポート</li> <li>タイプ (LDAP)</li> </ul>
キャプティブポータル	Active Directory LDAP	<ul style="list-style-type: none"> <li>ユーザ名</li> <li>現行の IP アドレス</li> <li>タイプ (LDAP)</li> </ul>
トラフィックベースの 検出	LDAP AIM Oracle SIP HTTP FTP MDNS	<ul style="list-style-type: none"> <li>ユーザ名</li> <li>現行の IP アドレス</li> <li>タイプ (AD)</li> </ul>
	POP3 IMAP	<ul style="list-style-type: none"> <li>ユーザ名</li> <li>現行の IP アドレス</li> <li>電子メール アドレス</li> <li>タイプ (pop3 または imap)</li> </ul>

ユーザを自動的にダウンロードするようにレلمを設定すると、Firepower Management Center は指定した間隔に基づいてサーバに対するクエリを実行します。システムが新しいユーザのログインを検出してから、Firepower Management Center データベースがユーザのメタデータを更新するまでに、5~10分かかることがあります。Firepower Management Centerは、ユーザごとに次の情報とメタデータを取得します。

- ユーザ名

- 姓と名
- 電子メール アドレス
- 部署
- 電話番号
- 現行の IP アドレス
- セキュリティ グループ タグ (SGT) (使用可能な場合)
- エンドポイントのプロファイル (使用可能な場合)
- エンドポイントの場所 (使用可能な場合)
- 開始ポート (使用可能な場合)
- 終了ポート (使用可能な場合)

Firepower Management Center がデータベースに格納できるユーザの数は、Firepower Management Center のモデルによって異なります。ホストに対して権限を持たないユーザがログインしていることが検出された場合、そのログインはユーザおよびホストの履歴に記録されます。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、ホストに対して権限を持つユーザのログインが検出された後は、権限を持つ別のユーザがログインした場合にのみ、現行ユーザが変わります。

AIM、Oracle、および SIP のログインがトラフィックベースで検出された場合は、システムが LDAP サーバから取得したどのユーザメタデータにも関連付けられないため、これらのログインにより重複したユーザレコードが作成されることに注意してください。これらのプロトコルから重複したユーザレコードを取得することに起因するユーザカウントの過度な使用を回避するには、これらのプロトコルを無視するようにトラフィックベースの検出を設定します。

データベースからユーザを検索、表示、削除することができます。また、データベースからすべてのユーザを消去することもできます。

一般的なユーザ関連のイベントトラブルシューティングについては、[レムとユーザのダウンロードのトラブルシューティング \(2182 ページ\)](#) を参照してください。

## ユーザデータの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

ユーザのテーブルを表示して、検索する情報に応じてイベントビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができますが、これには、検出されたすべてのユーザが記載されているユーザのテーブル ビューが含まれています。このワークフローは、ユーザの詳細ページで終了します。ユーザの詳細ページは、制約を満たす各ユーザについての情報を提供します。

## 手順

**ステップ 1** 次のように、ユーザ データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析 (Analysis)] > [ユーザ (Users)] > [ユーザ (Users)] を選択します。
- ユーザのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [ユーザ (Users)] を選択します。

**ステップ 2** 次の選択肢があります。

- [(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタムワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します (ディスカバリおよびアイデンティティワークフローの使用 (2695 ページ) を参照)。
- テーブルのカラムの内容について詳しく調べます (ユーザ関連フィールド (2741 ページ) を参照)。

## ユーザ アクティビティ データ

Firepower システムでは、ネットワーク上のユーザ アクティビティの詳細を伝達するイベントを生成します。システムがユーザ アクティビティを検出すると、そのユーザ アクティビティ データはデータベースに記録されます。ユーザ アクティビティは、表示、検索、および削除することも、すべてのユーザ アクティビティをデータベースから消去することもできます。

あるユーザがネットワーク上で初めて確認されると、システムはそのユーザ アクティビティ イベントをログに記録します。そのユーザがその後に確認された場合、新しいユーザ アクティビティ イベントはログに記録されません。ただし、そのユーザの IP アドレスが変わった場合、システムは新しいユーザ アクティビティ イベントをログに記録します。

Firepower システムでは、ユーザ アクティビティと他のタイプのイベントとの関連付けも行います。たとえば、侵入イベントは、そのイベントの発生時に送信元ホストと宛先ホストにログインしていたユーザを通知することができます。この関連付けにより、攻撃の対象になったホストにログインしていたユーザ、または内部攻撃やポートスキャンを開始したユーザがわかります。

ユーザ アクティビティは、関連ルールで使用することもできます。関連ルールは、ユーザ アクティビティのタイプだけでなく、指定した他の条件に基づいて作成することができます。相

関ルールが関連ポリシーで使用される場合、ネットワークトラフィックが条件を満たしたときは、関連ルールが修復およびアラートの応答を起動します。



- (注) ISE を設定していた場合、ホスト データがユーザ テーブルに表示されることがあります。ISE によるホスト検出は完全にはサポートされていないため、ISE が報告したホストデータを使用してユーザ制御を実行することはできません。

次に、4 つのタイプのユーザ アクティビティ データについて説明します。

#### 新しいユーザのアイデンティティ (New User Identity)

このタイプのイベントは、システムがデータベースに存在しない不明なユーザによるログインを検出したときに生成されます。

あるユーザがネットワーク上で初めて確認されると、システムはそのユーザ アクティビティ イベントをログに記録します。そのユーザがその後に確認された場合、新しいユーザ アクティビティ イベントはログに記録されません。ただし、そのユーザの IP アドレスが変わった場合、システムは新しいユーザ アクティビティ イベントをログに記録します。

#### ユーザ ログイン (User Login)

このタイプのイベントは、次のことが発生した後に生成されます。

- ユーザ エージェント、ISE、または TS エージェントが正常なユーザ ログインを報告した。
- キャプティブ ポータルのユーザ 認証の実行が成功または失敗した。
- トラフィック ベースの検出がユーザ ログインの成功または失敗を検出した。



- (注) トラフィック ベースの検出で検出された SMTP ログインは、一致する電子メール アドレスを持つユーザがデータベースにすでに存在する場合を除いて記録されません。

権限のないユーザがあるホストにログインすると、そのログインはユーザとホストの履歴に記録されます。権限のあるユーザがそのホストに関連付けられていない場合、権限のないユーザがそのホストの現行 (現在の) ユーザとなることが可能です。ただし、権限のあるユーザがそのホストにログインした後は、別の権限のあるユーザによるログインだけが現行ユーザを変更します。

キャプティブ ポータルまたはトラフィック ベースの検出を使用する場合、失敗したユーザ ログインと失敗したユーザ 認証データについて、次の点に注意してください。

- トラフィック ベースの検出 (LDAP、IMAP、FTP、および POP3 トラフィック) から報告された失敗したログインは、ユーザ アクティビティ のテーブルビューに表示されますが、ユーザのテーブルビューには表示されません。既知のユーザがログインに失敗した場合、システムではそのユーザをそのユーザ名で識別します。不明なユーザがログインに失敗し

た場合、システムではそのユーザ名として [失敗した認証 (Failed Authentication)] を使用します。

- キャプティブ ポータルから報告された失敗した認証は、ユーザアクティビティのテーブルビューとユーザのテーブルビューの両方に表示されます。既知のユーザが認証に失敗した場合、システムではそのユーザをそのユーザ名で識別します。不明なユーザが認証に失敗した場合、システムではそのユーザをそのユーザが入力したユーザ名で識別します。

### ユーザのアイデンティティの削除 (Delete User Identity)

このタイプのイベントは、データベースからユーザを手動で削除したときに生成されます。

### ドロップ (廃棄) されたユーザのアイデンティティ : ユーザ制限に到達 (User Identity Dropped: User Limit Reached)

このタイプのイベントは、システムがデータベースに存在しないユーザを検出したものの、Firepower Management Center のモデルで決定されているデータベースの最大ユーザ数に達したためにユーザを追加できなかったときに生成されます。

ユーザ制限に達すると、ほとんどの場合、データベースへの新しいユーザの追加が停止されます。新しいユーザを追加するには、古いユーザまたは非アクティブなユーザをデータベースから手動で削除するか、データベースからすべてのユーザを消去する必要があります。

ただし、システムでは権限のあるユーザが優先されます。すでに制限に達しており、これまでに検出されていない権限のあるユーザのログインが検出された場合、システムは長期間非アクティブな状態が続いている権限のないユーザを削除して、権限のある新しいユーザに置き換えます。

一般的なユーザ関連のイベントトラブルシューティングについては、[レルムとユーザのダウンロードのトラブルシューティング \(2182 ページ\)](#) を参照してください。

### 関連トピック

[ユーザアクティビティデータベース \(2033 ページ\)](#)

## ユーザアクティビティデータの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザアクティビティのテーブルを表示して、検索する情報に応じてイベントビューを操作することができます。ユーザアクティビティにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができます。このワークフローにはユーザアクティビティのテーブルビューが含まれており、制約を満た

すすべてのユーザの詳細が含まれている、ユーザの詳細ページで終了します。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

## 手順

**ステップ 1** 次のように、ユーザ アクティビティ データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析 (Analysis)] > [ユーザ (Users)] > [ユーザ アクティビティ (User Activity)] を選択します。
- ユーザ アクティビティのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [ユーザ アクティビティ (User Activity)] を選択します。

**ヒント** イベントが表示されない場合は、時間範囲の調整が必要な可能性があります ([時間枠の変更 \(2455 ページ\)](#) を参照)。

**ステップ 2** 次の選択肢があります。

- [(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタムワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(2695 ページ\)](#) を参照)。
- テーブルのカラムの内容について詳しく調べます ([ユーザ関連フィールド \(2741 ページ\)](#) を参照)。

## ユーザ プロファイルとホスト履歴

特定のユーザの詳細については、[ユーザ (User)] ポップアップウィンドウを表示して確認することができます。表示されるページ (このマニュアルでは「ユーザプロファイル」と呼んでいます) には、Web インターフェイスで「ユーザのアイデンティティ (User Identity)」というタイトルが付いています。

このウィンドウは、次のビューから表示できます。

- ユーザ データを他の種類のイベントに関連付けるすべてのイベント ビュー
- ユーザのテーブル ビュー

ユーザ情報は、ユーザ ワークフローの最終ページにも表示されます。

表示されるユーザ データは、ユーザのテーブル ビューで表示されるものと同じです。

### [侵害の兆候 (Indications of Compromise)] セクション

このセクションについては、次のセクションを参照してください。

- [侵害の兆候 \(2167 ページ\)](#)

- [侵害の兆候データ フィールド \(2720 ページ\)](#)
- [単一ホストにおける侵害の兆候のルール状態の編集 \(2721 ページ\)](#)
- [侵害の兆候タグの解決 \(2722 ページ\)](#)
- [侵害の兆候のタグのソース イベントの表示 \(2721 ページ\)](#)

### [ホストの履歴 (Host History) ] セクション

ホストの履歴には、過去 24 時間のユーザー アクティビティがグラフィック表示されます。ユーザーがログインおよびログオフしたホストの IP アドレスのリストには、ログインとログアウトの概算時間が棒グラフで示されます。一般的なユーザーは、1 日の間に複数のホストに対してログオンおよびログオフする可能性があります。たとえば、メールサーバに対する定期的な自動ログインは複数回の短時間のセッションとして示されますが、(勤務時間中などの) 長時間のログインは、長時間のセッションとして示されます。

トラフィック ベースの検出またはキャプティブ ポータルを使用して失敗したログインをキャプチャした場合、ホストの履歴にはユーザーがログインに失敗したホストも含まれます。

ホストの履歴を生成するために使用されるデータは、ユーザーの履歴データベースに格納されません。このデータベースには、デフォルトで 1000 万のユーザー ログイン イベントが格納されません。ホストの履歴に特定のユーザーに関するデータが表示されない場合、そのユーザーが非アクティブであるか、またはデータベースの制限を増やさなければならないことがあります。

#### 関連トピック


[ユーザーデータのフィールド](#)

### ユーザーの詳細およびホスト履歴の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

#### 手順

次の 2 つの対処法があります。

- ユーザーをリストする任意のイベント ビューで、ユーザー ID の横に表示されるユーザー アイコン (  ) をクリックします。
- いずれかのユーザー ワークフローで、[ユーザー (Users) ] の最終ページをクリックします。







## 第 111 章

# 関連イベントとコンプライアンス イベント

次のトピックでは、関連イベントとコンプライアンスイベントを表示する方法について説明します。

- [関連イベントの表示 \(2755 ページ\)](#)
- [コンプライアンス ホワイトリスト ワークフローの使用 \(2760 ページ\)](#)
- [修復ステータス イベント \(2766 ページ\)](#)

## 関連イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst

アクティブな関連ポリシーに含まれる関連ルールがトリガーとして使用されると、システムが関連イベントを生成してデータベースにそれを記録します。



(注) アクティブな関連ポリシーに含まれるコンプライアンスホワイトリストがトリガーとして使用されると、システムがホワイトリスト イベントを生成します。

関連イベントのテーブルを表示し、検索対象の情報に応じてイベントビューを操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

関連イベントにアクセスしたときに表示されるページは、使用するワークフローによって異なります。関連イベントのテーブルビューが含まれる定義済みワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

## 手順


**ステップ1** [分析 (Analysis)] > [関連 (Correlation)] > [関連イベント (Correlation Events)] を選択します。

オプションで、カスタムワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(ワークフローの切り替え) ((switch workflow))] をクリックします。

**ヒント** 関連イベントのテーブルビューが含まれないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックし、[関連イベント (Correlation Events)] を選択します。

**ステップ2** オプションで、[時間枠の変更 \(2455 ページ\)](#) の説明に従って、時間範囲を調整します。

**ステップ3** 次のいずれかの操作を実行します。

- 表示されるカラムの詳細については、[関連イベントのフィールド \(2757 ページ\)](#) を参照してください。
- IP アドレスのホスト プロファイルを表示するには、IP アドレスの横に表示されるホスト プロファイルアイコンをクリックします。
- ユーザ ID 情報を表示するには、ユーザ ID の横に表示されるユーザアイコン () をクリックします。
- 現在のワークフロー ページ内でイベントをソートしたり制限したり、または移動するには、[ワークフローの使用 \(2429 ページ\)](#) を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページリンクをクリックします。
- 特定の値に制限して、ワークフロー内の次のページにドリルダウンするには、[ドリルダウン ページの使用 \(2439 ページ\)](#) を参照してください。
- 一部またはすべての関連イベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除 (Delete)] をクリックするか、[すべて削除 (Delete All)] をクリックして現在の制約されているビューにあるすべてのイベントを削除することを確認します。
- 他のイベントビューに移動して関連イベントを表示するには、[ワークフロー間のナビゲーション \(2463 ページ\)](#) を参照してください。

## 関連トピック

[データベース イベント数の制限 \(930 ページ\)](#)

[ワークフローのページ \(2434 ページ\)](#)

## 関連イベントのフィールド

関連ルールがトリガーとして使用されると、システムは関連イベントを生成します。次の表では、表示および検索可能な関連イベント テーブルのフィールドについて説明します。

表 307: 関連イベントのフィールド

フィールド	説明
説明	<p>関連イベントについての説明。説明に示される情報は、ルールがどのようにトリガーとして使用されたかによって異なります。</p> <p>たとえば、オペレーティング システム情報の更新イベントによってルールがトリガーとして使用された場合、新しいオペレーティング システムの名前と信頼度レベルが表示されます。</p>
Device	ポリシー違反をトリガーとして使用したイベントを生成したデバイスの名前。
ドメイン	ポリシー違反をトリガーとして使用したモニタ対象トラフィックのデバイスのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
影響 (Impact)	<p>侵入データ、ディスカバリ データ、および脆弱性情報の間の関連に基づいて関連イベントに割り当てられた影響レベル。</p> <p>このフィールドを検索する場合、大文字と小文字を区別しない有効な値は、Impact 0、Impact Level 0、Impact 1、Impact Level 1、Impact 2、Impact Level 2、Impact 3、Impact Level 3、Impact 4、および Impact Level 4 です。影響アイコンの色または部分文字列は使用しないでください (たとえば、blue、level 1、または 0 を使用しないでください)。</p>
入力インターフェイス (Ingress Interface) または出力インターフェイス (Egress Interface)	ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力インターフェイス。
入力セキュリティゾーン (Ingress Security Zone) または出力セキュリティゾーン (Egress Security Zone)	ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力セキュリティゾーン。

フィールド	説明
インライン結果 (Inline Result)	<p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• 黒の下矢印：侵入ルールをトリガーとして使用したパケットがシステムによってドロップされたことを示します</li> <li>• グレーの下矢印：侵入ポリシー オプション [インライン時にドロップ (Drop when Inline) ] を有効にした場合、インライン型、スイッチ型、またはルーティング型展開でパケットがシステムによってドロップされたと想定されることを示します</li> <li>• 空白：トリガーとして使用された侵入ルールが [ドロップしてイベントを生成する (Drop and Generate Events) ] に設定されていないことを示します</li> </ul> <p>侵入イベントによってトリガーとして使用されたポリシー違反を検索するためにこのフィールドを使用する場合は、次のいずれかを入力します。</p> <ul style="list-style-type: none"> <li>• dropped は、インライン型、スイッチ型、またはルーティング型展開でパケットがドロップされたかどうかを示します。</li> <li>• would have dropped は仮定を表します。インライン型、スイッチ型、またはルーティング型展開でパケットをドロップするよう侵入ポリシーが設定されていると仮定した場合、パケットがドロップされるかどうかを示します。</li> </ul> <p>侵入ポリシーのドロップ動作やルール状態とは無関係に、パッシブ展開 (インラインセットがタップ モードである場合を含む) ではシステムがパケットをドロップしないことに注意してください。</p>
ポリシー	違反が発生したポリシーの名前。
[プライオリティ (Priority) ]	<p>関連イベントのプライオリティ。これは、トリガーとして使用されたルールのプライオリティまたは違反が発生した関連ポリシーのプライオリティによって決まります。このフィールドを検索するとき、プライオリティなしの場合は none を入力します。</p>
ルール (Rule)	ポリシー違反をトリガーとして使用したルールの名前。

フィールド	説明
セキュリティインテリジェンスカテゴリ (Security Intelligence Category)	<p>ブラックリスト化されたオブジェクトの名前。これは、ポリシー違反をトリガーとして使用したイベントでブラックリスト化された IP アドレスを示す (またはその IP アドレスを含む) オブジェクトです。</p> <p>このフィールドを検索する場合は、ポリシー違反をトリガーとして使用した関連イベントに関連付けられたセキュリティインテリジェンスのカテゴリを指定します。セキュリティインテリジェンスのカテゴリとして、セキュリティインテリジェンス オブジェクト、グローバルブラックリスト、カスタムセキュリティインテリジェンスリストまたはフィード、あるいはインテリジェンス フィードに含まれるいずれかのカテゴリを指定できます。</p>
送信元の大陸 (Source Continent) または宛先の大陸 (Destination Continent)	<p>ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホスト IP アドレスに関連付けられた大陸。</p>
送信元の国 (Source Country) または宛先の国 (Destination Country)	<p>ポリシー違反をトリガーとして使用したイベントの送信元または宛先 IP アドレスに関連付けられた国。</p>
送信元ホストの重大度 (Source Host Criticality) または宛先ホストの重大度 (Destination Host Criticality)	<p>関連イベントに関連する送信元または宛先ホストにユーザが割り当てたホスト重要度。None、Low、Medium、または High のいずれかです。</p> <p>ディスカバリ イベント、ホスト入力イベント、または接続イベントに基づくルールによって生成された関連イベントにのみ、送信元ホスト重要度が含まれることに注意してください。</p>
送信元 IP (Source IP) または宛先 IP (Destination IP)	<p>ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストの IP アドレス。</p>
送信元ポート/ICMP タイプ (Source Port/ICMP Type) または宛先ポート/ICMP コード (Destination Port/ICMP Code)	<p>ポリシー違反をトリガーとして使用したイベントに関連付けられた、送信元トラフィックの送信元ポート/ICMP タイプまたは宛先トラフィックの宛先ポート/ICMP コード。</p>
送信元ユーザ (Source User) または宛先ユーザ (Destination User)	<p>ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストにログインしたユーザの名前。</p>
時刻 (Time)	<p>関連イベントが生成された日時。このフィールドは検索できません。</p>
メンバー数 (Count)	<p>各行に表示される情報と一致するイベントの数。[カウント (Count)] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。</p>

## 関連トピック

[イベントの検索](#) (2467 ページ)

# コンプライアンス ホワイト リスト ワークフローの使用

スマート ライセ ンス	従来のライセンス	サポートされるデ バイス	サポートされるド メイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Discovery Admin

Firepower Management Center は、ネットワークで生成されるホワイトリストイベントおよびホワイトリスト違反の分析で使用できるワークフローセットを提供します。ワークフローはネットワークマップやダッシュボードとともに、ネットワーク資産のコンプライアンスに関する主要な情報源になります。

システムは、ホワイトリスト イベントとホワイト リスト違反のために事前定義されたワークフローを提供します。ユーザはカスタムワークフローを作成することもできます。コンプライアンス ホワイト リスト ワークフローを使用すると、多くの一般的なアクションを実行できます。

## 手順

**ステップ 1** [分析 (Analysis)] > [相関 (Correlation)] メニューを使用してホワイト リスト ワークフローにアクセスします。

**ステップ 2** 次の選択肢があります。

- ワークフローの切り替え：カスタム ワークフローなどの別のワークフローを使用するには、[(ワークフローの切り替え) ((switch workflow))] をクリックします。
- 時間範囲：時間範囲を調整（イベントが表示されない場合に役立ちます）する方法については、[時間枠の変更](#) (2455 ページ) を参照してください。
- ホスト プロファイル：IP アドレスのホスト プロファイルを表示するには、ホスト プロファイルのアイコン (🖥️) をクリックします。アクティブな侵害の兆候 (IOC) タグのあるホストの場合は、IP アドレスの横に表示される侵害されたホストのアイコン (🚨) をクリックします。
- ユーザ プロファイル (イベントのみ)：ユーザ ID 情報を表示するには、ユーザ ID の横に表示されるユーザ アイコン (👤) をクリックします。

- 制約：表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン（✕）をクリックします。表示されるポップアップウィンドウで、[適用（Apply）] をクリックします。

**ヒント** 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェックボックスをオンまたはオフにします。無効になったカラムをビューに再び追加するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- ドリルダウン： [ドリルダウン ページの使用（2439 ページ）](#) を参照してください。
- ソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- このページに移動する： [ワークフローページのトラバーサルツール（2436 ページ）](#) を参照してください。
- ページ間で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページリンクをクリックします。
- イベントビュー間で移動する：関連するイベントを表示するためその他のイベントビューに移動するには、[ジャンプ（Jump to）] をクリックし、ドロップダウンリストからイベントビューを選択します。
- イベントの削除（イベントのみ）：現在の制約されているビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。

#### 関連トピック

[ワークフローのページ（2434 ページ）](#)

[イベントビュー設定の設定（37 ページ）](#)

## ホワイトリストイベントの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Discovery Admin

最初の評価が行われた後、監視対象ホストがアクティブなホワイトリストに準拠しなくなると、システムはホワイトリストイベントを生成します。ホワイトリストイベントは、関連イベントの特殊な形態で、Management Center 関連イベント データベースに記録されます。

Firepower Management Center を使用して、コンプライアンス ホワイトリスト イベントのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベントビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ホワイトリスト イベントにアクセスしたときに表示されるページは使用しているワークフローによって異なります。イベントのテーブルビューで終わる事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

## 手順

**ステップ 1** [分析 (Analysis)] > [相関 (Correlation)] > [ホワイトリスト イベント (White List Events)] を選択します。

**ステップ 2** 次の選択肢があります。

- 基本的なワークフロー操作を実行するには、[コンプライアンス ホワイトリスト ワークフローの使用 \(2760 ページ\)](#) を参照してください。
- テーブルのカラムの内容について詳しく調べるには、[ホワイトリスト イベントのフィールド \(2762 ページ\)](#) を参照してください。

## ホワイトリスト イベントのフィールド

ワークフローを使用して表示および検索できるホワイトリスト イベントには、次のフィールドがあります。

### Device

ホワイトリスト違反を検出した管理対象デバイスの名前。

### 説明

ホワイトリスト違反の説明。次に例を示します。

```
Client "AOL Instant Messenger" is not allowed.
```

アプリケーションプロトコルに関する違反には、アプリケーションプロトコルの名前とバージョンだけでなく、使用されているポートとプロトコル (TCP または UDP) も示されます。禁止を特定のオペレーティング システムに限定する場合は、説明にオペレーティング システム名が含まれます。次に例を示します。

```
Server "ssh / 22 TCP (OpenSSH 3.6.1p2)" is not allowed on Operating System "Linux Linux 2.4 or 2.6".
```



### ドメイン

ホワイtrリストに準拠しなくなったホストのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

### ホストの重要度 (Host Criticality)

ホワイtrリストに準拠していないホストに対してユーザが割り当てた重要度 ([なし (None) ]、[低 (Low) ]、[中 (Medium) ]、または[高 (High) ])。

### [IPアドレス (IP Address) ]

ホワイtrリストに準拠しなくなったホストの IP アドレス。

### ポリシー

違反した相関ポリシー、つまりホワイtrリストを含む相関ポリシーの名前。

### [ポート (Port) ]

アプリケーションプロトコルホワイtrリスト違反 (非準拠アプリケーションプロトコルの結果として発生した違反) をトリガーした検出イベントに関連付けられているポート (存在する場合)。他のタイプのホワイtrリスト違反の場合、このフィールドは空白です。

### [プライオリティ (Priority) ]

ポリシーまたはポリシー違反をトリガーしたホワイtrリストに指定されている優先度。これは、相関ポリシー内のホワイtrリストの優先度または相関ポリシー自体の優先度によって決まります。ホワイtrリストの優先度は、そのポリシーの優先度より優先されることに注意してください。このフィールドを検索するとき、プライオリティなしの場合は none を入力します。

### 時刻 (Time)

ホワイtrリスト イベントが生成された日時。このフィールドは検索できません。

### ユーザ (User)

ホワイtrリストに準拠しなくなったホストにログインしている既知のユーザのアイデンティティ。

### ホワイtrリスト (White List)

ホワイtrリストの名前。

### メンバー数 (Count)

各行に表示される情報と一致するイベントの数。[カウント (Count) ]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

## ホワイトリスト違反の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Any Security Analyst/Discovery Admin

システムは、ネットワークの現在のホワイトリスト違反のレコードを保持します。違反はそれぞれ、ホストのいずれかで実行することが禁止されている事柄を表します。ホストが準拠するようになると、システムは、修正された違反をデータベースから削除します。

Firepower Management Center を使用して、アクティブなすべてのホワイトリストに対するホワイトリスト違反のテーブルを表示できます。ここでユーザは、検索する情報に応じてイベントビューを操作することができます。

ホワイトリスト違反にアクセスしたときに表示されるページは使用しているワークフローによって異なります。事前定義されたワークフローはホストビューで終了しますが、このホストビューには、制約を満たすすべてのホストに対して1つずつホストプロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

**ステップ 1** [分析 (Analysis)] > [相関 (Correlation)] > [ホワイトリスト違反 (White List Violations)] を選択します。

**ステップ 2** 次の選択肢があります。

- 基本的なワークフロー操作を実行するには、[コンプライアンス ホワイトリスト ワークフローの使用 \(2760 ページ\)](#) を参照してください。
- テーブルのカラムの内容について詳しく調べるには、[ホワイトリスト違反のフィールド \(2764 ページ\)](#) を参照してください。

## ホワイトリスト違反のフィールド

ワークフローを使用して表示および検索できるホワイトリスト違反には、次のフィールドがあります。

## ドメイン

非準拠ホストが存在するドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

## 情報

ホワイトリスト違反に関連付けられたすべての利用可能なベンダー、製品、またはバージョン情報。ホワイトリストに違反するプロトコルの場合、このフィールドには、違反の原因がネットワーク プロトコルとトランスポート プロトコルのどちらであるのかも示されます。

## [IPアドレス (IP Address) ]

非準拠ホストの IP アドレス。

## [ポート (Port) ]

アプリケーションプロトコル ホワイトリスト違反（非準拠アプリケーションプロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられているポート（存在する場合）。他のタイプのホワイトリスト違反の場合、このフィールドは空白です。

## プロトコル

アプリケーションプロトコル ホワイトリスト違反（非準拠アプリケーションプロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられているプロトコル（存在する場合）。他のタイプのホワイトリスト違反の場合、このフィールドは空白です。

## 時刻 (Time)

ホワイトリスト違反が検出された日時。

## タイプ (Type)

ホワイトリスト違反のタイプ、つまり、非準拠の結果として違反が発生したかどうか。

- オペレーティング システム (os)（このフィールドを検索する場合は、**os** または **operating system** と入力してください）。
- アプリケーション プロトコル (サーバ)
- クライアント
- プロトコル
- Web アプリケーション (web)（このフィールドを検索する場合は、**web application** と入力してください）。

## ホワイトリスト (White List)

違反されたホワイトリストの名前。

**メンバー数 (Count)**

各行に表示される情報と一致するイベントの数。[カウント (Count)] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

## 修復ステータスイベント

修復がトリガーされると、システムは修復ステータスイベントをデータベースに記録します。これらのイベントは、[修復ステータス (Remediation Status)] ページで確認できます。修復ステータスイベントを検索、表示、削除できます。

**関連トピック**

[修復ステータスのテーブル フィールド \(2767 ページ\)](#)

## 修復ステータスイベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

修復ステータスイベントにアクセスするときに表示されるページは、使用するワークフローにより異なります。修復のテーブルビューを含む定義済みワークフローを使用できます。テーブルビューには、各修復ステータスイベントの行が含まれます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

**手順**

**ステップ 1** [分析 (Analysis)] > [相関 (Correlation)] > [ステータス (Status)] を選択します。

**ステップ 2** オプションで、[時間枠の変更 \(2455 ページ\)](#) の説明に従って、時間範囲を調整します。

**ステップ 3** オプションで、カスタムワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(ワークフローの切り替え) ((switch workflow))] をクリックします。

**ヒント** 修復のテーブルビューが含まれないカスタム ワークフローを使用する場合、ワークフローのタイトルの横の [(ワークフローの切り替え) ((switch workflow))] メニューをクリックし、[修復ステータス (Remediation Status)] を選択します。

**ステップ 4** 次の選択肢があります。

- 表示されるカラムの詳細については、[修復ステータスのテーブル フィールド \(2767 ページ\)](#) を参照してください。

- イベントをソートしたり、制約したりするには、[ワークフローの使用 \(2429 ページ\)](#) を参照してください。
- 関連イベントビューに移動し関連するイベントを確認するには、[関連イベント (Correlation Events)] をクリックします。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク (Bookmark This Page)] をクリックします。ブックマークの管理ページに移動するには、[ブックマークの表示 (View Bookmarks)] をクリックします。
- テーブルビューのデータに基づいてレポートを生成するには、[イベントビューからのレポートテンプレートの作成 \(2312 ページ\)](#) で説明されているように、[レポートデザイナー (Report Designer)] をクリックします。
- ワークフローの次のページにドリルダウンするには、[ドリルダウン ページの使用 \(2439 ページ\)](#) を参照してください。
- システムから修復ステータスイベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除 (Delete)] をクリックするか、[すべて削除 (Delete All)] をクリックして現在の制約されているビューにあるすべてのイベントを削除することを確認します。
- 修復ステータスイベントを検索するには、[検索 (Search)] をクリックします。

### 関連トピック

[ワークフローの使用 \(2429 ページ\)](#)

## 修復ステータスのテーブル フィールド

次の表に、表示および検索できる修復のステートテーブルのフィールドを示します。

表 308: 修復ステータス フィールド

フィールド	説明
ドメイン (Domain)	監視対象のトラフィックがポリシー違反をトリガーとして使用し、次に修復をトリガーとして使用するデバイスのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
ポリシー	違反し、修復をトリガーとして使用した関連ポリシーの名前。
修復名	起動された修復の名前。

フィールド	説明
結果メッセージ	<p>修復が起動したときに発生した事象を示すメッセージ。ステータス メッセージには以下が含まれます。</p> <ul style="list-style-type: none"> <li>• Successful completion of remediation</li> <li>• Error in the input provided to the remediation module</li> <li>• Error in the remediation module configuration</li> <li>• Error logging into the remote device or server</li> <li>• Unable to gain required privileges on remote device or server</li> <li>• Timeout logging into remote device or server</li> <li>• Timeout executing remote commands or servers</li> <li>• The remote device or server was unreachable</li> <li>• The remediation was attempted but failed</li> <li>• Failed to execute remediation program</li> <li>• Unknown/unexpected error</li> </ul> <p>カスタム修復モジュールがインストールされている場合、カスタム モジュールによって実装される追加のステータス メッセージが表示される場合があります。</p>
ルール (Rule)	修復をトリガーとして使用したルールの名前。
時刻 (Time)	Firepower Management Center が修復を起動した日付と時刻。
メンバー数 (Count)	各行に表示される情報と一致するイベントの数。[カウント (Count) ]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

## 関連トピック

[イベントの検索](#) (2467 ページ)

## 修復ステータス イベント テーブルの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

イベントビューのレイアウトを変更したり、ビュー内のイベントをフィールド値で制限したりできます。

カラムを無効にすると、そのカラムは（後で元に戻さない限り）そのセッションの間中は無効になります。最初のカラムを無効にすると、[カウント (Count)] カラムが追加されます。

テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（次のページにはドリルダウンされません）。



---

**ヒント** テーブル ビューでは、必ずページ名に「Table View」が含まれます。

---

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができません。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

---

**ステップ 1** [分析 (Analysis)] > [相関 (Correlation)] > [ステータス (Status)] を選択します。

**ヒント** 修復のテーブル ビューが含まれないカスタム ワークフローを使用する場合、ワークフローのタイトルの横の [(ワークフローの切り替え) ((switch workflow))] メニューをクリックし、[修復ステータス (Remediation Status)] を選択します。

**ステップ 2** 次の選択肢があります。

- 表示されるカラムの詳細については、[修復ステータスのテーブル フィールド \(2767 ページ\)](#) を参照してください。
  - イベントをソートしたり、制約したりするには、[ワークフローの使用 \(2429 ページ\)](#) を参照してください。
-







## 第 112 章

# システムの監査

次のトピックでは、システム上のアクティビティを監査する方法について説明します。

- [システム監査について](#) (2771 ページ)
- [監査レコード](#) (2771 ページ)
- [システム ログ](#) (2781 ページ)

## システム監査について

システム上のアクティビティを 2 つの方法で監査できます。Firepower システムの一部であるアプライアンスによって、Web インターフェイスとユーザとの対話のそれぞれに対して監査レコードが生成され、システム ステータス メッセージがシステム ログに記録されます。

### 関連トピック

[標準レポートの概要](#) (2307 ページ)

## 監査レコード

Firepower Management Center および 7000 および 8000 シリーズ管理対象デバイスは、ユーザアクティビティに関する読み取り専用の監査情報をログに記録します。監査ログは標準イベントビューに表示され、監査ビュー内の任意の項目に基づいて監査ログ メッセージを表示、ソート、およびフィルタリングできます。監査情報を簡単に削除したり、それに関するレポートを作成したりすることができ、ユーザが行った変更に関する詳細なレポートを表示することもできます。

監査ログには最大 100,000 のエントリが保存されます。監査ログ エントリの数が 100,000 を超えると、アプライアンスは最も古いレコードをデータベースからプルーニングして、100,000 エントリまで数を削減します。



- (注) 7000 または 8000 シリーズデバイスをリブートした直後にすばやく補助 CLI にログインした場合、そこで実行するコマンドは、ローカル Web インターフェイスが使用可能になるまでは監査ログに記録されません。

## 監査レコードの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

Firepower Management Center または 7000 および 8000 シリーズデバイスで、監査レコードのテーブルを表示できます。事前定義された監査ワークフローには、イベントを示す単一のテーブルビューが含まれます。ユーザは検索する情報に応じてテーブルビューを操作することができます。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

### 手順

**ステップ 1** [システム (System)] > [モニタリング (Monitoring)] > [監査 (Audit)] を使用して監査ログのワークフローにアクセスします。

**ステップ 2** イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。詳細については、[イベント時間の制約 \(2451 ページ\)](#) を参照してください。

- (注) イベントビューを時間によって制約している場合は、(グローバルかイベント固有かに関係なく) アプライアンスに設定されている時間枠の外で生成されたイベントが、イベントビューに表示されます。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

**ステップ 3** 次の選択肢があります。

- テーブルのカラムの内容について詳しく調べるには、[システムログ \(2781 ページ\)](#) を参照してください。
- 現在のワークフロー ページでイベントをソートしたり、制限したりするには、[テーブルビュー ページの使用 \(2440 ページ\)](#) を参照してください。
- 現在のワークフロー ページ内で移動するには、[時間枠の進行 \(2459 ページ\)](#) を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページリンクをクリックします。詳細については、[ワークフローの使用 \(2429 ページ\)](#) を参照してください。

- ワークフローの次のページにドリルダウンするには、[ドリルダウン ページの使用 \(2439 ページ\)](#) を参照してください。
- 特定の値で制約するには、行内の値をクリックします。ドリルダウンページで値をクリックすると、次のページに移動し、その値だけに制約されます。テーブルビューの行内の値をクリックすると、テーブルビューが制限され、次のページにドリルダウンされないことに注意してください。詳細については、[イベントビューの制約 \(2460 ページ\)](#) を参照してください。

**ヒント** テーブル ビューでは、必ずページ名に「Table View」が含まれます。

- 監査レコードを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除 (Delete) ] をクリックするか、[すべて削除 (Delete All) ] をクリックして現在の制約されているビューにあるすべてのイベントを削除します。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク (Bookmark This Page) ] をクリックします。詳細については、[ブックマーク \(2464 ページ\)](#) を参照してください。
- ブックマークの管理ページに移動するには、[ブックマークの表示 (View Bookmarks) ] をクリックします。詳細については、[ブックマーク \(2464 ページ\)](#) を参照してください。
- 現在のビューのデータに基づいてレポートを生成するには、[レポート デザイナ (Report Designer) ] をクリックします。詳細については、[イベント ビューからのレポート テンプレートの作成 \(2312 ページ\)](#) を参照してください。
- 監査ログに記録された変更の概要を表示するには、[メッセージ (Message) ] カラムの該当するイベントの横にある比較アイコン (🔍) をクリックします。詳細については、[監査ログを使って変更を調査する \(2775 ページ\)](#) を参照してください。

#### 関連トピック

[イベント ビューの制約 \(2460 ページ\)](#)

## 監査ログのワークフロー フィールド

次の表で、表示および検索できる監査ログ フィールドについて説明します。

表 309: 監査ログのフィールド

フィールド	説明
時刻 (Time)	アプライアンスが監査レコードを生成した日時。
ユーザ (User)	監査イベントをトリガーしたユーザのユーザ名。

フィールド	説明
サブシステム	<p>監査レコードが生成されたときにユーザがたどったフルメニューパス。たとえば、<b>[システム (System)] &gt; [モニタリング (Monitoring)] &gt; [監査 (Audit)]</b>は、監査ログを表示するためのメニューパスです。</p> <p>メニューパスが該当しない数少ないケースでは、<b>[サブシステム (Subsystem)]</b>フィールドにイベントタイプのみが表示されます。たとえば、<b>Login</b>は、ユーザがログインしようとしたことを表します。</p>
メッセージ (Message)	<p>ユーザが実行したアクション、またはユーザがページでクリックしたボタン。</p> <p>たとえば、Page viewは、<b>[サブシステム (Subsystem)]</b>に示されているページをユーザが単に表示したことを意味します。saveは、ユーザがページの<b>[保存 (Save)]</b>ボタンをクリックしたことを意味します。</p> <p>Firepower システムに対する変更は比較アイコン (🔍) 付きで表示され、アイコンをクリックすると変更の概要を確認することができます。</p>
ソース IP	<p>ユーザが使用したホストに関連付けられている IP アドレス。</p> <p>注：このフィールドを検索する場合は、特定の IP アドレスを入力する必要があります。監査ログの検索で IP 範囲を使用することはできません。</p>
ドメイン (Domain)	<p>監査イベントがトリガーされたときのユーザの現行ドメイン。このフィールドは、マルチテナンシーのために <b>Firepower Management Center</b> を設定したことがある場合に表示されます。</p>
設定の変更 (Configuration Change) (検索専用)	<p>設定の変更の監査レコードを検索結果に表示するかどうかを指定します。(yes または no)</p>

フィールド	説明
メンバー数 (Count)	各行に表示される情報と一致するイベントの数。[カウント (Count)] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

#### 関連トピック

[イベントの検索](#) (2467 ページ)

## [監査イベント (Audit Events)] テーブルビュー

イベントビューのレイアウトを変更したり、ビュー内のイベントをフィールド値で制限したりできます。カラムを無効にする場合は、非表示にするカラム見出しの [閉じる (Close)] アイコン (✕) をクリックした後、表示されるポップアップ ウィンドウで [適用 (Apply)] をクリックします。カラムを無効にすると、そのカラムは (後で元に戻さない限り) そのセッションの間中は無効になります。最初のカラムを無効にすると、[カウント (Count)] カラムが追加されることに注意してください。

他のカラムを表示/非表示にしたり、無効になったカラムをビューに再び追加したりするには、該当するチェックボックスを選択またはクリアしてから [適用 (Apply)] をクリックします。

テーブルビューの行内の値をクリックすると、テーブルビューが制約されます (ワークフロー内の次のページにはドリルダウンされません)。



**ヒント** テーブルビューでは、必ずページ名に「テーブルビュー (Table View)」が含まれます。

#### 関連トピック

[ワークフローの使用](#) (2429 ページ)

## 監査ログを使って変更を調査する

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

監査ログを使用して、システムの変更に関する詳細レポートを表示できます。これらのレポートは、現在のシステム設定を、特定の変更が行われる直前の設定と比較します。

[設定の比較 (Compare Configurations)] ページには、変更前のシステム設定と、現在実行中の設定との違いが横並び形式で表示されます。監査イベントタイプ、最終変更時間、および変更を行ったユーザ名が、各設定の上のタイトルバーに表示されます。

2つの設定の違いは次のように強調表示されます。

- 青は、強調表示されている設定項目が2つの設定間で異なっていることを示し、異なっている部分は赤のテキストで表示されます。
- グリーンは、強調表示されている設定項目が一方の設定に含まれ、もう一方の設定には含まれないことを示します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

#### 手順

**ステップ 1** [システム (System)] > [モニタリング (Monitoring)] > [監査 (Audit)] を選択します。

**ステップ 2** [メッセージ (Message)] カラムの該当する監査ログ イベントの横にある比較アイコン (🔍) をクリックします。

**ヒント** タイトルバーの上の [前へ (Previous)] または [次へ (Next)] をクリックすると、個々の変更の間を移動できます。また、変更の概要が複数のページにまたがる場合は、右側のスクロールバーを使って追加の変更を表示できます。

## 監査レコードの抑制

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

監査ポリシーで、Firepower System/ユーザ間の特定のタイプのインタラクションを監査する必要がない場合は、それらのインタラクションによって、Firepower Management Center または 7000 および 8000 シリーズデバイス上で監査レコードが生成されないように設定できます。たとえば、デフォルトでは、ユーザがオンラインヘルプを表示するたびに、Firepower System は監査レコードを生成します。このようなインタラクションのレコードを保持する必要がない場合は、これらを自動的に抑制できます。

監査イベントの抑制を設定するには、アプライアンスの admin ユーザアカウントにアクセスできる必要があり、アプライアンスのコンソールにアクセスできる（またはセキュアシェルを開くことができる）必要があります。



**注意** 許可された担当者だけが、アプライアンスとその admin アカウントにアクセスできることを確認してください。

## 手順

/etc/sf ディレクトリに、次の形式で1つ以上の AuditBlock ファイルを作成します。タイプは、[監査ブロックタイプ \(2777 ページ\)](#) で説明されているいずれかのタイプになります。

AuditBlock.type

- (注) 特定のタイプの監査メッセージに関する AuditBlock.type ファイルを作成した後、もはやそれらを抑制しないことを決定した場合、AuditBlock.type ファイルの内容を削除する必要がありますが、ファイル自体は Firepower System に残してください。

## 監査ブロックタイプ

それぞれの監査ブロックタイプの内容は、以下の表に記載されているように、特定の形式でなければなりません。ファイル名の大文字/小文字を必ず正しく表記してください。また、ファイルの内容でも大文字と小文字が区別されることに注意してください。

AuditBlock ファイルを追加した場合、サブシステム Audit およびメッセージ Audit FiltertypeChanged を含む監査レコードが監査イベントに追加されることに注意してください。セキュリティ上の理由から、この監査レコードを抑制することはできません。

表 310: 監査ブロックタイプ

タイプ (Type)	説明
アドレス (Address)	AuditBlock.address という名前のファイルを作成し、監査ログから抑制する IP アドレスを1行に1つずつ含めます。部分的な IP アドレスを使用できます (ただし、アドレスの先頭から照合されます)。たとえば、部分的なアドレス 10.1.1 は、10.1.1.0 から 10.1.1.255 までのアドレスと一致します。
メッセージ	AuditBlock.message という名前のファイルを作成し、抑制するメッセージ部分文字列を1行に1つずつ含めます。  たとえば、backup をこのファイルに含めた場合、部分文字列の照合により backup という語を含むすべてのメッセージが抑制されることに注意してください。

タイプ (Type)	説明
サブシステム	<p>AuditBlock.subsystem という名前のファイルを作成し、抑制するサブシステムを1行に1つずつ含めます。</p> <p>部分文字列は照合されないことに注意してください。正確な文字列を使用する必要があります。監査対象のサブシステムのリストについては、<a href="#">監査対象のサブシステム (2778ページ)</a> を参照してください。</p>
ユーザ (User)	<p>AuditBlock.user という名前のファイルを作成し、抑制するユーザアカウントを1行に1つずつ含めます。部分文字列の照合を使用できません（ただし、ユーザ名の先頭から照合されます）。たとえば、部分的なユーザ名 IPSAnalyst はユーザ名 IPSAnalyst1 および IPSAnalyst2 と一致します。</p>

## 監査対象のサブシステム

次の表に、監査対象のサブシステムを示します。

表 311: サブシステム名

[名前 (Name)]	何に関するユーザインタラクションを含んでいるか
管理	管理機能（システムとアクセス権の設定、時刻の同期、バックアップと復元、デバイス管理、ユーザアカウントの管理、スケジュール設定など）
アラート (Alerting)	アラート機能（電子メールアラート、SNMPアラート、Syslogアラートなど）
監査ログ (Audit Log)	監査イベントの表示
監査ログ検索 (Audit Log Search)	監査イベントの検索
コマンドライン	コマンドラインインターフェイス
設定 (Configuration)	電子メールアラート機能
COOP	運用の継続性に関する機能
日付 (Date)	イベントビューの日時範囲



<b>[名前 (Name) ]</b>	何に関するユーザインタラクションを含んでいるか
デフォルトのサブシステム (Default Subsystem)	サブシステムが割り当てられていないオプション
検出および防止ポリシー (Detection & Prevention Policy)	侵入ポリシーのメニュー オプション
エラー (Error)	システム レベルのエラー
eStreamer	eStreamer 構成
EULA	エンドユーザ ライセンス契約書の確認
イベント	侵入および検出イベント ビュー
イベント クリップボード (Events Clipboard)	侵入イベント クリップボード
確認済みイベント (Events Reviewed)	確認済みの侵入イベント
イベント検索 (Events Search)	あらゆるイベント検索
ルール更新のインストールの失敗 (Failed to install rule update) rule_update_id	ルール更新のインストール
ヘッダー	ユーザログイン後のユーザインターフェイスの初回表示
状態	ヘルス モニタリング
ヘルス イベント (Health Events)	ヘルス モニタリング イベントの表示
ヘルプ	オンライン ヘルプ
高可用性	高可用性ペアでの Firepower Management Center の確立と管理
IDS インパクト フラグ (IDS Impact Flag)	インパクト フラグの設定
IDS ポリシー (IDS Policy)	侵入ポリシー
IDS ルール SID : sig_id リビジョン : rev_num	SID 別の侵入ルール
<b>[インシデント (Incidents) ]</b>	侵入インシデント
インストール (Install)	更新のインストール
侵入イベント	侵入イベント

[名前 (Name) ]	何に関するユーザインタラクションを含んでいるか
ログイン (Login)	Web インターフェイスのログイン/ログアウト機能
ログアウト	Web インターフェイス ログアウト機能
メニュー	あらゆるメニュー オプション
[設定のエクスポート (Configuration export) ] > [config_type] > [config_name]	特定のタイプと名前の設定のインポート
権限のエスカレーション (Permission Escalation)	ユーザ ロールのエスカレーション
初期設定	ユーザ設定 (ユーザアカウントのタイムゾーン、個々のイベント設定など)
ポリシー	侵入ポリシーを含む、あらゆるポリシー
登録	Management Center でのデバイスの登録
リモートストレージデバイス (RemoteStorageDevice)	リモートストレージデバイスの設定
レポート	レポートリスト機能およびレポートデザイン機能
ルール (Rules)	侵入ルール (侵入ルール エディタとルールのインポート プロセスを含む)
ルール更新インポートログ (Rule Update Import Log)	ルール更新インポート ログの表示
ルール更新インストーラ (Rule Update Install)	ルール更新のインストーラ
セッションの時間切れ	Web インターフェイスのセッション タイムアウト
ステータス (Status)	Syslog およびホストとパフォーマンスの統計
システム (System)	システム全体のさまざまな設定
タスク キュー (Task Queue)	バックグラウンドプロセスステータスの表示
Users	ユーザ アカウントとロールの作成および変更

## システム ログ

[システム ログ (System Log)] (syslog) ページには、アプライアンスのシステム ログ情報が表示されます。システム ログには、システムによって生成された各メッセージが表示されます。次の項目が順にリストされます。

- メッセージが生成された日付
- メッセージが生成された時刻
- メッセージを生成したホスト
- メッセージ自体

## システム ログの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin/Maint

システム ログ情報はローカルな情報です。たとえば、Firepower Management Center を使用して、管理対象デバイスのシステム ログ内のシステム ステータス メッセージを見ることはできません。

Firepower Management Center または 7000 & 8000 シリーズ デバイスでは、特定のコンポーネントでフィルタリングすることによって、システム ログ メッセージのビューを変更できます。

### 手順

**ステップ 1** [システム (System)] > [モニタリング (Monitoring)] > [Syslog] を選択します。

**ステップ 2** システム ログの特定のメッセージ内容を検索する場合は、[システム ログ メッセージのフィルタリング \(2781 ページ\)](#) を参照してください。

## システム ログ メッセージのフィルタリング

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin/Maint

Firepower Management Center または 7000 および 8000 シリーズ のデバイスで、特定のコンポーネントをフィルタリングして、システム ログ メッセージの表示を変更することができます。

フィルタリングにより、メッセージ内容に基づいて特定のメッセージを検索することができます。

フィルタリング機能は、UNIX ファイル検索ユーティリティ **Grep** を使用しているため、**Grep** で使用可能なほとんどの構文を使用できます。つまり、パターンマッチング用に **Grep** 互換の正規表現を使用できます。単一の語をフィルタとして使用したり、**Grep** でサポートされる正規表現を使用したりして内容を検索できます。

## 手順

**ステップ 1** [システム (System)] > [モニタリング (Monitoring)] > [Syslog] を選択します。

**ステップ 2** システム ログ フィルタの構文 (2782 ページ) に記載されているように、フィルタのフィールドに単語またはクエリを入力します。

(注) **Grep** 互換の検索構文のみがサポートされています。たとえば、フィルタとして `ntp` を使ってすべての NTP 関連システム ログ メッセージを検索したり、`Nov` をフィルタとして使って 11 月に生成されたすべてのメッセージを検索したりできます。

`Nov[:space:]*27` または `Nov.*27` を使用すると 11 月 27 日のメッセージを表示できますが、`Nov 27` または `Nov*27` を使ってこれらのメッセージを表示することはできません。

**ステップ 3** 大文字と小文字が区別されるようにするには、[大文字と小文字を区別する (Case-sensitive)] をチェックします。(デフォルトでは、フィルタで大文字/小文字は区別されません。)

**ステップ 4** オプションで、[除外 (Exclusion)] をチェックすると、入力した条件に一致しないすべてのシステム ログ メッセージが検索されます。

**ステップ 5** [移動 (Go)] をクリックします。

## 例

11 月 5 日に生成されたすべてのログ エントリを検索するには、`Nov[:space:]*5` を使用します。

ユーザ名 "Admin" を含むすべてのログ エントリを検索するには `Admin` を使用します。

11 月 5 日のデバッグ情報の認証を含むすべてのログ エントリを検索するには、`Nov[:space:]*5.*AUTH.*DEBUG` を使用します。

## システム ログ フィルタの構文

次の表に、システム ログ フィルタで使用できる正規表現構文を示します。

表 312: システム ログ フィルタ構文

構文のコンポーネント	説明	例
.	任意の文字またはスペースと一致します	Admi. は、Admin、Admin、Admi1、および Admi& と一致します。
[:alpha:]	任意の英文字と一致します	[:alpha:]dmin は、Admin、badmin、および cadmin と一致します
[:upper:]	任意の大文字の英文字と一致します	[:upper:]dmin は、Admin、Badmin、および cadmin と一致します
[:lower:]	任意の小文字の英文字と一致します	[:lower:]dmin は、admin、badmin、および cadmin と一致します
[:digit:]	任意の数字と一致します	[:digit:]dmin は、0dmin、1dmin、および 2dmin と一致します
[:alnum:]	任意の英数字と一致します	[:alnum:]dmin は、1dmin、admin、2dmin、および badmin と一致します
[:space:]	タブを含む、任意のスペースと一致します	Feb[:space:]29 は 2月29日のログと一致します
*	その前にある文字または式のゼロ個以上のインスタンスと一致します	ab* は、a、ab、abb、ca、cab、および cabb と一致します [ab]* はすべてのものと一致します
?	ゼロ個または1つのインスタンスと一致します	ab? は、a または ab と一致します
\	これを使用すると、通常は正規表現構文と解釈される文字を検索できます	alert\? は、alert? と一致します





## 付録 **A**

# セキュリティ、インターネットアクセス、および通信ポート

以下のトピックでは、システムセキュリティ、インターネットアクセス、および通信ポートに関する情報を提供します。

- [セキュリティ、インターネットアクセス、および通信ポートについて \(2785 ページ\)](#)
- [インターネットアクセス要件 \(2786 ページ\)](#)
- [通信ポートの要件 \(2787 ページ\)](#)

## セキュリティ、インターネットアクセス、および通信ポートについて

Firepower Management Center を保護するには、保護された内部ネットワークにインストールしてください。Firepower Management Center は必要なサービスとポートだけを使用するよう設定されますが、ファイアウォール外部からの攻撃がそこまで（または管理対象デバイスまで）決して到達できないようにする必要があります。

Firepower Management Center とその管理対象デバイスが同じネットワーク上に存在する場合は、デバイス上の管理インターフェイスを、Firepower Management Center と同じ保護された内部ネットワークに接続できます。これにより、Firepower Management Center からデバイスを安全に制御することができます。また、他のネットワーク上のデバイスからのトラフィックを Firepower Management Center で管理および分離できるように、複数の管理インターフェイスを設定することもできます。

アプライアンスの展開方法とは無関係に、アプライアンス間通信は暗号化されます。それでも、分散型サービス拒否 (DDoS) や中間者攻撃などの手段でシステムアプライアンス間の通信が中断、ブロック、改ざんされないよう何らかの対策を講じる必要があります。

また、Firepower システムの機能によってはインターネット接続が必要となることにも注意してください。デフォルトでは、システムアプライアンスがインターネットに直接接続するように設定されます。加えて、システムで特定のポートを開いたままにしておく必要があります。その目的は基本的なアプライアンス間通信、セキュアなアプライアンスアクセス、および特定

のシステム機能を正しく動作させるために必要なローカル/インターネット リソースへのアクセスを可能にすることです。

## インターネットアクセス要件

デフォルトでは、システム アプライアンスはポート 443/tcp (HTTPS) および 80/tcp (HTTP) でインターネットに直接接続するよう設定されます。これらのポートは Firepower システムのすべてのアプライアンスでデフォルトで開かれています。ほとんどのシステムアプライアンスではプロキシサーバの利用がサポートされている点に注意してください。プロキシサーバは whois アクセスに使用できない点にも注意が必要です。

## Firepower システム機能のインターネットアクセス要件

次の表に、Firepower システムの特定の機能におけるインターネットアクセス要件を示します。

表 313: Firepower システム機能のインターネットアクセス要件

機能	インターネットアクセスの用途	アプライアンス
AMP for Firepower	マルウェア クラウド検索を実行します。	Management Center
Cisco Advanced Malware Protection (Cisco AMP) 統合	エンドポイントベース (AMP for Endpoints) のマルウェア イベントを Cisco AMP クラウドから受信します。	Management Center
動的分析：照会	動的分析のために、送信済みファイルの脅威スコアを AMP Threat Grid クラウドに照会します。	Management Center
動的分析：送信	動的分析用にファイルを AMP Threat Grid クラウドに送信します。	あらゆるデバイス
侵入ルール、VDB、および GeoDB の更新	侵入ルール、GeoDB、または VDB の更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。	Management Center
ローカルマルウェア分析およびファイル事前分類の署名アップデート	ローカルマルウェア分析および事前分類エンジンに署名アップデートをダウンロードします。	Management Center
RSS フィード ダッシュボード ウィジェット	シスコを含む外部ソースから RSS フィード データをダウンロードします。	Management Center 7000 & 8000 シリーズ



機能	インターネット アクセスの用途	アプライアンス
セキュリティ インテリジェンス フィルタリング	シスコが提供するインテリジェンス フィードを含む、外部ソースからのセキュリティ インテリジェンス フィードデータをダウンロードします。	Management Center
システム ソフトウェアの更新	システム更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。	すべて (NGIPSv を除く)
URL フィルタリング	URL カテゴリおよびレピュテーションデータをアクセスコントロール用にダウンロードし、分類されていないURL に対してクエリを実行します。	Management Center
whois	外部ホストの whois 情報を要求します。	Management Center

## 通信ポートの要件

Firepower Management Center およびその管理対象デバイスは、（デフォルトでポート 8305/tcp を使用する）双方向 SSL 暗号化通信チャネルを使って通信します。基本的なプラットフォーム間通信にこのポートを開いたままにする**必要があります**。他のオープンポートの役割は次のとおりです。

- Web インターフェイスへのアクセス
- デバイスまたは Firepower Management Center へのセキュアなリモート接続
- 特定のシステム機能を正しく動作させるために必要なローカル/インターネット リソースへのアクセスを可能にする

一般に、機能関連のポートは、該当する機能を有効化または設定する時点まで、閉じたままになります。たとえば、Firepower Management Center をユーザーエージェントに接続するまでは、エージェント通信ポート (3306/tcp) は閉じたままになります。別の例として、LOM を有効にするまでは、7000 および 8000 シリーズ デバイス上のポート 623/udp が閉じたままになります。



**注意** 開いたポートを閉じると展開にどのような影響が及ぶか理解するまでは、開いたポートを閉じないでください。

たとえば、管理対象デバイスでポート 25/tcp (SMTP) アウトバウンドを閉じると、このデバイスが個々の侵入イベントに関する電子メール通知を送信できなくなります。別の例として、

ポート 443/tcp (HTTPS) を閉じることにより物理管理対象デバイスの Web インターフェイスへのアクセスを無効にできますが、それと同時に、動的分析のためにデバイスから疑わしいマルウェア ファイルを AMP Threat Grid クラウドに送信できなくなります。

次のように、システムのいくつかの通信ポートを変更できることに注意してください。

- システムと認証サーバ間の接続を設定するときに、LDAP および RADIUS 認証用のカスタム ポートを指定できます。
- 管理ポート (8305/tcp) を変更できます。ただし、シスコではデフォルト設定を維持することを強く推奨しています。管理ポートを変更する場合は、相互に通信する必要がある展開内のすべての Firepower Management Center およびその管理対象デバイスの管理ポートを変更する必要があります。
- ポート 32137/tcp を使用して、アップグレード対象の Management Center とシスコ AMP クラウドの通信を可能にすることができます。ただし、シスコではバージョン 5.3 以降の新規インストールのデフォルトであるポート 443 に切り替えることを推奨しています。

#### 関連トピック

[LDAP 認証サーバの特定](#) (109 ページ)

[RADIUS 接続の設定](#) (127 ページ)

## Firepower システムの機能と運用のためのデフォルト通信ポート

次の表は、Firepower システムの機能を最大限に活用できるように、各アプライアンス タイプに必要なオープン ポートを示しています。

表 314: Firepower システムの機能と運用のためのデフォルト通信ポート

[ポート (Port) ]	説明	方向 (Direction)	開いているアプライアンス	目的
22/tcp	SSH/SSL	双方向	任意 (Any)	アプライアンスへのセキュアなリモート接続を許可します。
25/tcp	SMTP	発信	任意 (Any)	アプライアンスから電子メール通知とアラートを送信します。
53/tcp	DNS	発信	任意 (Any)	DNS を使用します。
67/udp 68/udp	DHCP	発信	任意 (Any)	DHCP を使用します。これらのポートはデフォルトで閉じられていることに注意してください。

[ポート (Port) ]	説明	方向 (Direction)	開いているアプライアンス	目的
80/tcp	HTTP	発信	Management Center 7000 & 8000 シリーズ	RSS フィードダッシュボードウィジェットからリモート Web サーバに接続できるようにします。
		双方向	Management Center	HTTP 経由でカスタムおよびサードパーティのセキュリティインテリジェンスフィードを更新します。  URL カテゴリおよびレピュテーションデータをダウンロードします (さらにポート 443 も必要)。
161/udp	SNMP	双方向	任意 (Any)	SNMP ポーリング経由でアプライアンスの MIB にアクセスできるようにします。
162/udp	SNMP	発信	任意 (Any)	リモートトラップサーバに SNMP アラートを送信します。
389/tcp 636/tcp	LDAP	発信	すべて (NGIPSv を除く)	外部認証用に LDAP サーバと通信します。
389/tcp 636/tcp	LDAP	発信	Management Center	検出された LDAP ユーザに関するメタデータを取得します。
443/tcp	HTTPS	着信	すべて (NGIPSv を除く)	アプライアンスの Web インターフェイスにアクセスします。

[ポート (Port)]	説明	方向 (Direction)	開いているアプライアンス	目的
443/tcp	<p>HTTPS</p> <p>AMQP</p> <p>AMP クラウド、AMP Threat Grid クラウド、および脅威インテリジェンスの通信設定</p>	双方向	Management Center	<p>次のものを取得します。</p> <ul style="list-style-type: none"> <li>ソフトウェア、侵入ルール、VDB、および GeoDB の更新</li> <li>URL カテゴリおよびレピュテーションデータ (さらにポート 80 も必要)</li> <li>インテリジェンスフィードおよび他のセキュアなセキュリティインテリジェンスフィード</li> <li>エンドポイントベース (AMP for Endpoints) のマルウェア イベント</li> <li>ファイルに関してネットワークトラフィックで検出されたマルウェアの性質</li> <li>送信されたファイルに関する動的分析情報</li> </ul>
		双方向	Management Center、7000 & 8000 シリーズ	<p>デバイスのローカル Web インターフェイスを使用してソフトウェア更新をダウンロードします。</p>
		双方向	すべての管理対象デバイス	<p>動的分析のためにファイルを送信します。</p>

[ポート (Port) ]	説明	方向 (Direction)	開いているアプライアンス	目的
514/udp	syslog	発信	任意 (Any)	リモート syslog サーバにアラートを送信します。
623/udp	SOL/LOM	双方向	7000 & 8000 シリーズ	Serial Over LAN (SOL) 接続を使用して Lights-Out Management を実行できるようにします。
1500/tcp 2000/tcp	データベースアクセス	着信	Management Center	サードパーティクライアントによるデータベースへの読み取り専用アクセスを可能にします。
1812/udp 1813/udp	RADIUS	双方向	すべて (NGIPSv を除く)	外部認証とアカウントिंगのために RADIUS サーバと通信します。
3306/tcp	ユーザ エージェント	着信	Management Center	ユーザエージェントと通信します。
6514/tcp	syslog への監査ログのストリーミング	発信	Management Center、従来のデバイス	リモート syslog サーバに監査ログレコードを送信します。
8302/tcp	eStreamer	双方向	Management Center 、 7000 & 8000 シリーズ	eStreamer クライアントと通信します。
8305/tcp	アプライアンス通信	双方向	任意 (Any)	展開におけるアプライアンス間で安全に通信します。必須作業です。
8307/tcp	ホスト入力クライアント	双方向	Management Center	ホスト入力クライアントと通信します。
32137/tcp	AMP クラウドおよび脅威インテリジェンスの通信設定	双方向	Management Center	アップグレード対象の Management Center と Cisco AMP クラウドの通信を可能にします。





## 付録 **B**

# 従来型デバイスのコマンドラインリファレンス

このリファレンスでは、次のデバイスのコマンドラインインターフェイス（CLI）について説明します。

- 7000 および 8000 シリーズ
- ASA FirePOWER
- NGIPSv



(注) Firepower Management Center で CLI を使用することはできません。Firepower Management Center は、Linux シェルアクセスをサポートし、Cisco Technical Assistance Center (TAC) の監督下でのみサポートされます。



(注) Firepower Threat Defense コマンドリファレンスについては、『[Command Reference for Firepower Threat Defense](#)』を参照してください。

- [CLI について](#) (2793 ページ)
- [基本的な CLI コマンド](#) (2795 ページ)
- [show コマンド](#) (2798 ページ)
- [コンフィギュレーション コマンド](#) (2830 ページ)
- [system コマンド](#) (2851 ページ)

## CLI について

デバイスに CLI (従来型デバイスでのコマンドラインインターフェイスへのログイン (28 ページ) または [Firepower Threat Defense](#) デバイスのコマンドラインインターフェイスへのロ

[グイン \(29 ページ\)](#) を参照) を使用してログインすると、この章で説明するコマンドを使用して、デバイスを表示、設定、およびトラブルシューティングすることができます。



- (注) 7000 または 8000 シリーズ デバイスをリブートし、できるだけ早く CLI にログインしても、Web インターフェイスが使用できるようになるまで、実行するすべてのコマンドは監査ログに記録されません。

CLI コマンドでは大文字と小文字が区別されません。ただし、ユーザ名や検索フィルタなど、テキストが CLI フレームワークの一部ではないパラメータでは区別されるので注意してください。

#### 関連トピック

[Firepower システムのユーザ インターフェイス](#)

## CLI モード

CLI モードには `show` や `configure` など多数あり、これらのモードにはモード名で始まる一連のコマンドが含まれています。モードを開始して、そのモードで有効なコマンドを入力することも、任意のモードからフル コマンドを入力することもできます。たとえば、`Analyst1` というユーザアカウントの情報を表示するには、CLI プロンプトで次のように入力します。

```
show user Analyst1
```

すでに `show` モードを開始している場合は、CLI プロンプトで次のように入力します。

```
user Analyst1
```

## CLI アクセス レベル

各モードで、ユーザが使用できるコマンドは、ユーザの CLI アクセスによって異なります。ユーザアカウントを作成する場合は、手動で次のいずれかの CLI アクセス レベルに割り当てることができます。

- [基本 (Basic) ] : ユーザは読み取り専用のアクセス権を持ち、システムパフォーマンスに影響を与えるコマンドを実行することはできません。
- [設定 (Configuration) ] : ユーザは、読み取り/書き込みアクセス権があり、システムパフォーマンスに影響を与えるコマンドを実行することができます。
- [なし (None) ] : ユーザはシェルにログインできません。

7000 および 8000 シリーズ デバイスでは、Web インターフェイスの [ユーザ管理 (User Management) ] ページでコマンドラインの権限を割り当てることができます。NGIPSv と ASA FirePOWER では、CLI を使用してコマンドラインの権限を割り当てます。



## 基本的な CLI コマンド

基本的な CLI コマンドを使用して、CLI とやりとりすることができます。これらのコマンドはデバイスの動作に影響しません。基本的なコマンドは、すべての CLI ユーザが使用可能です。

### configure password

現行のユーザは、自身のパスワードを変更することができます。コマンドを発行すると、CLI は現在の（古い）パスワードを入力するようユーザに要求し、その後で新しいパスワードを 2 回入力するよう要求します。

#### アクセス (Access)

基本

#### 構文

```
configure password
```

#### 例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

## 終了

ユーザをデフォルトのモードに戻します。（ユーザは、いずれかの下位レベルの CLI コンテキストから上位のデフォルトモードへ移動します）。

#### アクセス (Access)

基本

#### 構文

```
end
```

#### 例

```
configure network ipv4> end
>
```

## exit

CLI コンテキストを、次に高い CLI コンテキスト レベルへ移動します。デフォルト モードからこのコマンドを発行すると、ユーザは現行の CLI セッションからログアウトします。これは、CLI コマンドの `logout` を発行するのと同じです。

### アクセス (Access)

基本

### 構文

```
exit
```

### 例

```
configure network ipv4> exit  
configure network>
```

## ヘルプ

CLI 構文の概要を表示します。

### アクセス (Access)

基本

### 構文

```
help
```

### 例

```
> help
```

## history

現行のセッションのコマンドラインの履歴を表示します。

### アクセス (Access)

基本

### 構文

```
history limit
```

ここで `limit` は履歴リストのサイズを設定します。サイズを無制限に設定するには、`0` を入力します。

### 例

```
history 25
```

## ログアウト

現行の CLI コンソールセッションから現行のユーザをログアウトします。

### アクセス (Access)

#### 基本

### 構文

```
logout
```

### 例

```
> logout
```

## ? (疑問符)

CLI コマンドと CLI パラメータの状況依存ヘルプを表示します。以下のように疑問符 (?) コマンドを使用します。

- 現在の CLI コンテキストで使用できるコマンドのヘルプを表示するには、コマンドプロンプトに疑問符 (?) を入力します。
- 特定の文字列セットで始まる使用可能なコマンドのリストを表示するには、疑問符 (?) の直後に短縮コマンドを入力します。
- コマンドの法的引数のヘルプを表示するには、コマンドプロンプトの引数の代わりに疑問符 (?) を入力します。

疑問符 (?) は、コンソールにエコーバックすることはない点にご注意ください。

### アクセス (Access)

#### 基本

## ?? (二重の疑問符)

## 構文

```
?
abbreviated_command ?
command [arguments] ?
```

## 例

```
> ?
```

## ?? (二重の疑問符)

CLI コマンドおよびパラメータの詳細な状況依存ヘルプを表示します。

## アクセス (Access)

## 基本

## 構文

```
??
abbreviated_command end??
command [arguments] ??
```

## 例

```
> configure manager add ??
```

## show コマンド

show コマンドは、デバイスの状態に関する情報を提供します。これらのコマンドはデバイスの動作モードを変更しません。また、これらのコマンドを実行しても、システムの動作に対する影響は最小限になります。ほとんどの show コマンドはすべての CLI ユーザが利用できますが、show user コマンドを発行できるのは、Configuration CLI アクセス権限を持つユーザのみです。

## access-control-config

現在展開されている次のようなアクセス制御設定を表示します。

- セキュリティ インテリジェンスの設定
- アクセス コントロール ポリシーで呼び出されるあらゆるサブポリシーの名前
- 侵入変数セット データ

- ロギングの設定
- ポリシー レベルのパフォーマンス、前処理、全般設定などのその他の詳細設定

また、送信元と宛先ポートのデータ (ICMP エントリのタイプとコードを含む) および各アクセス コントロール ルールに一致する接続数 (ヒット数) などの、ポリシーに関連する接続情報も表示します。

### アクセス (Access)

基本

構文

```
show access-control-config
```

例

```
> show access-control-config
```

## alarms

デバイスで現在アクティブ (障害/停止) 状態になっているハードウェアのアラームを表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

### アクセス (Access)

基本

構文

```
show alarms
```

例

```
> show alarms
```

## arp-tables

ネットワークに適用できる Address Resolution Protocol テーブルを表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

### アクセス (Access)

基本

### 構文

```
show arp-tables
```

### 例

```
> show arp-tables
```

## audit-log

監査ログを時系列の逆順に表示します。最も新しい監査ログ イベントが先頭になります。

### アクセス (Access)

基本

### 構文

```
show audit-log
```

### 例

```
> show audit-log
```

## audit\_cert

現行の監査ログ クライアント証明書を表示します。

### アクセス (Access)

基本

### 構文

```
show audit_cert
```

### 例

```
> show audit_cert
```

## bypass

7000 または 8000 シリーズ デバイスで、使用中のインラインセットを一覧表示し、それらのセットについて次のいずれかのバイパス モード ステータスを表示します。

- **armed** : インターフェイス ペアが、障害発生時にハードウェアバイパスになるように設定されている ([バイパス モード : バイパス (Bypass Mode: Bypass) ]) か、または、**configure bypass close** コマンドを使用して強制的にフェールクローズされました。
- **engaged** : インターフェイス ペアが、オープンに失敗したか、または、**configure bypass open** コマンドを使用して強制的にハードウェアバイパスになりました。
- **off** : インターフェイス ペアがフェールクローズ ([バイパスモード : 非バイパス (Bypass Mode: Non-Bypass) ]) に設定されており、インターフェイス ペアで障害が発生した場合にはパケットがブロックされます。

### アクセス (Access)

基本

構文

```
show bypass
```

例

```
> show bypass
slp1 ↔ slp2: status 'armed'
slp1 ↔ slp2: status 'engaged'
```

## High-availability コマンド

ハイ アベイラビリティの設定、ステータス、メンバー デバイスまたはスタックの情報を表示します。このコマンドは NGIPsv および ASA FirePOWER デバイスでは使用できません。

### アクセス (Access)

基本

## config

デバイスの高可用性の設定を表示します。

構文

```
show high-availability config
```

例

```
> show high-availability config
```

## high-availability ha-statistics

高可用性ペアのデバイスの状態共有統計を表示します。

構文

```
show high-availability ha-statistics
```

例

```
> show high-availability ha-statistics
```

## cpu

デバイス上のすべての CPU のプラットフォームに適合する現行の CPU の使用率の統計情報を表示します。7000 および 8000 シリーズ デバイスでは、次の値が表示されます。

- CPU : プロセッサ番号。
- ロード : 0 ~ 100 の数値で表される CPU 使用率。0 はロードされていない状態で、100 は完全にロードされたことを表します。

NGIPSv および ASA FirePOWER では、次の値が表示されます。

- CPU : プロセッサ番号。
- %user : ユーザレベル (アプリケーション) で実行中に生じた CPU 使用率の割合 (パーセンテージ)。
- %nice : 高い優先度のユーザレベルで実行中に生じた CPU 使用率の割合 (パーセンテージ)。
- %sys : システムレベル (カーネル) で実行中に生じた CPU 使用率の割合 (パーセンテージ)。これには、サービスの割り込みや softirqs で経過する時間は含まれません。softirq (ソフトウェアの割り込み) は、複数の CPU で同時に実行できる最大 32 個の列挙されたソフトウェア割り込みの 1 つです。
- %iowait : システムに未処理のディスク I/O 要求があったときに、CPU がアイドル状態だった時間の割合 (パーセンテージ)。
- %irq : 割り込みを行うために CPU が費やした時間の割合 (パーセンテージ)。
- %soft : softirqs を行うために CPU が費やした時間の割合 (パーセンテージ)。



- **%steal** : ハイパーバイザが別の仮想プロセッサを実行しているときに、仮想CPUが強制的な待機で費やした時間の割合（パーセンテージ）。
- **%guest** : 仮想プロセッサを実行するために CPU が費やした時間の割合（パーセンテージ）。
- **%idle** : CPU がアイドル状態で、システムに未処理のディスク I/O 要求がなかった時間の割合（パーセンテージ）。

## アクセス (Access)

基本

構文

```
show cpu [procnum]
```

ここで `procnum` は、使用率の情報を表示するプロセッサの数を表します。有効な値は 0 から、システム上の合計プロセッサ数から 1 引いた数までの範囲です。`procnum` が 7000 または 8000 シリーズデバイスで使用されている場合は無視されます。このプラットフォームについては、使用率の情報はすべてのプロセッサについてのみ表示されるためです。

例

```
> show cpu
```

## Database コマンド

データベースの表示 (`show database`) コマンドは、デバイスの管理インターフェイスを設定します。

### アクセス (Access)

基本

## processes

実行中のデータベース クエリのリストを表示します。

### アクセス (Access)

基本

構文

```
show database processes
```

例

```
> show database processes
```

## slow-query-log

データベースのスロークエリログを表示します。

アクセス (**Access**)

基本

構文

```
show database slow-query-log
```

例

```
> show database slow-query-log
```

## device-settings

現行のデバイスに特有のアプリケーションのバイパス設定に関する情報を表示します。

アクセス (**Access**)

基本

構文

```
show device-settings
```

例

```
> show device-settings
```

## disk

現行のディスクの使用率を表示します。

アクセス (**Access**)

基本

### 構文

```
show disk
```

### 例

```
> show disk
```

## disk-manager

システムの各パート（サイロ、低水位、高水位など）のディスク使用率の詳細情報を表示します。

### アクセス (Access)

#### 基本

### 構文

```
show disk-manager
```

### 例

```
> show disk-manager
```

## dns

現行の DNS サーバのアドレスと検索ドメインを表示します。

### アクセス (Access)

#### 基本

### 構文

```
show dns
```

### 例

```
> show dns
```

## expert

シェルを起動します。

### アクセス (Access)

基本

構文

```
expert
```

例

```
> expert
```

## fan-status

ハードウェア ファンの現在のステータスを表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

### アクセス (Access)

基本

構文

```
show fan-status
```

例

```
> show fan-status
```

## fastpath-rules

現在設定されている 8000 シリーズの fastpath ルールを表示します。このコマンドは 8000 シリーズ デバイスでは使用できません。

### アクセス (Access)

基本

構文

```
show fastpath-rules
```

**例**

```
> show fastpath-rules
```

## gui

Web インターフェイスの現在の状態を表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

**アクセス (Access)**

基本

**構文**

```
show gui
```

**例**

```
> show gui
```

## hostname

デバイスのホスト名およびアプライアンス UUID を表示します。CLI を使用してデバイスのホスト名を編集する場合は、管理する Firepower Management Center に変更が反映されることを確認します。場合によっては、デバイス管理設定を手動で編集する必要があります。

**アクセス (Access)**

基本

**構文**

```
show hostname
```

**例**

```
> show hostname
```

## hosts

ASA FirePOWER モジュールの /etc/hosts ファイルの内容を表示します。

### アクセス (Access)

基本

### 構文

```
show hosts
```

### 例

```
> show hosts
```

## hyperthreading

ハイパースレッディングが有効か無効かを表示します。このコマンドは ASA FirePOWER では使用できません。

### アクセス (Access)

基本

### 構文

```
show hyperthreading
```

### 例

```
> show hyperthreading
```

## inline-sets

すべてのインラインセキュリティゾーンと関連するインターフェイスの設定データを表示します。このコマンドは ASA FirePOWER では使用できません。

### アクセス (Access)

基本

### 構文

```
show inline-sets
```

**例**

```
> show inline-sets
```

## interfaces

パラメータが指定されていない場合は、設定されているすべてのインターフェイスのリストが表示されます。パラメータが指定されている場合は、指定されたインターフェイスの詳細情報が表示されます。

**アクセス (Access)**

基本

**構文**

```
show interfaces interface
```

ここで *interface* は詳細情報を表示する特定のインターフェイスです。

**例**

```
> show interfaces
```

## ifconfig

ASA FirePOWER モジュールに対するインターフェイスの設定を表示します。

**アクセス (Access)**

基本

**構文**

```
show ifconfig
```

**例**

```
> show ifconfig
```

## lcd

LCD のハードウェア ディスプレイが有効か無効かを表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

### アクセス (Access)

基本

### 構文

```
show lcd
```

### 例

```
> show lcd
```

## Link-aggregation コマンド

`show link-aggregation` コマンドは、リンク集約グループ (LAG) の設定および統計情報を表示します。このコマンドは、NGIPSv および ASA FirePOWER デバイスでは使用できません。

### アクセス (Access)

基本

### 設定 :

LAG ID、インターフェイスの数、設定モード、ロードバランシングモード、LACP 情報、物理インターフェイスのタイプなど、設定された各 LAG の構成の詳細を表示します。

### アクセス (Access)

基本

### 構文

```
show link-aggregation configuration
```

### 例

```
> show link-aggregation configuration
```



## 統計情報

ステータス、リンクステートと速度、コンフィギュレーションモード、送受信されたパケットのカウント、および送受信されたバイトのカウントなど、設定された各LAGの統計情報をインターフェイスごとに表示します。

### アクセス (Access)

基本

### 構文

```
show link-aggregation statistics
```

### 例

```
> show link-aggregation statistics
```

## link-state

デバイスのポートのタイプ、リンク、スピード、速度、デュプレックスの状態およびバイパスモードを表示します。このコマンドはASA FirePOWERデバイスでは使用できません。

### アクセス (Access)

基本

### 構文

```
show link-state
```

### 例

```
> show link-state
```

## log-ips-connection

記録された侵入イベントに関連付けられている接続イベントのロギングが有効か無効かを表示します。

### アクセス (Access)

基本

### 構文

```
show log-ips-connection
```

### 例

```
> show log-ips-connection
```

## managers

Firepower Management Center の設定および通信のステータスを表示します。登録キーおよび NAT ID は、登録が保留中の場合のみ表示されます。

デバイスが、スタック設定のセカンダリデバイスとして設定されている場合、管理している両方の Management Center、およびプライマリデバイスに関する情報が表示されます。

### アクセス (Access)

#### 基本

### 構文

```
show managers
```

### 例

```
> show managers
```

## memory

デバイスの合計メモリ、使用中のメモリ、使用可能なメモリを表示します。

### アクセス (Access)

#### 基本

### 構文

```
show memory
```

### 例

```
> show memory
```

## model

デバイスのモデル情報を表示します。

### アクセス (Access)

基本

### 構文

```
show model
```

### 例

```
> show model
```

## mpls-depth

管理インターフェイスに設定されている MPLS レイヤ数を 0~6 で表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

### アクセス (Access)

基本

### 構文

```
show mpls-depth
```

### 例

```
> show mpls-depth
```

## NAT コマンド

show nat コマンドは、管理インターフェイスの NAT データと設定情報を表示します。このコマンドは、NGIPSv および ASA FirePOWER デバイスでは使用できません。

### アクセス (Access)

基本

## active-dynamic

ダイナミックルールに従って変換されている NAT フローを表示します。これらのエントリは、フローがルールに一致している場合に、ルールがタイムアウトになるまで表示されます。したがって、リストは正確ではないことがあります。タイムアウトはプロトコルに依存します。ICMP は 5 秒、UDP は 120 秒、TCP は 3600 秒、他のすべてのプロトコルは 60 秒です。

### 構文

```
show nat active-dynamic
```

### 例

```
> show nat active-dynamic
```

## active-static

スタティックルールに従って変換されている NAT フローを表示します。これらのエントリは、デバイスにルールが展開されるとすぐに表示されます。リストは、スタティックな NAT ルールに一致しているアクティブなフローを示しているわけではありません。

### 構文

```
show nat active-static
```

### 例

```
> show nat active-static
```

## allocators

すべての NAT アロケータの情報、ダイナミックルールで使用されている変換済みアドレスのプールを表示します。

### 構文

```
show nat allocators
```

### 例

```
> show nat allocators
```

## config

管理インターフェイスの現在の NAT ポリシーの設定を表示します。

### 構文

```
show nat config
```

### 例

```
> show nat config
```

## dynamic-rules

指定されたアロケータ ID を使用しているダイナミックな NAT ルールを表示します。

### 構文

```
show nat dynamic-rules allocator_id
```

ここで *allocator\_id* は有効なアロケータ ID 番号です。

### 例

```
> show nat dynamic-rules 9
```

## flows

指定されたアロケータ ID を使用しているルールについてフローの数を表示します。

### 構文

```
show nat flows allocator-id
```

ここで *allocator\_id* は有効なアロケータ ID 番号です。

### 例

```
> show nat flows 81
```

## static-rules

すべてのスタティック NAT ルールを表示します。

### 構文

```
show nat static-rules
```

**例**

```
> show nat static-rules
```

## netstat

ASA FirePOWER モジュールのアクティブなネットワーク接続を表示します。

**アクセス (Access)**

基本

**構文**

```
show netstat
```

**例**

```
> show netstat
```

## network

管理インターフェイスの IPv4 および IPv6 の設定、MAC アドレス、HTTP プロキシアドレス、ポート、ユーザ名（設定されている場合）を表示します。

**アクセス (Access)**

基本

**構文**

```
show network
```

**例**

```
> show network
```

## network-modules

インストールされているすべてのモジュール、およびモジュールの情報（シリアル番号など）を表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

### アクセス (Access)

基本

### 構文

```
show network-modules
```

### 例

```
> show network-modules
```

## network-static-routes

インターフェイス、宛先アドレス、ネットワークマスク、およびゲートウェイアドレスなど、設定済みのすべてのネットワークスタティックルートとその情報が表示されます。

### アクセス (Access)

基本

### 構文

```
show network-static-routes
```

### 例

```
> show network-static-routes
```

## ntp

NTP コンフィギュレーションを表示します。

### アクセス (Access)

基本

### 構文

```
show ntp
```

### 例

```
> show ntp
```

## perfstats

デバイスのパフォーマンスの統計情報を表示します。

### アクセス (Access)

基本

構文

```
show perfstats
```

例

```
> show perfstats
```

## portstats

デバイスのすべての挿入されたポートのポート統計を表示します。このコマンドはNGIPSvおよびASA FirePOWERでは使用できません。

### アクセス (Access)

基本

構文

```
show portstats [copper | fiber | internal | external | all]
```

銅線は、すべての銅線ポートを指定します。光ファイバはすべての光ファイバポートを指定します。内部はすべての内部ポートをします。外部はすべての外部（銅線および光ファイバ）ポートをします。すべてはすべてのポート（外部および内部）を指定します。

例

```
> show portstats fiber
```

## power-supply-status

現在のハードウェアの電源状態を表示します。このコマンドはNGIPSvおよびASA FirePOWERでは使用できません。





- (注) 8000 シリーズ 管理対象デバイスで電源障害が発生すると、CLI コマンドの `show power-supply-status` が正しいステータスを反映するまでに 15 分かかる場合があります。

### アクセス (Access)

基本

### 構文

```
show power-supply-status
```

### 例

```
> show power-supply-status
```

## process-tree

デバイスで実行中のプロセスについて、タイプごとにツリー形式でソートして表示します。

### アクセス (Access)

基本

### 構文

```
show process-tree
```

### 例

```
> show process-tree
```

## processes

デバイス上で現在実行中のプロセスについて、CPU 使用率の降順で表示します。

### アクセス (Access)

基本

### 構文

```
show processes sort-flag filter
```

ここで、メモリ（の降順）でソートする場合は、*sort-flag* に *-m* を指定し、プロセス名ではなくユーザ名でソートする場合は *-u* を指定します。また、コマンドのフルネームおよびパスを表示する場合は *verbose* を指定します。*filter* パラメータは、コマンドの検索語または結果をフィルタするために使用するユーザ名を指定します。見出し行は表示されたままです。

#### 例

```
> show processes -u user1
```

## ルート

ASA FirePOWER モジュールに関するルーティング情報を表示します。

### アクセス (Access)

基本

### 構文

```
show route
```

#### 例

```
> show route
```

## routing-table

パラメータが指定されていない場合は、すべての仮想ルータに関するルーティング情報を表示します。パラメータが指定されている場合は、指定のルータに関するルーティング情報や、該当する場合には、指定のルーティングプロトコルタイプを表示します。パラメータはすべてオプションです。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

### アクセス (Access)

基本

### 構文

```
show routing-table name [ ospf | rip | static ]
```

*name* は、情報を必要とする特定のルータ名です。ospf、rip、static は、ルーティングプロトコルタイプを指定します。

**例**

```
> show routing-table Vrouter1 static
```

## serial-number

シャーシのシリアル番号を表示します。このコマンドは NGIPsv では使用できません。

**アクセス (Access)**

基本

**構文**

```
show serial-number
```

**例**

```
> show serial-number
```

## ssl-policy-config

現在適用されている SSL ポリシーの設定（ポリシーの説明、デフォルトのロギング設定、有効なすべての SSL ルールとルールの設定など）、信頼できる CA 証明書、および復号化不可能なトラフィックのアクションを表示します。

**アクセス (Access)**

基本

**構文**

```
show ssl-policy-config
```

**例**

```
> show ssl-policy-config
```

## stacking

管理対象デバイスのスタッキングの設定とポジションを表示します。プライマリとして設定されているデバイスでは、すべてのセカンダリデバイスのデータも示されます。高可用性ペアの

スタックの場合、このコマンドは、スタックが高可用性ペアのメンバーであることも示します。スタッキングを有効または無効にする（大半の場合は無効にする）には、ユーザは Web インターフェイスを使用する必要があります。スタッキングが有効になっていない場合、コマンドは `Stacking not currently configured` というメッセージを返します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

### アクセス (Access)

基本

### 構文

```
show stacking
```

### 例

```
> show stacking
```

## summary

デバイスに関して最もよく使用される情報（バージョン、タイプ、UUID など）のサマリーを表示します。詳細は次の `show` コマンドを参照してください。 `version`、`interfaces`、`device-settings`、および `access-control-config`。

### アクセス (Access)

基本

### 構文

```
show summary
```

### 例

```
> show summary
```

## syslog

システムのログを時系列の逆順で表示します。オプションでフィルタを指定して、ページビューごとに表示するコンテンツとレコード数に基づいて（デフォルトは25）、特定のレコードを表示できます。

### アクセス (Access)

基本

## 構文

```
show syslog ["filter" records_per_page]
```

*filter* が Grep 互換の検索フィルタを指定し、*records\_per\_page* が各ページビューに表示するレコード数を指定する場合。検索フィルタの詳細については、「[システムログフィルタの構文 \(2782 ページ\)](#)」を参照してください。

## 例

```
> show syslog "ssh" 20
```

システムは文字列「ssh」を含む 20 件の直近の syslog レコードを表示します。次の 20 件のレコードを表示するには Enter キーを押し、表示を停止するには q を入力します。

# 時刻

現在の日付と時刻を、UTC および現行のユーザに設定されているローカルタイムゾーンで表示します。

## アクセス (Access)

基本

## 構文

```
show time
```

## 例

```
> show time
```

# traffic-statistics

パラメータが指定されていない場合は、すべてのポートから送信された、および受信したバイトの詳細情報を表示します。ポートが指定されている場合は、指定されたポートの情報のみを表示します。ASA FirePOWER モジュールに対してポートを指定することはできません。システムはデータプレーンインターフェイスのみを表示します。

## アクセス (Access)

基本

## 構文

```
show traffic-statistics port
```

ここで *port* は、情報を表示させたい特定のポートです。

## 例

```
> show traffic-statistics s1p1
```

## user

NGIPSv のみに適用できます。指定されたユーザに関する設定の詳細情報を表示します。次の値が表示されます。

- Login : ログイン名
- UID : ユーザ ID (数値)
- Auth (Local または Remote) : ユーザがどのように認証されているか
- Access (Basic または Config) : ユーザの権限レベル
- Enabled (Enabled または Disabled) : ユーザがアクティブかどうか
- Reset (Yes または No) : 次のログイン時にユーザがパスワードを変更する必要があるかどうか
- Exp (Never または数値) : ユーザのパスワード変更が必要になるまでの日数
- Warn (N/A または数値) : パスワードの有効期限が切れる前に、ユーザがパスワード変更のために与えられる日数
- Str (Yes または No) : ユーザのパスワードが強度チェックの基準を満たす必要があるかどうか
- Lock (Yes または No) : ログインの失敗が多すぎる場合に、ユーザのアカウントがロックされるかどうか
- Max (N/A または数値) : ユーザのアカウントがロックされる前に失敗するログインの最大回数

## アクセス (Access)

設定 (Configuration)

## 構文

```
show user username username username ...
```

ここで *username* はユーザの名前を表します。複数の *username* はスペースで区切って指定します。

#### 例

```
> show user jdoe
```

## ユーザ

NGIPSV のみに適用できます。すべてのローカルユーザの設定の詳細情報を表示します。次の値が表示されます。

- **Login** : ログイン名
- **UID** : ユーザ ID (数値)
- **Auth** (Local または Remote) : ユーザがどのように認証されているか
- **Access** (Basic または Config) : ユーザの権限レベル
- **Enabled** (Enabled または Disabled) : ユーザがアクティブかどうか
- **Reset** (Yes または No) : 次のログイン時にユーザがパスワードを変更する必要があるかどうか
- **Exp** (Never または数値) : ユーザのパスワード変更が必要になるまでの日数
- **Warn** (N/A または数値) : パスワードの有効期限が切れる前に、ユーザがパスワード変更のために与えられる日数
- **Str** (Yes または No) : ユーザのパスワードが強度チェックの基準を満たす必要があるかどうか
- **Lock** (Yes または No) : ログインの失敗が多すぎる場合に、ユーザのアカウントがロックされるかどうか
- **Max** (N/A または数値) : ユーザのアカウントがロックされる前に失敗するログインの最大回数

### アクセス (Access)

設定 (Configuration)

### 構文

```
show users
```

## 例

```
> show users
```

## version

製品のバージョンとビルドを表示します。**detail** パラメータが指定されている場合は、追加のコンポーネントのバージョンが表示されます。

### アクセス (Access)

基本

### 構文

```
show version [detail]
```

## 例

```
> show version
```

## virtual-routers

パラメータが指定されていない場合は、現在設定されているすべての仮想ルータのリスト、および DHCP リレー、OSPF、および RIP の情報が表示されます。パラメータが指定されている場合は、指定されたルータに関する情報が、指定されたルートタイプによって制限されて表示されます。パラメータはすべてオプションです。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

### アクセス (Access)

基本

### 構文

```
show virtual-routers [ dhcprelay | ospf | rip ] name
```

ここで `dhcprelay`、`ospf`、および `rip` はルートタイプを表します。`name` は、情報を表示する特定のルータの名前を表します。`ospf` を指定した場合は、ルートタイプ、および（存在する場合は）ルート名に対して `neighbors`、`topology`、または `lsadb` を指定することができます。

## 例

```
> show virtual-routers ospf VRouter2
```



## virtual-switches

パラメータが指定されていない場合は、設定されているすべての仮想スイッチのリストが表示されます。パラメータが指定されている場合は、指定されたスイッチに関する情報が表示されます。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

### アクセス (Access)

基本

構文

```
show virtual-switches name
```

例

```
> show virtual-switches Vswitch1
```

## vmware-tools

VMware Tools が、仮想デバイス上で現在有効になっているかどうかを示します。このコマンドは、NGIPSv のみで使用できます。

VMware ツールは、仮想マシンのパフォーマンスを向上させるためのユーティリティスイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。このシステムは、すべての仮想アプライアンスで次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup

VMware ツールおよびサポートされるプラグインの詳細については、VMware の Web サイト (<http://www.vmware.com>) を参照してください。

### アクセス (Access)

基本

構文

```
show vmware-tools
```

**例**

```
> show vmware-tools
```

## VPN コマンド

show VPN コマンドは、VPN ステータス、および VPN 接続の設定情報を表示します。このコマンドは、NGIPSv デバイスと ASA FirePOWER デバイスでは使用できません。

**アクセス (Access)**

基本

**config**

すべての VPN 接続の設定を表示します。

**構文**

```
show vpn config
```

**例**

```
> show vpn config
```

**config by virtual router**

仮想ルータについて、すべての VPN 接続の設定を表示します。

**構文**

```
show vpn config virtual router
```

**例**

```
> show vpn config VRouter1
```

**status**

VPN 接続すべてのステータスを表示します。

**構文**

```
show vpn status
```

**例**

```
> show vpn status
```

**status by virtual router**

仮想ルータについて、すべての VPN 接続のステータスを表示します。

**構文**

```
show vpn status virtual router
```

**例**

```
> show vpn status VRouter1
```

**counters**

すべての VPN 接続のカウンタを表示します。

**構文**

```
show vpn counters
```

**例**

```
> show vpn counters
```

**counters by virtual router**

仮想ルータについて、すべての VPN 接続のカウンタを表示します。

**構文**

```
show vpn counters virtual router
```

**例**

```
> show vpn counters VRouter1
```

# コンフィギュレーションコマンド

コンフィギュレーションコマンドを使用して、システムを設定および管理することができます。これらのコマンドはシステムの動作に影響を与えます。そのため、基本 (Basic) レベルのパスワード設定 (configure password) コマンドを除き、設定 CLI アクセス権限を持つユーザのみがこれらのコマンドを発行できます。

## audit\_cert コマンド

audit\_cert コマンドは、安全性監査ログストリーミングを行うためにデバイスの監査ログクライアント証明書の設定を行います。

### アクセス (Access)

設定 (Configuration)

## 削除

セキュアな監査ログストリーミングの現行のクライアント証明書を削除します。

### 構文

```
configure audit_cert delete
```

### 例

```
> configure audit_cert delete
```

## import

セキュアな監査ログストリーミングのクライアント証明書をインポートします。ユーザは、コマンドを入力すると、クライアント証明書と秘密キー、または証明書チェーンを CLI から入力するように求められます。

### 構文

```
configure audit_cert import
```

### 例

```
> configure audit_cert import
*****Import Audit Client Certificate*****

1 Import Client Certificate and Private Key
```

```

2 Import Certificate Chain
0 Exit

*****
Enter choice: 1
Enter your audit client certificate (PEM format) here:
-----BEGIN CERTIFICATE-----
MIIEoTCCA4mgAwIBAgICAR4wDQYJKOZIhvcNaQALBWAugYICzAJBqNVBATYAIVT
...certificate details ...
Tx*FAhnXeUZ78hFepglyHQMWTkd7hCqmSN3UkAb1l0IoBcxTA==
-----END CERTIFICATE-----

Enter your private key (PEM format) here:
-----BEGIN RSA PRIVATE KEY-----
miiieOWobabkc3qwaOgVx0Tt61eY83Mrqa+bek_qPetcHRAW6ea4p0TlMVVsE7qr
...private key details ...
nRI6QNkoumLUT9EvjF6bFoT3M6eDI7+NdDIhjVeOP*E4+hxEX50jM
-----END RSA PRIVATE KEY-----

Client certificate import succeed, exiting...

```

## bypass

7000 または 8000 シリーズ デバイスで、インライン ペアをフェールオープン（ハードウェアバイパス）モードまたはフェールクローズモードにします。このコマンドは、インラインセットの [バイパス モード (Bypass Mode) ] オプションが [バイパス (Bypass) ] に設定されている場合にのみ使用できます。

デバイスを再起動するとインラインセットのフェールオープンモードが解除されるということに注意してください。

### アクセス (Access)

#### 設定 (Configuration)

#### 構文

```
configure bypass {open | close} {interface}
```

ここで、interface はインライン ペアのいずれかのハードウェア ポートの名前です。

#### 例

```
> configure bypass open slp1
```

## high-availability

デバイスで高可用性のバイパスを無効にしたり、設定したりします。このコマンドは、NGIPSv、ASA FirePOWER、またはセカンダリ スタック メンバとして設定されているデバイスでは使用できません。

**アクセス (Access)**

設定 (Configuration)

**構文**

```
configure high-availability {disable | bypass}
```

**例**

```
> configure high-availability disable
```

**gui**

デバイスの Web インターフェイス（システムのメジャーな更新時に表示される、簡潔なアップグレード Web インターフェイスなど）を有効または無効にします。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

**アクセス (Access)**

設定 (Configuration)

**構文**

```
configure gui [enable | disable]
```

**例**

```
> configure gui disable
```

**lcd**

デバイスの正面の LCD ディスプレイを有効または無効にします。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

**アクセス (Access)**

設定 (Configuration)

**構文**

```
configure lcd {enable | disable}
```

### 例

```
> configure lcd disable
```

## log-ips-connections

記録された侵入イベントに関連付けられている接続イベントのロギングを有効または無効にします。

### アクセス (Access)

設定 (Configuration)

### 構文

```
configure log-ips-connections {enable | disable}
```

### 例

```
> configure log-ips-connections disable
```

## manager コマンド

`configure manager` コマンドは、管理元の Firepower Management Center へのデバイスの接続を設定します。

### アクセス (Access)

設定 (Configuration)

## 追加

管理元の Firepower Management Center からの接続を承認するようデバイスを設定します。このコマンドは、デバイスがアクティブに管理されていない場合にのみ機能します。

デバイスを Firepower Management Center に登録するには、常に一意の英数字の登録キーが必要です。ほとんどの場合は、登録キーと一緒にホスト名または IP アドレスを指定する必要があります。ただし、デバイスと Firepower Management Center が NAT デバイスによって分離されている場合は、登録キーと一緒に一意の NAT ID を入力し、ホスト名の代わりに `DONTRESOLVE` を指定します。

### 構文

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey  
[nat_id]
```

ここで、{hostname | IPv4\_address | IPv6\_address | DONTRESOLVE} は、このデバイスを管理する Firepower Management Center の DNS ホスト名、または IP アドレス (IPv4 または IPv6) を指定します。Firepower Management Center を直接アドレス指定できない場合は、DONTRESOLVE を使用します。DONTRESOLVE を使用する場合は nat\_id が必要です。regkey は、デバイスを Firepower Management Center に登録するために必要な一意の英数字の登録キーです。nat\_id は、Firepower Management Center とデバイス間の登録プロセスで使用される任意の英数字の文字列です。hostname が DONTRESOLVE に設定されている場合に必要です。

#### 例

```
> configure manager add DONTRESOLVE abc123 efg456
```

## 削除

Firepower Management Center の接続情報をデバイスから削除します。このコマンドは、デバイスがアクティブに管理されていない場合のみ機能します。

#### 構文

```
configure manager delete
```

#### 例

```
> configure manager delete
```

## mpls-depth

管理インターフェイスで MPLS レイヤの数を設定します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

#### アクセス (Access)

設定 (Configuration)

#### 構文

```
configure mpls-depth depth
```

ここで *depth* は 0~6 の数値です。

#### 例

```
> configure mpls-depth 3
```



## network コマンド

`configure network` コマンドは、デバイスの管理インターフェイスを設定します。

アクセス (Access)

設定 (Configuration)

### dns searchdomains

DNS 検索ドメインの現行のリストを、コマンドで指定されたリストに置き換えます。

構文

```
configure network dns searchdomains {searchlist}
```

`searchlist` はカンマで区切られたドメインのリストです。

例

```
> configure network dns searchdomains foo.bar.com,bar.com
```

### dns servers

DNS サーバの現行のリストを、コマンドで指定されたリストに置き換えます。

構文

```
configure network dns servers {dnslist}
```

`dnslist` は、カンマで区切られた DNS サーバのリストです。

例

```
> configure network dns servers 10.123.1.10,10.124.1.10
```

### hostname

デバイスのホスト名を設定します。

構文

```
configure network hostname {name}
```

`name` は新しいホスト名です。

**例**

```
> configure network hostname sfrocks
```

**http-proxy**

7000 & 8000 シリーズ および NGIPSv デバイスで、HTTP プロキシを設定します。コマンドを発行した後で、CLI はユーザに対して HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかを尋ねます。認証が必要な場合はプロキシのユーザ名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

NGIPSv 上でこのコマンドを使用して、HTTP プロキシサーバを設定し、仮想デバイスが動的解析のためにファイルを AMP クラウドへ送信できるようにします。

**構文**

```
configure network http-proxy
```

**例**

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address:
Enter HTTP Proxy Port:
Use Proxy Authentication? (y/n) [n]:
Enter Proxy Username:
Enter Proxy Password:
Confirm Proxy Password:
```

**http-proxy-disable**

7000 シリーズ、8000 シリーズ、または NGIPSv デバイスで、任意の HTTP プロキシの設定を削除します。

**構文**

```
configure network http-proxy-disable
```

**例**

```
> configure network http-proxy-disable
Are you sure that you wish to delete the current
http-proxy configuration? (y/n):
```

**ipv4 delete**

デバイスの管理インターフェイスの IPv4 設定を無効にします。

## 構文

```
configure network ipv4 delete [management_interface]
```

ここで、*management\_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベントインターフェイスでは **eth1** です。

## 例

```
> configure network ipv4 delete eth1
```

## ipv4 dhcp

デバイスの管理インターフェイスの IPv4 設定を DHCP に設定します。管理インターフェイスは DHCP サーバと通信して、設定情報を取得します。

## 構文

```
configure network ipv4 dhcp [management_interface]
```

ここで、*management\_interface* は管理インターフェイス ID です。DHCP はデフォルトの管理インターフェイスでのみサポートされているため、この引数を使用する必要はありません。

## 例

```
> configure network ipv4 dhcp
```

## ipv4 manual

デバイスの管理インターフェイスの IPv4 設定を手動で設定します。

## 構文

```
configure network ipv4 manual ipaddr netmask [gw] [management_interface]
```

ここで *ipaddr* は IP アドレスで、*netmask* はサブネットマスク、*gw* はデフォルト ゲートウェイの IPv4 アドレスです。*management\_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラット

フォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベントインターフェイスでは **eth1** です。

#### 例

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

## ipv6 delete

デバイスの管理インターフェイスの IPv6 設定を無効にします。

#### 構文

```
configure network ipv6 delete [management_interface]
```

ここで、*management\_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベントインターフェイスでは **eth1** です。

#### 例

```
> configure network ipv6 delete
```

## ipv6 dhcp

デバイスの管理インターフェイスの IPv6 設定を DHCP に設定します。管理インターフェイスは DHCP サーバと通信して、設定情報を取得します。

#### 構文

```
configure network ipv6 dhcp [management_interface]
```

ここで、*management\_interface* は管理インターフェイス ID です。DHCP はデフォルトの管理インターフェイスでのみサポートされているため、この引数を使用する必要はありません。

#### 例

```
> configure network ipv6 dhcp
```

## ipv6 manual

デバイスの管理インターフェイスの IPv6 設定を手動で設定します。

### 構文

```
configure network ipv6 manual ip6addr/ip6prefix [ip6gw] [management_interface]
```

ここで *ip6addr/ip6prefix* は IP アドレスとプレフィックス長、*ip6gw* はデフォルト ゲートウェイの IPv6 アドレスを表します。*management\_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベントインターフェイスでは **eth1** です。

### 例

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

## ipv6 router

デバイスの管理インターフェイスの IPv6 設定をルータに設定します。管理インターフェイスは IPv6 ルータと通信して、設定情報を取得します。

### 構文

```
configure network ipv6 router [management_interface]
```

ここで、*management\_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベントインターフェイスでは **eth1** です。

### 例

```
> configure network ipv6 router
```

## management-interface disable

管理インターフェイスを無効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

### 構文

```
configure network management-interface disable ethn
```

*n* は、設定する管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベント インターフェイスです。シスコでは、管理チャンネルとイベントチャンネルの両方を有効にして、**eth0** デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、[管理インターフェイス \(931 ページ\)](#) を参照してください。

### 例

```
> configure network management-interface disable eth1
```

## management-interface disable-event-channel

指定された管理インターフェイスでイベント トラフィック チャンネルを無効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

### 構文

```
configure network management-interface disable-event-channel ethn
```

*n* は、設定する管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベント インターフェイスです。シスコでは、管理チャンネルとイベントチャンネルの両方を有効にして、**eth0** デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、[管理インターフェイス \(931 ページ\)](#) を参照してください。

### 例

```
> configure network management-interface disable-event-channel eth1
```

## management-interface disable-management-channel

指定された管理インターフェイスで管理トラフィック チャンネルを無効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

## 構文

```
configure network management-interface disable-management-channel ethn
```

$n$  は、設定する管理インターフェイスの数です。 **eth0** デフォルト管理インターフェイスです。 **eth1** はオプションのイベント インターフェイスです。 シスコでは、管理チャンネルとイベントチャンネルの両方を有効にして、**eth0** デフォルト管理インターフェイスを有効のままにすることを推奨しています。 Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、 [管理インターフェイス \(931 ページ\)](#) を参照してください。

## 例

```
> configure network management-interface disable-management-channel eth1
```

## management-interface enable

指定した管理インターフェイスを有効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

## 構文

```
configure network management-interface enable ethn
```

$n$  は、有効にする管理インターフェイスの数です。 **eth0** デフォルト管理インターフェイスです。 **eth1** はオプションのイベント インターフェイスです。

デバイスを管理する場合、Firepower Management Center 管理インターフェイスには2つの別個のトラフィックチャンネルがあります。管理トラフィックチャンネルはすべての内部トラフィック（デバイスの管理に固有のデバイス間トラフィックなど）を伝送し、イベントトラフィックチャンネルはすべてイベントトラフィック（Web イベントなど）を伝送します。必要に応じて、Management Center で個別のイベント専用インターフェイスを設定し、イベントトラフィックを処理することもできます（Firepower Management Center Web インタフェースで、この設定が実行されていることを確認してください）。イベント専用インターフェイスは1つだけ設定できます。イベントトラフィックは大量の帯域幅を使用する可能性があるため、管理トラフィックからイベントトラフィックを分離することで、Management Center のパフォーマンスを向上させることができます。

デフォルトの **eth0** インターフェイスには、デフォルトで管理とイベントチャンネルの両方が含まれています。必要に応じて、イベント専用インターフェイスとして **eth0** インターフェイスを有効にできます。可能であれば、デバイスイベントインターフェイスと Firepower Management Center イベント インターフェイスの間で、イベントトラフィックが送信されます。イベントネットワークがダウンすると、イベントトラフィックは、デフォルトの管理インターフェイスに戻ります。可能な場合には別個のイベント インターフェイスが使用されますが、管理インターフェイスが常にバックアップとなります。

管理インターフェイスを有効にすると、管理とイベントチャンネルの両方がデフォルトで有効にされます。管理チャンネルとイベントチャンネルの両方にデフォルト管理インターフェイスを使

用することをお勧めします。その後、別個のイベント専用インターフェイスを有効にします。Firepower Management Center イベント専用インターフェイスは管理チャンネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャンネルを単に無効にしてください。

**configure network {ipv4|ipv6} manual** コマンドを使用して、管理インターフェイスのアドレスを設定します。

#### 例

```
> configure network management-interface enable eth1
> configure network management-interface disable-management-channel eth1
```

## management-interface enable-event-channel

指定された管理インターフェイスでイベント トラフィック チャンネルを有効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

#### 構文

```
configure network management-interface enable-event-channel ethn
```

*n* は、設定する管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベント インターフェイスです。シスコでは、管理チャンネルとイベントチャンネルの両方を有効にして、**eth0** デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベントインターフェイスを使用する方法の詳細については、[管理インターフェイス \(931 ページ\)](#) を参照してください。

#### 例

```
> configure network management-interface enable-event-channel eth1
```

## management-interface enable-management-channel

指定された管理インターフェイスで管理トラフィックチャンネルを有効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

#### 構文

```
configure network management-interface enable-management-channel ethn
```

*n* は、設定する管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベント インターフェイスです。シスコでは、管理チャンネルとイベント



チャンネルの両方を有効にして、eth0 デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベントインターフェイスを使用する方法の詳細については、[管理インターフェイス \(931 ページ\)](#) を参照してください。

#### 例

```
> configure network management-interface enable-management-channel eth1
```

## management-interface tcpport

管理用の TCP ポートの値を変更します。

#### 構文

```
configure network management-interface tcpport port
```

*port* は設定する管理ポートの値です。

#### 例

```
> configure network management-interface tcpport 8500
```

## management-port

デバイスの TCP 管理ポートの値を設定します。

#### 構文

```
configure network management-port number
```

*number* は設定する管理ポートの値を表します。

#### 例

```
> configure network management-port 8500
```

## static-routes ipv4 add

指定した管理インターフェイスの IPv4 スタティック ルートを追加します。

#### 構文

```
configure network static-routes ipv4  
add interface destination netmask gateway
```

**interface** は管理インターフェイス、**destination** は宛先 IP アドレス、**netmask** はネットワーク マスク アドレス、**gateway** は追加するゲートウェイ アドレスです。

#### 例

```
> configure network static-routes ipv4
add eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

## static-routes ipv4 delete

指定した管理インターフェイスの IPv4 スタティック ルートを削除します。

#### 構文

```
configure network static-routes ipv4
delete interface destination netmask gateway
```

**interface** は管理インターフェイス、**destination** は宛先 IP アドレス、**netmask** はネットワーク マスク アドレス、**gateway** は削除するゲートウェイ アドレスです。

#### 例

```
> configure network static-routes ipv4
delete eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

## static-routes ipv6 add

指定した管理インターフェイスの IPv6 スタティック ルートを追加します。

#### 構文

```
configure network static-routes ipv6
add interface destination prefix gateway
```

**interface** は管理インターフェイス、**destination** は宛先 IP アドレス、**prefix** は IPv6 プレフィックス長、**gateway** は追加するゲートウェイ アドレスです。

#### 例

```
> configure network static-routes ipv6
add eth1 2001:DB8:3ffe:1900:4545:3:200: f8ff:fe21:67cf 64
```

## static-routes ipv6 delete

指定した管理インターフェイスの IPv6 スタティック ルートを削除します。

## 構文

```
configure network static-routes ipv6  
delete interface destination prefix gateway
```

`interface` は管理インターフェイス、`destination` は宛先 IP アドレス、`prefix` は IPv6 プレフィックス長、`gateway` は削除するゲートウェイアドレスです。

## 例

```
> configure network static-routes ipv6  
delete eth1 2001:DB8:3ffe:1900:4545:3:200:f8ff: fe21:67cf 64
```

# password

現行のユーザは、自身のパスワードを変更することができます。コマンドを発行すると、CLI は現在の（古い）パスワードを入力するようユーザに要求し、その後で新しいパスワードを 2 回入力するよう要求します。

## アクセス (Access)

### 基本

## 構文

```
configure password
```

## 例

```
> configure password  
Enter current password:  
Enter new password:  
Confirm new password:
```

# スタッキングの無効化

7000 および 8000 シリーズのデバイスでは、次のデバイスに存在するスタック構成はすべて削除されます。

- プライマリとして設定されているデバイスでは、スタックは完全に削除されます。
- セカンダリとして設定されているデバイスでは、そのデバイスはスタックから削除されません。

このコマンドは、NGIPSv または ASA FirePOWER モジュールでは使用できません。また、これを使用してデバイスの高可用性ペアを解除することはできません。

スタッキング階層の上位アプライアンスとの通信を確立できない場合は、このコマンドを使用します。Firepower Management Centerを通信で使用できる場合は、代わりにFirepower Management CenterのWebインターフェイスを使用するよう伝えるメッセージが表示されます。同様に、プライマリデバイスを使用できる場合に、セカンダリとして設定されているデバイス上でstacking disableを入力すると、プライマリデバイスからコマンドを入力するよう伝えるメッセージが表示されます。

### アクセス (Access)

設定 (Configuration)

#### 構文

```
configure stacking disable
```

#### 例

```
> configure stacking disable
```

## user コマンド

NGIPSvでのみ使用できます。configure user コマンドは、デバイスのローカルユーザデータベースを管理します。

### アクセス (Access)

設定 (Configuration)

## アクセス

指定したユーザのアクセスレベルを変更します。このコマンドは、指定されたユーザが次にログインするときに有効になります。

#### 構文

```
configure user access username [basic | config]
```

*username* は、アクセスを変更するユーザの名前を表します。basicはbasicアクセスを、configはconfigurationアクセスを表します。

#### 例

```
> configure user access jdoe basic
```

## 追加

指定された名前とアクセスレベルを使用して新しいユーザを作成します。このコマンドでは、ユーザのパスワードを入力するよう要求されます。

### 構文

```
configure user add username [basic | config]
```

ここで、**username** は新しいユーザの名前を指定します。basic は基本アクセス、config は設定アクセスを表します。

### 例

```
> configure user add jdoe basic
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

## aging

ユーザのパスワードに有効期限を設定します。

### 構文

```
configure user aging username max_days warn_days
```

ここで、**username** はユーザの名前、**max\_days** はパスワードが有効な最大日数、**warn\_days** は有効期限が切れる前にユーザがパスワードを変更するために確保されている日数を表します。

### 例

```
> configure user aging jdoe 100 3
```

## 削除

ユーザとユーザのホームディレクトリを削除します。

### 構文

```
configure user delete username
```

**username** はユーザの名前を表します。

### 例

```
> configure user delete jdoe
```

## disable

ユーザを無効にします。無効なユーザはログインできません。

### 構文

```
configure user disable username
```

*username* はユーザの名前を表します。

### 例

```
> configure user disable jdoe
```

## enable

ユーザを有効にします。

### 構文

```
configure user enable username
```

*username* はユーザの名前を指定します。

### 例

```
> configure user enable jdoe
```

## forcereset

ユーザが次にログインするときに、パスワードの変更を要求します。ユーザがログインしてパスワードを変更すると、強度のチェックが自動的に有効になります。

### 構文

```
configure user forcereset username
```

*username* はユーザの名前を表します。

### 例

```
> configure user forcereset jdoe
```

## maxfailedlogins

指定したユーザが、ログインで失敗できる最大回数を設定します。

### 構文

```
configure user maxfailedlogins username number
```

*username* はユーザの名前、*number* は、ログインで失敗できる最大回数を表します。

### 例

```
> configure user maxfailedlogins jdoe 3
```

## password

ユーザのパスワードを設定します。このコマンドでは、ユーザのパスワードを入力するよう要求されます。

### 構文

```
configure user password username
```

*username* はユーザの名前を表します。

### 例

```
> configure user password jdoe
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

## strengthcheck

ユーザのパスワードに対する強度の要件を有効または無効にします。ユーザパスワードの有効期限が切れた場合、または `configure user forcereset` コマンドを使用した場合は、ユーザが次にログインしたときにこの要件が自動的に有効になります。

### 構文

```
configure user strengthcheck username {enable | disable}
```

*username* はユーザの名前を表します。enable は指定されたユーザのパスワードの要件を設定し、disable は、指定されたユーザのパスワードの要件を削除します。

### 例

```
> configure user strengthcheck jdoe enable
```

## unlock

ログイン失敗の最大数を超過したユーザをロック解除します。

## 構文

```
configure user unlock username
```

*username* はユーザの名前を表します。

## 例

```
> configure user unlock jdoe
```

# vmware-tools

NGIPSv での VMware Tools の機能を有効または無効にします。このコマンドは、NGIPSv のみで使用できます。

VMware ツールは、仮想マシンのパフォーマンスを向上させるためのユーティリティスイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。このシステムは、すべての仮想アプライアンスで次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup

VMware ツールおよびサポートされるプラグインの詳細については、VMware の Web サイト (<http://www.vmware.com>) を参照してください。

## アクセス (Access)

### 基本

### 構文

```
configure vmware-tools [enable | disable]
```

### 例

```
> configure vmware-tools enable
```



## system コマンド

system コマンドを使用して、システム全体のファイルおよびアクセス コントロールの設定を管理することができます。Configuration CLI アクセス権を持つユーザのみが、システム モードでコマンドを発行できます。

## アクセス制御コマンド

system access-control コマンドは、ユーザがデバイス上でアクセス制御設定を管理できるようにします。

アクセス (**Access**)  
設定 (Configuration)

### archive

現在展開されているアクセス コントロール ポリシーをテキスト ファイルとして /var/common に保存します。

#### 構文

```
system access-control archive
```

#### 例

```
> system access-control archive
```

### clear-rule-counts

アクセス コントロール ルールのヒット数を 0 にリセットします。

#### 構文

```
system access-control clear-rule-counts
```

#### 例

```
> system access-control clear-rule-counts
```

### rollback

これまでに導入されたアクセス制御設定に対して、システムの復帰を行います。このコマンドをスタックまたは高可用性ペアのデバイスで使用することはできません。

### 構文

```
system access-control rollback
```

### 例

```
> system access-control rollback
```

## コンプライアンス コマンド

コンプライアンス (compliance) コマンドは、デバイスのセキュリティ認定コンプライアンスモードの表示、設定を行います。



---

**注意** この設定を有効にすると、無効化することはできません。無効化する必要がある場合は、サポート窓口にご連絡ください。

---

### アクセス (Access)

#### 設定 (Configuration)

## enable cc

デバイスのセキュリティ認定準拠をコモンクライテリア (CC) モードに設定します。



---

**注意** この設定を有効にした後は、無効にすることはできません。無効にする必要がある場合は、サポートにお問い合わせください。

---

### 構文

```
system compliance enable cc
```

### 例

```
> system compliance enable cc
```

## enable ucapl

デバイスのセキュリティ認定準拠を統合機能承認取得済み製品リスト (UCAPL) モードに設定します。



**注意** この設定を有効にした後は、無効にすることはできません。無効にする必要がある場合は、サポートにお問い合わせください。

#### 構文

```
system compliance enable ucapl
```

#### 例

```
> system compliance enable ucapl
```

## show

デバイスの現在のセキュリティ認定のコンプライアンス モードを表示します。

#### 構文

```
system compliance show
```

#### 例

```
> system compliance show
```

## disable-http-user-cert

システム上に存在するすべての HTTP ユーザ証明書を削除します。

#### アクセス (Access)

#### 設定 (Configuration)

#### 構文

```
system disable-http-user-cert
```

#### 例

```
> system disable-http-user-cert
```

## file コマンド

`system file` コマンドを使用すると、ユーザは、デバイス上の `common` ディレクトリにあるファイルを管理することができます。

### アクセス (Access)

設定 (Configuration)

## copy

FTP を使用して、ログインユーザ名を使用しているホスト上のリモートロケーションへファイルを転送します。ローカルファイルは `common` ディレクトリに配置する必要があります。

### 構文

```
system file copy hostname username path filenames filenames ...
```

`hostname` はターゲットのリモートホストの名前または IP アドレスを表します。`username` はリモートホスト上のユーザの名前、`path` はリモートホスト上の宛先パス、`filenames` は転送するローカルファイルを表します。複数のファイル名はスペースで区切って指定します。

### 例

```
> system file copy sfrocks jdoe /pub *
```

## 削除

`common` ディレクトリから、指定したファイルを削除します。

### 構文

```
system file delete filenames filenames ...
```

`filenames` は削除するファイルを指定します。複数のファイル名はスペースで区切って指定します。

### 例

```
> system file delete *
```

## list

ファイル名が指定されていない場合は、`common` ディレクトリ内のすべてのファイルについて変更の時刻、サイズ、およびファイル名が表示されます。ファイル名が指定されている場合

は、指定されたファイル名と一致したファイルで、変更の時刻、サイズ、およびファイル名が表示されます。

### 構文

```
system file list filenames
```

*filenames* は表示するファイルを表します。複数のファイル名はスペースで区切って指定します。

### 例

```
> system file list
```

## secure-copy

SCP を使用して、ログインユーザ名でホストのリモートロケーションにファイルを転送します。ローカルファイルは、`/var/common` ディレクトリに配置する必要があります。

### 構文

```
system file secure-copy hostname username path filenames filenames ...
```

*hostname* では、対象のリモートホストの名前または IP アドレスを指定します。*username* では、リモートホストのユーザ名を指定します。*path* では、リモートホストの宛先パスを指定します。*filenames* では、転送するローカルファイルを指定します。ファイル名はスペースで区切ります。

### 例

```
> system file secure-copy 10.123.31.1 jdoe /tmp *
```

## generate-troubleshoot

シスコが解析に使用するトラブルシューティングデータを生成します。

### アクセス (Access)

### 設定 (Configuration)

### 構文

```
system generate-troubleshoot
```

この構文は、どのトラブルシューティングデータを表示するかを指定するための、オプションのパラメータのリストを表示します。

## 例

```
> system generate-troubleshoot
```

## ldapsearch

ユーザが、指定されたLDAPサーバのクエリを実行できるようにします。すべてのパラメータが必須であることに注意してください。

### アクセス (Access)

設定 (Configuration)

### 構文

```
system ldapsearch host port baseDN userDN basefilter
```

hostはLDAPサーバのドメイン、portはLDAPサーバのポート、baseDNは検索するDN（識別名）、userDNはLDAPディレクトリへバンドするユーザのDN、basefilterは検索するレコードを表します。

## 例

```
> system ldapsearch ldap.example.com 389 cn=users,  
dc=example,dc=com cn=user1,cn=users,dc=example,dc=com, cn=user2
```

## lockdown-sensor

expert コマンドを削除し、デバイス上の bash シェルへアクセスします。



**注意** このコマンドは、サポートからのホットフィックスがない場合は取り消すことはできません。使用には注意が必要です。

### アクセス (Access)

設定 (Configuration)

### 構文

```
system lockdown-sensor
```

**例**

```
> system lockdown-sensor
```

## nat rollback

以前に適用していたNATの設定に、システムを戻します。このコマンドはNGIPSvまたはASA FirePOWERでは使用できません。このコマンドをスタックまたは高可用性ペアのデバイスで使用することはできません。

**アクセス (Access)**

設定 (Configuration)

**構文**

```
system nat rollback
```

**例**

```
> system nat rollback
```

## reboot

デバイスをリブートします。

**アクセス (Access)**

設定 (Configuration)

**構文**

```
system reboot
```

**例**

```
> system reboot
```

## restart

デバイスのアプリケーションを再起動します。

**アクセス (Access)**

設定 (Configuration)

**構文**

```
system restart
```

**例**

```
> system restart
```

## support コマンド

system support コマンドを使用することで、デバイス上の特殊な SSL ClientHello 処理を管理できます。

**アクセス (Access)**

設定 (Configuration)

## ssl-client-hello-display

SSL ハンドシェイク時に ClientHello メッセージを処理するための現在の設定を表示します。これらの設定の説明については、ssl-client-hello-enabled および ssl-client-hello-tuning コマンドを参照してください。

**アクセス (Access)**

基本

**構文**

```
system support ssl-client-hello-display
```

**例**

```
> system support ssl-client-hello-display
```

## ssl-client-hello-enabled

SSL ハンドシェイク時に ClientHello メッセージの特殊な処理を制御します。



**注意** サポートからの指示がない限り、このコマンドは使用しないでください。



## アクセス (Access)

### 設定 (Configuration)

#### 構文

```
system support ssl-client-hello-enabled setting {true | false}
```

*Setting* に指定できる値は次のとおりです。

#### feature

ClientHello メッセージのすべての特殊な処理を制御します。

#### curves

Firepower システムでサポートされていない楕円曲線の削除を制御します。

- **true** (有効) : サポートされていないすべての楕円曲線を ClientHello メッセージから削除し、トラフィックの復号の確率が向上します。 **extensions** 設定を有効にする必要もあります。
- **false** (無効) : ClientHello メッセージ内のサポートされていない楕円曲線を保持し、トラフィックの復号の確率が低下します。

#### ciphers

Firepower システムでサポートされていない暗号スイートの削除を制御します。

- **true** (有効) : サポートされていない暗号スイートを ClientHello メッセージから削除し、トラフィックの復号の確率が向上します。
- **false** (無効) : ClientHello メッセージ内のサポートされていない暗号スイートを保持します。これによりトラフィックの復号の確率が低下し、関連する接続イベントの SSL Flow Error フィールドで多数の Unsupported エラーや Unknown Cipher エラーが発生する可能性があります。

#### 内線番号

復号を妨げる TLS 拡張の削除を制御します。

- **true** (有効) : 復号を妨げる TLS 拡張を特定し、ClientHello メッセージから削除します。 **curves**、**session\_ticket**、および **alpn** を有効にする場合、この値を指定する必要があります。
- **false** (無効) : ClientHello メッセージ内のすべての TLS 拡張を保持します。これによりトラフィックの復号の確率が低下し、関連する接続イベントの SSL Flow Error フィールドで Unknown Session エラーが発生する可能性があります。

#### session\_ticket

ClientHello メッセージの SessionTicket 拡張の処理を制御します。システムが着信 ClientHello メッセージ内の SessionTicket 値をキャッシュされたセッションデータと照合できる場合、クライアントとサーバで完全な SSL ハンドシェイクが実行されなくてもセッションを再開できます。

- `true` (有効) : 認識されない `SessionTicket` 値を `ClientHello` メッセージから削除します。これにより、再開されたセッションでトラフィックの復号の確率が向上します。`extensions` 設定を有効にする必要もあります。
- `false` (無効) : `ClientHello` メッセージ内のすべての `SessionTicket` 値を保持します。これによりトラフィックの復号の確率が低下し、関連する接続イベントの `SSL Flow Error` フィールドで `Uncached Session` エラーが発生する可能性があります。

### `session_id`

`ClientHello` メッセージのセッション識別子要素の処理を制御します。システムが着信 `ClientHello` メッセージ内のセッション識別子をキャッシュされたセッションデータと照合できる場合、クライアントとサーバで完全な `SSL` ハンドシェイクが実行されなくてもセッションを再開できます。

- `true` (有効) : 認識されないセッション識別子値を `ClientHello` メッセージから削除します。これにより、再開されたセッションでトラフィックの復号の確率が向上します。
- `false` (無効) : `ClientHello` メッセージ内のすべてのセッション識別子値を保持します。これによりトラフィックの復号の確率が低下し、関連する接続イベントの `SSL Flow Error` フィールドで `Uncached Session` エラーが発生する可能性があります。

### `alpn`

復号できない `ALPN` プロトコル値、特に `SPDY` および `HTTP2` プロトコルの削除を制御します。

- `true` (有効) : クライアントが `SPDY` または `HTTP2` セッションを確立することを禁止し、トラフィックの復号および検査の確率が向上します。`extensions` 設定を有効にする必要もあります。
- `false` (無効) : クライアントがサーバと `SPDY` または `HTTP2` セッションを確立することを許可し、トラフィックの復号および検査の確率が低下します。

### `compression`

`ClientHello` メッセージからの `TLS` 圧縮要求の削除を制御します。

- `true` (有効) : クライアントがサーバと `TLS` 圧縮セッションを確立することを禁止します。
- `false` (無効) : クライアントがサーバと `TLS` 圧縮セッションを確立することを許可します。これによりセッションのトラフィックの復号が妨げられ、関連する接続イベントの `SSL Flow Error` フィールドで `Compression Used` エラーが発生する可能性があります。

### 例

```
> system support ssl-client-hello-enabled feature false
```

## ssl-client-hello-force-reset

デフォルト値に処理する ClientHello メッセージの設定可能な設定をリセットします。システムはユーザの確認を必要とせず続行します。



---

**注意** サポートからの指示がない限り、このコマンドは使用しないでください。

---

### アクセス (Access)

設定 (Configuration)

### 構文

```
system support ssl-client-hello-force-reset
```

### 例

```
> system support ssl-client-hello-force-reset
```

## ssl-client-hello-reset

デフォルト値に処理する ClientHello メッセージの設定可能な設定をリセットします。システムは、続行する前にユーザの確認を必要とします。



---

**注意** サポートからの指示がない限り、このコマンドは使用しないでください。

---

### アクセス (Access)

設定 (Configuration)

### 構文

```
system support ssl-client-hello-reset
```

### 例

```
> system support ssl-client-hello-reset
```

## ssl-client-hello-tuning

SSLハンドシェイク時に管理対象デバイスが ClientHello メッセージをどのように変更するか調整できます。このコマンドは、ClientHello メッセージで許可される暗号スイート、楕円曲線、および拡張のデフォルトリストを調整します。このコマンドは、許可される値のデフォルト

リストにエントリを追加するか、許可される値のデフォルトリストからエントリを削除するだけです。デフォルトリストは上書きされません。



**注意** サポートからの指示がない限り、このコマンドは使用しないでください。

## アクセス (Access)

### 設定 (Configuration)

#### 構文

```
system support ssl-client-hello-tuning setting value
```

*value* 要素は値のカンマ区切りのリストをサポートします。*setting* および *value* 要素の設定可能な値には次が含まれます。

設定	システムのアクション	値
ciphers_allow	ClientHello メッセージで指定された暗号スイートを許可します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージで指定された暗号スイートを保持します。	IANA の Web サイトから個々の暗号スイートの数を取得します。 <a href="https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4">https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4</a>  IANA は 16 進数の値を提供します。このコマンドを使用してそれらを 10 進数に変換します。
ciphers_remove	ClientHello メッセージで指定された暗号スイートを拒否します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージから指定された暗号スイートを削除します。	

設定	システムのアクション	値
curves_allow	ClientHello メッセージで指定された楕円曲線を許可します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージで指定された楕円曲線を保持します。	IANA の Web サイトから曲線の数を取得します。 <a href="https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8">https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8</a>
curves_remove	ClientHello メッセージで指定された楕円曲線を拒否します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージから指定された楕円曲線を削除します。	
extensions_allow	ClientHello メッセージで指定された拡張を許可します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージで指定された拡張を保持します。	IANA の Web サイトから拡張の数を取得します。 <a href="https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xhtml">https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xhtml</a>
extensions_remove	ClientHello メッセージで指定された楕円曲線を拒否します。システムは変更するすべての ClientHello メッセージから指定された拡張を削除します。デフォルトでは、システムは拡張 22、23、および 30032 を拒否します。	

## 例

```
> system support ssl-client-hello-tuning ciphers_allow 4,7,16,22
```

## shutdown

デバイスをシャットダウンします。このコマンドは ASA FirePOWER モジュールでは使用できません。

アクセス (**Access**)

設定 (Configuration)

構文

```
system shutdown
```

例

```
> system shutdown
```