Firepower Management Center バージョン 6.0 コンフィギュレーション ガイド

初版：2015 年 11 月 11 日

最終更新：2017 年 06 月 21 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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

目 次

第 1 章

Firepower の概要

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

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

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

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

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

- *ASA with FirePOWER Services Local Management Configuration Guide*

管理対象デバイスの概要

ネットワークセグメントにインストールされている管理対象デバイスは、分析のためにトラフィックを監視します。パッシブな展開の場合、管理対象デバイスは、ホスト、オペレーティング システム、アプリケーション、ユーザ、送信されたファイル（マルウェアを含む）、脆弱性など、組織の資産に関する詳細情報を収集します。Firepowerシステムがこの情報を分析用に関連付けることで、ユーザがアクセスするWebサイトと使用するアプリケーションをモニタし、トラフィックパターンを評価して、侵入や他の攻撃の通知を受信できます。

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

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

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

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

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

7000 および 8000 シリーズ 管理対象デバイス

Cisco Firepower 7000 および 8000 シリーズ アプライアンスは、Firepower システム用に作られた物理デバイスです。7000 および 8000 シリーズ デバイスのスループットはさまざまですが、多数の同じ機能を共有します。一般に、8000 シリーズ デバイスは 7000 シリーズ よりも高性能で、8000 シリーズ 高速パス ルール、リンク集約、およびスタックなどの追加機能もサポートします。

NGIPSv

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

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

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

Cisco ASA with FirePOWER Services

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

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

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

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

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

従来のデバイス モデルによるネットワーク管理機能

Firepowerシステムの従来のデバイスのスループットと機能は、モデルおよびライセンスによって異なります。次の表で、システムのネットワーク管理機能と 7000 および 8000 シリーズ デバイス、および有効にする必要があるライセンスが一致します。従来のデバイスのすべてのモデルは、アクセス制御を実行できます。

表 *1*：各デバイス モデルでサポートされる管理およびネットワーク管理機能

機能	7000 & 8000 シリーズ	ASA FirePOWER	NGIPSv	従来のライセンス
トラフィック チャネル	Yes	No	No	任意（Any）
複数の管理インターフェイス	Yes	No	No	任意（Any）
リンク集約	Yes	No	No	任意（Any）
Firepower システムの Web インターフェイス	限定的	No	No	任意（Any）
制限された（補助）コマンドライン インターフェイス（CLI）	Yes	Yes	Yes	任意（Any）
外部認証	Yes	No	No	任意（Any）
eStreamer クライアントへの接続	Yes	Yes	No	任意（Any）
自動アプリケーション バイパス	Yes	Yes	Yes	任意（Any）
タップ モード（tap mode）	Yes	No	No	任意（Any）
8000 シリーズ 高速パス ルール	8000 シリーズ	No	No	任意（Any）
厳密な TCP の適用	Yes	No	No	Protection
インライン セットのバイパス モード	NetMod/SFP によって異なる	No	No	Protection

機能	7000 & 8000 シリーズ	ASA FirePOWER	NGIPSv	従来のライセンス
マルウェア ストレージ パック	Yes	No	No	マルウェア
スイッチング、ルーティング、スイッチドおよびルーテッド集約インターフェイス	Yes	No	No	Control
NAT ポリシー	Yes	No	No	Control
デバイス スタッキング	8140 82xx ファミリ 83xx ファミリ	No	No	任意（Any）
デバイスのハイ アベイラビリティ	Yes	No	No	Control
デバイス スタック高可用性	8140 82xx ファミリ 83xx ファミリ	No	No	Control
VPN	Yes	No	No	VPN

関連トピック

Firepower Management Center の機能, （6 ページ）

Firepower Management Center の概要

Firepower Management Center は、Firepower システム展開の一元的な管理コンソールとデータベース リポジトリを提供するフォールト トレラントな専用ネットワーク アプライアンスです。また、VMware vSphere と KVM（カーネル ベースの仮想マシン）ハイパーバイザ環境を使用して、また Amazon Web Services（AWS）クラウド プラットフォームを使用して、64 ビットの仮想 Firepower Management Center を展開することもできます。Firepower Management Center は、さまざまなデバイス管理、イベント保存、ホスト モニタリング、およびユーザ モニタリング機能を備えています。どの Firepower Management Center でも、任意の種類の Firepower システム デバイスを管理することができます。

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

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

- デバイス、ライセンス、およびポリシー管理

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

Firepower Management Center の機能

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

Firepower Management Center Web インターフェイスで利用可能な機能の構成は、管理しているデバイスのライセンスやモデルによって制限されていることがあります。
MC4000 では、シスコのユニファイド コンピューティング システム（UCS）プラットフォームが Firepower システムに導入されます。MC4000 は、ベースボード管理コントローラ（BMC）上で UCS Manager や Cisco Integrated Management Controller（CIMC）などのツールを使用するシスコの機能をサポートしないことに注意してください。

関連トピック

従来のデバイス モデルによるネットワーク管理機能, （4 ページ）
デバイス管理, （457 ページ）
データベース イベント数の制限の設定, （562 ページ）

バージョン 6.0 付属のアプライアンス

表 *2*：バージョン *6.0 Firepower* システムの *Management Center* とデバイス

モデル/ファミリ	シリーズ/グループ	タイプ（Type）
70xx ファミリ。 • Firepower 7010、7020、7030、7050	Firepower 7000 シリーズ、FirePOWER ソフトウェア、クラシック デバイス	デバイス
71xx ファミリ。 • Firepower 7110、7120 • Firepower 7115、7125 • AMP7150	Firepower 7000 シリーズ、FirePOWER ソフトウェア、クラシック デバイス	デバイス

モデル/ファミリ	シリーズ/グループ	タイプ（Type）
81xx ファミリ。 • Firepower 8120、8130、8140 • AMP8050 • AMP8150	Firepower 8000 シリーズ、FirePOWER ソフトウェア、従来のデバイス	デバイス
82xx ファミリ。 • Firepower 8250 • Firepower 8260、8270、8290	Firepower 8000 シリーズ、FirePOWER ソフトウェア、従来のデバイス	デバイス
83xx ファミリ。 • Firepower 8350 • Firepower 8360、8370、8390 • AMP8350 • AMP8360/8370/8390	Firepower 8000 シリーズ、FirePOWER ソフトウェア、従来のデバイス	デバイス
NGIPSv 64 ビット仮想デバイス	従来のデバイス	デバイス
ASA 5585-X の ASA FirePOWER	ASA with FirePOWER サービス	ASA FirePOWER ハードウェア モジュール
ASA 5000 X シリーズの ASA FirePOWER • ASA 5506-X • ASA 5506H-X • ASA 5506W-X • ASA 5508-X • ASA 5512-X • ASA 5515-X • ASA 5516-X • ASA 5525-X • ASA 5545-X • ASA 5555-X	ASA with FirePOWER サービス	ASA FirePOWER ソフトウェア モジュール

モデル/ファミリ	シリーズ/グループ	タイプ（Type）
Firepower Management Center • MC750、MC1500、MC3500 • MC2000、MC4000	Management Center	Management Center
64 ビット仮想 Firepower Management Center	Management Center	Management Center

Firepower システムのコンポーネント

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

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

冗長性およびリソース共有

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

デバイス スタッキング

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

7000 および 8000 シリーズ デバイスのハイ アベイラビリティ

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

ほとんどの場合、SFRP を使用することによって、ハイ アベイラビリティ ペアを構成することなくレイヤ 3 の冗長性を実現できます。SFRP では、指定した IP アドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。ネットワークの冗長性では、2 つ以上のデバイ

スまたはスタックが同じネットワーク接続を提供し、ネットワーク上の他のホストに対する接続性を保証するよう設定することができます。

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

Firepower システムのネットワーク トラフィック管理機能を使用すれば、7000 および 8000 シリーズ デバイスを組織のネットワーク インフラストラクチャの一部として機能させることができます。ユーザは、スイッチド、ルーテッド、または（この両者を組み合わせた）ハイブリッドの環境内で機能するよう 7000 および 8000 シリーズ のデバイスを設定し、ネットワーク アドレス変換（NAT）を実行することができます。また、安全な仮想プライベート ネットワーク（VPN）トンネルを構築することができます。

スイッチング（Switching）

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

ルーティング

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

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

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

NAT

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

VPN

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

マルチテナント機能

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

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

検出とアイデンティティ

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

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

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

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

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

アクセス制御

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

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

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

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

SSL インスペクション

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

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

侵入検知と防御

侵入検知および侵入防御は、トラフィックが宛先に許可される前のシステムの最後の防御ラインです。侵入ポリシーは、アクセスコントロールポリシーによって呼び出される侵入検知および侵

入防御の設定の定義済みセットです。侵入ルールおよびその他の設定を使用して、これらのポリシーはセキュリティ違反がないかトラフィックを検査し、インライン展開では、悪意のあるトラフィックをブロックまたは変更できます。

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

システムが提供するポリシーが組織のセキュリティのニーズに十分に対応していない場合は、カスタム ポリシーを作成することで、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。設定できるカスタム ポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

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

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

ファイル制御

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

AMP for Firepower

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

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

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

AMP for Endpoint の統合

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

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

ネットワーク ファイル トラジェクトリ

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

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

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

Cisco AMP プライベート クラウド仮想アプライアンス

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

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

Cisco AMP Threat Grid オンプレミス アプライアンス

組織にパブリックの AMP Threat Grid クラウドへのファイルの送信に関してプライバシーまたはセキュリティ上の懸念がある場合、オンプレミスの AMP Threat Grid アプライアンスを展開すること

ができます。このオンプレミスアプライアンスは、パブリック クラウドと同様に適格なファイルをサンドボックス環境で実行し、脅威スコアと動的分析レポートを Firepower システムに返します。ただし、このオンプレミス アプライアンスは、ご使用のネットワークの外部にあるパブリック クラウドや他のすべてのシステムとは通信しません。

アプリケーション プログラミング インターフェイス

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

eStreamer

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

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

外部データベース アクセス

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

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

ホスト入力

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

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

修復

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

Firepower のオンライン ヘルプとドキュメンテーション

オンライン ヘルプには、Web インターフェイスからアクセスできます。

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

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

ドキュメンテーションのライセンス ステートメント

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

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

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

ライセンスの詳細については、Firepower の機能ライセンスについて，（127 ページ）を参照してください。

関連トピック

従来のデバイス モデルによるネットワーク管理機能，（4 ページ）
Firepower の機能ライセンスについて，（127 ページ）

ドキュメント内のサポート対象デバイスに関する記述

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

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

ドキュメント内のアクセス ステートメント

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

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

ユーザ ロールの詳細については、定義済みのユーザ ロール, （50 ページ）およびカスタム ユーザ ロール, （52 ページ）を参照してください。

Firepower システムの IP アドレス表記法

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

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

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

第 I 部

ユーザ アカウント

第 2 章

Firepower システムへのログイン

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

Firepower システムのユーザ アカウント

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

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

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

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

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

Firepower Management Center

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

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

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

7000 & 8000 シリーズ デバイス

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

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

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

NGIPSv デバイス

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

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

ASA FirePOWER デバイス

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

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

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

Firepower システムのユーザ インターフェイス

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

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

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

表 *3*：アプライアンス別のローカル アクセス

アプライアンス	グラフィカルユーザインターフェイス	CLI アクセス	Linux シェルへのアクセス
Firepower Management Center	• Firepower Web インターフェイス • 事前定義された admin ユーザとカスタムユーザアカウントでサポートされます • アドミニストレーティブタスク、管理タスク、分析タスクに使用することができます	none	• 事前定義された admin ユーザでサポートされます • シリアルまたはキーボードを使用してアクセス可能であり、接続をモニタできます • Cisco TAC の指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください
7000 & 8000 シリーズ デバイス	• Firepower Web インターフェイス • 事前定義された admin ユーザとカスタムユーザアカウントでサポートされます • 初期設定、基本的な分析、および設定タスクに使用することができます	• 事前定義された admin ユーザとカスタム ユーザ アカウントでサポートされます • SSH 接続を使用してアクセスできます • Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます	• 事前定義された admin ユーザとカスタム ユーザ アカウントでサポートされます • **Configuration** アクセス権を持つ CLI ユーザが expert コマンドを使用してアクセスできます • Cisco TAC の指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください

アプライアンス	グラフィカルユーザインターフェイス	CLI アクセス	Linux シェルへのアクセス
NGIPSv デバイス	none	• 事前定義された admin ユーザとカスタム ユーザ アカウントでサポートされます • SSH 接続を使用してアクセスできます • Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます	• 事前定義された admin ユーザとカスタム ユーザ アカウントでサポートされます • **Configuration** アクセス権を持つ CLI ユーザが expert コマンドを使用してアクセスできます • Cisco TAC の指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください

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

Web インターフェイスに関する考慮事項

- 組織が認証に共通アクセス カード（CAC）を使用している場合は、CAC クレデンシャルを使用してアプライアンスの Web インターフェイスにアクセスすることができます。
- Web セッション時にアプライアンスのホーム ページに初めてアクセスした際に、そのアプライアンスに対する最後のログイン セッションに関する情報を表示できます。最後のログインについて、次の情報を表示できます。
  - ログインの曜日、月、日、年
  - ログイン時のアプライアンスのローカル時間（24 時間表記）
  - アプライアンスにアクセスするために最後に使用されたホストとドメイン名
- デフォルトのホーム ページの上部に表示されるメニューおよびメニュー オプションは、ユーザ アカウントの権限に基づきます。ただし、デフォルト ホームページのリンクには、ユー

ザアカウントの権限の範囲に対応するオプションが含まれています。アカウントに付与されている権限とは異なる権限が必要なリンクをクリックすると、システムから警告メッセージが表示され、そのアクティビティがログに記録されます。

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

関連トピック

ホームページの指定, （37 ページ）

セッションのタイムアウト（Session Timeout）

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

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

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

関連トピック

セッション タイムアウトの設定, （609 ページ）

Web インターフェイスによる Firepower Management Center へのログイン

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

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

はじめる前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- Cisco Firepower Management Center Getting Started Guide for Models 750, 1500, 2000, 3500 and 4000 およびユーザ アカウントの作成, （78 ページ） の説明に従って、初期セットアップ手順を完了し、ユーザ アカウントを作成します。

手順

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

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

- ユーザ名は大文字/小文字を区別しません。
- マルチドメイン導入環境では、ユーザアカウントが作成されたドメインをユーザ名の前に付加します。先祖ドメインを前に付加する必要はありません。たとえばユーザ アカウントを SubdomainB で作成し、そのドメインの先祖ドメインが DomainA である場合、次の形式でユーザ名を入力します。

  ```
  SubdomainB\username
  ```

- 組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が `1111` で、SecurID トークンが `222222` の場合は、`1111222222` と入力します。Firepower システムにログインする前に、SecurID PIN を生成しておく必要があります。

ステップ 3 [ログイン（Login）] をクリックします。

関連トピック

セッションのタイムアウト（Session Timeout）, （24 ページ）

Web インターフェイスによる管理対象デバイスへのログイン

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

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

はじめる前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- デバイスに該当する Firepower クイック スタート ガイドおよびユーザ アカウントの作成，（78 ページ） の説明に従って、初期セットアップ手順を完了し、ユーザ アカウントを作成します。

手順

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

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

- ユーザ名は大文字/小文字を区別しません。
- 組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が `1111` で、SecurID トークンが `222222` の場合は、`1111222222` と入力します。Firepower システムにログインする前に、SecurID PIN を生成しておく必要があります。

ステップ 3 [ログイン（Login）] をクリックします。

関連トピック

セッションのタイムアウト（Session Timeout），（24 ページ）

CAC クレデンシャルを使用した Firepower Management Center へのログイン

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

ユーザは単一のアクティブなセッションに制限されます。

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

はじめる前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- Cisco Firepower Management Center Getting Started Guide for Models 750, 1500, 2000, 3500 and 4000 およびユーザ アカウントの作成, （78 ページ） の説明に従って、初期セットアップ手順を完了し、ユーザ アカウントを作成します。
- CAC 認証の設定, （91 ページ）の説明に従って、CAC の認証と認可を設定します。

手順

ステップ 1 組織の指示に従って CAC を挿入します。

ステップ 2 ブラウザで `https://hostname/` にアクセスします。ここで、*hostname* は Firepower Management Center のホスト名に対応します。

ステップ 3 プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられた PIN を入力します。

ステップ 4 プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。

ステップ 5 [続行（Continue）] をクリックします。

関連トピック

CAC 認証, （90 ページ）
セッションのタイムアウト（Session Timeout）, （24 ページ）

CAC クレデンシャルを使用した管理対象デバイスへのログイン

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

ユーザは単一のアクティブなセッションに制限されます。

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

はじめる前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- デバイスに該当する Firepower クイック スタート ガイドおよびユーザ アカウントの作成, （78 ページ） の説明に従って、初期セットアップ手順を完了し、ユーザ アカウントを作成します。
- CAC 認証の設定, （91 ページ）の説明に従って、CAC の認証と認可を設定します。

手順

ステップ 1 組織の指示に従って CAC を挿入します。

ステップ 2 ブラウザで `https://hostname/` にアクセスします。ここで、*hostname* はアクセスするアプライアンスのホスト名に対応します。

ステップ 3 プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられた PIN を入力します。

ステップ 4 プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。

ステップ 5 [続行（Continue）] をクリックします。

関連トピック

CAC 認証, （90 ページ）
セッションのタイムアウト（Session Timeout）, （24 ページ）

コマンドライン インターフェイスへのログイン

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

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

はじめる前に

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

- 7000 & 8000 シリーズ デバイスで、ユーザ アカウントの作成, （78 ページ）の説明に従って、Web インターフェイスでユーザ アカウントを作成します。
- すべてのデバイスで、CLI にログインできる追加のユーザ アカウントを **configure user add** コマンドを使用して作成します。

手順

ステップ 1 SSH を使用して、管理インターフェイスのホスト名または IP アドレスに接続します。または、コンソール ポートに接続することもできます。

ステップ 2 「`log in as:`」コマンド プロンプトに対してユーザ名を入力し、Enter を押します。

ステップ 3 「`Password:`」プロンプトに対してパスワードを入力し、Enter を押します。
組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が `1111` で、SecurID トークンが `222222` の場合は、`1111222222` と入力します。Firepower システムにログインする前に、SecurID PIN を生成しておく必要があります。

ステップ 4 CLI プロンプトで、コマンド ライン アクセスのレベルで許可されている任意のコマンドを使用します。

Web インターフェイスでの基本システム情報の表示

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

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

手順

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

ステップ 2 [バージョン情報（About）] を選択します。

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

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

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

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

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

- 先祖ドメインは表示されますが、使用しているユーザ アカウントに割り当てられた権限に応じて、先祖ドメインへのアクセスが無効である場合があります。
- 兄弟ドメインや子孫ドメインを含め、使用しているユーザ アカウントでアクセスできない他のドメインは非表示になります。

ドメインを切り替えると、以下の項目が表示されます。

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

手順

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

Firepower システム Web インターフェイスからのログアウト

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

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

手順

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

関連トピック

セッションのタイムアウト（Session Timeout），（24 ページ）

コンテキスト メニュー

Firepower システム Web インターフェイスの特定のページでは、右クリック（最も一般的）および左クリックでコンテキスト メニューを表示できます。コンテキスト メニューは、Firepower システム内の他の機能にアクセスするためのショートカットとして使用できます。コンテキスト メニューの内容はどこでこのメニューにアクセスするか（どのページかだけでなく特定のデータにアクセスしているか）によって異なります。

次に例を示します。

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

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

ポリシー エディタ

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

侵入ルール エディタ

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

イベント ビューア

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

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

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

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

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

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

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

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

侵入イベントのパケット ビュー

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

ダッシュボード

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

Context Explorer

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

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

関連トピック

セキュリティ インテリジェンスのリストとフィード, （418 ページ）

第 3 章

ユーザ設定の指定

以下のトピックでは、ユーザ設定を指定する方法について説明します。

ユーザ設定の概要

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

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

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

パスワードの変更

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

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

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

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

手順

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ プリファレンス（User Preferences）] を選択します。

ステップ 2 [現在のパスワード（Current Password）] を入力して、[変更（Change）] をクリックします。

ステップ 3 [新しいパスワード（New Password）] および [確認（Confirm）] フィールドに、新しいパスワードを入力します。

ステップ 4 [変更（Change）] をクリックします。

失効パスワードの変更

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

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

手順

パスワードの有効期限の警告のページには 2 つの選択肢があります。

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

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

- 後でパスワードを変更するには、[後で（Skip）] をクリックします。

ホームページの指定

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

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

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

手順

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 [ホームページ（Home Page）] をクリックします。

ステップ 3 ホーム ページとして使用するページをドロップダウン リストから選択します。
ドロップダウン リスト内のオプションは、ユーザ アカウントのアクセス権限に基づいて表示されます。詳細については、ユーザ アカウントの権限, （53 ページ）を参照してください。

ステップ 4 [Save] をクリックします。

イベント ビュー設定の設定

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

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

手順

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 [イベント ビュー設定（Event View Settings）] をクリックします。

ステップ 3 [イベント設定（Event Preferences）] セクションで、イベント ビューの基本特性を設定します。イベント ビュー設定, （38 ページ）を参照してください。

ステップ 4 [ファイル設定（File Preferences）] セクションで、ファイル ダウンロードを設定します。ファイル ダウンロード設定, （40 ページ）を参照してください。

ステップ 5 [デフォルト時間帯（Default Time Windows）] セクションで、デフォルトの時間帯を設定します。デフォルト時間枠, （41 ページ）を参照してください。

ステップ 6 [デフォルト ワークフロー（Default Workflow）] セクションで、デフォルト ワークフローを設定します。デフォルト ワークフロー, （43 ページ）を参照してください。

ステップ 7 [保存（Save）] をクリックします。

イベント ビュー設定

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

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

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

たとえば、この設定が有効である場合、イベント ビューで [すべて削除（Delete All）] をクリックすると、アプライアンスがデータベースからの削除を実行する前に、現在の制約を満たすすべてのイベント（現在のページに表示されていないイベントを含む）を削除することをユーザが確認する必要があります。

- [IP アドレスの解決（Resolve IP Addresses）] フィールドを使用すると、可能な場合には常に、アプライアンスで IP アドレスの代わりにホスト名がイベント ビューに表示されるようになります。

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

- [パケット ビューの展開（Expand Packet View）] フィールドでは、侵入イベントのパケット ビューをどのように表示するかを設定できます。デフォルトでは、アプライアンスによるパケット ビューの表示は折りたたまれた状態になっています。

  - [なし（None）] : パケット ビューの [パケット情報（Packet Information）] セクションのサブセクションをすべて折りたたんだ状態にします。
  - [パケット テキスト（Packet Text）] : [パケット テキスト（Packet Text）] サブセクションだけを展開します。
  - [パケット バイト（Packet Bytes）] : [パケット バイト（Packet Bytes）] サブセクションだけを展開します。
  - [すべて（All）] : すべてのセクションを展開します。

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

- [1 ページあたりの行数（Rows Per Page）] フィールドは、ドリル ダウン ページとテーブル ビューに表示する、ページごとのイベントの行数を制御します。
- [更新間隔（Refresh Interval）] フィールドは、イベント ビューの更新間隔を分単位で設定します。0 を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。
- [統計更新間隔（Statistics Refresh Interval）] は、[侵入イベント統計（Intrusion Event Statistics）] や [ディスカバリ統計（Discovery Statistics）] ページなどのイベントのサマリー ページの更新間隔を制御します。0 を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。
- [ルールの非アクティブ化（Deactivate Rules）] フィールドは、標準テキスト ルールによって生成される侵入イベントのパケット ビューに、どのリンクを表示させるかを次のように制御します。

  - [すべてのポリシー（All Policies）] : すべてのローカルで定義されたカスタム侵入ポリシーで標準テキスト ルールを非アクティブにする単一リンク

- [現在のポリシー（Current Policy）]：現在展開中の侵入ポリシーだけで標準テキスト ルールを非アクティブにする単一リンク。デフォルトのポリシーのルールは非アクティブにできないことに注意してください。
- [質問（Ask）]：これらの個々のオプションへのリンク

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

関連トピック

管理インターフェイス，（564 ページ）

ファイル ダウンロード設定

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

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

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

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

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

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

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

または不明瞭な文字を表示するかを切り替えます。このフィールドをオフにすると、[zipファイル パスワード（Zip File Password）] には不明瞭な文字が表示されます。

デフォルト時間枠

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

このセクションへのユーザ ロール アクセスは以下のとおりです。

- Administrators と Maintenance Users は、セクション全体にアクセスできます。
- Security Analysts と Security Analysts（読み取り専用）は、[監査ログの時間枠（Audit Log Time Window）] 以外のすべてのオプションにアクセスできます。
- Access Admins、Discovery Admins、External Database Users、Intrusion Admins、Network Admins、および Security Approvers は、[Events Time Window] オプションにのみアクセスできます。

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

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

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

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

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

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

以下の 3 つのタイプの時間枠があります。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

デフォルト ワークフロー

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

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

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

デフォルト タイム ゾーンの設定

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

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

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

手順

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 [タイムゾーン設定（Time Zone Preference）] タブをクリックします。

ステップ 3 左側のリスト ボックスで、使用するタイム ゾーンを含む大陸または地域を選択します。

ステップ 4 右側のリスト ボックスで、使用するタイム ゾーンに対応するゾーン（都市名）を選択します。

ステップ 5 [保存（Save）] をクリックします。

デフォルトのダッシュボードの指定

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

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

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

手順

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 [ダッシュボード設定（Dashboard Settings）] をクリックします。

ステップ 3 デフォルトとして使用するダッシュボードをドロップダウンリストから選択します。[なし（None）] を選択した場合、[概要（Overview）] > [ダッシュボード（Dashboards）] を選択するときに、表示するダッシュボードを選択できます。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

ダッシュボードの表示, （249 ページ）

第 II 部

Firepower システムの管理

第 4 章

Firepower システム ユーザ管理

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

ユーザの役割

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

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

LDAP グループを使用したアクセス権の管理を設定した場合、ユーザのアクセス権は LDAP グループのそのメンバーシップに基づきます。属しているグループの中で最も高いレベルのアクセスを持つグループのデフォルト アクセス権が付与されます。ユーザがどのグループにも属していない場合にグループ アクセスを設定していた場合、ユーザには、LDAP サーバの認証オブジェクトで設定されているデフォルト ユーザ アクセス権が付与されます。グループ アクセスを設定すると、

それらの設定によってプラットフォーム設定ポリシーのデフォルト アクセス設定がオーバーライドされます。

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

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

定義済みのユーザ ロール

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

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

次の表では、利用可能な定義済みのロールを簡単に説明します。

アクセス管理者（Access Admin）

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

管理者（Administrator）

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

セキュリティ上の理由から、管理者ロールの使用を制限する必要があります。

検出管理者（Discovery Admin）

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

外部データベースのユーザ（External Database User）

JDBC SSL 接続に対応しているアプリケーションを用いて、Firepower System データベースに対して読取り専用のアクセスが可能です。Firepower システム アプライアンスの認証を行うサードパーティのアプリケーションについては、システム設定内でデータベースへのアクセスを有効にする必要があります。Web インターフェイスでは、外部データベース ユーザは、[ヘルプ（Help）] メニューのオンライン ヘルプ関連のオプションのみにアクセスできます。このロールの機能は、webインターフェイスに搭載されていないため、サポートやパスワードの変更を容易にするためにのみアクセスが可能です。

侵入管理者（Intrusion Admin）

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

メンテナンス ユーザ（Maintenance User）

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

ネットワーク管理者（Network Admin）

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

セキュリティ アナリスト（Security Analyst）

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

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

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

セキュリティ承認者（Security Approver）

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

外部認証ユーザは、他のロールを割当てられていない場合、LDAP または RADIUS 認証オブジェクトの設定やプラットフォーム設定に基づいて、最低限のアクセス権を有します。追加の権利を

外部ユーザに割り当てることはできますが、最低限のアクセス権を削除するまたは変更するには、以下のタスクを実施する必要があります。

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

関連トピック

ユーザ アカウントの権限, （53 ページ）

カスタム ユーザ ロール

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

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

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

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

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

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

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

関連トピック

ユーザ アカウントの権限, （53 ページ）
外部データベース アクセスの設定, （560 ページ）

例：カスタム ユーザ ロールとアクセス制御

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

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

表 *4*：アクセス制御のカスタム ロールの例

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

ユーザ アカウントの権限

ここでは、Firepower システムでの設定可能なユーザ アクセス許可と、それらのアクセス許可にアクセスできる事前定義ユーザ ロールの一覧を示します。管理対象デバイスでは使用できないアク

セス許可があります。Firepower Management Center でのみ使用可能なアクセス許可には、そのようにマークが付いています。

[概要（Overview）] メニュー

次の表は、[概要（Overview）] メニューの各オプションにアクセスするために必要なユーザ ロール特権と、ユーザ ロールがオプション内のサブ権限にアクセスできるかどうかを順に示しています。Security Approver、Discovery Admin、Intrusion Admin、Access Admin、Network Admin、および External Database User の各ロールには、[概要（Overview）] メニューでのアクセス許可がありません。

表 *5*：*[*概要（*Overview*）*]* メニュー

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

権限	管理	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（**RO**）
[製品ライセンス（Product Licensing）] ウィジェット（*Management Center* のみ）	Yes	Yes	No	No
[製品の更新（Product Updates）] ウィジェット	Yes	Yes	No	No
[RSS フィード（RSS Feed）] ウィジェット	Yes	Yes	Yes	Yes
[システムの負荷（System Load）] ウィジェット	Yes	Yes	Yes	Yes
[システム時刻（System Time）] ウィジェット	Yes	Yes	Yes	Yes
[ホワイトリスト イベント（White List Events）] ウィジェット（*Management Center* のみ）	Yes	No	Yes	Yes
[レポート（Reporting）]（*Management Center* のみ）	Yes	No	Yes	Yes
[レポートの管理テンプレート（Manage Report Templates）]（*Management Center* のみ）	Yes	No	Yes	Yes
要約	Yes	No	Yes	Yes
[侵入イベント統計（Intrusion Event Statistics）]（*Management Center* のみ）	Yes	No	Yes	Yes
侵入イベント パフォーマンス（Intrusion Event Performance）	Yes	No	No	No
[侵入イベント グラフ（Intrusion Event Graphs）]（*Management Center* のみ）	Yes	No	Yes	Yes
[検出統計情報（Discovery Statistics）]（*Management Center* のみ）	Yes	No	Yes	Yes
[ディスカバリ パフォーマンス（Discovery Performance）]（*Management Center* のみ）	Yes	No	No	No
[接続の概要（Connection Summary）]（*Management Center* のみ）	Yes	No	Yes	Yes

[分析（Analysis）] メニュー

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

表 *6* : *[分析（Analysis）] メニュー*

メニュー	管理	検出管理者	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（**RO**）
コンテキスト エクスプローラ（Context Explorer）	Yes	No	No	Yes	Yes
接続イベント	Yes	No	No	Yes	Yes
接続イベントの変更（Modify Connection Events）	Yes	No	No	Yes	No
接続サマリー イベント（Connection Summary Events）	Yes	No	No	Yes	Yes
接続サマリー イベントの変更（Modify Connection Summary Events）	Yes	No	No	Yes	No
セキュリティ インテリジェンス イベント	Yes	No	No	Yes	Yes
セキュリティ インテリジェンス イベントの変更（Modify Security Intelligence Events）	Yes	No	No	Yes	No
侵入（Intrusion）	Yes	No	No	Yes	Yes
侵入イベント	Yes	No	No	Yes	Yes
侵入イベントの変更（Modify Intrusion Events）	Yes	No	No	Yes	No
ローカル ルールの表示（View Local Rules）	Yes	No	No	Yes	Yes
確認済みイベント（Reviewed Events）	Yes	No	No	Yes	Yes
クリップボード（Clipboard）	Yes	No	No	Yes	Yes

メニュー	管理	検出管理者	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（RO）
[インシデント（Incidents）]	Yes	No	No	Yes	Yes
インシデントの変更（Modify Incidents）	Yes	No	No	Yes	No
ファイル（Files）	Yes	No	No	Yes	Yes
マルウェア イベント	Yes	No	No	Yes	Yes
マルウェア イベントの変更（Modify Malware Events）	Yes	No	No	Yes	No
ファイル イベント	Yes	No	No	Yes	Yes
ファイル イベントの変更（Modify File Events）	Yes	No	No	Yes	No
キャプチャ ファイル（Captured Files）	Yes	No	No	Yes	Yes
キャプチャ ファイル（Captured Files）の編集（Modify Captured Files）	Yes	No	No	Yes	No
File Trajectory	Yes	No	No	Yes	Yes
ファイルのダウンロード（File Download）	Yes	No	No	Yes	Yes
ダイナミック ファイル分析（Dynamic File Analysis）	Yes	No	No	Yes	No
Hosts	Yes	No	No	Yes	Yes
ネットワーク マップ（Network Map）	Yes	No	No	Yes	Yes
Hosts	Yes	No	No	Yes	Yes
ホストの変更（Modify Hosts）	Yes	No	No	Yes	No
Indications of Compromise	Yes	No	No	Yes	Yes
侵害の兆候の変更（Modify Indications of Compromise）	Yes	No	No	Yes	No
サーバ	Yes	No	No	Yes	Yes
サーバの変更（Modify Servers）	Yes	No	No	Yes	No

メニュー	管理	検出管理者	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（RO）
脆弱性（Vulnerabilities）	Yes	No	No	Yes	Yes
脆弱性の変更（Modify Vulnerabilities）	Yes	No	No	Yes	No
ホスト属性（Host Attributes）	Yes	No	No	Yes	Yes
ホスト属性の変更（Modify Host Attributes）	Yes	No	No	Yes	No
アプリケーション	Yes	No	No	Yes	Yes
アプリケーション詳細（Application Details）	Yes	No	No	Yes	Yes
アプリケーションの詳細の変更（Modify Application Details）	Yes	No	No	Yes	No
ホスト属性の管理（Host Attribute Management）	Yes	No	No	No	No
検出イベント（Discovery Events）	Yes	No	No	Yes	Yes
検出イベントの変更（Modify Discovery Events）	Yes	No	No	Yes	No
Users	Yes	Yes	No	Yes	Yes
ユーザ アクティビティ（User Activity）	Yes	Yes	No	Yes	Yes
ユーザアクティビティイベントの変更（Modify User Activity Events）	Yes	Yes	No	Yes	No
Users	Yes	Yes	No	Yes	Yes
ユーザの変更（Modify Users）	Yes	Yes	No	Yes	No
脆弱性（Vulnerabilities）	Yes	No	No	Yes	Yes
サードパーティの脆弱性（Third-party Vulnerabilities）	Yes	No	No	Yes	Yes
サードパーティの脆弱性の変更（Modify Third-party Vulnerabilities）	Yes	No	No	Yes	No
相関（Correlation）	Yes	Yes	No	Yes	Yes
相関イベント（Correlation Events）	Yes	Yes	No	Yes	Yes

メニュー	管理	検出管理者	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（RO）
相関イベントの変更（Modify Correlation Events）	Yes	Yes	No	Yes	No
ホワイトリスト イベント（White List Events）	Yes	Yes	No	Yes	Yes
ホワイトリストイベントの変更（Modify White List Events）	Yes	Yes	No	Yes	No
ホワイトリスト違反（White List Violations）	Yes	Yes	No	Yes	Yes
修復ステータス（Remediation Status）	Yes	Yes	No	No	No
修復ステータスの変更（Modify Remediation Status）	Yes	Yes	No	No	No
カスタム（Custom）	Yes	No	No	Yes	Yes
カスタム ワークフロー（Custom Workflows）	Yes	No	No	Yes	Yes
カスタム ワークフローの管理（Manage Custom Workflows）	Yes	No	No	Yes	Yes
カスタム テーブル（Custom Tables）	Yes	No	No	Yes	Yes
カスタム テーブルの管理（Manage Custom Tables）	Yes	No	No	Yes	Yes
検索（Search）	Yes	No	Yes	Yes	Yes
検索の管理（Manage Search）	Yes	No	No	No	No
ブックマーク（Bookmarks）	Yes	No	No	Yes	Yes
ブックマークの管理（Manage Bookmarks）	Yes	No	No	Yes	Yes
アプリケーション統計（Application Statistics）	Yes	No	No	Yes	Yes
地理位置情報の統計（Geolocation Statistics）	Yes	No	No	Yes	Yes
ユーザ統計（User Statistics）	Yes	No	No	Yes	Yes
URL カテゴリ統計（URL Category Statistics）	Yes	No	No	Yes	Yes

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

ポリシー メニュー

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

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

表 7: ポリシー メニュー

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

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
SSL ポリシー（SSL Policy）	Yes	Yes	No	No	Yes	Yes
SSL ポリシーの変更（Modify SSL Policy）	Yes	Yes	No	No	Yes	No
管理者ルールの変更（Modify Administrator Rules）	Yes	Yes	No	No	Yes	No
ルート ルールの変更（Modify Root Rules）	Yes	Yes	No	No	Yes	No
ネットワーク ディスカバリ（Network Discovery）	No	Yes	Yes	No	No	Yes
カスタムフィンガープリント（Custom Fingerprinting）	No	Yes	Yes	No	No	No
カスタム フィンガープリントの変更（Modify Custom Fingerprinting）	No	Yes	Yes	No	No	No
カスタム トポロジ（Custom Topology）	No	Yes	Yes	No	No	No
カスタム トポロジの変更（Modify Custom Topology）	No	Yes	No	No	No	No
ネットワーク検出の変更（Modify Network Discovery）	No	Yes	Yes	No	No	No
アプリケーション ディテクタ（Application Detectors）	No	Yes	Yes	No	No	No
アプリケーション ディテクタの変更（Modify Application Detectors）	No	Yes	Yes	No	No	No
ユーザ サードパーティ マッピング（User 3rd Party Mappings）	No	Yes	Yes	No	No	No
ユーザ サードパーティ マッピングの変更（Modify User 3rd Party Mappings）	No	Yes	No	No	No	No
カスタム製品のマッピング（Custom Product Mappings）	No	Yes	Yes	No	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
カスタム製品マッピングの変更（Modify Custom Product Mappings）	No	Yes	No	No	No	No
相関（Correlation）	No	Yes	No	No	No	No
ポリシーの管理（Policy Management）	No	Yes	No	No	No	No
ポリシーの管理の変更（Modify Policy Management）	No	Yes	Yes	No	No	No
ルールの管理（Rule Management）	No	Yes	No	No	No	No
ルールの管理の変更（Modify Rule Management）	No	Yes	Yes	No	No	No
ホワイト リスト（White List）	No	Yes	No	No	No	No
ホワイトリストの変更（Modify White List）	No	Yes	Yes	No	No	No
トラフィック プロファイル（Traffic Profiles）	No	Yes	No	No	No	No
トラフィック プロファイルの変更（Modify Traffic Profiles）	No	Yes	Yes	No	No	No
アクション（Actions）	No	Yes	Yes	No	No	Yes
アラート（Alerts）	No	Yes	Yes	No	No	Yes
影響度フラグ アラート（Impact Flag Alerts）	No	Yes	Yes	No	No	No
影響度フラグアラートの変更（Modify Impact Flag Alerts）	No	Yes	Yes	No	No	No
検出イベント アラート（Discovery Event Alerts）	No	Yes	Yes	No	No	No
検出イベントアラートの変更（Modify Discovery Event Alerts）	No	Yes	Yes	No	No	No
E メール	No	Yes	No	Yes	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	ネットワーク管理者	セキュリティ承認者
E メールの変更（Modify Email）	No	Yes	No	Yes	No	No
アラートの変更（Modify Alerts）	No	Yes	Yes	No	No	No
スキャナ（Scanners）	No	Yes	Yes	No	No	No
スキャン結果（Scan Results）	No	Yes	Yes	No	No	No
スキャン結果の変更（Modify Scan Results）	No	Yes	Yes	No	No	No
スキャナの変更（Modify Scanners）	No	Yes	Yes	No	No	No
グループ（Groups）	No	Yes	No	No	No	No
グループの変更（Modify Groups）	No	Yes	Yes	No	No	No
モジュール（Modules）	No	Yes	No	No	No	No
モジュールの変更（Modify Modules）	No	Yes	Yes	No	No	No
インスタンス（Instances）	No	Yes	No	No	No	No
インスタンスの変更（Modify Instances）	No	Yes	Yes	No	No	No

[デバイス（Devices）] メニュー

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

表 *8*：*[デバイス（Devices）] メニュー*

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

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

[オブジェクト マネージャ（Object Manager）] メニュー

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

表 *9* : *[オブジェクト マネージャ（Object Manager）] メニュー*

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

Cisco AMP

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

デバイスへの設定の展開

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

[システム（System）] メニュー

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

表 *10* : *[システム（System）]* メニュー

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

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	メンテナンスユーザ	ネットワーク管理者	セキュリティ承認者	セキュリティアナリスト	セキュリティアナリスト（**RO**）
アイデンティティ ソースを変更（Modify Identity Sources）（*Management Center* のみ）	Yes	Yes	No	No	No	Yes	No	No	No
eStreamer	No	Yes	No	No	No	No	No	No	No
ホスト入力クライアント（Host Input Client）（*Management Center* のみ）	No	Yes	No	No	No	No	No	No	No
スマート ソフトウェア サテライト（Smart Software Satellite）（*Management Center* のみ）	Yes	Yes	No	No	No	Yes	Yes	No	No
スマート ソフトウェア サテライトを変更（Modify Smart Software Satellite）（*Management Center* のみ）	Yes	Yes	No	No	No	Yes	No	No	No
ユーザ管理（User Management）	No	Yes	No	No	No	No	No	No	No
Users	No	Yes	No	No	No	No	No	No	No
ユーザの役割	No	Yes	No	No	No	No	No	No	No
外部認証（External Authentication）（*Management Center* のみ）	No	Yes	Yes	No	No	No	No	No	No
変更点	No	Yes	No	No	No	No	No	No	No
ルール更新（Rule Updates）（*Management Center* のみ）	No	Yes	No	Yes	No	No	No	No	No
ルール更新のインポート ログ（Rule Update Import Log）（*Management Center* のみ）	No	Yes	No	No	No	No	No	No	No
ライセンス	No	Yes	No	No	No	No	No	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	メンテナンスユーザ	ネットワーク管理者	セキュリティ承認者	セキュリティアナリスト	セキュリティアナリスト（RO）
スマート ライセンス（Smart Licences）	No	Yes	No	No	No	No	No	No	No
スマート ライセンスの変更（Modify Smart Licenses）	No	Yes	No	No	No	No	No	No	No
クラシック ライセンス（Classic Licenses）	No	Yes	No	No	No	No	No	No	No
正常性（Health）（*Management Center* のみ）	No	Yes	No	No	Yes	No	No	Yes	Yes
正常性ポリシー（Health Policy）（*Management Center* のみ）	No	Yes	No	No	Yes	No	No	Yes	No
正常性ポリシーを変更（Modify Health Policy）（*Management Center* のみ）	No	Yes	No	No	Yes	No	No	Yes	No
正常性ポリシーを適用（Apply Health Policy）（*Management Center* のみ）	No	Yes	No	No	Yes	No	No	Yes	No
ヘルス イベント（Health Events）（*Management Center* のみ）	No	Yes	No	No	Yes	No	No	Yes	Yes
ヘルス イベントを変更（Modify Health Events）（*Management Center* のみ）	No	Yes	No	No	Yes	No	No	Yes	No
モニタリング（Monitoring）	No	Yes	No	No	Yes	Yes	Yes	Yes	No
監査（Audit）	No	Yes	No	No	Yes	No	No	No	No
監査ログを変更（Modify Audit Log）	No	Yes	No	No	Yes	No	No	No	No
Syslog	No	Yes	No	No	Yes	No	No	No	No
統計情報（Statistics）	No	Yes	No	No	Yes	No	No	No	No

メニュー	アクセス管理者	管理者	検出管理者	侵入管理者	メンテナンスユーザ	ネットワーク管理者	セキュリティ承認者	セキュリティアナリスト	セキュリティアナリスト（**RO**）
ツール	No	Yes	No	No	Yes	No	No	Yes	No
バックアップ管理（Backup Management）	No	Yes	No	No	Yes	No	No	No	No
バックアップを復元（Restore Backup）	No	Yes	No	No	Yes	No	No	No	No
スケジューリング（Scheduling）	No	Yes	No	No	Yes	No	No	No	No
その他のユーザのスケジュール済みタスクを削除（Delete Other Users' Scheduled Tasks）	No	Yes	No	No	No	No	No	No	No
インポート/エクスポート（Import/Export）	No	Yes	No	No	No	No	No	No	No
ディスカバリ データの消去（Discovery Data Purge）（*Management Center* のみ）	No	Yes	No	No	No	No	No	Yes	No
whois（*Management Center* のみ）	No	Yes	No	No	Yes	No	No	Yes	Yes

[ヘルプ（Help）] メニュー

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

ユーザ ロールの管理

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

Firepower システムの各ユーザは、ユーザ アクセス ロール（1 つまたは複数）に関連付けられています。これに該当するユーザ ロールには、システムのメニューなどのオプションへのアクセスを

決定する権限が割り当てられます。たとえばアナリストは、ネットワークのセキュリティを分析するためにイベントデータへのアクセスが必要ですが、Firepowerシステム自体の管理機能へのアクセスが必要になることはありません。アナリストにはSecurity Analystのアクセス権を付与し、Firepowerシステムを管理する1人以上のユーザに対してAdministratorロールを予約しておくことができます。

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

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

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

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

手順

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

ステップ2 [ユーザロール（User Roles）]タブをクリックします。

ステップ3 ユーザロールを管理します。

- アクティブ化：事前定義されたユーザロールをアクティブ化または非アクティブ化します。詳細については、ユーザロールのアクティブおよび非アクティブの設定，（71ページ）を参照してください。
- 作成：カスタムユーザロールを作成します。詳細については、次を参照してください。カスタムユーザロールの作成，（72ページ）
- コピー：新しいカスタムユーザロールを作成するために、既存のユーザロールをコピーします。詳細については、ユーザロールのコピー，（72ページ）を参照してください。
- 編集：カスタムユーザロールを編集します。詳細については、カスタムユーザロールの編集，（73ページ）を参照してください。
- 削除：削除するカスタムロールの横にある削除アイコン（  ）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- （注） 削除されたロールが、特定のユーザに割り当てられていた唯一のロールである場合、そのユーザはログインして[ユーザ設定（User Preferences）]メニューにアクセスできますが、Firepowerシステムにはアクセスできなくなります。

ユーザ ロールのアクティブおよび非アクティブの設定

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

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

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

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

手順

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

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

ステップ 3 アクティブまたは非アクティブにするユーザ ロールの横にあるスライダをクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

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

カスタム ユーザ ロールの作成

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

手順

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

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

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

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

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

ステップ 6 新しいロールのメニューベースのアクセス許可を選択します。
アクセス許可を選択すると、その下位にあるアクセス許可もすべて選択され、複数値を持つアクセス許可では最初の値が使用されます。上位のアクセス許可をクリアすると、下位のアクセス許可もすべてクリアされます。アクセス許可を選択しても、下位のアクセス許可を選択しない場合、アクセス許可がイタリックのテキストで表示されます。

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

ステップ 7 必要に応じて、[外部データベース アクセス（External Database Access）] チェックボックスをオンまたはオフにして、新規ロールのデータベース アクセス権限を設定します。

ステップ 8 エスカレーションに使用するカスタム ユーザ ロールの設定, （75 ページ）の説明に従って、必要に応じて Firepower Management Center で、新規ユーザ ロールのエスカレーション アクセス許可を設定します。

ステップ 9 [保存（Save）] をクリックします。

ユーザ ロールのコピー

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

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

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

手順

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

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

ステップ 3 コピーするユーザ ロールの横にあるコピー アイコン（  ）をクリックします。

ステップ 4 新しい名前を入力します。
システムは、元のユーザ ロールの名前と `(copy)` サフィックスを組み合わせた新しいユーザ ロールのデフォルト名を作成します。

ステップ 5 [説明（Description）] ボックスに新しい説明を入力します。
上書きしないことを選択した場合、システムは元のユーザ ロールの説明を保持します。

ステップ 6 オプションで、元のユーザ ロールから継承されたメニュー ベースの権限を変更します。
アクセス許可を選択すると、その下位にあるアクセス許可もすべて選択され、複数値を持つアクセス許可では最初の値が使用されます。上位のアクセス許可をクリアすると、下位のアクセス許可もすべてクリアされます。アクセス許可を選択しても下位のアクセス許可を選択しない場合、そのアクセス許可はイタリック体のテキストで表示されます。

ステップ 7 オプションで、[外部データベース アクセス（External Database Access）] チェックボックスをオンまたはオフにすることで、新しいロールのデータベース アクセス権限を設定します。

ステップ 8 オプションで、エスカレーションに使用するカスタム ユーザ ロールの設定, （75 ページ）の説明に従って、新しいユーザ ロールのエスカレーション権限を設定します。

ステップ 9 [保存（Save）] をクリックします。

カスタム ユーザ ロールの編集

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

事前定義ユーザ ロールは編集できません。

マルチドメイン展開では、現在のドメインで作成されたカスタムユーザ ロールが表示されます。これは編集できます。先祖ドメインで作成されたカスタムユーザ ロールも表示されますが、これ

は編集できません。下位のドメインのカスタムユーザロールを表示および編集するには、そのドメインに切り替えます。

手順

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

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

ステップ 3 変更するカスタムユーザロールの横にある編集アイコン（  ）をクリックします。代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [名前（Name）] フィールドと [説明（Description）] フィールドを変更します。ユーザ ロール名では、大文字と小文字が区別されます。

ステップ 5 ユーザ ロールのメニューベースのアクセス許可を選択します。
アクセス許可を選択すると、その下位にあるアクセス許可もすべて選択され、複数値を持つアクセス許可では最初の値が使用されます。上位のアクセス許可をクリアすると、下位のアクセス許可もすべてクリアされます。アクセス許可を選択しても下位のアクセス許可を選択しない場合、そのアクセス許可はイタリック体のテキストで表示されます。

ステップ 6 必要に応じて、[外部データベース アクセス（External Database Access）] チェックボックスをオンまたはオフにすることにより、ロールのデータベース アクセス権限を設定します。

ステップ 7 必要に応じて、エスカレーションに使用するカスタム ユーザ ロールの設定, （75 ページ）の説明に従って Firepower Management Center で、ユーザ ロールにエスカレーション アクセス許可を設定します。

ステップ 8 [保存（Save）] をクリックします。

ユーザ ロールのエスカレーション

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

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

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

エスカレーション ターゲット ロールの設定

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

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

手順

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

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

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

ステップ 4 ドロップダウン リストからユーザ ロールを選択します。

ステップ 5 [OK] をクリックして変更を保存します。

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

エスカレーションに使用するカスタム ユーザ ロールの設定

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

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

手順

ステップ 1 カスタム ユーザ ロールの作成, （72 ページ）の説明に従って、カスタム ユーザ ロールの設定を開始します。

ステップ 2 [システム権限（System Permissions）] で、[このロールをエスカレーションする：（Set this role to escalate to:）] チェックボックスをオンにします。
現在のエスカレーション ターゲット ロールは、チェックボックスの横に表示されます。

ステップ 3 このロールがエスカレーションするときに使用するパスワードを選択します。次の 2 つの対処法があります。

- このロールが割り当てられているユーザがエスカレーション時に各自のパスワードを使用できるようにするには、[割り当てられているユーザのパスワードで認証（Authenticate with the assigned user's password）] を選択します。
- このロールが割り当てられているユーザが、別のユーザのパスワードを使用するようにするには、[指定されたユーザのパスワードで認証（Authenticate with the specified user's password）] を選択し、そのユーザ名を入力します。

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

ステップ 4 [保存（Save）] をクリックします。
これで、このロールが割り当てられているユーザはターゲットユーザロールにエスカレーションできます。

ユーザ ロールのエスカレーション

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

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

はじめる前に

- 管理者が、エスカレーション ターゲット ロールの設定, （75 ページ）またはエスカレーションに使用するカスタムユーザ ロールの設定, （75 ページ）に従って、エスカレーションター

ゲット ロールまたはカスタム ユーザ ロールをエスカレーション用に設定済みであることを確認してください。

手順

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

ステップ 2 認証パスワードを入力します。

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

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

ユーザ アカウント

Firepower Management Center デバイスまたは Firepower 7000 および 8000 シリーズ デバイス上の管理者アカウント、およびオプションのカスタムのユーザ アカウントを使用すれば、ユーザはこれらのデバイスにログインすることができます。内部認証ユーザについては、アカウントを手動で作成する必要があります。外部認証ユーザについては、アカウントが自動的に作成されます。

関連トピック

Firepower システムのユーザ アカウント
Firepower システムのユーザ インターフェイス

ユーザ アカウントの管理

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

手順

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

ステップ 2 ユーザ アカウントを管理します。

- アクティブ化/非アクティブ化：ユーザの横にあるスライダをクリックすると、非アクティブ化されたユーザの場合は再アクティブ化され、アクティブなユーザアカウントの場合は削除せずに無効化されます。アクティブ化/非アクティブ化できるのは内部で認証されたユーザのみです。
- 作成：新しいユーザ アカウントを作成します（ユーザ アカウントの作成, （78 ページ）を参照）。
- 編集：既存のユーザ アカウントを編集します（ユーザ アカウントの編集, （79 ページ）を参照）。
- 削除：ユーザを削除する場合は、削除アイコン（）をクリックします。adminアカウント以外のユーザ アカウントはシステムからいつでも削除できます。admin アカウントは削除できません。

関連トピック

Lights-Out 管理のユーザ アクセス設定, （613 ページ）
定義済みのユーザ ロール, （50 ページ）
カスタム ユーザ ロール, （52 ページ）

ユーザ アカウントの作成

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

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

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

手順

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

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

ステップ 3 [ユーザ名（User Name）] に入力します。

ステップ 4 ログイン オプションを変更します（ユーザ アカウント ログイン オプション, （81 ページ）を参照）。

ステップ 5 [パスワード（Password）] と [パスワードの確認（Confirm Password）] に値を入力します。
入力する値は、以前に設定したパスワード オプションに基づいている必要があります。

ステップ 6 7000 または 8000 シリーズ デバイスでユーザ アカウントを作成する場合、コマンド ラインのアクセス レベル, （83 ページ）の説明に従って、適切なレベルの [コマンドライン インターフェイス アクセス（Command-Line Interface Access）] を割り当てます。

ステップ 7 次のようにして、ユーザ ロールを割り当てます。

- ユーザに割り当てるユーザ ロールの横のチェックボックスをオンまたはオフにします。
- マルチドメイン展開では、子孫ドメインを持つドメインにユーザ アカウントを追加する場合、ユーザ ロールのチェック ボックスの代わりに表示される [ドメインの追加（Add Domains）] ボタンをクリックします。複数のドメインでのユーザ ロールの割り当て, （80 ページ）の手順に従って進みます。

（注） ユーザ ロールによって、ユーザのアクセス権が決定します。詳細については、ユーザ ロールの管理, （69 ページ）を参照してください。

ステップ 8 [Save] をクリックします。

ユーザ アカウントの編集

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

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

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

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

手順

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

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

ステップ 3 ユーザ アカウントの作成, （78 ページ）の説明に従って設定を変更します。

ステップ 4 [保存（Save）] をクリックします。

複数のドメインでのユーザ ロールの割り当て

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

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

手順

ステップ 1 ユーザ アカウント エディタで、[ドメインの追加（Add Domain）] をクリックします。

ステップ 2 [ドメイン（Domain）] ドロップダウン リストからドメインを選択します。

ステップ 3 ユーザを割り当てるユーザ ロールをオンにします。

ステップ 4 [保存（Save）] をクリックします。

内部認証から外部認証へのユーザの変換

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

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

はじめる前に

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

手順

ステップ 1 LDAP（CAC を使用する場合または使用しない場合）あるいは RADIUS 認証を有効にします。詳細については、LDAP 認証, （88 ページ）またはRADIUS 認証, （113 ページ）を参照してください。

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

ユーザ アカウント ログイン オプション

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

（注）
- パスワード管理オプションは、外部ディレクトリ サーバに対して認証されるユーザには適用されません。これらの設定は外部認証サーバで管理します。[外部認証方式を使用する（Use External Authentication Method）] を有効にすると、ディスプレイからパスワード管理オプションが削除されます。
- アプライアンスで STIG コンプライアンスまたは Lights-Out Management（LOM）を有効にすると、異なるパスワード制限が適用されます。STIG コンプライアンスの詳細については、STIG コンプライアンスの有効化, （603 ページ）を参照してください。

表 *11* : ユーザ アカウント ログイン オプション

オプション	説明
外部認証方式を使用する（Use External Authentication Method）	このユーザの資格情報を外部で認証する場合に、このチェックボックスをオンにします。このオプションを有効にすると、パスワード管理オプションが表示されなくなります。 （注） • 外部ディレクトリ サーバに対してユーザを認証する場合は、使用するサーバの認証オブジェクトを作成し、認証が有効な状態でプラットフォーム設定ポリシーを適用します。 • 外部認証ユーザの場合、サーバの認証オブジェクトを無効にすると、[ユーザ（Users）] リストの [認証方式（Authentication Method）] カラムに [外部（無効）（External (Disabled)）] と表示されます。 • ユーザに対してこのオプションを選択した場合に外部認証サーバが使用できないと、そのユーザは Web インターフェイスにログインできますが、どの機能にもアクセスできません。
ログイン失敗の最大許容回数（Maximum Number of Failed Logins）	各ユーザが、ログイン試行の失敗後に、アカウントがロックされるまでに試行できるログインの最大回数を示す整数を、スペースなしで入力します。デフォルト設定は 5 回です。ログイン失敗回数を無制限にするには、0 を設定します。
パスワード長の最小値（Minimum Password Length）	ユーザのパスワードの必須最小長（文字数）を示す整数を、スペースなしで入力します。デフォルト設定は 8 です。値 0 は、最小長が必須ではないことを示します。 [パスワード強度のチェック（Check Password Strength）] オプションを有効にして、[パスワード長の最小値（Minimum Password Length）] を 8 文字を超える値に設定すると、いずれか大きい値が適用されます。
パスワードの有効期限の残日数（Days Until Password Expiration）	ユーザのパスワードの有効期限までの日数を入力します。デフォルト設定は、パスワードが期限切れにならないことを示す 0 です。このオプションを設定すると、[ユーザ（Users）] リストの [パスワードのライフタイム（Password Lifetime）] カラムに、各ユーザのパスワードの残っている日数が表示されます。
パスワードの有効期限の残日数警告（Days Before Password Expiration Warning）	パスワードが実際に期限切れになる何日前に、ユーザがパスワードを変更する必要があるという警告を表示するかを入力します。デフォルト設定は 0 日間です。 （注） 警告日数は、パスワードの残りの有効期間の日数**未満**である必要があります。
ログイン時にパスワードのリセットを強制（Force Password Reset on Login）	次回ログイン時に、ユーザに強制的に各自のパスワードを変更させるには、このオプションを選択します。

オプション	説明
パスワード強度のチェック（Check Password Strength）	強力なパスワードを必須にするには、このオプションを選択します。強力なパスワードとは、8 文字以上の英数字からなり、大文字と小文字を使用し、1 つ以上の数字と 1 つ以上の特殊文字を使用するパスワードです。辞書に記載されている単語や、同じ文字を連続して繰り返し使用することはできません。
ブラウザセッション タイムアウトから除外する（Exempt from Browser Session Timeout）	操作が行われなかったことが原因でユーザのログインセッションが終了しないようにするには、このオプションを選択します。管理者ロールが割り当てられているユーザを除外することはできません。

コマンド ラインのアクセス レベル

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

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

なし（None）

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

設定（Configuration）

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

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

基本

特定の一連のコマンドはユーザが実行できます。それらは、次のとおりです。

表 *12*：基本的なコマンド ライン コマンド

`configure password`	`interfaces`

終了	lcd
exit	link-state
ヘルプ	log-ips-connection
history	managers
ログアウト	memory
?	model
??	mpls-depth
access-control-config	NAT
alarms	network
arp-tables	network-modules
audit-log	ntp
bypass	perfstats
high-availability	portstats
cpu	power-supply-status
データベース	process-tree
device-settings	processes
disk	routing-table
disk-manager	serial-number
dns	stacking
expert	summary
fan-status	時刻
fastpath-rules	traffic-statistics
gui	version
hostname	virtual-routers

hyperthreading	virtual-switches
inline-sets	

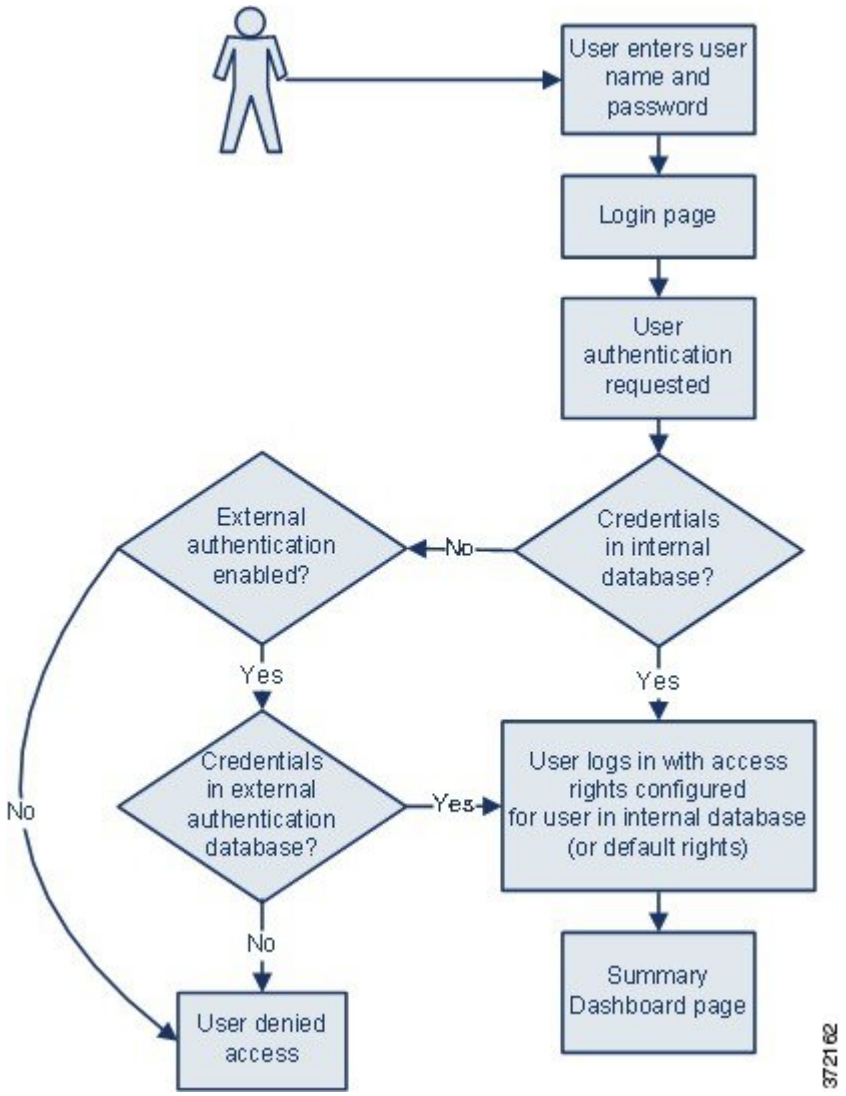
Firepower システムのユーザ認証

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

認証には次の 2 種類あります。

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

認証プロセスは、次のとおりです。



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

内部認証

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

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

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

外部認証（External Authentication）

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

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

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

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

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

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

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

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

関連トピック

LDAP 認証, （88 ページ）
RADIUS 認証, （113 ページ）

LDAP 認証

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

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

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

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

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

LDAP 認証オブジェクトを作成するために必要な情報

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

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

基本的な認証オブジェクトを作成するには、少なくとも以下が必要です。

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

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

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

表 *13*：追加の *LDAP* 設定情報

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

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

CAC 認証

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

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

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

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

CAC 認証の設定

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

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

はじめる前に

- LDAP 認証オブジェクトを作成するために必要な情報, （88 ページ）の説明に従って情報を収集します。

手順

ステップ 1 組織の指示に従い CAC を挿入します。

ステップ 2 ブラウザで `https://hostname/` を開きます（hostname はご使用の Firepower Management Center のホスト名に対応しています）。

ステップ 3 プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられた PIN を入力します。

ステップ 4 プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。

ステップ 5 ログイン ページで、[ユーザ名（Username）] フィールドと [パスワード（Password）] フィールドに、管理者権限を持つユーザとしてログインします。ユーザ名では、大文字と小文字が区別されます。

ヒント CAC 認証および認可の設定が完了するまで、CAC クレデンシャルを使用したログインは**できません**。

ステップ 6 [システム（System）] > [ユーザ（Users）] に移動し、[外部認証（External Authentication）] タブをクリックします。

ステップ 7 および拡張 LDAP 認証オブジェクトの作成, （95 ページ）の手順に従い、CAC 認証および認可専用の LDAP 認証オブジェクトを作成します。次の設定を行う必要があります。

- [LDAP 固有パラメータ（LDAP-Specific Parameters）] セクションの詳細設定オプションの [ユーザ名テンプレート（User Name Template）]。
- [属性マッピング（Attribute Mapping）] セクションの [UI アクセス属性（UI Access Attribute）]。
- [グループ制御アクセス ロール（Group Controlled Access Roles）] セクションの既存の LDAP グループの識別名（LDP グループ メンバーシップによってアクセス権を事前に設定する場合）。

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

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 外部認証の有効化, （632 ページ）の説明に従って、外部認証と CAC 認証を有効にします。

注意 設定変更を展開するまで変更は有効に**なりません**。

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

ステップ 11 HTTPS サーバ証明書をインポートし、必要に応じて サーバ証明書のアップロード, （558 ページ）で説明する手順に従います。

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

ステップ 12 [HTTPS ユーザ証明書設定（HTTPS User Certificate Settings）] の [ユーザ証明書を有効にする（Enable User Certificates）] を選択します。詳細については、有効なユーザ証明書の強制, （559 ページ）を参照してください。

次の作業

- ユーザが初めてログインした後、手動でユーザのアクセス権を追加または削除できます。権限を変更しない場合、そのユーザにはデフォルトで付与される権限のみが設定されます。詳細については、ユーザ アカウントの編集, （79 ページ）を参照してください。

関連トピック

LDAP グループ フィールド, （106 ページ）
LDAP 固有フィールド, （101 ページ）
CAC クレデンシャルを使用した管理対象デバイスへのログイン, （28 ページ）
CAC クレデンシャルを使用した Firepower Management Center へのログイン, （27 ページ）

基本 LDAP 認証オブジェクトの作成

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

LDAP 認証オブジェクトをセットアップできます。LDAP 認証オブジェクトでは多くの値をカスタマイズします。ただし、特定ディレクトリ内のすべてのユーザを認証するだけの場合は、そのディレクトリのベース DN を使用して基本認証オブジェクトを作成できます。ご使用のサーバ タイプでベース DN のデフォルトを設定し、サーバからユーザ データを取得するために使用するア

カウントの認証クレデンシャルを指定すれば、認証オブジェクトを簡単に作成できます。このためには、次の手順に従います。

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

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

はじめる前に

- LDAP 認証オブジェクトを作成するために必要な情報, （88 ページ）の説明に従って情報を収集します。

手順

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

ステップ 2 [外部認証（External Authentication）] タブをクリックします。

ステップ 3 [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。

ステップ 4 [認証方式（Authentication Method）] ドロップダウンリストから [LDAP] を選択します。

ステップ 5 LDAP 認証サーバの特定, （100 ページ）の説明に従って、[名前（Name）]、[説明（Description）]、[サーバ タイプ（Server Type）]、[プライマリ サーバ ホスト名/IP アドレス（Primary Server Host Name/IP Address）] を入力します。

ヒント [デフォルトの設定（Set Defaults）] をクリックすると、システムにより、[ユーザ名テンプレート（User Name Template）]、[UI アクセス属性（UI Access Attribute）]、[シェル アクセス属性（Shell Access Attribute）]、[グループ メンバ属性（Group Member Attribute）]、[グループ メンバ URL 属性（Group Member URL Attribute）] フィールドにデフォルト値が設定されます。

ステップ 6 LDAP 固有パラメータの設定, （103 ページ）の説明に従って、[DN の取得（Fetch DNs）] を選択して基本識別名を指定し、オプションで [基本フィルタ（Base Filter）] に入力します。

ステップ 7 LDAP 固有パラメータの設定, （103 ページ）の説明に従って、[ユーザ名（User Name）] として識別名を入力し、LDAP サーバを参照するための十分なクレデンシャルを持っているユーザの [パスワード（Password）] を入力します。

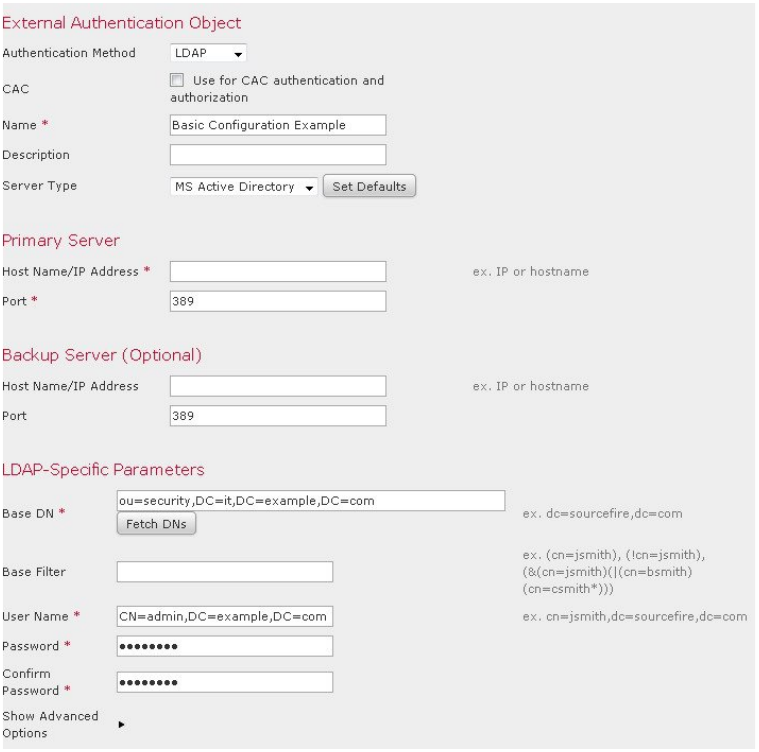
ステップ 8 [パスワードの確認（Confirm Password）] フィールドに、パスワードを再度入力します。

ステップ 9 LDAP 認証接続のテスト, （110 ページ）の説明に従って、接続をテストします。

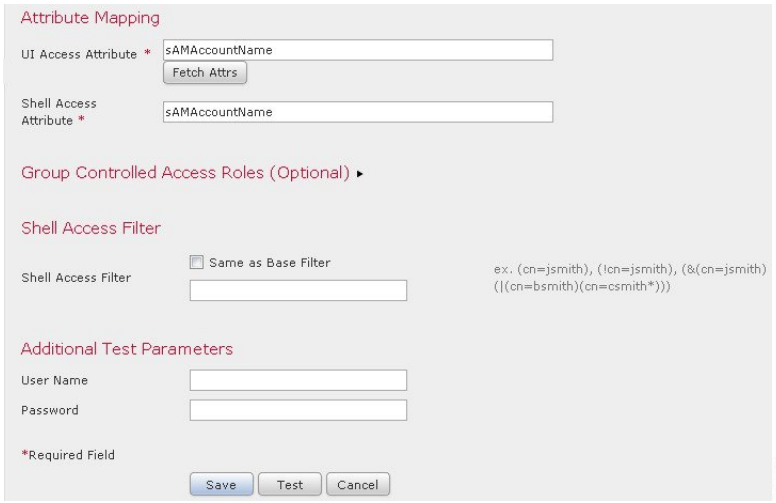
ステップ 10 [保存（Save）] をクリックします。

例

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



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



ただし、このサーバが Microsoft Active Directory Server であるため、ユーザ名の保存に `uid` 属性ではなく `sAMAccountName` 属性が使用されます。サーバのタイプとして MS Active Directory を選択し、

[デフォルトの設定（Set Defaults）] をクリックすると、[UI アクセス属性（UI Access Attribute）] が `sAMAccountName` に設定されます。その結果、ユーザが Firepower システムへのログインを試行すると、Firepower システムは各オブジェクトの `sAMAccountName` 属性を検査し、一致するユーザ名を検索します。

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

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

次の作業

- LDAP 認証を有効にするには、外部認証の有効化, （632 ページ）の説明に従って、認証オブジェクトを有効にします。
- 取得されるユーザのリストを絞り込む場合の詳細は、LDAP 認証接続のトラブルシューティング, （111 ページ）を参照してください。

拡張 LDAP 認証オブジェクトの作成

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

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

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

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

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

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

はじめる前に

- LDAP 認証オブジェクトを作成するために必要な情報, （88 ページ）の説明に従って情報を収集します。
- シェルアクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証シェル ユーザをすべて削除します。

手順

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

ステップ 2 [外部認証（External Authentication）] タブをクリックします。

ステップ 3 [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。

ステップ 4 LDAP 認証サーバの特定, （100 ページ）の説明に従って、認証サーバを指定します。

ステップ 5 LDAP 固有パラメータの設定, （103 ページ）の説明に従って、認証設定を行います。

ステップ 6 オプションで、グループによるアクセス権の設定, （107ページ）の説明に従って、デフォルトアクセス ロール割り当ての基準として使用する LDAP グループを設定します。

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

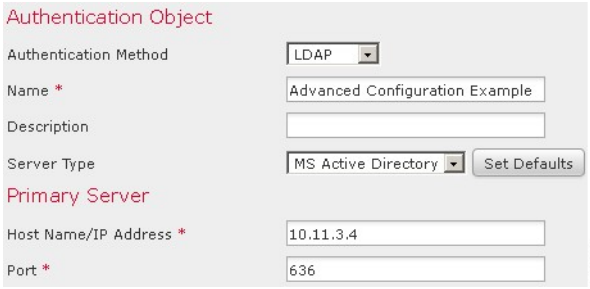
ステップ 7 オプションで、LDAP シェルアクセスの設定, （109ページ）の説明に従って、シェルアクセスの認証設定を行います。

ステップ 8 LDAP 認証接続のテスト, （110 ページ）の説明に従って、設定をテストします。

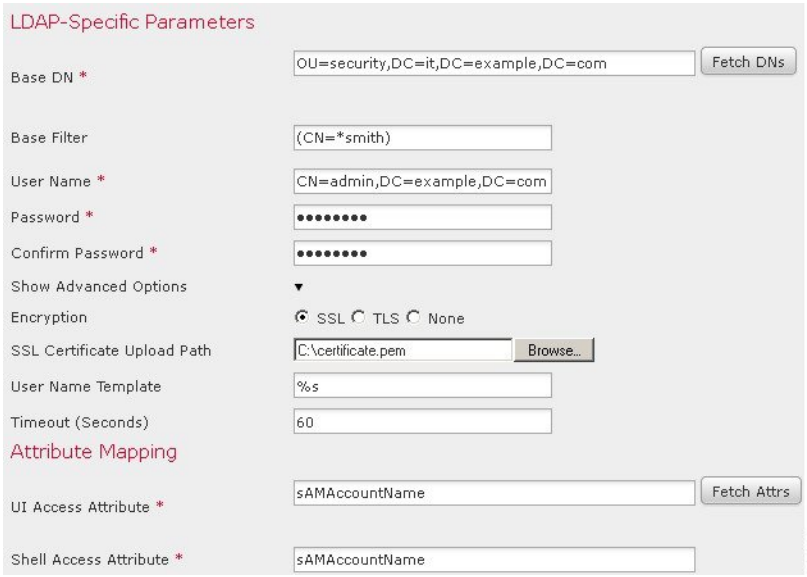
ステップ 9 [保存（Save）] をクリックします。

例

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



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

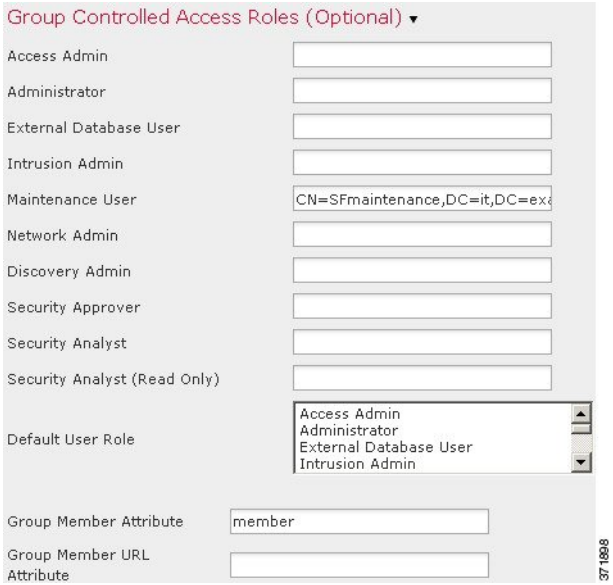


サーバへの接続が SSL を使用して暗号化され、`certificate.pem` という名前の証明書が接続に使用されます。また、[タイムアウト（Timeout）] の設定により、60 秒経過後にサーバへの接続がタイムアウトします。

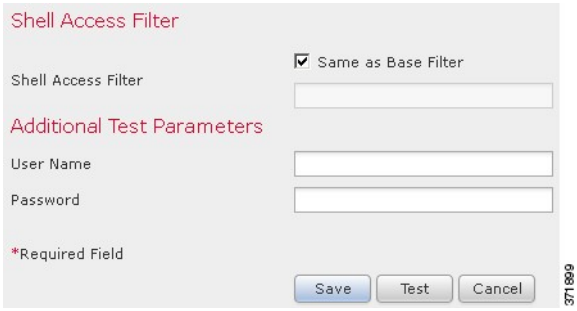
このサーバが Microsoft Active Directory Server であるため、ユーザ名の保存に `uid` 属性ではなく `sAMAccountName` 属性が使用されます。設定では、[UI アクセス属性（UI Access Attribute）] が `sAMAccountName` であることに注意してください。その結果、ユーザが Firepower システムへのログインを試行すると、Firepower システムは各オブジェクトの `sAMAccountName` 属性を検査し、一致するユーザ名を検索します。

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

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



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



次の作業

- LDAP 認証を有効にするには、で認証オブジェクトを有効化します。外部認証の有効化, （632 ページ）

LDAP 認証サーバのフィールド

CAC

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

[名前（Name）]

認証サーバの名前。

説明

認証サーバの説明。

サーバ タイプ（Server Type）

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

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

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

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

認証データを取得するプライマリ サーバの IP アドレスまたはホスト名。

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

[プライマリ サーバのポート（Primary Server Port）]

プライマリ認証サーバで使用されるポート。

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

認証データを取得するバックアップ サーバの IP アドレスまたはホスト名。

[バックアップサーバポート（Backup Server Port）]

バックアップ認証サーバで使用されるポート。

LDAP 認証サーバの特定

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

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

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

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

手順

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

ステップ 2 [外部認証（External Authentication）] タブをクリックします。

ステップ 3 [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。

ステップ 4 [認証方式（Authentication Method）] ドロップダウンリストから [LDAP] を選択します。

ステップ 5 オプションで、CAC 認証および認可にこの認証オブジェクトを使用する予定の場合は、[CAC] チェックボックスをオンにします。

（注） CAC 認証および認可を完全に設定するには、CAC 認証の設定，（91 ページ）の手順に従う必要があります。

ステップ 6 [名前（Name）] フィールドと [説明（Description）] フィールドに、認証サーバの名前と説明を入力します。

ステップ 7 ドロップダウンリストから [サーバタイプ（Server Type）] を選択します。詳細については、LDAP 認証サーバのフィールド，（98 ページ）を参照してください。必要に応じて、[デフォルトの設定（Set Defaults）] をクリックします。

ステップ 8 [プライマリ サーバのホスト名または IP アドレス（Primary Server Host Name/IP Address）] を入力します。

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

ステップ 9 必要に応じて、[プライマリ サーバ ポート（Primary Server Port）] を入力します。

ステップ 10 必要に応じて、[バックアップ サーバのホスト名または IP アドレス（Backup Server Host Name/IP Address）] を入力します。

ステップ 11 必要に応じて、[バックアップ サーバ ポート（Backup Server Port）] を入力します。

次の作業

- LDAP 認証オブジェクトの作成を続行します。詳細については、拡張 LDAP 認証オブジェクトの作成, （95 ページ）を参照してください。

LDAP 固有フィールド

次の表で、各 LDAP 固有パラメータについて説明します。

表 *14* : *LDAP* 固有パラメータ

設定	説明	例
ベース DN（Base DN）	アプライアンスがユーザ情報を検索する LDAP サーバのディレクトリのベース識別名を指定します。 通常、ベース DN には、企業ドメインおよび部門を示す基本構造があります。 プライマリ サーバを特定したら、そのサーバから使用可能なベース DN のリストが自動的に取得され、該当するベース DN を選択できることに注意してください。	Example 社のセキュリティ（Security）部門のベース DN は、`ou=security,dc=example,dc=com` となります。
[基本フィルタ（Base Filter）]	ベース DN でフィルタに設定されている特定の属性と値のペアを含むオブジェクトだけを取得することで、検索を絞り込みます。基本フィルタは、カッコ内に囲まれるフィルタとして使用する属性タイプ、比較演算子、および属性値です。	F で始まる一般名を持つユーザのみをフィルタで検出するには、フィルタ `(cn=F*)` を使用します。
[ユーザ名（User Name）]/[パスワード（Password）]	ローカル アプライアンスがユーザ オブジェクトにアクセスできるようにします。取得する認証オブジェクトに対する適切な権限を持つユーザのユーザ資格情報を指定します。指定するユーザの識別名は、LDAP サーバのディレクトリ情報ツリーで一意である必要があります。Microsoft Active Directory Server に関連付けられたサーバ ユーザ名の末尾の文字が `$` であってはなりません。	Example 社のセキュリティ（Security）部門の `admin` ユーザのユーザ名は、`cn=admin, ou=security, dc=example,dc=com` となります。

設定	説明	例
暗号化（Encryption）	通信が暗号化されるかどうかと、暗号化方法を示します。暗号化なし、Transport Layer Security（TLS）、または Secure Sockets Layer（SSL）暗号化を選択できます。TLS または SSL 経由で接続するときに認証に証明書を使用する場合、証明書の LDAP サーバ名が、指定するユーザ名と一致している**必要がある**ことに注意してください。 ポートを指定した後で暗号化方式を変更すると、ポートが、選択されているサーバ タイプのデフォルト値にリセットされます。	外部認証の設定に `10.10.10.250` を、証明書に `computer1. example.com` を入力すると、`computer1. example.com` に IP アドレス `10.10.10.250` がある場合であっても、接続に失敗します。外部認証設定のサーバ名を `computer1. example.com` に変更すると、接続が正常に行われます。
[SSL 証明書アップロード パス（SSL Certificate Upload Path）]	ローカル コンピュータで、暗号化に使用する証明書のパスを指定します。	`c:/server.crt`
[ユーザ名テンプレート（User Name Template）]	文字列変換文字（`%s`）をユーザの [UI アクセス属性（UI Access Attribute）] の値にマッピングすることで、ログイン時に入力されるユーザ名の形式を指定します。ユーザ名テンプレートは、認証に使用する識別名の形式です。ユーザがログイン ページにユーザ名を入力すると、アプライアンスにより文字列変換文字が名前に置き換えられ、その結果生成される識別名がユーザ資格情報の検索に使用されます。 CAC 認証および許可にこのオブジェクトを使用するには、[ユーザ名テンプレート（User Name Template）] に入力する必要があります。	`%s@security.example.com`, `%s@mail.com`, `%s@mil`, `%s@smil.mil`,
Timeout	プライマリ サーバへの接続試行のタイムアウトを設定します。これにより、接続がバックアップ サーバにロールオーバーされます。プライマリ認証サーバからの応答がない状態でこのフィールドに示されている秒数（または LDAP サーバのタイムアウト）が経過すると、アプライアンスはバックアップ サーバに対してクエリを実行します。 ただし LDAP がプライマリ LDAP サーバのポートで実行されており、何らかの理由で要求の処理を拒否する場合は、バックアップ サーバへのフェールオーバーは行われません。	プライマリ サーバで LDAP が無効な場合、アプライアンスはバックアップ サーバに対してクエリを実行します。

設定	説明	例
[UIアクセス属性（UI Access Attribute）]	ローカルアプライアンスに対し、ユーザ識別名の値ではなく、特定の属性の値の照合を行うように指示します。Firepowerシステム Webインターフェイスの有効なユーザ名が値として設定されている属性であれば、どの属性でも使用できます。いずれかのオブジェクトに一致するユーザ名とパスワードがある場合は、ユーザ ログイン要求が認証されます。 サーバ タイプを選択し、デフォルトを設定すると、[UI アクセス属性（UI Access Attribute）] に、そのサーバ タイプに適した値が取り込まれます。 このフィールドを空白のままにすると、ローカル アプライアンスは、LDAP サーバの各ユーザ レコードのユーザ識別名値を調べ、ユーザ名に一致しているかどうかを確認します。 CAC 認証および許可にこのオブジェクトを使用するには、[ユーザ名テンプレート（User Name Template）] の値に対応する値を入力する必要があります。	`sAMAccountName`, `userPrincipalName`, メール アドレス

LDAP 固有パラメータの設定

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

LDAP 固有パラメータ セクションの設定により、アプライアンスがユーザ名を検索する LDAP ディレクトリの領域が決定され、アプライアンスから LDAP サーバへの接続の詳細が制御されます。

有効なユーザ名は一意のユーザ名であり、アンダースコア（_）、ピリオド（.）、ハイフン（-）、英数字を使用できます。

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

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

手順

ステップ 1 [外部認証オブジェクトの作成（Create External Authentication Object）] ページの [LDAP 固有パラメータ（LDAP-Specific Parameters）] セクションには、ベース DN を設定する 2 つのオプションがあります。

- [DN の取得（Fetch DNs）] をクリックし、ドロップダウン リストから適切なベース識別名を選択します。
- アクセスする LDAP ディレクトリのベース識別名を [ベース DN（Base DN）] フィールドに入力します。たとえば、Example 社のセキュリティ（Security）部門の名前を認証するには、`ou=security,dc=example,dc=com` と入力します。

ステップ 2 必要に応じて、[基本フィルタ（Base Filter）] を入力します。

例：
たとえば、ディレクトリ ツリー内のユーザ オブジェクトに physicalDeliveryOfficeName 属性が設定されており、New York 支店のユーザに対しこの属性に値 `NewYork` が設定されている場合、New York 支店のユーザだけを取得するには、`(physicalDeliveryOfficeName=NewYork)` と入力します。

ステップ 3 LDAP サーバを参照する十分なクレデンシャルがあるユーザの [ユーザ名（User Name）] として識別名と、[パスワード（Password）] を入力します。

例：
たとえば、ユーザ オブジェクトに `uid` 属性が含まれている OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門の管理者のオブジェクトの `uid` に値 `NetworkAdmin` が設定されている場合は、`uid=NetworkAdmin,ou=security,dc=example,dc=com` と入力します。

注意 Microsoft Active Directory Server に接続する場合は、末尾の文字が `$` のサーバ ユーザ名は指定できません。

ステップ 4 [パスワードの確認（Confirm Password）] フィールドに、パスワードを再度入力します。

ステップ 5 基本的な LDAP 固有パラメータの設定後に行う手順には、いくつかの選択肢があります。

- 詳細オプションにアクセスするには、[詳細オプションを表示（Show Advanced Options）] の横の矢印をクリックし、次のステップに進みます。
- LDAP グループ メンバーシップに基づいてユーザ デフォルト ロールを設定する場合は、グループによるアクセス権の設定, （107 ページ）に進みます。

- 認証にLDAPグループを使用しない場合は、LDAPシェルアクセスの設定, （109ページ）に進みます。

ステップ6 必要に応じて、LDAP接続に[暗号化（Encryption）]モードを選択します。

（注） ポートを指定した後で暗号化方式を変更すると、ポートがその方式のデフォルト値にリセットされることに注意してください。[なし（None）]または[TLS]の場合、ポートはデフォルト値389を使用します。SSL暗号化を選択した場合は、ポートはデフォルト値636を使用します。

ステップ7 TLSまたはSSLが暗号化を選択し、認証に証明書を使用する場合は、有効なTLSまたはSSL証明書の場所を参照します。

（注） 以前にアップロードした証明書を置き換えるには、新しい証明書をアップロードし、設定をアプライアンスに再展開して、新しい証明書を上書きコピーします。

ステップ8 必要に応じて、[UIアクセス属性（UI Access Attribute）]に対応する[ユーザ名テンプレート（User Name Template）]を指定します。

例：
たとえば、UIアクセス属性が`uid`であるOpenLDAPサーバに接続し、Example社のセキュリティ（Security）部門で働くすべてのユーザを認証するには、[ユーザ名テンプレート（User Name Template）]フィールドに`uid=%s,ou=security,dc=example,dc=com`と入力します。Microsoft Active Directory Serverの場合は`%s@security.example.com`と入力します。

（注） 認証および認可にCAC資格情報を使用するには、[ユーザ名テンプレート（User Name Template）]フィールドに値を入力する**必要があります**。

ステップ9 オプションで、バックアップ接続にロールオーバーするまでの経過秒数を[タイムアウト（Timeout）]フィールドに入力します。

ステップ10 オプションで、ベースDNおよび基本フィルタの代わりに属性に基づいてユーザを取得する場合、2つのオプションがあります。

- [属性を取得（Fetch Attrs）]をクリックして使用可能な属性のリストを取得し、適切な属性を選択します。
- [UIアクセス属性（UI Access Attribute）]を入力します。たとえばMicrosoft Active Directory Serverでは、Active Directory Serverユーザ オブジェクトに`uid`属性がないため、[UIアクセス属性（UI Access Attribute）]を使用してユーザを取得することがあります。代わりに[UIアクセス属性（UI Access Attribute）]フィールドに`userPrincipalName`と入力して、`userPrincipalName`属性を検索できます。

（注） 認証および認可にCAC資格情報を使用するには、[UIアクセス属性（UI Access Attribute）]フィールドに値を入力する**必要があります**。

次の作業

- 拡張LDAP認証オブジェクトの作成, （95ページ）の説明に従って、引き続きLDAP認証オブジェクトを作成します。

LDAP グループ フィールド

参照するグループはすべて LDAP サーバに存在している必要があります。スタティック LDAP グループまたはダイナミック LDAP グループを参照できます。スタティック LDAP グループとは、特定のユーザを指し示すグループ オブジェクト属性によってメンバーシップが決定されるグループであり、ダイナミック LDAP グループとは、ユーザ オブジェクト属性に基づいてグループ ユーザを取得する LDAP 検索を作成することでメンバーシップが決定されるグループです。ロールのグループ アクセス権は、グループのメンバーであるユーザにのみ影響します。

ユーザが Firepower システムにログインするときに付与されるアクセス権は、LDAP 構成によって異なります。

- LDAP サーバでグループ アクセス権が設定されていない場合、新しいユーザがログインすると、Firepower システムはそのユーザを LDAP サーバに対して認証し、プラットフォーム設定ポリシーに設定されているデフォルトの最小アクセス ロールに基づいてユーザ権限を付与します。
- グループ設定を設定すると、指定されたグループに属している新しいユーザは、メンバーとなっているグループの最小アクセス設定を継承します。
- 新しいユーザが指定のどのグループにも属していない場合は、認証オブジェクトの [グループ制御アクセス ロール（Group Controlled Access Roles）] セクションに指定されているデフォルトの最小アクセス ロールが割り当てられます。
- 設定されている複数のグループにユーザが属している場合、ユーザは最も高いアクセスを持つグループのアクセス ロールを最小アクセス ロールとして受け取ります。

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

（注） ダイナミック グループを使用する場合、LDAP クエリは、LDAP サーバで設定されている通りに使用されます。この理由から、検索構文エラーが原因で無限ループが発生することを防ぐため、Firepower システムでは検索の再帰回数が 4 回に制限されています。この再帰回数内でユーザのグループ メンバーシップが確立されない場合、[グループ制御アクセス ロール（Group Controlled Access Roles）] セクションで定義されているデフォルト アクセス ロールがユーザに付与されます。

[Firepower システムのユーザ権限（Firepower System User Roles）]

各ユーザ ロールを割り当てる必要があるユーザを含む LDAP グループの識別名。

[デフォルトのユーザ ロール（Default User Role）]

指定したグループのいずれにも属していないユーザのデフォルトの最小アクセス。

[グループ メンバーの属性（Group Member Attribute）]

スタティック グループに LDAP 検索文字列を含む LDAP 属性。

[グループ メンバーの URL 属性（Group Member URL Attribute）]

ダイナミック グループのメンバーシップを指定する LDAP 属性。

グループによるアクセス権の設定

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

LDAP グループのユーザのメンバーシップに基づいてデフォルト アクセス権を設定する場合は、Firepower システムにより使用される各アクセス ロールに、LDAP サーバの既存のグループの識別名を指定できます。これを行うと、LDAP によって検出された、指定のどのグループにも属さないユーザのデフォルト アクセス設定を設定できます。ユーザがログインすると、Firepower システムは LDAP サーバを動的に検査し、ユーザの現在のグループ メンバーシップに基づいてデフォルト アクセス権を割り当てます。

グループ制御アクセス ロールを使用してユーザの権限を事前に設定していない場合、ユーザには、プラットフォーム設定ポリシーでデフォルトで付与される権限だけが与えられています。

CAC 認証および認可にオブジェクトを使用する予定の場合、CAC 認証ユーザへのアクセス ロール割り当ての管理のために LDAP グループを設定することを推奨します。

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

はじめる前に

- 参照する予定のグループが LDAP サーバに存在することを確認します。

手順

ステップ 1 [外部認証オブジェクトの作成（Create External Authentication Object）] ページで、[グループ制御アクセス ロール（Group Controlled Access Roles）] の横の下矢印をクリックします。

ステップ 2 必要に応じて、Firepower システム ユーザ ロールに対応する [DN] フィールドに、これらのロールに割り当てる必要があるユーザを含む LDAP グループの識別名を入力します。

例：

たとえば、Example 社の情報テクノロジー（Information Technology）部門の名前を認証するには、[管理者（Administrator）] フィールドに次のように入力します。

```
cn=itgroup,ou=groups, dc=example,dc=com
```

ステップ 3 [デフォルト ユーザ ロール（Default User Role）] を選択します。

ステップ 4 スタティック グループを使用する場合は、[グループ メンバー属性（Group Member Attribute）] を入力します。

例：
たとえば、デフォルトの Security Analyst アクセスのために参照するスタティック グループのメンバーシップを示すために member 属性を使用する場合は、member と入力します。

ステップ 5 ダイナミック グループを使用する場合は、[グループ メンバー URL 属性（Group Member URL Attribute）] を入力します。

例：
たとえば、デフォルトの Admin アクセスに対して指定したダイナミック グループのメンバーを取得する LDAP 検索が memberURL 属性に含まれている場合は、memberURL と入力します。

次の作業

- 拡張 LDAP 認証オブジェクトの作成, （95 ページ）の説明に従って、引き続き LDAP 認証オブジェクトを作成します。

LDAP シェル アクセスのフィールド

admin アカウントを除き、シェル アクセスは設定したシェル アクセス属性によって完全に制御されます。設定するシェル アクセス フィルタにより、シェルにログインできる LDAP サーバのユーザが決定します。

ログイン時に各シェル ユーザのホーム ディレクトリが作成されること、および（LDAP 接続を無効にすることで）LDAP シェル アクセス ユーザ アカウントが無効になっている場合はディレクトリが維持されますが、ユーザ シェルは /etc/password 内の /bin/false に設定され、シェルが無効になることに注意してください。ユーザが再度有効になると、同じホーム ディレクトリを使用してシェルがリセットされます。

シェル ユーザは、小文字、大文字、または小文字と大文字が混在するユーザ名を使用してログインすることができます。シェルのログイン認証では大文字と小文字が区別されます。

[シェル アクセス属性（Shell Access Attribute）]

ユーザがフィルタリング用に使用するアクセス属性です。シェル アクセスの有効なユーザ名が値として設定されている属性であれば、どの属性でも使用できます。

このフィールドを空白のままにした場合、シェル アクセス認証にはユーザ識別名が使用されます。

ヒント　サーバ タイプを選択し、デフォルトを設定すると、そのサーバ タイプに適した属性がこのフィールドに事前に取り込まれます。

[シェル アクセス フィルタ（Shell Access Filter）]

シェル アクセス用の管理ユーザのエントリを取得するために使用する属性値です。フィルタは、属性名、比較演算子、および属性値です。

[ベース フィルタと同じ（Same as Base Filter）] チェックボックスを使用すると、ベース DN で限定されるすべてのユーザが、シェル アクセス権限でも限定される場合に、より効率的に検索できます。通常、ユーザを取得する LDAP クエリは、基本フィルタとシェル アクセス フィルタを組み合わせます。シェル アクセス フィルタが基本フィルタと同一である場合は、同じクエリが 2 回実行されることになり、不必要に時間を消費することになります。[ベース フィルタと同じ（Same as Base Filter）] オプションを使用すると、この両方の目的でクエリを 1 回だけ実行することができます。

このフィールドを空白のままにすると、シェル アクセスの LDAP 認証が回避されます。

LDAP シェル アクセスの設定

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

LDAP サーバを使用して、管理対象デバイスまたは Firepower Management Center でシェル アクセス用のアカウントを認証できます。シェル アクセスを付与するユーザの項目を取得する検索フィルタを指定します。

同一認証オブジェクトで CAC 認証および認可とシェル アクセスの両方を設定することは**できません**。代わりに、別の認証オブジェクトを作成し、有効にします。

シェル アクセスの認証オブジェクトは、Firepower Management Center の最初の認証オブジェクトである必要があります。

シスコは、NGIPSv デバイスまたは ASA FirePOWER デバイスの外部認証をサポートしていません。さらに、シェル アクセス認証では IPv6 がサポートされていません。

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

同一認証オブジェクトで CAC 認証および認可とシェル アクセスの両方を設定することは**できません**。[CAC] チェックボックスをオンにすると、そのページのシェル アクセス設定のオプションが無効になります。代わりに、別の認証オブジェクトを作成し、有効にします。

はじめる前に

- シェル アクセス フィルタに含まれている外部認証ユーザと同じユーザ名を持つ内部認証CLIまたはシェル ユーザを削除します。

手順

ステップ 1 [外部認証オブジェクトの作成（Create External Authentication Object）] ページで、ユーザ識別以外のシェル アクセス属性を使用する場合は、[シェル アクセス属性（Shell Access Attribute）] に入力します。

例：
たとえば、Microsoft Active Directory Server で `sAMAccountName` シェル アクセス属性を使用してシェル アクセス ユーザを取得するには、[シェル アクセス属性（Shell Access Attribute）] フィールドに `sAMAccountName` と入力します。

ステップ 2 シェル アクセス アカウント フィルタを設定します。次の複数のオプションがあります。

- 属性値に基づいて管理ユーザ項目を取得するには、属性名、比較演算子、およびフィルタとして使用する属性値を、カッコで囲んで [シェル アクセス フィルタ（Shell Access Filter）] フィールドに入力します。たとえば、すべてのネットワーク管理者の `manager` 属性に属性値 `shell` が設定されている場合は、基本フィルタ `(manager=shell)` を設定できます。
- 認証設定の設定時に指定したものと同じフィルタを使用するには、[基本フィルタと同じ（Same as Base Filter）] を選択します。
- シェル アクセスの LDAP 認証を防止するには、このフィールドを空白にします。

次の作業

- 拡張 LDAP 認証オブジェクトの作成, （95 ページ）の説明に従って、引き続き LDAP 認証オブジェクトを作成します。

LDAP 認証接続のテスト

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

LDAP サーバを設定し、認証設定を行ったら、これらの設定をテストするため、認証できる必要があるユーザのユーザ資格情報を指定できます。

[ユーザ名（User Name）] にテストに使用するユーザの `uid` 属性の値を入力できます。Microsoft Active Directory Server に接続して `uid` の代わりに UI アクセス属性を指定する場合は、ユーザ名としてこの属性の値を使用します。ユーザの完全修飾識別名も指定できます。

同じユーザのパスワードを使用します。

テスト出力には、有効なユーザ名と無効なユーザ名が示されます。有効なユーザ名は一意のユーザ名であり、アンダースコア（_）、ピリオド（.）、ハイフン（-）、英数字を使用できます。

Web インターフェイスのページ サイズ制限のため、ユーザ数が 1000 を超えているサーバへの接続をテストする場合、返されるユーザの数は 1000 であることに注意してください。

ヒント テスト ユーザの名前とパスワードを誤って入力すると、サーバ設定が正しい場合でもテストが失敗します。最初に、追加のテスト パラメータを使用せずにサーバ設定をテストします。正常に完了した場合は、テストする特定ユーザのユーザ名とパスワードを指定します。

手順

ステップ 1 [外部認証オブジェクトの追加（Add External Authentication Object）] ページで、[ユーザ名（User Name）] と [パスワード（Password）] を入力します。

例：
たとえば、Example 社のユーザ `JSmith` の資格情報を取得できるかどうかをテストするには、「`JSmith`」および「`password`」を入力します。

ステップ 2 [テスト（Test）] をクリックします。次の 2 つの対処法があります。

- テストが成功した場合、テストの出力がページ下部に表示されます。[保存（Save）] をクリックします。
- テストが失敗した場合は、接続のトラブルシューティングの提案事項について、LDAP 認証接続のトラブルシューティング，（111 ページ）を参照してください。

次の作業

- LDAP 認証を有効にするには、外部認証の有効化，（632 ページ）の説明に従って、認証オブジェクトを有効にします。

LDAP 認証接続のトラブルシューティング

LDAP認証オブジェクトを作成したが、選択したサーバへの接続が失敗したか、または必要なユーザのリストが取得されなかった場合は、そのオブジェクトの設定を調整できます。

接続のテストで接続が失敗する場合は、設定のトラブルシューティングに関する次の推奨手順を試してください。

- 画面上部とテスト出力に示されるメッセージから、問題の原因となっているオブジェクトの部分を確認します。
- オブジェクトに使用したユーザ名とパスワードが有効であることを確認します。
  - サードパーティのLDAPブラウザを使用してLDAPサーバに接続し、ベース識別名に示されているディレクトリを参照する権限がユーザにあることを確認します。
  - ユーザ名が、LDAPサーバのディレクトリ情報ツリーで一意であることを確認します。
  - テスト出力にLDAPバインドエラー49が示される場合は、ユーザのユーザバインディングが失敗しています。サードパーティアプリケーションを使用してサーバ認証を試行し、その接続でも同様にバインディングが失敗するかどうかを確認します。
- サーバを正しく指定していることを確認します。
  - サーバのIPアドレスまたはホスト名が正しいことを確認します。
  - ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認します。
  - サーバへのアクセスがファイアウォールによって妨げられないこと、およびオブジェクトで設定されているポートがオープンしていることを確認します。
  - 証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、サーバに使用されているホスト名と一致している必要があります。
  - シェル アクセスを認証する場合は、サーバ接続に IPv6 アドレスを使用していないことを確認します。
  - サーバ タイプのデフォルトを使用している場合は、正しいサーバ タイプであることを確認し、[デフォルトを設定（Set Default）] をもう一度クリックしてデフォルト値をリセットします。
- ベース識別名を入力した場合は、[DN を取得（Fetch DNs）] をクリックし、サーバで使用可能なすべてのベース識別名を取得し、リストから名前を選択します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、それぞれが有効であり正しく入力されていることを確認します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、各設定を削除し、設定なしでオブジェクトをテストしてみます。
- 基本フィルタまたはシェル アクセス フィルタを使用している場合は、フィルタがカッコで囲まれており、有効な比較演算子を使用していることを確認します。
- より制限された基本フィルタをテストするには、特定のユーザだけを取得するため、フィルタにそのユーザのベース識別名を設定します。
- 暗号化接続を使用する場合：

- 証明書のLDAPサーバの名前が、接続に使用するホスト名と一致していることを確認します。
- 暗号化されたサーバ接続でIPv6アドレスを使用していないことを確認します。

- テストユーザを使用する場合、ユーザ名とパスワードが正しく入力されていることを確認します。
- テスト ユーザを使用する場合、ユーザ資格情報を削除してオブジェクトをテストします。
- 次の構文を使用して、接続するアプライアンスでコマンド ラインから LDAP サーバに接続し、使用するクエリをテストします。

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

たとえば、`domainadmin@myrtle.example.com` ユーザと基本フィルタ (`cn=*`) を使用して `myrtle.example.com` のセキュリティ ドメインに接続する場合は、次のステートメントを使用して接続をテストできます。

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

接続のテストが正常に完了したが、プラットフォーム設定ポリシーの適用後に認証が機能しない場合は、使用する認証とオブジェクトの両方が、アプライアンスに適用されるプラットフォーム設定ポリシーで有効になっていることを確認します。

正常に接続されたが、接続で取得されたユーザ リストを調整する必要がある場合は、基本フィルタまたはシェル アクセス フィルタを追加または変更するか、ベース DN をさらに制限するかまたは制限を緩めて使用することができます。

RADIUS 認証

Remote Authentication Dial In User Service（RADIUS）は、ネットワーク リソースへのユーザ アクセスの認証、認可、およびアカウンティングに使用される認証プロトコルです。RFC 2865 に準拠するすべての RADIUS サーバで、認証オブジェクトを作成できます。

RADIUS サーバで認証されたユーザが初めてログインすると、認証オブジェクトでそのユーザに指定されている権限がユーザに付与されます。どのユーザ ロールにもリストされていないユーザには、認証オブジェクトで選択されているデフォルト アクセス権限が付与されます。認証オブジェクトでデフォルト アクセス権限が選択されていない場合は、プラットフォームの設定ポリシーに設定されているデフォルト アクセス権限が付与されます。設定が認証オブジェクトのユーザ リストを介して付与されていない場合は、必要に応じてユーザの権限を変更できます。属性照合を使用してRADIUSサーバで認証されたユーザが初めてログインしようとすると、ユーザ アカウントが作成されているためログインが拒否されることに注意してください。ユーザはもう一度ログインする必要があります。

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

Firepower システムの RADIUS 実装では、SecurID® トークンの使用がサポートされています。SecurID を使用したサーバによる認証を設定すると、そのサーバに対して認証されているユーザが、SecurID PIN の末尾に SecurID トークンを付加し、Cisco システムへのログイン時にそれをパスワードとして使用します。SecurID が外部のユーザを認証するように適切に設定されている限り、これらのユーザは PIN と SecurID を使用して Firepower Management Center または 7000 または 8000 シリーズ デバイスにログインできるので、追加の設定は不要です。

RADIUS 認証オブジェクトの作成

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

RADIUS 認証オブジェクトの作成時に、認証サーバに接続できるようにする設定を定義します。また、特定のユーザおよびデフォルト ユーザにユーザ ロールを付与します。RADIUS サーバから、認証予定のユーザのカスタム属性が返される場合は、これらのカスタム属性を定義する必要があります。オプションで、CLI またはシェル アクセス認証も設定できます。

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

はじめる前に

- ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認します。

手順

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

ステップ 2 [外部認証（External Authentication）] タブをクリックします。

ステップ 3 [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。

ステップ 4 [認証方式（Authentication Method）] ドロップダウン リストから [RADIUS] を選択します。

ステップ 5 RADIUS 接続の設定, （117 ページ）の説明に従って、認証サーバを指定します。

ステップ 6 RADIUS ユーザ ロールの設定, （119 ページ）の説明に従って、ユーザ ロールを設定します。

ステップ 7 オプションで、RADIUS シェルアクセスの設定, （120 ページ）の説明に従ってシェルアクセスを設定します。

ステップ 8 オプションで、カスタム RADIUS 属性の定義, （122 ページ）の説明に従ってカスタム属性を定義します。

ステップ 9 RADIUS 認証接続のテスト, （123 ページ）の説明に従って、設定をテストします。

例

次の図は、IP アドレスが 10.10.10.98 で FreeRADIUS が稼働しているサーバのサンプル RADIUS ログイン認証オブジェクトを示します。接続ではアクセスのためにポート 1812 が使用されること、および不使用期間が 30 秒を経過するとサーバ接続がタイムアウトになり、バックアップ認証サーバへの接続試行前に、サーバ接続が 3 回再試行されることに注意してください。

次の例は、RADIUS ユーザ ロール設定の重要な特徴を示します。

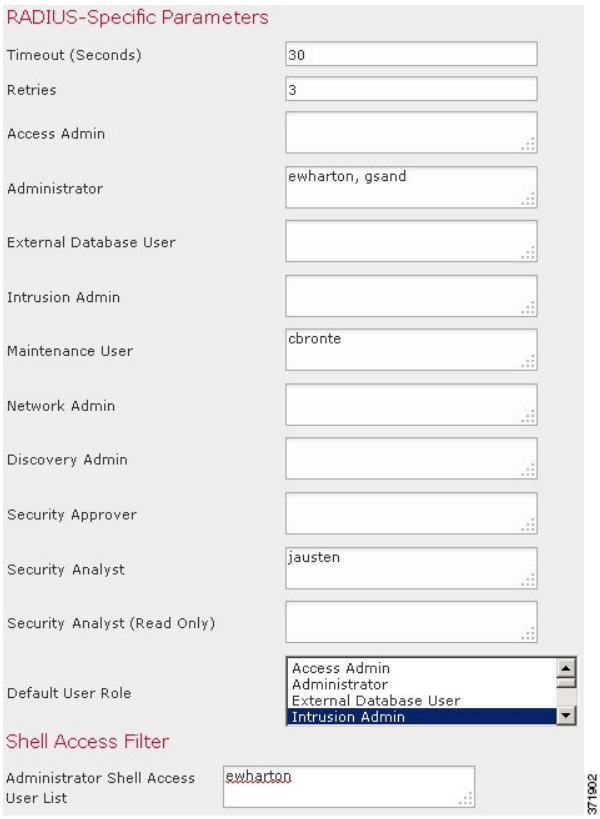
ユーザ `ewharton` と `gsand` には、この認証オブジェクトが有効になっているアプライアンスへの管理アクセスが付与されます。

ユーザ `cbronte` には、この認証オブジェクトが有効になっているアプライアンスへの [メンテナンス ユーザ（Maintenance User）] アクセスが付与されます。

ユーザ `cbronte` には、この認証オブジェクトが有効になっているアプライアンスへの [セキュリティ アナリスト（Security Analyst）] アクセスが付与されます。

ユーザ `ewharton` は、シェル アカウントを使用してアプライアンスにログインできます。

次の図に、この例のロール設定を示します。

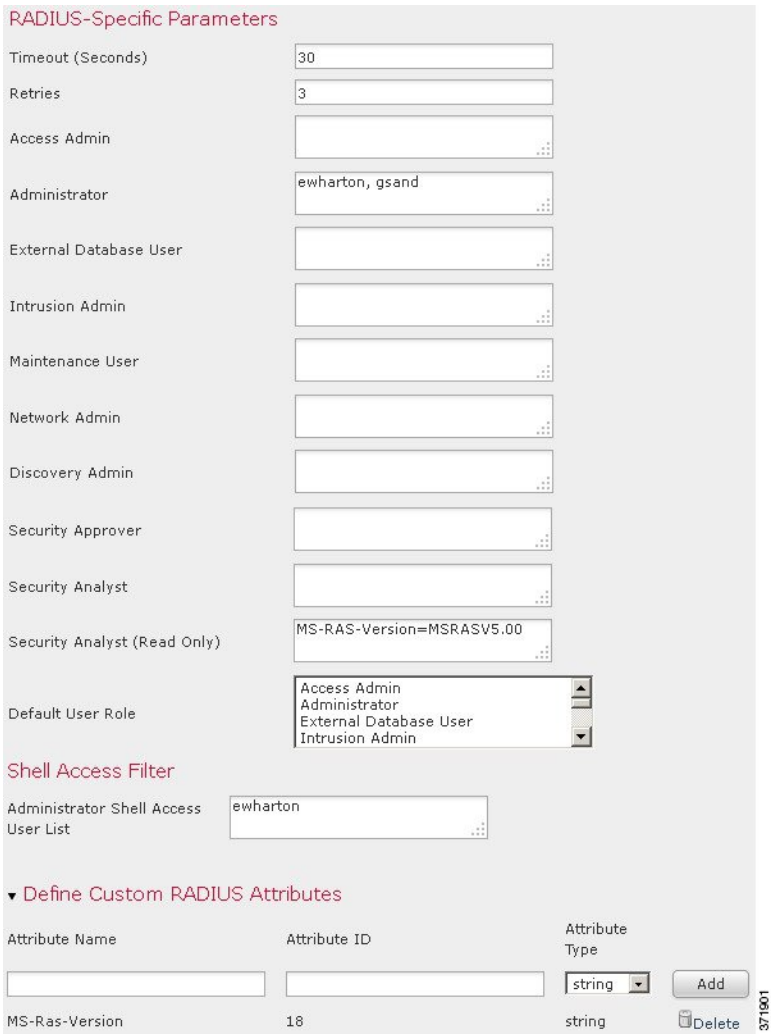


例

属性と値のペアを使用して、特定のユーザ ロールが付与される必要があるユーザを示すこともできます。使用する属性がカスタム属性の場合、そのカスタム属性を定義する必要があります。

次の図は、前述の例と同じ FreeRADIUS サーバのサンプル RADIUS ログイン認証オブジェクトでのロール設定とカスタム属性の定義を示します。

ただしこの例では、Microsoft リモート アクセス サーバが使用されているため、1 人以上のユーザの `MS-RAS-Version` カスタム属性が返されます。`MS-RAS-Version` カスタム属性は文字列であることに注意してください。この例では、Microsoft v. 5.00 リモート アクセス サーバ経由で RADIUS にログインするすべてのユーザに対し、[セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] ロールが付与される必要があります。このため、属性と値のペア `MS-RAS-Version=MSRASV5.00` を [セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] フィールドに入力します。



次の作業

- RADIUS認証を有効にするには、外部認証の有効化, （632ページ）の説明に従って認証オブジェクトを有効にします。

RADIUS 接続の設定

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

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

（注） RADIUS が正しく機能するためは、ファイアウォールで認証ポートとアカウンティング ポート（デフォルトでは 1812 および 1813）を開く必要があります。

バックアップ認証サーバを指定する場合は、プライマリ サーバへの接続試行操作のタイムアウトを設定できます。プライマリ認証サーバからの応答がない状態で[タイムアウト（Timeout）]フィールド（または LDAP サーバのタイムアウト）に指定された秒数が経過すると、アプライアンスはプライマリ サーバに対してクエリを再実行します。

アプライアンスがプライマリ認証サーバに対してクエリを再実行した後に、プライマリ認証サーバからの応答がない状態で [再試行（Retries）] フィールドに指定された回数を超え、[タイムアウト（Timeout）] フィールドに指定された秒数が再び経過すると、アプライアンスはバックアップ サーバにロールオーバーします。

たとえば、プライマリ サーバで RADIUS が無効な場合、アプライアンスはバックアップ サーバに対してクエリを実行します。ただし RADIUS がプライマリ RADIUS サーバのポートで実行されており、何らかの理由（誤った設定またはその他の問題など）で要求の処理を拒否する場合は、バックアップ サーバへのフェールオーバーは行われません。

手順

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

ステップ 2 [外部認証（External Authentication）] タブをクリックします。

ステップ 3 [外部の作成（Create External）]> [認証オブジェクト（Authentication Object）] をクリックします。

ステップ 4 [認証方式（Authentication Method）] ドロップダウン リストから [RADIUS] を選択します。

ステップ 5 認証サーバの名前と説明を入力します。

ステップ 6 認証データを取得するプライマリ RADIUS サーバの IP アドレスまたはホスト名を [プライマリ サーバ ホスト名/IP アドレス（Primary Server Host Name/IP Address）] フィールドに入力します。

（注） シェル認証では IPv6 アドレスはサポートされていません。プライマリ RADIUS サーバに IPv6 アドレスを使用するときにシェル認証を許可するには、サーバの IPv4 アドレスを使用して認証オブジェクトをセットアップし、Firepower Management Center の最初の認証オブジェクトとしてその IPv4 オブジェクトを使用します。

ステップ 7 オプションで、[プライマリ サーバ ポート（Primary Server Port）] フィールドでプライマリ RADIUS 認証サーバが使用するポートを変更します。

（注） 認証ポート番号とアカウンティング ポート番号が連続番号ではない場合は、このフィールドを空白にします。システムは、アプライアンスの `/etc/services` ファイルの `radius` データと `radacct` データから RADIUS ポート番号を判断します。

ステップ 8 プライマリ RADIUS 認証サーバの RADIUS 秘密キーを入力します。

ステップ 9 オプションで、認証データを取得するバックアップ RADIUS 認証サーバの IP アドレスまたはホスト名を [バックアップ サーバ ホスト名/IP アドレス（Backup Server Host Name/IP Address）] フィールドに入力します。

ステップ 10 バックアップ サーバを設定する場合は、[バックアップ サーバ ポート（Backup Server Port）]、[RADIUS 秘密キー（RADIUS Secret Key）]、および [タイムアウト（Timeout）] を変更し、[再試

行（Retries）]フィールドに、バックアップ接続にロールオーバーするまでプライマリ サーバ接続を試行する回数を入力します。

（注） 認証ポート番号とアカウンティング ポート番号が連続番号ではない場合は、このフィールドを空白にします。システムは、アプライアンスの `/etc/services` ファイルの `radius` データと `radacct` データから RADIUS ポート番号を判断します。

次の作業

- RADIUS 認証オブジェクトの作成, （114 ページ）の説明に従って、引き続き RADIUS 認証オブジェクトを作成します。

RADIUS ユーザ ロールの設定

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

ユーザがログインすると、Firepower システムは RADIUS サーバを検査し、RADIUS 構成に基づいてアクセス権を付与します。

- ユーザに対して特定のアクセス権が設定されておらず、デフォルト アクセス ロールが指定されていない場合、新しいユーザがログインすると、Firepower システムは RADIUS サーバに対してそのユーザを認証してから、プラットフォーム設定ポリシーで設定されているデフォルト アクセス ロールに基づいてユーザ権限を付与します。
- 新しいユーザがどのリストにも指定されておらず、認証オブジェクトの [デフォルト ユーザ ロール（Default User Role）] リストでデフォルト アクセス ロールが指定されている場合、ユーザにはこのデフォルト アクセス ロールが割り当てられます。
- 1 つ以上の特定のロールのリストにユーザを追加すると、割り当てられているすべてのアクセス ロールがそのユーザに付与されます。

また、ユーザ名の代わりに属性と値のペアを使用して、特定のユーザ ロールが付与される必要があるユーザを示すこともできます。たとえば、セキュリティ アナリストとする必要があるすべてのユーザの `User-Category` 属性の値が `Analyst` である場合、これらのユーザにそのロールを付与するには、[セキュリティ アナリスト リスト（Security Analyst List）] フィールドに `User-Category=Analyst` と入力します。

外部認証されるが、特定のロールにリストされないすべてのユーザに、デフォルトのユーザ ロールを割り当てることができます。[デフォルト ユーザ ロール（Default User Role）] リストでは、複数のロールを指定できます。

Firepower システムのユーザ管理ページで RADIUS ユーザ リスト メンバーシップが設定されているため、アクセス ロールが割り当てられているユーザの最小アクセス権を削除することはできません。ただし、追加の権限を割り当てることはできます。

注意 ユーザの最小アクセス設定を変更するには、[RADIUS 固有パラメータ（RADIUS Specific Parameters）] セクションのリスト間でユーザを移動するかまたは RADIUS サーバでユーザの属性を変更する他に、構成を管理対象デバイスに再展開し、ユーザ管理ページで割り当てられているユーザ権限を削除する必要があります。

はじめる前に

- ユーザ ロール メンバーシップの設定に使用する場合は、カスタム RADIUS 属性の定義, （122 ページ）の説明に従ってカスタム属性を定義します。

手順

ステップ 1 [外部認証オブジェクトの作成（Create External Authentication Object）] ページで、Firepower システムのユーザ ロールに対応するフィールドに、各ユーザの名前を入力するか、またはそれらのロールに割り当てる属性と値のペアを指定します。
ユーザ名と属性と値のペアは、カンマで区切ります。

例：
たとえば、ユーザ `jsmith` と `jdoe` に管理者ロールを付与する場合は、[管理者（Administrator）] フィールドに `jsmith, jdoe` と入力します。もう 1 つの例として `User-Category` の値が `Maintenance` であるすべてのユーザにメンテナンス ユーザ ロールを付与するには、[メンテナンス ユーザ（Maintenance User）] フィールドに `User-Category=Maintenance` と入力します。

ステップ 2 [デフォルト ユーザ ロール（Default User Role）] リストから、指定のどのグループにも属していないユーザのデフォルト最小アクセス ロールを選択します。

次の作業

- RADIUS 認証オブジェクトの作成, （114 ページ）の説明に従って、引き続き RADIUS 認証オブジェクトを作成します。

RADIUS シェル アクセスの設定

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

RADIUS サーバを使用して、ローカル アプライアンス（管理対象デバイスまたは Firepower Management Center）で、CLI またはシェル アクセスについてアカウントを認証することもできます。CLI またはシェル アクセスを付与するユーザのユーザ名を指定します。

（注） シェル認証では IPv6 アドレスはサポートされていません。IPv6 アドレスを使用してプライマリ RADIUS サーバを設定し、管理シェル アクセスも設定すると、シェル アクセスの設定は無視されます。プライマリ RADIUS サーバに IPv6 アドレスを使用するときにシェル認証を許可するには、サーバの IPv4 アドレスを使用して別の認証オブジェクトをセットアップし、Firepower Management Center の最初の認証オブジェクトとしてそのオブジェクトを使用します。

Admin アカウント以外は、RADIUS 認証オブジェクトで設定したシェル アクセス リストにより、アプライアンスでの CLI またはシェル アクセスが完全に制御されます。CLI またはシェル ユーザは、プラットフォーム設定ポリシーを展開するときに、アプライアンスでローカル ユーザとして設定されます。属性照合を使用して RADIUS サーバで認証されたユーザが初めてログインしようとすると、ユーザ アカウントが作成されているためログインが拒否されることに注意してください。ユーザはもう一度ログインする必要があります。

ログイン時に各 CLI またはシェル ユーザのホーム ディレクトリが作成されること、および（RADIUS 接続を無効にすることで）RADIUS シェル アクセス ユーザ アカウントが無効になっている場合はディレクトリが維持されますが、ユーザ シェルは `/etc/password` 内の `/bin/false` に設定され、シェルが無効になることに注意してください。ユーザが再度有効になると、同じホーム ディレクトリを使用してシェルがリセットされます。

CLI またはシェル ユーザは、小文字、大文字、または小文字と大文字が混在するユーザ名を使用してログインできます。CLI またはシェルのログイン認証では大文字と小文字が区別されます。

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

手順

[外部認証オブジェクトの作成（Create External Authentication Object）] ページで、[管理者シェル アクセス ユーザ リスト（Administrator Shell Access User List）] フィールドにユーザ名をカンマで区切って入力します。

（注） シェル アクセス フィルタを指定しないことを選択すると、認証オブジェクトの保存時に、フィルタを空白のままにすることを確認する警告が表示されます。

次の作業

- RADIUS 認証オブジェクトの作成, （114 ページ）の説明に従って、引き続き RADIUS 認証オブジェクトを作成します。

カスタム RADIUS 属性の定義

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

RADIUS サーバが、`/etc/radiusclient/` 内の `dictionary` ファイルに含まれていない属性の値を返し、これらの属性を使用してユーザにユーザ ロールを設定する予定の場合は、ログイン認証オブジェクトでこれらの属性を定義する必要があります。RADIUS サーバでユーザ プロファイルを調べると、ユーザについて返される属性を見つけることができます。

属性を定義する場合は、英数字からなる属性名を指定します。属性名の中の単語を区切るには、スペースではなくダッシュを使用することに注意してください。また、指定する属性 ID は整数であり、`etc/radiusclient/dictionary` ファイルの既存の属性 ID と競合していてはなりません。属性のタイプ（文字列、IP アドレス、整数、または日付）も指定します。

RADIUS 認証オブジェクトの作成時に、そのオブジェクトの新しいディクショナリ ファイルがアプライアンスの `/var/sf/userauth` ディレクトリに作成されます。認証オブジェクトに追加するカスタム属性はすべて、そのディクショナリ ファイルに追加されます。

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

手順

ステップ 1 [外部認証オブジェクトの追加（Add External Authentication Object）] ページで、矢印をクリックして [カスタム RADIUS 属性の定義（Define Custom RADIUS Attributes）] セクションを展開します。

ステップ 2 [属性名（Attribute Name）] フィールドに属性名を入力します。

ステップ 3 [属性 ID（Attribute ID）] フィールドに、属性 ID を整数形式で入力します。

ステップ 4 [属性タイプ（Attribute Type）] ドロップダウン リストから、属性のタイプを選択します。

ステップ 5 認証オブジェクトにカスタム属性を追加するには、[追加（Add）] をクリックします。

ヒント 認証オブジェクトからカスタム属性を削除するには、その属性の横にある [削除（Delete）] をクリックします。

例

シスコ ルータが接続しているネットワーク上で RADIUS サーバが使用される場合に、`Ascend-Assign-IP-Pool` 属性を使用して、特定の IP アドレス プールからログインするすべてのユー

ザに特定のロールを付与するとします。Ascend-Assign-IP-Pool は、ユーザがログインできるアドレス プールを定義する整数属性であり、割り当てられる IP アドレス プールの番号を示す整数が指定されます。

そのカスタム属性を宣言するには、属性名が Ascend-IP-Pool-Definition、属性 ID が 218、属性タイプが integer のカスタム属性を作成します。

次に、Ascend-IP-Pool-Definition 属性値が 2 のすべてのユーザに対し、読み取り専用の Security Analyst 権限を付与するには、Ascend-Assign-IP-Pool=2 を [セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] フィールドに入力します。

次の作業

- RADIUS 認証オブジェクトの作成, （114 ページ）の説明に従って、引き続き RADIUS 認証オブジェクトを作成します。

RADIUS 認証接続のテスト

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

RADIUS 接続、ユーザ ロール、およびカスタム属性を設定したら、これらの設定をテストするため、認証できる必要があるユーザのユーザ資格情報を指定できます。

ユーザ名として、テストするユーザのユーザ名を入力できます。

UI のページ サイズ制限のため、ユーザ数が 1000 を超えているサーバへの接続をテストする場合、返されるユーザの数は 1000 であることに注意してください。

ヒント テスト ユーザの名前とパスワードを誤って入力すると、サーバ設定が正しい場合でもテストが失敗します。サーバ設定が正しいことを確認するには、最初に [追加のテスト パラメータ（Additional Test Parameters）] フィールドにユーザ情報を入力せずに [テスト（Test）] をクリックします。正常に完了した場合は、テストする特定ユーザのユーザ名とパスワードを指定します。

手順

ステップ 1 [外部認証オブジェクトの追加（Add External Authentication Object）] ページの [ユーザ名（User Name）] フィールドと [パスワード（Password）] フィールドに、RADIUS サーバへのアクセスの検証に資格情報が使用されるユーザのユーザ名とパスワードを入力します。

例：

たとえば、Example 社の jsmith のユーザ資格情報を取得できるかどうかをテストするには、「jsmith」と入力します。

ステップ 2 [詳細の表示（Show Details）] を選択し、[テスト（Test）] をクリックします。

ステップ 3 テストが成功した場合は [保存（Save）] をクリックします。

次の作業

- RADIUS 認証を有効にするには、外部認証の有効化，（632 ページ）の説明に従って、認証オブジェクトを有効にします。

シングル サインオン（SSO）

シングル サインオン（SSO）により、Cisco Security Manager（CSM）バージョン 4.7 以上と Firepower Management Center を統合して、ログインの追加認証なしで CSM から Firepower Management Center にアクセスできるようにすることができます。ASA FirePOWER モジュールの管理では、モジュールに展開したポリシーの変更が必要となる場合もあります。CSM で Firepower Management Center を管理して、Web ブラウザで起動するという方法を選択することもできます。

ユーザ ロールに基づくアクセス権限がある場合、CSM でクロス起動したデバイスの [デバイス管理（Device Management）] ページの [デバイス（Device）] タブに移動します。それ以外の場合は、[サマリー ダッシュボード（Summary Dashboard）] ページ（[概要（Overview）]>[ダッシュボード（Dashboards）]）に移動します。ただしダッシュボードにアクセスできないユーザ アカウントの場合は、[ようこそ（Welcome）] ページが使用されます。

Firepower Management Center で STIG コンプライアンスが有効にされいている場合、システムにより SSO が無効化されます。

（注） 組織で認証に CAC が使用されている場合、シングル サインオンでログインすることはできません。

関連トピック

STIG コンプライアンス，（602 ページ）

SSO の設定

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

シングル サインオンを設定する前に、CSM から Firepower Management Center への一方向の暗号化認証パスを設定する必要があります。

NAT 環境では、Firepower Management Center と CSM は NAT 境界の同じ側に存在している必要があります。CSM と Firepower Management Center 間の通信を有効にする特定の基準を入力する必要があります。

（注） 組織で認証に CAC が使用されている場合は、シングル サインオンでログインできません。

手順

ステップ 1 CSM から、接続を識別する SSO 共有暗号キーを生成します。詳細については、CSM のマニュアルを参照してください。

ステップ 2 Firepower Management Center から、[システム（System）] > [ユーザ（Users）] を選択します。

ステップ 3 [CSM シングル サインオン（CSM Single Sign-on）] を選択します。

ステップ 4 CSM ホスト名または IP アドレスとサーバのポートを入力します。

ステップ 5 CSM から生成した共有キーを入力します。

ステップ 6 オプションで、Firepower Management Center のプロキシ サーバを使用して CSM と通信する場合は、[接続にプロキシを使用（Use Proxy For Connection）] チェックボックスをオンにします。

ステップ 7 [送信（Submit）] をクリックします。

ステップ 8 [証明書の確認（Confirm Certificate）] をクリックして証明書を保存します。
これで CSM から Firepower Management Center にログインできるようになります。追加のログインを実行する必要はありません。

関連トピック

管理インターフェイスの設定, （569 ページ）

第 5 章

Firepower システムのライセンス

ここでは、Firepower システムのライセンスを適用する方法について説明します。

Firepower の機能ライセンスについて

組織に対して Firepower システムの最適な展開を実現するために、さまざまな機能についてライセンスを取得することができます。Firepower Management Center では、これらの機能ライセンスを管理してデバイスに割り当てることができます。

（注） Firepower Management Center はデバイスの機能ライセンスを管理しますが、Firepower Management Center を使用するための機能ライセンスは必要ありません。

Firepower 機能ライセンスは、デバイスの種類に応じて次のように異なります。

- 従来型ライセンスは 7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv デバイスに使用可能です。従来のライセンスを使用するデバイスは、クラシック デバイスと呼ばれることもあります。

1 つの Firepower Management Center で従来のライセンスとスマート ライセンスの両方を管理できます。

Firepower 機能のサービス サブスクリプション

サービス サブスクリプションは、所定の時間内限定で、管理対象デバイス上の特定の Firepower 機能を有効にします。サービス サブスクリプションは、1 年、3 年、または 5 年単位で購入できます。サブスクリプションの期限が切れると、サブスクリプションの更新が必要であることが通知されます。クラシック デバイスのサブスクリプションの期限が切れた場合、機能のタイプによっては、関連機能を使用できなくなることがあります。

サービス サブスクリプションは、Firepower システムで管理対象デバイスに割り当てるライセンスと、次のように対応しています。

表 *15*：サブスクリプションおよび対応するクラシック ライセンス

購入するサブスクリプション	Firepower システム内で割り当てるクラシック ライセンス
TA	制御 + 保護（別名「脅威 & アプリ」、システム更新に必要）
TAC	制御 + 保護 + URL フィルタリング
TAM	制御 + 保護 + マルウェア
TAMC	制御 + 保護 + URL フィルタリング + マルウェア
URL	URL フィルタリング（TA が既に存在する場合はアドオン）
AMP	マルウェア（TA が既に存在する場合はアドオン）

クラシック ライセンスを使用する管理対象デバイスを購入すると、制御および保護のライセンスが自動的に提供されます。これらのライセンスは無期限ですが、システムの更新を有効にするには、TA サービス サブスクリプションを購入する必要があります。追加機能のサービス サブスクリプションはオプションです。

Firepower システムのクラシック ライセンス

クラシック ライセンスでは、製品認証キー（PAK）をアクティブ化する必要があり、デバイス間で譲渡することはできません。クラシック ライセンスは、「従来のライセンス」と呼ばれることもあります。

7000 および 8000 シリーズ デバイス、NGIPSv デバイス、および ASA FirePOWER モジュールはクラシック ライセンスを使用します。

製品ライセンス登録ポータル

Firepower 機能のクラシック ライセンスを 1 つ以上購入する場合は、それらのライセンスを Cisco Product License Registration ポータルで管理します。

http://www.cisco.com/web/go/license

このポータルの使用方法の詳細については、次を参照してください。

https://www.cisco.com/web/fw/tools/swift/xui/html/help.html

従来のライセンスのタイプと制約事項

ここでは、Firepower システム展開環境で使用可能な従来のライセンスのタイプについて説明します。デバイスで有効にできるライセンスは、デバイスのモデル、バージョン、および他の有効なライセンスによって異なります。

7000 および 8000 シリーズ デバイス、NGIPSv デバイス、および ASA FirePOWER モジュールの場合、ライセンスはモジュール固有です。ライセンスがデバイスのモデルと完全に一致しない限り、管理対象デバイスでライセンスを有効にすることはできません。たとえば、Firepower 8250 マルウェア ライセンス（FP8250-TAM-LIC=）を使用して 8140 デバイスでマルウェア関連の機能を有効にすることはできません。Firepower 8140 マルウェア ライセンス（FP8140-TAM-LIC=）を購入する必要があります。

（注） NGIPSv または ASA FirePOWER では、制御ライセンスを使用してユーザとアプリケーションの制御を実行できますが、それらのデバイスはスイッチング、ルーティング、スタッキング、または 7000 および 8000 シリーズ デバイスの高可用性をサポートしていません。

Firepower システムでライセンス付き機能にアクセスできなくなる状況がいくつかあります。

- Firepower Management Center から従来のライセンスを削除することができますが、そのようにすると、すべての管理対象デバイスに影響します。
- 特定の管理対象デバイスでライセンス付き機能を無効にすることができます。

いくつかの例外がありますが、期限切れライセンスまたは削除済みライセンスに関連付けられている機能は使用できません。

次の表に、Firepower システムにおける従来のライセンスの概要を示します。

表 *16* : *Firepower* システムの従来のライセンス

Firepowerシステムで割り当てるライセンス	購入するサービスサブスクリプション	プラットフォーム	付与される機能	併せて必要なライセンス	有効期限設定可/不可
任意（Any）	TA、TAC、TAM、またはTAMC	7000および8000シリーズ ASA FirePOWER NGIPSv	ホスト、アプリケーション、ユーザ検出 SSL暗号化トラフィックとTLS暗号化トラフィックの復号および検査	none	ライセンスによって異なる
プロテクション（Protection）	TA（デバイスに付属）	7000および8000シリーズ ASA FirePOWER NGIPSv	侵入検知と防御 ファイル制御 セキュリティ インテリジェンスフィルタリング	none	No
Control	なし（デバイスに付属）	7000および8000シリーズ	ユーザおよびアプリケーション制御 スイッチングとルーティング 7000および8000シリーズ デバイスの高可用性 7000および8000シリーズ ネットワーク アドレス変換（NAT）	Protection	No
Control	なし（デバイスに付属）	ASA FirePOWER NGIPSv	ユーザおよびアプリケーション制御	Protection	No
マルウェア（Malware）	TAM、TAMC、またはAMP	7000および8000シリーズ ASA FirePOWER NGIPSv	AMP for Firepower（ネットワークベースの高度なマルウェア防御）	Protection	Yes
URLフィルタリング（URL Filtering）	TAC、TAMC、またはURL	7000および8000シリーズ ASA FirePOWER NGIPSv	カテゴリとレピュテーションに基づくURLフィルタリング	Protection	Yes
VPN	なし（詳細は販売担当者にお問い合わせください）	7000および8000シリーズ	バーチャルプライベートネットワークの展開	Control	Yes

プロテクション ライセンス

プロテクションライセンスでは、侵入検知および防御、ファイル制御、およびセキュリティインテリジェンス フィルタリングを実行できます。

- 侵入検知および防御により、侵入とエクスプロイトを検出するためネットワーク トラフィックを分析できます。またオプションで違反パケットをドロップできます。
- ファイル制御により、特定のアプリケーションプロトコルを介した特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード（送信）またはダウンロード（受信）をブロックできます。マルウェア ライセンスが必要な *AMP for Firepower* を使用すると、制限されたファイル タイプ セットを、その処置に基づいて検査およびブロックすることができます。
- セキュリティ インテリジェンス フィルタリングにより、トラフィックをアクセス制御ルールによる分析対象にする前に、特定の IP アドレス、URL、および DNS ドメイン名をブラックリストに追加（その IP アドレスとの間のトラフィックを拒否）できます。ダイナミック フィードにより、最新の情報に基づいて接続をただちにブラックリストに追加できます。オプションで、セキュリティ インテリジェンス フィルタリングに「モニタのみ」設定を使用できます。

プロテクション ライセンス（制御ライセンスと共に）は、クラシック管理対象デバイスの購入時に自動的に組み込まれます。このライセンスは無期限ですが、システムの更新を有効にするには、TA サブスクリプションも購入する必要があります。

ライセンスがない状態でプロテクション関連の検査を実行するようにアクセス制御ポリシーを設定できますが、プロテクション ライセンスを Firepower Management Center に追加し、ポリシー展開対象デバイス上でこのライセンスを有効にするまではポリシーを展開できません。

プロテクション ライセンスを Firepower Management Center から削除するか、または管理対象デバイスでプロテクションを無効にすると、Firepower Management Center は対象デバイスからの侵入イベントとファイル イベントを認識しなくなります。結果として、トリガー条件としてこれらのイベントを使用する相関ルールがトリガーしなくなります。また、Firepower Management Center はシスコ提供またはサードパーティのセキュリティインテリジェンス情報を取得するためにインターネットに接続しなくなります。プロテクションを再度有効にするまでは、既存のポリシーを再度展開することはできません。

プロテクション ライセンスは URL フィルタリング、マルウェア、および制御ライセンスに必要であるため、プロテクションライセンスを削除または無効にすると、URL フィルタリング、マルウェア、または制御ライセンスを削除または無効にすることと同じ効果があります。

制御ライセンス

制御ライセンスでは、アクセス コントロール ルールにユーザとアプリケーションの条件を追加することで、ユーザとアプリケーションの制御を実装できます。7000 および 8000 シリーズ デバイスでは、このライセンスを使用して、スイッチングとルーティング（DHCP リレーおよび NAT を含む）、およびデバイスのハイ アベイラビリティ ペアも構成できます。管理対象デバイスの制御

ライセンスを有効にするには、保護ライセンスも有効にする必要があります。制御ライセンスは（保護ライセンスとともに）、従来の管理対象デバイスの購入時に自動的に付属します。このライセンスは無期限ですが、システムの更新を有効にするには、TA サブスクリプションも購入する必要があります。

従来の管理対象デバイスの制御ライセンスを有効にしない場合は、アクセス コントロール ポリシーのルールにユーザおよびアプリケーションの条件を追加できますが、デバイスにポリシーを展開することはできません。7000 または 8000 シリーズ デバイスの制御ライセンスを明確に有効にしないと、次の操作も行えません。

- スイッチド、ルーテッド、またはハイブリッド インターフェイスの作成
- NAT エントリの作成
- 仮想ルータの DHCP リレーの設定
- デバイスへのスイッチまたはルーティングが含まれているデバイス設定の展開
- デバイス間のハイ アベイラビリティの確立

（注） 制御ライセンスがなくても仮想スイッチおよびルータを作成できますが、データを取り込むスイッチドインターフェイスおよびルーテッドインターフェイスがない状態ではこれらのスイッチとルータは有用ではありません。

制御ライセンスを Firepower Management Center から削除するか、または個別のデバイスで制御を無効にしても、対象デバイスでのスイッチングとルーティングの実行が行われなくなったり、デバイスのハイ アベイラビリティ ペアが解除されたりすることは**ありません**。既存の設定の編集や削除を続けることはできますが、影響を受けるデバイスに対する変更を展開することはできません。新しいスイッチド インターフェイス、ルーテッド インターフェイス、またはハイブリッド インターフェイスを追加することも、新しい NAT エントリの追加、DHCP リレーの設定、7000 または 8000 シリーズ デバイスのハイ アベイラビリティの確立もできません。既存のアクセス コントロール ポリシーに、ユーザ条件またはアプリケーション条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。

従来のデバイスの URL フィルタリング ライセンス

URL フィルタリングにより、モニタ対象ホストにより要求される URL に基づいて、ネットワーク内を移動できるトラフィックを判別するアクセス制御ルールを作成することができます。URL フィルタリング ライセンスを有効にする場合は、保護ライセンスも有効にする必要があります。従来のデバイスの URL フィルタリング ライセンスは、脅威 & アプリ（TAC）または脅威 & アプリおよびマルウェア（TAMC）サブスクリプションと組み合わせてサービス サブスクリプションとして購入できます。また、脅威 & アプリ（TA）が既に有効になっているシステムの場合は、アドオン サブスクリプションとして購入できます。

ヒント URL フィルタリング ライセンスがない状態で、許可またはブロックする個別 URL または URL グループを指定できます。これにより、Web トラフィックをカスタムできめ細かく制御できますが、URL カテゴリおよびレピュテーション データをネットワーク トラフィックのフィルタリングに使用することはできません。

URL フィルタリング ライセンスがない状態でも、アクセス制御ルールにカテゴリ ベースの URL 条件およびレピュテーション ベースの URL 条件を追加できますが、Firepower Management Center は URL 情報をダウンロードしません。最初に URL フィルタリング ライセンスを Firepower Management Center に追加し、ポリシー適用対象デバイスで有効にするまでは、アクセス コントロール ポリシーを適用できません。

Firepower Management Center からライセンスを削除するか、または管理対象デバイスで URL フィルタリングを無効にすると、URL フィルタリングにアクセスできなくなることがあります。また、URL フィルタリング ライセンスの有効期限が切れることもあります。ライセンスが期限切れになるか、ライセンスを削除または無効化すると、URL 条件が含まれているアクセス制御ルールは URL フィルタリングを直ちに停止し、Firepower Management Center は URL データのアップデートをダウンロードできなくなります。既存のアクセス コントロール ポリシーに、カテゴリ ベースまたはレピュテーション ベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。

従来のデバイスのマルウェア ライセンス

マルウェア ライセンスを使用すると、AMP for Firepower および AMP Threat Grid を使用して Cisco Advanced Malware Protection（AMP）を実行することができます。管理対象デバイスを使用して、ネットワーク上で伝送されるファイルのマルウェアを検出してブロックできます。マルウェア ライセンスを有効にするには、保護も有効にする必要があります。マルウェア ライセンスは、脅威 & アプリ（TAM）と組み合わせたサブスクリプションまたは脅威 & アプリおよび URL フィルタリング（TAMC）サブスクリプションとして購入できます。また、脅威 & アプリ（TA）が既に有効になっているシステムの場合は、アドオン サブスクリプションとして購入できます。

（注） マルウェア ライセンスが有効になっている 7000 および 8000 シリーズ 管理対象デバイスは、動的分析を設定していない場合でも、定期的に AMP クラウドへの接続を試行します。このため、デバイスの [インターフェイス トラフィック（Interface Traffic）] ダッシュボード ウィジェットには、送信済みトラフィックが表示されます。これは正常な動作です。

ファイル ポリシーの一部として AMP for Firepower を設定し、その後 1 つ以上のアクセス コントロール ルールを関連付けます。ファイル ポリシーは、特定のアプリケーション プロトコルを使用して特定のファイルをアップロードまたはダウンロードするユーザを検出できます。AMP for Firepower によって、ローカル マルウェア分析とファイルの事前分類を使用して、これらの制限されたファイル タイプのセットにマルウェアがないかを検査できます。特定のファイル タイプをダウンロードして AMP Threat Grid クラウドにアップロードして、動的 Spero 分析でマルウェアが含まれているかどうかを判別することもできます。これらのファイルでは、ファイルがネットワーク内で経由する詳細なパスを示すネットワーク ファイル トラジェクトリを表示できます。マル

ウェア ライセンスでは、ファイル リストに特定のファイルを追加し、そのファイル リストをファイル ポリシー内で有効にすることもできます。これにより、検出時にこれらのファイルを自動的に許可またはブロックできます。

AMP for Firepower 構成を含むアクセス コントロール ポリシーを展開する前に、マルウェア ライセンスを追加してから、そのポリシー展開対象デバイスで有効にする**必要があります**。デバイスでライセンスを後で無効にする場合、既存のアクセス コントロール ポリシーをそれらのデバイスに再度展開することはできません。

マルウェア ライセンスをすべて削除するか、それらがすべて期限切れになると、システムは AMP への問い合わせを停止し、AMP クラウドから送信される遡及的イベントの確認応答も停止します。既存のアクセス コントロール ポリシーに AMP for Firepower 構成が含まれている場合は、それらのポリシーを再展開することができません。マルウェア ライセンスが失効したか削除された後、システムが既存のキャッシュ ファイルの性質を使用できるのは極めて短時間のみであることに注意してください。この時間枠の経過後、システムは `Unavailable` という性質をこれらのファイルに割り当てます。

マルウェア ライセンスが必要なのは AMP for Firepower および AMP Threat Grid を展開する場合のみです。マルウェア ライセンスがなければ、Firepower Management Center は AMP クラウドからエンドポイント向け AMP マルウェア イベントおよび侵害の兆候（IOC）を受信できます。

関連トピック

ファイル制御および Cisco AMP の基本, （954 ページ）

VPN ライセンス

VPN を使用すると、インターネットやその他のネットワークなどの公共ソースを経由してエンドポイント間にセキュア トンネルを確立できます。7000 および 8000 シリーズ デバイスの仮想ルータ間で安全な VPN トンネルを構築するよう、Firepower システムを設定することができます。VPN を有効にするには、保護および制御のライセンスも有効にする必要があります。VPN ライセンスを購入するには、販売担当者までお問い合わせください。

VPN ライセンスがないと、7000 および 8000 シリーズ デバイスで VPN 導入環境を設定できません。導入環境の作成はできますが、データを取り込むための 1 つ以上の VPN 対応スイッチド インターフェイスおよびルーテッド インターフェイスがない状態では、導入環境は有用ではありません。

VPN ライセンスを Firepower Management Center から削除するか、または個別のデバイスで VPN を無効にすると、対象デバイスは現在の VPN 導入環境をブレイク**しません**。既存の導入環境を編集または削除できますが、対象デバイスに変更を適用することはできません。

デバイス スタックおよびハイ アベイラビリティ ペアのクラシック ライセンス

スタックや 7000 または 8000 シリーズ デバイス ハイ アベイラビリティ ペアを構成するデバイスは、それぞれが同等のライセンスを持っている必要があります。デバイスのスタック構成後に、スタック全体のライセンスを変更できます。ただし、7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアでは有効なライセンスを変更することはできません。

従来型ライセンスの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	任意（Any）	従来型（Classic）	グローバルのみ	Admin

[Classic ライセンス（Classic Licenses）] ページを使用して、Firepower Management Center に追加した Classic ライセンスを表示します。展開環境内の管理対象デバイスのタイプごとに、所有しているライセンスの総数と、使用中のライセンスの割合がこのページにリストされます。

[ライセンス（Licenses）] ページには、各ライセンスの詳細も表示されます。モデルごとに、各タイプの所有ライセンス数、各タイプのライセンスでライセンス付与できる管理対象デバイスの数が表示されます。有効期限のあるライセンスの場合、このページに有効期限が表示されます。

次のように、ライセンスおよびライセンス制限を表示できます。

- [製品ライセンス（Product Licensing）] ダッシュボード ウィジェットはライセンスの概要を示します。
- [デバイス管理（Device Management）] ページ（[デバイス（Devices）]>[デバイス管理（Device Management）]）は、各管理対象デバイスに適用されているライセンスをリストします。
- ヘルス ポリシーで使用される際に、Classic ライセンス モニタのヘルス モジュールはライセンス ステータスを伝達します。

手順

[システム（System）]>[ライセンス（Licenses）]>[クラシック ライセンス（Classic Licenses）]を選択します。

ライセンス キーの特定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	任意（Any）	従来型（Classic）	グローバルのみ	Admin

ライセンス キーによって、Firepower Management Center はシスコ ライセンス登録ポータルで一意に識別されます。これは、Firepower Management Center の製品コード（66）と MAC アドレスで構成されます（たとえば、66:00:00:77:FF:CC:88）。

シスコ ライセンス登録ポータルでは、ライセンス キーを使用して、Firepower Management Center にライセンスを追加する際に必要になるライセンス テキストを取得する必要があります。

手順

ステップ 1 [システム（System）] > [ライセンス（Licenses）] > [クラシック ライセンス（Classic Licenses）]を選択します。

ステップ 2 [新規ライセンスの追加（Add New License）] をクリックします。

ステップ 3 [機能ライセンスの追加（Add Feature License）] ダイアログの上部にある [ライセンス キー（License Key）] フィールドの値をメモします。

次の作業

- ライセンスを Firepower Management Center に追加します。Firepower Management Center への従来型ライセンスの追加, （136 ページ）を参照してください。

Firepower Management Center への従来型ライセンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	任意（Any）	従来型（Classic）	グローバルのみ	Admin

（注） バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを（それらが使用されている場所をメモした上で）削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。

ヒント サポート サイトにログインした後で、[ライセンス（Licenses）] タブでライセンスを要求することもできます。

はじめる前に

- ライセンス購入時に Cisco が提供したソフトウェア権利証明書にある製品アクティベーション キー（PAK）をお手元にご用意ください。レガシーの、以前のシスコのライセンスの場合は、サポートに問い合わせてください。
- Firepower Management Center のライセンス キーの種類を確認します。ライセンス キーの特定, （135 ページ） を参照してください。

手順

ステップ 1 [システム（System）]>[ライセンス（Licenses）]>[クラシック ライセンス（Classic Licenses）]を選択します。

ステップ 2 [新規ライセンスの追加（Add New License）] をクリックします。

ステップ 3 必要に応じ、続いて以下を行います。

- ライセンス テキストをすでに取得している場合は、ステップ 8 にスキップしてください。
- ライセンスのテキストを取得する必要がある場合は、次の手順を実行します。

ステップ 4 [ライセンス取得（Get License）] をクリックして、Cisco ライセンス登録ポータルを開きます。

（注） ご使用のコンピュータからインターネットにアクセスできない場合は、アクセスできるコンピュータから http://cisco.com/go/licenseを探します。

ステップ 5 ライセンス登録ポータルで、PAK からライセンスを生成します。詳細については、https://www.cisco.com/web/fw/tools/swift/xui/html/help.htmlを参照してください。
この手順には、購入時に入手した PAK と、Firepower Management Center のライセンスキーが必要です。

ステップ 6 ライセンス登録ポータルの表示から、ないしはライセンス登録ポータルより送られてくるメールからライセンス テキストをコピーします。

ステップ 7 Firepower Management Center の web インターフェイスの [機能ライセンスの追加（Add Feature License）] ページに戻ります。

ステップ 8 [ライセンス（License）] フィールドにライセンス テキストを貼り付けます。

ステップ 9 [ライセンスの検証（Verify License）] をクリックします。
ライセンスが無効となる場合は、ライセンス テキストが正しくコピーされているか確認します。

ステップ 10 [ライセンスの提出（Submit License）] をクリックします。

次の作業

- 管理対象デバイスにライセンスを割り当てます。管理対象デバイスへのライセンスの割り当て，（137ページ） を参照してください。管理対象デバイスのライセンス取得済み機能を使用するには、これらのデバイスにライセンスを割り当てる**必要があります**。

管理対象デバイスへのライセンスの割り当て

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

一部の例外はありますが、管理対象デバイスでライセンスを無効にすると、そのライセンスに関連づけられている機能は使用できなくなります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 ライセンスを割り当てまたは無効にするデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [ライセンス（License）] セクションの横にある編集アイコン（  ）をクリックします。

ステップ 5 適切なチェックボックスをオンまたはオフにして、デバイスのライセンスを割り当て、または無効にします。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 6 章

システム ソフトウェア更新

ここでは、Firepower システム ソフトウェアを更新する方法について説明します。

システム ソフトウェア アップデートの概要

Cisco は、以下を含む各種のアップデートを電子的に配信します。

- システム ソフトウェア自体に対するメジャーおよびマイナー アップデート
- 侵入ルールの更新
- 地理位置情報データベース（GeoDB）の更新
- 脆弱性データベース（VDB）の更新

ほとんどのタイプの更新では、ダウンロードとインストールをスケジュールすることができます。

注意 この章では、Firepower システムの更新に関する全般的な情報について説明します。Firepower システムのいずれかの部分（VDB、GeoDB、侵入ルールなど）を更新する前に、更新に付随しているリリース ノートまたはアドバイザリ テキストを読んでおく**必要があります**。リリース ノートでは、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストールおよびアンインストールの手順など重要なデータが提供されます。

表 *17* : ***Firepower*** システム アップデートのタイプ

更新のタイプ	説明	スケジュールを行うか	アンインストールをするか	タブ	ドメイン
Firepower システムに対するパッチ	パッチには、限定された範囲の修正が含まれています（また通常は、6.0.0.1 のようにバージョン番号の 4 桁目が変更されます）。	Yes	Yes	製品の更新	グローバルのみ
Firepower システムの機能の更新	機能の更新はパッチよりも包括的であり、通常は新しい機能が含まれています（また通常は、6.0.1 のようにバージョン番号の 3 桁目が変更されます）。	Yes	Yes	製品の更新	グローバルのみ
Firepower システムに対するメジャーな更新（メジャーおよびマイナー バージョンのリリース）	メジャーな更新はアップグレードと呼ばれることもあります。この更新には新しい機能が含まれており、製品に対する大規模な変更が含まれることがあります（通常は、6.1 または 6.2 のようにバージョン番号の最初の桁または 2 桁目が変更されます）。メジャーな更新では、Cisco エンド ユーザ ライセンス契約（EULA）の再承認が必要な場合があります。	No	No	製品の更新	グローバルのみ
脆弱性データベース（VDB）	VDB の更新は、オペレーティング システム、アプリケーション、クライアントによって検出された脆弱性、および Firepower システムによって報告された脆弱性に影響を与えます。	Yes	No	製品の更新	グローバルのみ

更新のタイプ	説明	スケジュールを行うか	アンインストールをするか	タブ	ドメイン
侵入ルール	侵入ルールの更新には、新規および更新された侵入ルールとプリプロセッサ ルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が含まれています。ルールの更新では、ルールが削除されたり、新しいルール カテゴリとデフォルトの変数が提供されたり、デフォルトの変数値が変更されたりすることもあります。	Yes	No	ルールの更新	• 侵入ルールの更新：グローバルのみ • ローカル ルールのインポート：任意
位置情報データベース（GeoDB）	GeoDB の更新には、物理的な場所や接続タイプなど、検出されたルート可能な IP アドレスにシステムが関連付けることができるものに関する更新情報が含まれています。位置情報データは、アクセス コントロール ルールとして使用できます。位置情報の詳細を表示するには、GeoDB をインストールする必要があります。	Yes	No	地理位置情報の更新	グローバルのみ

ただし、Firepower システムに対するパッチや他のマイナーな更新はアンインストールできますが、VDB、GeoDB、侵入ルールに対するメジャーな更新をアンインストールしたり、前のバージョンに戻したりすることはできません。自分のアプライアンスを、Firepower システムの新しいメジャー バージョンに更新した場合、古いバージョンに戻す必要がある場合は、サポートに連絡してください。

リリース ノートまたはアドバイザリ テキストに特に記載されていない限り、アプライアンスを更新しても設定は変更されず、アプライアンスの設定はそのまま保持されます。

Firepower システムのソフトウェア アップデート

Firepowerシステムの展開を更新するには、いくつかの基本的な手順があります。最初にリリースノートを参照し、必要な更新前のタスクをすべて完了することで更新の準備を整えておく**必要があります**。その後に更新を開始することができます。まずFirepower Management Centerを更新し、

次にこれが管理するデバイスを更新します。更新が完了し、更新が正常に終了したことを確認するまで、更新の進捗状況を監視する必要があります。最後に、更新後の必要な手順を完了させます。

Firepower システムのソフトウェア アップデートの準備

更新を開始する前に、リリース ノートをよく読んで理解する必要があります。リリース ノートはサポート サイトからダウンロードすることができます。リリース ノートには、サポートされているプラットフォーム、新しい機能、既知および解決済みの問題、製品の互換性について記載されています。また、リリース ノートには前提条件、警告、および特別なのインストールおよびアンインストールの手順についての重要な情報が含まれています。

Firepower システムのバージョンの要件

アプライアンス（ソフトウェアベースのデバイスを含む）が、Firepower システムの正しいバージョンを実行していることを確認する必要があります。リリース ノートには必要なバージョンが示されています。古いバージョンを実行している場合は、サポート サイトから更新を取得することができます。

オペレーティング システム要件

ソフトウェアベースのデバイスをインストールしたコンピュータが、オペレーティング システムの正しいバージョンを実行していることを確認します。リリース ノートには必要なバージョンが示されています。NGIPSv デバイスでサポートされるオペレーティング システムの詳細については、『*Firepower System Virtual Installation Guide*』を参照してください。

時間とディスク スペース要件

十分な空きディスク領域があることを確認し、更新のために十分な時間を確保しておく必要があります。管理対象デバイスを更新する場合は、Firepower Management Center 上に追加のディスク領域が必要になります。リリース ノートには、ディスク領域と時間の要件が示されています。

設定とイベント バックアップのガイドライン

更新を開始する前に、アプライアンスに残っているバックアップを外部の場所にコピーしてから、アプライアンス上のバックアップを削除することを強く推奨します。また、現在のイベント データと設定データを外部の場所にバックアップする必要があります。Firepower Management Center は、以前の更新でローカルに保存されたバックアップを消去します。イベント データは更新プロセスの一部としてバックアップ**されません**。

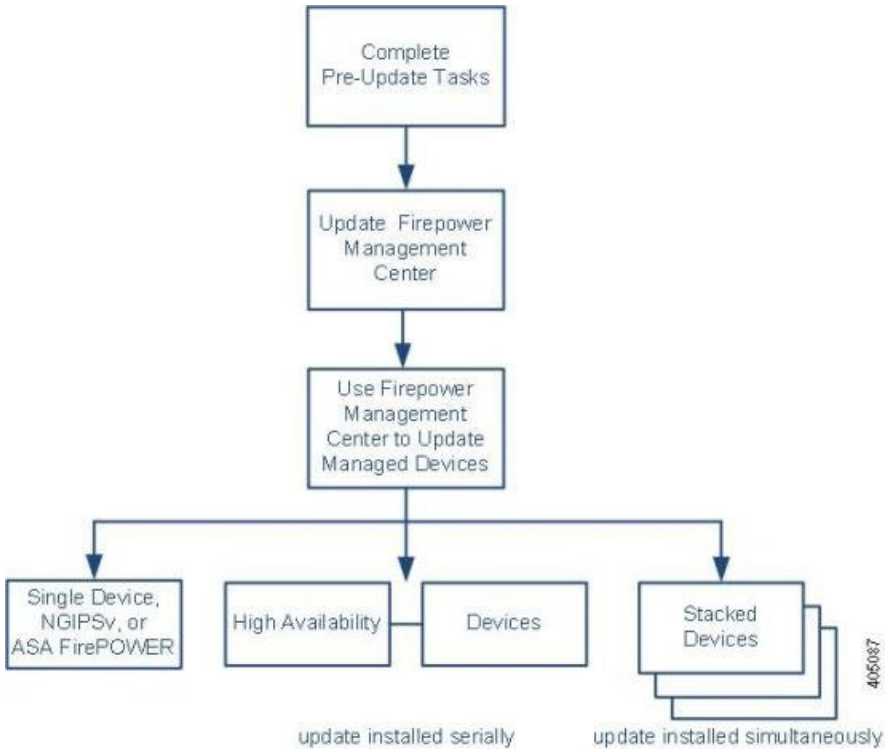
Firepower Management Center を使用して、そのイベント データと設定データ、および管理しているデバイスのイベント データと設定データをバックアップできます。

更新を実行するタイミング

注意 更新プロセスはトラフィックの調査、トラフィック フロー、およびリンク ステートに影響を与えることがあること、および更新を行っている間は Data Correlator が無効になっていることにより、保守を行っている間、または中断が展開に及ぼす影響が最も少ない時間に更新を行うことをお勧めします。

Firepower システムのソフトウェア アップデート プロセス

次のフローチャートは、Firepower システムの更新プロセスを示しています。



更新の順序

使用している Firepower Management Center を更新してから、それらが管理するデバイスを更新する**必要があります**。

Firepower Management Centerを使用した更新の実行

Firepower Management Center の Web インターフェイスを使用して、アプライアンス自体とその管理対象デバイスを更新します。

ヒント　パッチおよび機能の更新では、自動更新機能を利用することができます。

管理対象デバイスの更新は、2段階のプロセスです。まず、サポートサイトから更新をダウンロードして、管理元の Firepower Management Center にアップロードします（http://www.cisco.com/cisco/web/support/index.html）。

次に、ソフトウェアをインストールします。

注意　トラフィックのインスペクション、トラフィック フロー、およびリンク ステートは、デバイスがどのように設定および展開されているか、更新がどのコンポーネントに影響を及ぼすか、更新によってデバイスがリブートされるかどうかよって、更新中に影響を受けることがあります。特定の更新に対してネットワーク トラフィックがいつ、どのように影響を受けるかについての具体的な情報は、対象の更新のリリース ノートを参照してください。

ハイ アベイラビリティ ペアの 7000 および 8000 シリーズ デバイスの更新

ハイ アベイラビリティ ペアの 7000 または 8000 シリーズ デバイスまたはデバイス スタック上で更新をインストールすると、システムは、複数のデバイスまたはスタック上で同時に更新を実行します。更新を開始すると、システムは最初にバックアップ デバイスまたはスタックに更新を適用し、必要なプロセスが再開され、デバイスまたはスタックがトラフィックを再処理するまでメンテナンス モードになります。システムは、アクティブなデバイスまたはスタックに更新を適用し、同じプロセスを行います。

ハイ アベイラビリティペアのスタック内のデバイスを更新するには、ハイ アベイラビリティ ペアのすべてのメンバー上で同時に、管理している Firepower Management Center から更新を実行する必要があります。デバイスから直接更新を実行することはできません。

スタック内の 8000 シリーズ デバイスの更新

スタック構成のデバイスで更新をインストールする場合、システムは更新を同時に実行します。各デバイスは、更新が完了すると通常の動作を再開します。次の点に注意してください。

- すべてのセカンダリ デバイスの更新が完了する前にプライマリ デバイスの更新が完了すると、すべてのデバイスで更新が完了するまでスタックは限定的な、バージョンが混在している状態で動作します。
- すべてのセカンダリ デバイスの更新が完了した後でプライマリ デバイスの更新が完了した場合は、プライマリ デバイスで更新が完了したときに、スタックは通常の動作を再開します。

トラフィック フローとインスペクション

管理対象デバイスから更新をインストールまたはアンインストールすると、次の機能に影響を及ぼすことがあります。

- トラフィック インスペクション（アプリケーションおよびユーザの認識と制御、URL フィルタリング、セキュリティ インテリジェンス フィルタリング、侵入/ファイル/マルウェアのインスペクションと制御、接続のロギングなど）
- トラフィック フロー（スイッチング、ルーティング、NAT、VPN、関連機能など）
- リンク ステート

Data Correlator は、システムの更新中は動作しません。更新が完了すると再開します。

ネットワーク トラフィックの中断の方法と期間は、更新が影響を及ぼす Firepower システムのコンポーネント、デバイスがどのように設定および展開されているか、更新によりデバイスがリブートされるかどうか、によって異なります。特定の更新に対してネットワーク トラフィックがいつ、どのように影響を受けるかについての情報は、リリース ノートを参照してください。

ヒント ハイ アベイラビリティ ペア内の 7000 または 8000 シリーズ デバイスを更新する場合、システムは、トラフィックの中断を回避するために、一度に 1 つずつ更新を実行します。

更新中の Web インターフェイスの使用

更新のタイプに関係なく、更新中のアプライアンスの Web インターフェイスを使用して、更新のモニタ以外のタスクを実行**しないで**ください。

メジャーな更新中にユーザがアプライアンスを使用しないようにし、メジャーな更新の進捗をユーザが簡単にモニタできるようにするために、アプライアンスの Web インターフェイスが合理化されています。メッセージ センターでマイナーな更新の進捗をモニタできます。マイナーな更新中に Web インターフェイスを使用することは禁止されていませんが、シスコでは推奨していません。

ヒント 管理対象デバイスの更新をモニタするには、Firepower Management Center でメッセージ センターを使用します。

マイナーな更新であっても、更新プロセス中は、更新しているアプライアンスの Web インターフェイスは使用できないか、またはアプライアンスでユーザがログアウトされることがあります。これは想定されている動作です。これが発生した場合は、再度ログインして、メッセージ センター（マイナー更新の場合）または [更新ステータス（Update Status）] ページ（メジャー更新の場合）を表示します。まだ更新が実行中の場合は、更新が完了するまで Web インターフェイスを使用**しないで**ください。更新中は、管理対象デバイスが 2 回リブートされることがありますが、これは予想される動作です。

注意 （Web インターフェイスに更新が失敗したことが示されている、メッセージ センターまたは [更新ステータス（Update Status）] ページに進捗が表示されないなど）更新で問題が発生した場合には、更新を再開**しない**でください。代わりに、サポートに連絡してください。

更新後

リリース ノートに記載されている更新後のタスクをすべて完了し、展開が正常に実行されていることを確認する**必要があります**。

注意 Firepower Management Center の更新後、およびその管理対象デバイスの更新後に**再度**、設定を展開する必要があります。

また、次の作業を実行する必要があります。

- 更新が正常に終了したことを確認する
- 展開のすべてのアプライアンスが正常に通信していることを確認する
- 必要に応じて侵入ルール、VDB、および GeoDB を更新する
- リリース ノートの情報に基づいて、必要な設定変更を行う
- リリース ノートに記載されている、更新後の追加タスクを実行する

Firepower システム ソフトウェア アップデートに関する注意事項

更新のタイプ、および Firepower Management Center がインターネットへアクセスできるかどうかによって、Firepower Management Center の Firepower システム ソフトウェアを次のいずれかの方法で更新できます。

- Firepower Management Center がインターネットにアクセスできる場合は、サポート サイトから直接アップデートを取得します。このオプションは、メジャーな更新ではサポート**されていません**。
- サポート サイトからアップデートを手動でダウンロードして、Firepower Management Center へアップロードします。Firepower Management Center がインターネットへアクセスできない場合、またはメジャーな更新を実行している場合は、この方法を選択します。

（注） 上記のいずれかの方法を使用して、アップデートを取得します。電子メールで更新ファイルを転送すると、破損する可能性があります。

[製品アップデート（Product Updates）]ページ（[システム（System）]>[更新（Updates）]）には、それぞれの更新のバージョン、およびその更新が生成された日時が表示されます。また、更新の一環としてリブートが必要かどうかも示されます。

サポートから取得した更新をアプライアンスへアップロードすると、更新がページに示されます。パッチ機能および機能の更新のアンインストーラも表示されます。Firepower Management Center で、ページに VDB 更新を表示できます。

メジャーな更新の場合は、Firepower Management Center を更新すると、以前の更新のアンインストーラが削除されます。

Firepower Management Center でのソフトウェアの更新

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

はじめる前に

- Firepower Management Center で実行時間が長いタスクの実行を許可します。
- Firepower Management Center に更新をアップロードします。詳細については、Firepower システムのソフトウェア更新のダウンロード，（148 ページ）と Firepower Management Center にソフトウェア更新をアップロードする，（149 ページ）を参照してください。

手順

ステップ 1 リリース ノートを読んで、更新前の必要なタスクを完了させます。

ステップ 2 展開内でデバイスが正常に通信していること、およびヘルス モニタによって問題が報告されていないことを確認します。

ステップ 3 [システム（System）] > [更新（Updates）]を選択します。

ステップ 4 アップロードした更新の横にあるインストール アイコンをクリックします。

ステップ 5 Firepower Management Center を選択し、[インストール（Install）] をクリックします。プロンプトが表示されたら、更新をインストールすることを確認して Firepower Management Center をリブートします。

ステップ 6 オプションで、更新ステータスをモニタします。

- マイナー更新については、タスク メッセージの表示，（303 ページ）を参照してください。
- メジャー更新については、主要な Firepower システム ソフトウェア更新のモニタリング，（151 ページ）を参照してください。

注意 更新のタイプに関係なく、更新が完了するまで、更新の監視以外のタスクを実行するために Web インターフェイスを使用**しないで**ください。必要な場合は、Firepower Management Center を再起動します。

更新で問題が発生した場合（更新に失敗したことがメッセージ センターに示されている場合、またはメッセージに進捗が表示されない場合など）、更新を再開**しないでください**。代わりに、サポートに連絡してください。

ステップ 7 更新が完了したら、必要に応じて Firepower Management Center にログインします。

ステップ 8 メジャー更新の後に最初にログインするユーザの場合、エンド ユーザ ライセンス契約（EULA）を確認して同意し、続行します。

ステップ 9 ブラウザのキャッシュを消去し、ブラウザを強制的にリロードします。そうしない場合、ユーザ インターフェイスが予期しない動作を示すことがあります。

ステップ 10 システム情報を表示するには、[ヘルプ（Help）] > [バージョン情報（About）]を選択します。

ステップ 11 システム情報ページで、ソフトウェア バージョンが正しくリストされていることを確認し、Firepower Management Center のルールの更新および VDB のバージョンをメモします。これらの情報が後で必要になります。

ステップ 12 すべての管理対象デバイスが、Firepower Management Center と正常に通信していることを確認します。

次の作業

- 新しい侵入ルールの更新があれば、それをインポートします（侵入ルールの更新, （157 ページ）を参照）。
- Firepower Management Center 上の VDB より新しい VDB があれば、サポート サイトからインストールします（脆弱性データベースの更新, （155 ページ）を参照）。
- 管理対象デバイスのシステム ソフトウェアを更新します（ を参照）。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

Firepower システムのソフトウェア更新のダウンロード

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

メジャー アップデートを除くすべてのアップデートについて、Firepower Management Center にソフトウェア アップデートをダウンロードできます。ダウンロードするには、Firepower Management Center がインターネットにアクセスできる必要があります。

はじめる前に

- Firepower Management Center にインターネット アクセス権があることを確認してください（セキュリティ、インターネット アクセス、および通信ポート, （2187 ページ）を参照）。

手順

ステップ 1 [システム（System）] > [更新（Updates）]を選択します。

ステップ 2 [アップデートのダウンロード（Download Updates）] をクリックして、Cisco サポート サイト（http://www.cisco.com/cisco/web/support/index.html）の最新の更新を確認します。

ステップ 3 更新をインストールします。詳細については、Firepower Management Center でのソフトウェアの更新, （147 ページ）と 脆弱性データベースの更新, （156 ページ）を参照してください。

Firepower Management Center にソフトウェア更新をアップロードする

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

次の場合に、Firepower Management Center に更新をアップロードする必要があります。

- メジャー更新を実行している。
- Firepower Management Center にインターネットへのアクセスがない。
- 管理対象デバイスを更新している。

手順

ステップ 1 シスコのサポート サイト（http://www.cisco.com/cisco/web/support/index.html）から更新を手動でダウンロードします。

ステップ 2 [システム（System）] > [更新（Updates）]を選択します。

ステップ 3 [更新のアップロード（Upload Update）] をクリックします。

ステップ 4 更新を参照し、[アップロード（Upload）] をクリックします。

次の作業

- 更新をインストールします。詳細については、Firepower Management Center でのソフトウェアの更新, （147 ページ）と 脆弱性データベースの更新, （156 ページ）を参照してください。

管理対象デバイスでのソフトウェア更新

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

この手順のすべてのステップは、注記がない限り、Firepower Management Center で実行されます。

はじめる前に

- デバイスを管理する Firepower Management Center で Firepower System ソフトウェアを更新します。詳細については、Firepower システム ソフトウェア アップデートに関する注意事項, （146 ページ）を参照してください。
- Firepower Management Center に更新をアップロードします。詳細については、Firepower Management Center にソフトウェア更新をアップロードする, （149 ページ）を参照してください。

手順

ステップ 1 リリース ノートを読んで、更新前に必要なタスクを完了させます（Firepower システム ソフトウェア アップデートに関する注意事項, （146 ページ）およびFirepower システムのソフトウェア アップデートの準備, （142 ページ）を参照）。

ステップ 2 展開内でアプライアンスが正常に通信していること、およびヘルス モニタによって問題が報告されていないことを確認します。

ステップ 3 [システム（System）] > [更新（Updates）]を選択します。

ステップ 4 インストール中の更新の横にあるインストール アイコンをクリックします。

ステップ 5 更新をインストールするデバイスを選択し、[インストール（Install）] をクリックします。
同じ更新が使用される場合、複数のデバイスを一度に更新することができます。プロンプトが表示されたら、更新をインストールすることを確認してデバイスを再起動します。

ファイルのサイズによっては、すべてのデバイスで更新をインストールするのに時間がかかることがあります。更新中に、管理対象デバイスが 2 回再起動されることがありますが、これは正常な動作です。

ステップ 6 オプションで、更新ステータスをモニタします。

- マイナー更新については、タスク メッセージの表示, （303 ページ）を参照してください。
- メジャー更新については、主要な Firepower システム ソフトウェア更新のモニタリング, （151 ページ）を参照してください。

注意 更新のタイプに関係なく、更新が完了するまで、更新の監視以外のタスクを実行するために Web インターフェイスを使用**しないで**ください。必要な場合は、管理対象デバイスを再起動します。

更新で問題が発生した場合（更新に失敗したことがメッセージ センターに示されている場合、またはメッセージに進捗が表示されない場合など）、更新を再開**しないでください**。代わりに、サポートに連絡してください。

ステップ 7 ブラウザのキャッシュを消去し、ブラウザを強制的にリロードします。そうしない場合、ユーザインターフェイスが予期しない動作を示すことがあります。

ステップ 8 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択して、更新したデバイスに正しいバージョンがリストされていることを確認します。

ステップ 9 更新したデバイスが、Firepower Management Center と正常に通信していることを確認します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。
- オプションで、7000 または 8000 シリーズ デバイスへのメジャー更新の後でデバイスのローカル Web インターフェイスにログインします。メジャー更新の後に最初にログインするユーザには、エンド ユーザ ライセンス契約（EULA）が表示されることがあります。EULA を確認して承認し、処理を続行します。Web インターフェイスではなくコマンドライン インターフェイスを介して最初にログインした場合も EULA が表示されるので、必ず承認してください。

主要な Firepower システム ソフトウェア更新のモニタリング

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

この手順は、アプライアンスのローカル Web インターフェイスを使用して実行する必要があります。

手順

ステップ 1 アプライアンスが必要な更新前チェックを完了するまで、メジャー ソフトウェア アップデートの進行を Message Center でモニタします。

この時点で、自分も含めてすべてのユーザは、システムによってWebインターフェイスからログアウトされます。管理者またはメンテナンス ユーザ以外は、更新が完了するまでログインし直すことはできません。

ステップ 2 管理者の場合は、Web インターフェイスにログインし直します。簡略化された更新ページが表示されます。

ステップ 3 更新ログを表示するには、[現在のスクリプトのログを表示する（show log for current script）] をクリックします。ログをもう一度非表示にするには、[現在のスクリプトのログを非表示する（hide log for current script）] をクリックします。

注意 更新で問題が生じた場合は（簡略化された更新ページを手動更新しても長時間にわたって進捗が表示されない場合など）、更新を再開**しないでください**。代わりに、サポートに連絡してください。

次の作業

- 何らかの理由で更新に失敗した場合は、このページにエラーメッセージが表示され、失敗した日時、更新が失敗したときに実行していたスクリプト、およびサポートへの連絡方法が示されます。更新は再開**しないで**ください。
- 更新が正常に完了すると、ページに成功メッセージが表示され、アプライアンスがリブートされます。アプライアンスのリブートが完了したら、ページを更新してログインし、更新後の必要な手順を完了します。

Firepower システムのソフトウェア アップデートのアンインストール

パッチまたは機能の更新を適用すると、更新プロセスによってアンインストーラが作成されます。これにより、Web インターフェイスを使用してアプライアンスから更新を削除することができます。

更新をアンインストールした場合、結果として保持されるバージョンは、アプライアンスの更新パスに応じて異なります。たとえば、アプライアンスをバージョン 6.0 からバージョン 6.0.0.2 へ直接更新した場合のシナリオについて考えてみます。バージョン 6.0.0.2 のパッチをアンインストールすると、バージョン 6.0.0.1 の更新をインストールしたことがなくても、バージョン 6.0.0.1 を実行するアプライアンスが結果として生成されます。更新をアンインストールしたときに結果として生成される Firepower ソフトウェアのバージョンの詳細については、リリース ノートを参照してください。

注意 メジャーな更新では、Webインターフェイスからのアンインストールはサポートされていません。アプライアンスを Firepower システムの新しいメジャー バージョンに更新して、古いバージョンに戻す必要がある場合は、サポートに連絡してください。

アンインストールの順序

更新は、インストールと逆の順序でアンインストールします。つまり、最初に管理対象デバイスから更新をアンインストールしてから、Firepower Management Center からアンインストールします。

ローカル Web インターフェイスを使用した更新のアンインストール

更新をアンインストールするにはローカル Web インターフェイスを使用する必要があります。Firepower Management Center を使用して、管理対象デバイスから更新をアンインストールすることはできません。ローカル Web インターフェイスを持たないデバイス（NGIPSv デバイスなど）からパッチをアンインストールする場合の詳細については、リリース ノートを参照してください。

ハイ アベイラビリティ ペアからの 7000 および 8000 シリーズ デバイスのアンインストール

ハイ アベイラビリティ ペアの 7000 または 8000 シリーズ デバイスは、同じバージョンの Firepower システムを実行する必要があります。アンインストール プロセスは自動フェールオーバーをトリガーしますが、不一致のハイ アベイラビリティ ペアの 7000 または 8000 シリーズ デバイスは、設定情報を共有せず、同期の一部として更新をインストールまたはアンインストールすることもありません。冗長デバイスから更新をアンインストールする必要がある場合は、即時および連続的にアンインストールを実行するように計画します。

アンインストールによって、これらのデバイスが、ハイ アベイラビリティへのスタックの設定がサポートされないバージョンに戻される場合は、ハイ アベイラビリティ ペアとして設定されたスタックの 7000 または 8000 シリーズ デバイスから更新をアンインストールできません。

運用の継続性を保証するために、ハイ アベイラビリティ ペアのデバイスから一度に 1 つずつ更新をアンインストールします。まず、セカンダリ デバイスから更新をアンインストールします。アンインストール プロセスが完了するまで待ってから、すぐにプライマリ デバイスから更新をアンインストールします。

注意 ハイ アベイラビリティ ペアのデバイスでのアンインストール プロセスが失敗した場合は、アンインストールを再開したり、ピアの設定を変更したり**しないで**ください。代わりに、サポートに連絡してください。

スタック構成のデバイスからの更新のアンインストール

スタック内のすべてのデバイスが、同じバージョンの Firepower システムを実行する必要があります。スタック構成のデバイスのいずれかから更新をアンインストールすると、そのスタックではデバイスが限定的な、バージョンが混在する状態になります。

展開への影響を最小にするために、スタック構成のデバイスから更新を同時にアンインストールします。スタック内のすべてのデバイスで更新が完了すると、スタックは通常の動作を再開します。

アンインストールによって、これらのデバイスが、ハイ アベイラビリティへのスタックの設定がサポートされないバージョンに戻される場合は、ハイ アベイラビリティ ペアとして設定されたスタックの 7000 または 8000 シリーズ デバイスから更新をアンインストールできません。

トラフィック フローとインスペクション

管理対象デバイスから更新をアンインストールすると、トラフィックのインスペクション、トラフィック フロー、およびリンク ステートに影響を及ぼすことがあります。特定の更新に対してネットワーク トラフィックがいつ、どのように影響を受けるかについての情報は、リリース ノートを参照してください。

アンインストール後

更新をアンインストールした後で、展開が正しく機能していることを確認するために、いくつかの手順を実行する必要があります。これらはアンインストールが成功したこと、および展開のすべてのアプライアンスが正常に通信していることを確認することが含まれます。それぞれの更新に特定の情報については、リリース ノートを参照してください。

Firepower システムのソフトウェア更新のアンインストール

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

この手順は、Firepower Management Center と 7000 & 8000 シリーズ デバイスで実行できます。

はじめる前に

- アプライアンスを Firepower System の新しいメジャー バージョンに更新した後に、古いバージョンに戻す必要が生じた場合は、サポートに連絡してください。メジャー更新では、Web インターフェイスからのアンインストールはサポートされていません。

手順

ステップ 1 [システム（System）] > [更新（Updates）]を選択します。

ステップ 2 削除する更新のアンインストーラの隣にあるインストール アイコンをクリックします。プロンプトが表示されたら、更新をアンインストールすることを確認して、アプライアンスをリブートします。

- Firepower Management Center で、[アップデートをインストール（Install Update）] ページが表示されます。Firepower Management Center を選択し、[インストール（Install）] をクリックします。
- 管理対象デバイスには、操作のページがありません。

注意 アンインストールが完了するまで、更新の監視以外のタスクを実行するために Web インターフェイスを使用**しないで**ください。必要に応じて、アプライアンスをリブートします。

ステップ 3 必要に応じて、タスクのステータスをモニタします（タスク メッセージの表示, （303 ページ）を参照）。

ステップ 4 アンインストールが完了したら、必要に応じてアプライアンスにログインします。

ステップ 5 ブラウザのキャッシュを消去し、ブラウザを強制的にリロードします。そうしない場合、ユーザインターフェイスが予期しない動作を示すことがあります。

ステップ 6 [ヘルプ（Help）] > [バージョン情報（About）] を選択し、ソフトウェアのバージョンが正しく示されていることを確認します。

次の作業

- パッチをアンインストールしたアプライアンスが正常に管理対象デバイスと通信していること（Firepower Management Center の場合）、または管理元のFirepower Management Center と通信していること（管理対象デバイスの場合）を確認します。
- アンインストールが成功したこと、および展開環境のすべてのアプライアンスが正常に通信していることを確認します。それぞれの更新に特定の情報については、リリース ノートを参照してください。

脆弱性データベースの更新

シスコの脆弱性データベース（VDB）は、オペレーティング システム、クライアント、およびアプリケーションのフィンガープリントだけでなく、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。Firepower システムはフィンガープリントと脆弱性を関連付けて、特定のホストがネットワークの侵害のリスクを増大させているかどうかを判断するのをサポートします。Cisco Talos Security Intelligence and Research Group（Talos） では、VDB の定期的な更新を配布しています。

VDB を更新するには、Firepower Management Center で [製品の更新（Product Updates）] ページを使用します。サポートから取得した VDB 更新をアプライアンスへアップロードすると、このページに、アップロードした更新と Firepower システムの更新およびそのアンインストーラの更新が表示されます。

（注） 手動でまたは [アップデートのダウンロード（Download Updates）] をクリックして、サポート サイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、破損する可能性があります。

脆弱性のマッピングを更新するのにかかる時間は、ネットワーク マップ内のホストの数によって異なります。システムのダウンタイムの影響を最小にするために、システムの使用率が低い時間

帯に更新をスケジュールすることをお勧めします。一般的に、更新の実行にかかるおおよその時間（分）を判断するには、ネットワーク上のホストの数を 1000 で割ります。

VDB を更新した後、更新されたアプリケーション ディテクタとオペレーティング システム フィンガープリントを有効にするために、設定を展開する必要があります。

注意 VDB アップデートをインストールした後、初めて脆弱性データベース（VDB）アップデートをインストールするか、またはアクセス コントロール ポリシーを展開すると、すぐに Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

自動更新機能を利用して VDB 更新をスケジュールすることができます。

脆弱性データベースの更新

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

この手順は、Firepower Management Center でしか実行できません。

はじめる前に

- Firepower Management Center に更新をアップロードします。詳細については、Firepower システムのソフトウェア更新のダウンロード, （148 ページ）と Firepower Management Center にソフトウェア更新をアップロードする, （149 ページ）を参照してください。

注意 VDB アップデートをインストールした後、初めて脆弱性データベース（VDB）アップデートをインストールするか、またはアクセス コントロール ポリシーを展開すると、すぐに Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

手順

ステップ 1 更新用の VDB 更新アドバイザリ テキストを読みます。このアドバイザリ テキストには、更新で作成された VDB に対する変更、および製品の互換性情報が含まれています。

ステップ 2 [システム（System）] > [更新（Updates）]を選択します。

ステップ 3 [製品の更新（Product Updates）] タブで、VDB 更新の横にあるインストール アイコンをクリックします。

ステップ 4 Firepower Management Center エントリの横にあるチェックボックスをオンにします。

ステップ 5 [Install（インストール）]をクリックします。ネットワーク マップ内のホストの数によっては、更新のインストールに時間がかかることがあります。

ステップ 6 必要に応じて、タスクのステータスをモニタします（タスク メッセージの表示, （303 ページ）を参照）。

注意 更新が完了するまで、マップされた脆弱性に関連するタスクを実行するために Web インターフェイスを使用**しないで**ください。更新で問題が発生した場合には（たとえば、メッセージ センターに進捗が表示されない、更新が失敗したことが示されているなど）、更新を再開**しない**でください。代わりに、サポートに連絡してください。

ステップ 7 更新が終了したら、[ヘルプ（Help）] > [バージョン情報（About）] を選択して、VDB のビルド番号が、インストールした更新と一致していることを確認します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。
- オプションで、VDB 更新をスケジュールします（脆弱性データベースの更新の自動化, （210 ページ）を参照）。

関連トピック

Snort® の再起動シナリオ , （324 ページ）

侵入ルールの更新

新しい脆弱性が明らかになるのに伴い、Cisco Talos Security Intelligence and Research Group（Talos）は侵入ルールの更新をリリースします。これらの更新を Firepower Management Center にインポートして、変更後の設定を管理対象デバイスに導入することで、侵入ルールの更新を実装できます。それらの更新は、侵入ルール、プリプロセッサ ルール、およびルールを使用するポリシーに影響を及ぼします。

侵入ルール更新は更新を累積されていくものなので、常に最新の更新をインポートすることをお勧めします。現在インストールされているルールのバージョン以前の侵入ルールの更新をインポートすることはできません。

侵入ルールの更新では、次のものを提供します。

- **新規または変更されたルールおよびルール ステータス**：ルール更新は、新規および更新された侵入ルールとプリプロセッサ ルールを提供します。新規ルールの場合は、システム付属の各侵入ポリシーでルール ステータスが異なることがあります。たとえば、新規ルールが、Security over Connectivity 侵入ポリシーでは有効になっており、Connectivity over Security 侵入ポリシーでは無効になっていることがあります。ルールの更新では、既存のルールのデフォルトの状態が変更されたり、既存のルールが完全に削除されることもあります。
- **新しいルール カテゴリ**：ルール更新には、常に追加される新しいルール カテゴリが含まれている場合があります。
- **変更されたプリプロセッサおよび詳細設定**：ルール更新によって、システム付属侵入ポリシーの詳細設定、およびシステム付属ネットワーク分析ポリシーのプリプロセッサ設定が変更されることがあります。また、アクセス コントロール ポリシーの高度な前処理およびパフォーマンスのオプションのデフォルト値も変更される場合があります。
- **新規および変更された変数**：ルール更新によって、既存のデフォルト変数のデフォルト値が変更されることがありますが、ユーザによる変更は上書きされません。新しい変数が常に追加されます。

マルチドメイン展開では、ローカル侵入ルールを任意のドメインにインポートできますが、グローバル ドメイン内の Talos からでなければ、侵入ルールの更新をインポートすることはできません。

侵入ルールの更新によってポリシーが変更されるタイミングについて

侵入ルールの更新は、システムが提供するネットワーク分析ポリシーとカスタム ネットワーク分析ポリシーの両方だけでなく、すべてのアクセス コントロール ポリシーにも影響する場合があります。

- **システム提供**：システムが提供するネットワーク解析および侵入ポリシーへの変更は、その他のアクセス コントロールの詳細設定と同様に、更新後にポリシーを再適用すると自動的に有効になります。
- **カスタム**：すべてのカスタム ネットワーク分析ポリシーと侵入ポリシーは、システム付属ポリシーをそのベースとして、またはポリシー チェーンの根本的ベースとして使用しているので、ルール更新によってカスタム ネットワーク分析ポリシーと侵入ポリシーが影響を受けることがあります。ただし、ルール更新によるこれらの自動的な変更は回避することができます。これにより、ルール更新のインポートとは関係ないスケジュールで、システムによって提供される基本ポリシーを手動で更新できます。ユーザによる選択（カスタム ポリシーごとに実装）とは関係なく、システム付属ポリシーに対する更新によって、カスタマイズ済みの設定が上書きされることは**ありません**。

ルール更新をインポートすると、ネットワーク分析ポリシーと侵入ポリシーのキャッシュされていた変更がすべて廃棄されるので注意してください。便宜のために、[ルールの更新（Rule Updates）] ページには、キャッシュされている変更があるポリシー、および変更を行ったユーザが表示されます。

侵入ルールの更新の展開

侵入ルールの更新によって行われた変更を有効にするには、設定を再導入する必要があります。侵入ルールの更新をインポートする際に、影響を受けるデバイスに自動的に再導入するようシステムを設定できます。この手法が特に役立つのは、侵入ルールの更新によるシステム提供の基本侵入ポリシーの変更を許可する場合です。

注意 ルール更新をインポートするときには、設定の変更を展開するとSnortプロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。ルール更新のダウンロードおよびインストール プロセスがセキュリティ ポリシーに従っていることを確認してください。また、侵入ルールの更新のサイズは大きいことがあるため、ルールのインポートはネットワークの使用量が少ないときに行うようにしてください。

侵入ルールの更新の繰り返し

[ルールの更新（Rule Updates）] ページを使用して、ルール更新を日次、週次、または月次ベースでインポートすることができます。

侵入ルールの更新のインポートに適用されるサブタスクは、ダウンロード、インストール、ベース ポリシーの更新、設定の展開の順で実行されます。1 つのサブタスクが完了すると、次のサブタスクが開始されます。

スケジュールされた時間になると、システムはルールの更新をインストールして、前のステップで指定したように変更後の設定を展開します。インポートの前、またはインポート中にログオフすることも、Web インターフェイスを使用して他のタスクを実行することもできます。インポート中に [ルールの更新ログ（Rule Update Log）] にアクセスすると、赤色のステータス アイコン（  ）が表示され、[ルールの更新ログ（Rule Update Log）] 詳細ビューに表示されるメッセージを確認できます。ルール更新のサイズと内容によっては、ステータス メッセージが表示されるまでに数分かかることがあります。

ローカル侵入ルールのインポート

ローカル侵入ルールは、ASCII または UTF-8 エンコーディングによるプレーン テキスト ファイルとしてローカル マシンからインポートするカスタム標準テキスト ルールです。Snort ユーザ マニュアル（http://www.snort.org で入手可能）の指示に従って、ローカル ルールを作成することができます。

マルチドメイン展開では、任意のドメインにローカル侵入ルールをインポートできます。現在のドメインと親ドメインにインポートされたローカル侵入ルールを表示できます。

侵入ルールのワンタイム手動更新

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

Firepower Management Center にインターネット アクセスがない場合、新しい侵入ルールの更新を手動でインポートします。

手順

ステップ 1 シスコのサポート サイト（http://www.cisco.com/cisco/web/support/index.html）から更新を手動でダウンロードします。

ステップ 2 [システム（System）]>[更新（Updates）] を選択し、[ルールの更新（Rule Updates）] タブをクリックします。

ステップ 3 削除されるフォルダに作成またはインポートしたすべてのユーザ定義ルールを移動する場合、ツールバーで [すべてのローカル ルールの削除（Delete All Local Rules）] をクリックして [OK] をクリックする必要があります。

ステップ 4 [アップロードおよびインストールするルールの更新またはテキスト ルール ファイル（Rule Update or text rule file to upload and install）] を選択し、[参照（Browse）] をクリックして、ルール アップデート ファイルを選択します。

ステップ 5 更新が完了した後に、ポリシーを管理対象デバイスに自動的に再展開する場合、[ルールの更新のインポートが完了した後にすべてのポリシーを再適用する（Reapply all policies after the rule update import completes）] をオンにします。

ステップ 6 [インポート（Import）] をクリックします。ルールの更新がインストールされ、[ルール アップデート ログ（Rule Update Log）] 詳細ビューが表示されます。

（注） ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

侵入ルールのワンタイム自動更新

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

新しい侵入ルールの更新を自動的にインポートするには、サポート サイトに接続するためのインターネット アクセスがアプライアンスで必要になります。

はじめる前に

- Firepower Management Center にインターネット アクセス権があることを確認してください（セキュリティ、インターネット アクセス、および通信ポート，（2187 ページ） を参照）。

手順

ステップ 1 [システム（System）] > [更新（Updates）]を選択します。

ステップ 2 [ルールの更新（Rule Updates）] タブをクリックします。

ステップ 3 削除されるフォルダに作成またはインポートしたすべてのユーザ定義ルールを移動する場合、ツールバーで [すべてのローカル ルールの削除（Delete All Local Rules）] をクリックして [OK] をクリックします。

ステップ 4 [サポート サイトから新しいルールの更新をダウンロードする（Download new Rule Update from the Support Site）] を選択します。

ステップ 5 更新が完了した後に、変更した設定を管理対象デバイスに自動的に再展開する場合、[ルールの更新のインポートが完了した後にすべてのポリシーを再適用する（Reapply all policies after the rule update import completes）] チェックボックスをオンにします。

ステップ 6 [インポート（Import）] をクリックします。
ルールの更新がインストールされ、[ルール アップデート ログ（Rule Update Log）] 詳細ビューが表示されます。

注意 ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

定期的な侵入ルール更新の設定

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

手順

ステップ 1 [システム（System）] > [更新（Updates）]を選択します。

ステップ 2 [ルールの更新（Rule Updates）] タブをクリックします。

ステップ 3 作成した、または削除されたフォルダにインポートしたすべてのユーザ定義ルールを移動するには、ツールバーで [すべてのローカル ルールの削除（Delete All Local Rules）] をクリックし、[OK] をクリックします。

ステップ 4 [ルール アップデートの再帰的なインポートを有効にする（Enable Recurring Rule Update Imports）] チェックボックスをオンにします。
[ルール アップデートの再帰的なインポート（Recurring Rule Update Imports）] セクションの見出しの下に、インポート ステータスに関するメッセージが表示されます。

ステップ 5 [インポート頻度（Import Frequency）] フィールドで、次を指定します。

- 更新の頻度（[日次（Daily）]、[週次（Weekly）]、または [月次（Monthly）]）。
- 更新が必要な曜日または日付。
- 更新を開始する時刻。

ステップ 6 更新の完了後、変更された設定を管理対象デバイスに自動的に再展開するには、[ルール更新の完了後、更新されたポリシーを管理対象デバイスに展開する（Deploy updated policies to targeted devices after rule update completes）] チェックボックスをオンにします。

ステップ 7 [保存（Save）] をクリックします。

注意 侵入ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

[ルール アップデートの再帰的なインポート（Recurring Rule Update Imports）] セクションの見出しの下のステータス メッセージが変わり、ルールの更新がまだ実行されていないことが示されます。

ローカル侵入ルール ファイル インポート

ローカル ルール ファイルをインポートする際には次のガイドラインに従います。

- ルールのインポータには、すべてのカスタム ルールが ASCII または UTF-8 でエンコードされるプレーン テキスト ファイルにインポートされることが必要です。
- テキスト ファイル名には英数字とスペースを使用できますが、下線（_）、ピリオド（.）、ダッシュ（-）以外の特殊記号は使用できません。
- システムは、単一のポンド文字（#）で始まるローカル ルールをインポートしますが、これらには削除のフラグが立てられます。
- 単一のポンド文字（#）で始まるローカル ルールはインポートされますが、2 つのポンド文字（##）で始まるローカル ルールはインポートされません。
- ルールにはエスケープ文字を含めることはできません。
- ローカル ルールをインポートするときにはジェネレータ ID（GID）を指定する必要はありません。指定する場合は、標準テキスト ルールに GID 1 のみを指定します。

- ルールを初めてインポートするときには、Snort ID（SID）またはリビジョン番号を指定**しない**でください。これにより、削除されたルールを含むその他のルールの SID の競合を回避できます。システムはルールに対して、1000000 以上の次に使用できるカスタム ルール SID 、およびリビジョン番号 の 1 を自動的に割り当てます。

  SID を持つルールをインポートする必要がある場合、SID は 1,000,000 ～ 9,999,999 の間の一意の数字でなければなりません。

  マルチドメイン展開では、SID が Firepower Management Center 上のすべてのドメインによって使用される共有プールからインポートされたルールに割り当てられます。複数の管理者がローカル ルールを同時にインポートしている場合、個々のドメイン内の SID が連続していないように見える場合があります。それは、数字が別のドメインにシーケンスに割り込んで指定されたためです。

- 以前にインポートしたローカル ルールの更新バージョンをインポートするとき、または削除したローカル ルールを元に戻すときは、システムによって指定された SID および現在のリビジョン番号より大きいリビジョン番号を含める**必要があります**。ルールを編集して、現在のルールまたは削除されたルールのリビジョン番号を判別できます。

  （注） ローカル ルールを削除すると、システムは自動的にリビジョン番号を増やします。これは、ローカル ルールを元に戻すための方法です。削除されたすべてのローカル ルールは、ローカル ルール カテゴリから、削除されたルール カテゴリへ移動されます。

- ルールに次のいずれかが含まれていると、インポートに失敗します。

  - 2147483647 より大きい SID。
  - 64 文字よりも長い送信元ポートまたは宛先ポートのリスト。

- 非推奨の `threshold` キーワードと侵入イベントしきい値機能を組み合わせて使用しているローカル ルールをインポートして、侵入ポリシーで有効にすると、ポリシーの検証に失敗します。
- インポートされたすべてのローカル ルールは、ローカル ルール カテゴリに自動的に保存されます。
- システムによって、インポートしたローカル ルールは常に無効なルール状態に設定されます。ローカル ルールを侵入ポリシーで使用できるようにするには、ローカル ルールの状態を手動で設定する必要があります。

ローカル侵入ルール ファイルのインポート

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

次の説明に従ってインポートした進入ルールは、ローカル ルール カテゴリに保存されます。

手順

ステップ 1 [システム（System）] > [更新（Updates）]を選択します。

ステップ 2 [ルールの更新（Rule Updates）] タブをクリックします。

ステップ 3 [ルールの更新またはアップロードおよびインストールするテキスト ルール ファイル（Rule Update or text rule file to upload and install）] を選択して、ルール ファイルにナビゲートするために [参照（Browse）] をクリックします。

ステップ 4 [インポート（Import）] をクリックします。

次の作業

- 侵入ポリシーで、適切なルールが有効になっていることを確認してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ルールの更新ログ

Firepower Management Center は、ユーザがインポートする各ルール更新およびローカル ルール ファイルごとに 1 つのレコードを生成します。

各レコードにはタイム スタンプ、ファイルをインポートしたユーザの名前、およびインポートが正常に終了したか失敗したかを示すステータス アイコンが含まれています。ユーザは、インポートしたすべてのルール更新とローカル ルール ファイルのリストを管理したり、リストからレコードを削除したり、インポートしたすべてのルールとルール更新コンポーネントに関する詳細レコードにアクセスすることができます。

[ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューには、ルール更新またはローカル ルール ファイルにインポートされた各オブジェクトの詳細レコードが表示されます。表示されるレコードのうち、自分のニーズに合う情報のみを含むカスタム ワークフローまたはレポートを作成することもできます。

侵入ルール更新のログ テーブル

表 *18*：侵入ルール更新のログ フィールド

フィールド	説明
要約	インポート ファイルの名前。インポートが失敗した場合は、ファイル名の下に、失敗した理由の簡単な説明が表示されます。
時刻（Time）	インポートが開始された日時。

フィールド	説明
ユーザ ID（User ID）	インポートをトリガーとして使用したユーザ名。
ステータス（Status）	インポートの状態を表します • 正常終了（） • 失敗、または実行中（） インポート中には [ルールアップデートログ（Rule Update Log）] ページで、正常終了しなかった、または完了していないことを示す赤いステータスアイコンが表示され、インポートが正常終了した場合のみこれが緑色のアイコンに変わります。

ヒント　侵入ルール更新のインポートの進行中に示される、インポートの詳細を表示することができます。

侵入ルールの更新ログの表示

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

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1　[システム（System）] > [更新（Updates）]を選択します。

ヒント　侵入ルール エディタ ページ（[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]）の [インポート ページ（Import Rules）] をクリックすることもできます。

ステップ 2　[ルールの更新（Rule Updates）] タブをクリックします。

ステップ 3　[ルールアップデートログ（Rule Update Log）] をクリックします。

ステップ 4　次の 2 つの対処法があります。

- 詳細の表示：ルールの更新またはローカル ルール ファイルにインポートされる各オブジェクトの詳細を表示するには、表示するファイルの横にある表示アイコン（）をクリックします（侵入ルールの更新インポート ログの詳細の表示, （168 ページ）を参照）。
- 削除：インポート ログからインポート ファイル レコード（ファイルに含まれるすべてのオブジェクトに関する詳細レコードを含む）を削除するには、インポート ファイル名の横にある削除アイコン（）をクリックします。

  （注） ログからファイルを削除しても、インポート ファイルにインポートされているオブジェクトはいずれも削除されませんが、インポート ログ レコードのみは削除されます。

ルール アップデートのインポート ログの詳細ビュー

ヒント 1 つのインポート ファイルのレコードのみが表示されている [ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューからツールバーの [検索（Search）] をクリックして検索を開始した場合でも、[ルール アップデートのインポート ログ（Rule Update Import Log）]データベースの全体が検索されます。検索の対象とするすべてのオブジェクトが含まれるように、時間制限が設定されていることを確認します。

表 *19* : *[*ルール アップデートのインポート ログ（***Rule Update Import Log***）*]* 詳細ビューのフィールド

フィールド	説明
操作（Action）	オブジェクト タイプについて、次のいずれかが発生していることを示します。 • [新規（new）]（ルールで、このアプライアンスにルールが最初に格納された場合） • [変更済み（changed）]（ルール更新コンポーネントまたはルール用。ルール更新コンポーネントが変更された場合、またはルールのリビジョン番号が大きく、GID と SID が同じ場合） • [競合（collision）]（ルール更新コンポーネントまたはルール用。アプライアンス上の既存のコンポーネントまたはルールとリビジョンが競合しているため、インポートがスキップされた場合） • [削除済み（deleted）]（ルール用。ルール更新からルールが削除された場合） • [有効（enabled）]（ルール更新の編集で、プリプロセッサ、ルール、または他の機能が、システムで提供されるデフォルト ポリシーで有効になっていた場合） • [無効（disabled）]（ルールで、システム提供のデフォルト ポリシーでルールが無効になっていた場合） • [ドロップ（drop）]（ルールで、システムで提供されるデフォルト ポリシーで、ルールが [ドロップおよびイベントの生成（Drop and Generate Events）] に設定されていた場合） • [エラー（error）]（ルール更新またはローカル ルール ファイル用。インポートに失敗した場合） • [適用（apply）]（インポートに対して [ルール更新のインポート完了後にすべてのポリシーを再適用する（Reapply all policies after the rule update import completes）] オプションが有効だった場合）
デフォルト アクション（Default Action）	ルールの更新によって定義されたデフォルトのアクション。インポートされたオブジェクトのタイプが [ルール（rule）] の場合、デフォルトのアクションは [通過（Pass）]、[アラート（Alert）]、または [ドロップ（Drop）]になります。インポートされた他のすべてのオブジェクト タイプには、デフォルトのアクションはありません。
詳細（Details）	コンポーネントまたはルールに対する一意の文字列。ルールの場合、変更されたルールの GID、SID、および旧リビジョン番号は、`previously (GID:SID:Rev)` と表示されます。変更されていないルールについては、このフィールドは空白です。
ドメイン（Domain）	侵入ポリシーで更新されたルールを使用できるドメイン。子孫ドメインの侵入ポリシーもルールを使用できます。このフィールドは、マルチドメイン展開の場合にのみ存在します。
GID	ルールのジェネレータ ID。たとえば、`1`（標準テキスト ルール）または `3`（共有オブジェクト ルール）。

フィールド	説明
[名前（Name）]	インポートされたオブジェクトの名前。ルールの場合はルールの [メッセージ（Message）] フィールドに対応した名前で、ルール更新コンポーネントの場合はコンポーネント名です。
ポリシー	インポートされたルールの場合、このフィールドには [すべて（All）] が表示されます。これは、インポートされたルールがデフォルトのすべての侵入ポリシーに含まれていたことを意味します。インポートされた他のタイプのオブジェクトについては、このフィールドは空白です。
Rev	ルールのリビジョン番号。
ルール アップデート（Rule Update）	ルール更新のファイル名。
SID	ルールの SID。
時刻（Time）	インポートが開始された日時。
タイプ（Type）	インポートされたオブジェクトのタイプで、有効な値は次のいずれかです。 • [ルール更新コンポーネント（rule update component）]（ルール パックやポリシー パックなどのインポートされたコンポーネント） • [ルール（rule）]（ルール用。新しいルールまたは更新されたルール。バージョン 5.0.1 では、廃止された `update` 値の代わりにこの値が使用されます）。 • [ポリシー適用（policy apply）]（インポートに対して [ルール更新のインポート完了後にすべてのポリシーを再適用する（Reapply all policies after the rule update import completes）] オプションが有効だった場合）
メンバー数（Count）	各レコードのカウント（1）。テーブルが制限されており、[ルール アップデート ログ（Rule Update Log）] 詳細ビューがデフォルトでルール更新レコードに制限されている場合は、テーブル ビューに [メンバー数（Count）] フィールドが表示されます。このフィールドは検索できません。

関連トピック

侵入ルールの更新インポート ログの詳細の表示, （168 ページ）

侵入ルールの更新インポート ログの詳細の表示

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

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [システム（System）] > [更新（Updates）]を選択します。

ステップ 2 [ルールの更新（Rule Updates）] タブをクリックします。

ステップ 3 [ルールアップデートログ（Rule Update Log）] をクリックします。

ステップ 4 表示する詳細レコードが含まれているファイルの隣にある表示アイコン（  ）をクリックします。

ステップ 5 次のいずれかの処理を実行できます。

- ブックマーク：現在のページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。
- 検索の編集：現在の単一制約が事前入力されている検索ページを開くには、検索制約の横にある [検索の編集（Edit Search）] または [検索の保存（Save Search）] を選択します。
- ブックマークの管理：ブックマークの管理ページに移動するには、[レポートデザイナ（Report Designer）] をクリックします。
- レポート：現在のビューのデータに基づいてレポートを生成するには、[レポート デザイナ（Report Designer）] をクリックします。
- 検索：ルールの更新インポート ログ データベース全体でルールの更新インポート レコードを検索するには、[検索（Search）] をクリックします。
- ソート：現在のワークフローページでレコードをソートしたり制約したりするには、詳細についてドリルダウン ページの使用, （1844 ページ）を参照してください。
- ワークフローの切り替え：別のワークフローを一時的に使用するには、[(ワークフローの切り替え)（(switch workflows)）] をクリックします。

地理位置情報データベースの更新

シスコ地理位置情報データベース（GeoDB）は、ルーティング可能なIPアドレスと関連付けられた地理的データ（国、都市、座標など）および接続関連のデータ（インターネットサービスプロバイダー、ドメイン名、接続タイプなど）のデータベースです。検出されたIPアドレスと一致するGeoDB情報が検出された場合は、そのIPアドレスに関連付けられている位置情報を表示できます。国や大陸以外の位置情報の詳細を表示するには、システムにGeoDBをインストールする必要があります。シスコでは、GeoDBの定期的な更新を提供しています。

GeoDBを更新するには、Firepower Management Centerで [位置情報の更新（Geolocation Updates）] ページ（[システム（System）] > [更新（Updates）] > [位置情報の更新（Geolocation Updates）]）

を使用します。サポートまたは自身のアプライアンスから取得したGeoDBの更新をアップロードすると、それらがこのページに表示されます。

（注） [位置情報の更新（Geolocation Updates）]ページで[位置情報の更新をサポートサイトからダウンロードおよびインストールする（Download and install geolocation update from the Support Site）]をクリックするか、または手動でサポートサイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、破損する可能性があります。

GeoDBの更新にかかる時間はアプライアンスによって異なります。インストールには通常、30～40分かかります。GeoDBの更新によって他のシステム機能（進行中の位置情報収集など）が中断されることはありませんが、更新が完了するまでシステムリソースが消費されます。更新を計画する場合には、この点について考慮してください。

GeoDBを更新すると、GeoDBの以前のバージョンが上書きされ、すぐに有効になります。GeoDBを更新すると、Firepower Management Centerにより、管理対象デバイス上の関連データが自動的に更新されます。GeoDBの更新が展開全体で有効になるまでに数分かかることがあります。更新後に再度展開する必要はありません。

手動による GeoDB の更新（インターネット接続）

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

新しいGeoDB更新プログラムは、アプライアンスがインターネットにアクセスできる場合にのみ、サポートサイトに接続することで自動的にインポートできます。

手順

ステップ1 [システム（System）]>[更新（Updates）]を選択します。

ステップ2 [位置情報の更新（Geolocation Updates）]タブをクリックします。

ステップ3 [サポートサイトから地理位置情報の更新をダウンロードしてインストールする（Download and install geolocation update from the Support Site）]を選択します。

ステップ4 [インポート（Import）]をクリックします。

システムは [地理位置情報の更新（Geolocation Update）] タスクをキューに入れます。このタスクは、最新の更新について、シスコ サポート サイト（http://www.cisco.com/cisco/web/support/index.html）で確認します。

ステップ 5 必要に応じて、タスクのステータスをモニタします。タスク メッセージの表示, （303 ページ）を参照してください。

ステップ 6 更新が終了したら、[地理位置情報の更新（Geolocation Updates）]ページに戻るか、[ヘルプ（Help）] >[バージョン情報（About）] を選択して、GeoDB のビルド番号がインストールした更新と一致していることを確認します。

地理位置情報データベース（GeoDB）の手動更新：インターネット接続なし

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

Firepower Management Center がインターネットにアクセスできない場合は、シスコ サポート サイトからネットワーク上のローカル マシンに GeoDB の更新をダウンロードして、その更新を手動で Firepower Management Center にアップロードできます。

手順

ステップ 1 シスコ サポート サイト（http://www.cisco.com/cisco/web/support/index.html）から、手動で更新をダウンロードします。

ステップ 2 [システム（System）] > [更新（Updates）]を選択します。

ステップ 3 [位置情報の更新（Geolocation Updates）] タブをクリックします。

ステップ 4 [地理位置情報の更新のアップロードとインストール（Upload and install geolocation update）] を選択します。

ステップ 5 ダウンロードした更新を参照して、[アップロード（Upload）] をクリックします。

ステップ 6 [インポート（Import）] をクリックします。

ステップ 7 必要に応じて、タスクのステータスをモニタします。タスク メッセージの表示, （303 ページ）を参照してください。

ステップ 8 更新が終了したら、[地理位置情報の更新（Geolocation Updates）]ページに戻るか、[ヘルプ（Help）] >[バージョン情報（About）] を選択して、GeoDB のビルド番号がインストールした更新と一致していることを確認します。

GeoDB 更新のスケジューリング

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

地理位置情報データベース（GeoDB）の定期更新を自動化できます。GeoDB の定期更新は 7 日ごとに 1 度（週 1 回）実行されます。週ごとに更新が繰り返される時刻を設定できます。

手順

ステップ 1 [システム（System）] > [更新（Updates）]を選択します。

ステップ 2 [位置情報の更新（Geolocation Updates）] タブをクリックします。

ステップ 3 [位置情報の定期更新（Recurring Geolocation Updates）] の下で、[週ごとの定期更新を有効にする（Enable Recurring Weekly Updates）] チェックボックスをオンにします。

ステップ 4 [更新の開始時刻（Update Start Time）] フィールドで、週ごとに GeoDB 更新を行う曜日と時刻を指定します。

ステップ 5 [保存（Save）] をクリックします。

第 7 章

バックアップと復元

次のトピックでは、Firepower システムでバックアップおよび復元機能を使用する方法について説明します。

バックアップと復元の概要

災害から回復する能力は、システム保守計画の重要な部分を占めます。

Firepower Management Center または 7000/8000 シリーズ デバイスでデータをバックアップしたり復元したりすることができます。

バックアップと復元に関する制限事項

アプライアンスまたはローカル コンピュータにバックアップ ファイルを保存できます。Firepower Management Center を使用してバックアップを実行する場合は、リモート ストレージを使用できます。

（注） バックアップ データの収集中に、データの相関付けが一時的に停止してバックアップ関連の設定を変更できなくなることがあります。

バックアップと復元に関する次の制限事項に注意してください。

- 代替アプライアンスにバックアップを復元できるのは、2 台のアプライアンスが同じモデルであり、同じバージョンの Firepower システム ソフトウェアを実行している場合のみです。
- バックアップには、キャプチャされたファイル データは含まれません。
- NGIPSv、、あるいは ASA FirePOWER モジュールのバックアップ ファイルを作成または復元することは**できません**。イベント データをバックアップするには、管理元の Firepower Management Center のバックアップを実行します。
- アプライアンス間で設定をコピーするためにバックアップおよび復元プロセスを使用しないでください。バックアップ ファイルは、アプライアンスを一意に識別する情報を含んでおり、共有することはできません。
- Firepower Management Center を復元した後、最新の侵入ルールの更新を適用する必要があります。
- PKI オブジェクトに関連付けられている秘密キーは、アプライアンスに保存されるときに、ランダムに生成されたキーで暗号化されます。PKI オブジェクトに関連付けられている秘密キーを含むバックアップを実行すると、秘密キーは復号されてから、暗号化されていないバックアップ ファイルに含められます。バックアップ ファイルは安全な場所に保存してください。
- PKI オブジェクトに関連付けられている秘密キーを含むバックアップを復元すると、その秘密キーはランダムに生成されたキーで暗号化されてからアプライアンスに保存されます。
- クリーン リストとカスタム検出リストのいずれかを有効にしてファイル ポリシーを含むバックアップを復元すると、復元されるファイルのリストとあらゆる既存のファイル リストがマージされます。
- バックアップを実行してから、確認済みの侵入イベントを削除し、そのバックアップを使用して復元すると、削除された侵入イベントは復元されますが、それらの確認済みステータスは復元されません。それらの復元された侵入イベントは、[確認済みイベント（Reviewed Events）] ではなく [侵入イベント（Intrusion Events）] に表示されます。
- 侵入イベントのデータを含むバックアップを、そのデータがすでに含まれているアプライアンスに復元すると、重複したイベントが作成されることになります。そのようなことが起こらないようにするため、侵入イベントのバックアップは、以前の侵入イベント データが含まれていないアプライアンスにのみ復元してください。
- セキュリティ ゾーンとのインターフェイス アソシエーションが設定されている場合、それらのアソシエーションはバックアップされません。それらは、復元後に再設定する必要があります。

- Firepower Management Center では、バックアップ機能と復元機能はグローバル ドメインのみで使用できます。サブドメインの範囲内では、バックアップと復元の代わりにエクスポート機能とインポート機能を使用することができます。

関連トピック

リモート ストレージ管理, （582 ページ）
コンフィギュレーションのインポート/エクスポートについて, （187 ページ）
侵入イベントを確認済みとしてマーク, （1974 ページ）
セキュリティ ゾーン, （392 ページ）

バックアップ ファイル

実行するバックアップのタイプに応じて、さまざまなデータがバックアップされます。キャプチャされたファイル データはバックアップ**されない**ことに注意してください。次の表を使用して、どのようなタイプのバックアップを実行するかを決定します。

表 *20*：それぞれのバックアップ タイプで保存されるデータ

バックアップ タイプ	構成データが含まれるか	イベント データが含まれるか	統合ファイルが含まれるか
Firepower Management Center	○	○	[いいえ（No）]
7000 & 8000 シリーズ（デバイス自体から実行）	[はい（Yes）]	[いいえ（No）]	[いいえ（No）]
7000 & 8000 シリーズ（管理元の Firepower Management Center から実行）	[はい（Yes）]	[いいえ（No）]	○

（注） NGIPSv デバイス、、あるいは ASA FirePOWER モジュールについては、バックアップ ファイルを作成または復元することは**できません**。イベント データをバックアップするには、管理元の Firepower Management Center のバックアップを実行します。

イベントデータに加えて、アプライアンスの復元に必要なすべてのコンフィギュレーションファイルを含むバックアップ ファイルを定期的に保存する必要があります。設定の変更をテストする際にもシステムをバックアップして、必要に応じて保存されている設定に戻すことができます。

バックアップファイルを、アプライアンスに保存するか、ローカルコンピュータに保存するかを選択できます。

あるいは、バックアップ ファイルが 4GB を超える場合は、SCP 経由でリモート ホストにコピーします。4 GB を超えるファイルのアップロードは Web ブラウザでサポートされていないため、バックアップファイルがそのように大きい場合には、ローカルコンピュータからバックアップをアップロードすることはできません。Firepower Management Center では、バックアップ ファイルをリモート ロケーションに保存できます。

関連トピック

リモート ストレージ管理, （582 ページ）

Firepower Management Center のバックアップ

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

はじめる前に

- アプライアンスに十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の 90%以上を使用すると、バックアップは失敗することがあります。必要に応じて、古いバックアップ ファイルを削除するか、古いバックアップ ファイルをアプライアンスの外部に転送するか、リモート ストレージを使用してください。リモート ストレージ管理, （582 ページ） を参照してください。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] を選択します。

ステップ 2 [Firepower 管理バックアップ（Firepower Management Backup）] をクリックします。

ステップ 3 [名前（Name）] を入力します。

ステップ 4 その他以下の 2 つの対処法があります。

- 設定をアーカイブするには、[設定をバックアップ（Back Up Configuration）] を選択します。マルチドメイン展開では、このオプションを無効にできません。
- イベント データベース全体をアーカイブするには、[イベントをバックアップ（Back Up Events）] を選択します。

ステップ 5 バックアップの完了時に通知を受けるためには、[電子メール（Email）] チェックボックスを選択して、用意されているテキスト ボックスに電子メール アドレスを入力します。

（注） 電子メール通知を受信するには、メール リレー ホストおよび通知アドレスの設定, （596 ページ） で説明されているように、リレー ホストを設定する必要があります。

ステップ 6 セキュアなコピー（SCP）を使用してバックアップ アーカイブを異なるマシンにコピーするには、[完了時にコピー（Copy when complete）] チェックボックスを選択してから、用意されているテキストボックスに以下の情報を入力します。

- [ホスト（Host）] フィールドに、バックアップのコピー先となるマシンのホスト名または IP アドレス
- [パス（Path）] フィールドに、バックアップのコピー先となるディレクトリへのパス
- [ユーザ（User）] フィールドに、リモート マシンへのログインに使用するユーザ名
- [パスワード（Password）] フィールドに、そのユーザ名のパスワード。パスワードの代わりに SSH 公開キーを使用してリモート マシンにアクセスする場合は、そのマシンの指定ユーザの `authorized_keys` ファイルに、[SSH 公開キー（SSH Public Key）] フィールドの内容をコピーします。

ヒント このオプションをオフにする場合、バックアップ中に使用された一時ファイルがシステムによってリモート サーバに保存されます。このオプションをオンにする場合は、一時ファイルはリモート サーバに保存され**ません**。Cisco は、システム障害が発生した場合にアプライアンスを復元できるように、バックアップをリモート ロケーションに定期的に保存することを推奨します。

ステップ 7 次の選択肢があります。

- バックアップ ファイルをアプライアンスに保存するには、[バックアップ開始（Start Backup）] をクリックします。バックアップ ファイルは`/var/sf/backup`ディレクトリに保存されます。
- この設定を後で使用できるバックアップ プロファイルとして保存するには、[新規として保存（Save As New）] をクリックします。

次の作業

- バックアップファイルに PKI オブジェクトデータが含まれる場合は、バックアップ内に暗号化されていない秘密キーが含まれています。このため、バックアップはセキュアな場所に保存してください。

管理対象デバイスのローカルでのバックアップ

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

アプライアンスのローカル Web インターフェイスを使用して、次の手順を実行する必要があります。

はじめる前に

- アプライアンスに十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の 90%以上を使用すると、バックアップは失敗することがあります。必要に応じて、古いバックアップ ファイルを削除するか、古いバックアップ ファイルをアプライアンスの外部に転送してください。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] を選択します。

ステップ 2 [デバイス バックアップ（Device Backup）] をクリックします。

ステップ 3 [名前（Name）] フィールドに、バックアップ ファイルの名前を入力します。

ステップ 4 バックアップの完了時に通知を受けるためには、[電子メール（Email）] チェックボックスを選択して、用意されているテキスト ボックスに電子メール アドレスを入力します。

（注） 電子メール通知を受信するには、メール リレー ホストおよび通知アドレスの設定, （596 ページ） で説明されているように、リレー ホストを設定する必要があります。

ステップ 5 セキュアなコピー（SCP）を使用してバックアップアーカイブを異なるマシンにコピーするには、[完了時にコピー（Copy when complete）] チェックボックスを選択してから、用意されているテキストボックスに以下の情報を入力します。

- [ホスト（Host）] フィールドに、バックアップのコピー先となるマシンのホスト名または IP アドレス。
- [パス（Path）] フィールドに、バックアップのコピー先となるディレクトリへのパス。
- [ユーザ（User）] フィールドに、リモート マシンへのログインに使用するユーザ名。
- [パスワード（Password）] フィールドに、そのユーザ名のパスワード。パスワードの代わりに SSH 公開キーを使用してリモート マシンにアクセスする場合は、そのマシンの指定ユーザの `authorized_keys` ファイルに、[SSH 公開キー（SSH Public Key）] フィールドの内容をコピーします。

ヒント このオプションをオフにする場合、バックアップ中に使用された一時ファイルがシステムによってリモート サーバに保存されます。このオプションをオンにする場合は、一時ファイルはリモート サーバに保存されません。Cisco は、システム障害が発生した場合にアプライアンスを復元できるように、バックアップをリモート ロケーションに定期的に保存することを推奨します。

ステップ 6 次の選択肢があります。

- バックアップ ファイルをアプライアンスに保存するには、[バックアップ開始（Start Backup）] をクリックします。バックアップ ファイルは/var/sf/backupディレクトリに保存されます。
- この設定を後で使用できるバックアップ プロファイルとして保存するには、[新規として保存（Save As New）] をクリックします。

次の作業

- バックアップファイルに PKI オブジェクトデータが含まれる場合は、バックアップ内に暗号化されていない秘密キーが含まれています。このため、バックアップはセキュアな場所に保存してください。

Firepower Management Center からの管理対象デバイスのバックアップ

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

はじめる前に

- アプライアンスに十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の 90%以上を使用すると、バックアップは失敗することがあります。必要に応じて、古いバックアップ ファイルを削除するか、古いバックアップ ファイルをアプライアンスの外部に転送するか、リモート ストレージを使用してください。リモート ストレージ管理, （582 ページ） を参照してください。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] を選択します。

ステップ 2 [管理対象デバイスのバックアップ（Managed Device Backup）] をクリックします。

ステップ 3 [管理対象デバイス（Managed Devices）] フィールドで、1 つ以上の管理対象デバイスを選択します。

ステップ 4 設定データと共に統合ファイルも含めるには、[すべての統合ファイルを含める（Include All Unified Files）] チェックボックスを選択します。統合ファイルは、管理対象デバイスがまだ Firepower

Management Center へ送っていない、分析と保管のためのイベントデータのバイナリファイルです。

ステップ 5 Firepower Management Center にバックアップファイルのコピーを保存するには、[管理センターで取得する（Retrieve to Management Center）] チェックボックスを選択します。各デバイスのバックアップ ファイルをそのデバイス自体のみに保存するには、このチェックボックスをオフにしておいてください。

（注） [管理センターで取得する（Retrieve to Management Center）] を選択したのに Firepower Management Center がリモートストレージにバックアップするよう設定されている場合は、デバイスのバックアップファイルはリモートに設定されている場所に保存されます。

ステップ 6 [バックアップ開始（Start Backup）] をクリックします。バックアップ ファイルは`/var/sf/backup` ディレクトリに保存されます。

次の作業

- バックアップファイルに PKI オブジェクトデータが含まれる場合は、バックアップ内に暗号化されていない秘密キーが含まれています。このため、バックアップはセキュアな場所に保存してください。

バックアップ プロファイルの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

この手順は、デバイスの Web ユーザ インターフェイスを使用して実行する必要があります。

さまざまな種類のバックアップに使用する設定値を含むバックアップ プロファイルを作成できます。後にアプライアンスのファイルをバックアップするときに、これらのプロファイルの 1 つを選択できます。

ヒント 新規ファイル名を使用して Firepower Management Center のバックアップ ファイルを作成する場合、システムにより自動的に、その名前でバックアップ プロファイルが作成されます。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] を選択します。

ステップ 2 [バックアップ プロファイル（Backup Profiles）] タブをクリックします。

ステップ 3 [プロファイルの作成（Create Profile）] をクリックします。

ステップ 4 バックアップ プロファイルの名前を入力します。

ステップ 5 バックアップ プロファイルを設定します。Firepower Management Center のバックアップ, （176 ページ）を参照してください。

ステップ 6 バックアップ プロファイルを保存するには、[新規として保存（Save As New）] をクリックします。

ローカル ホストからのバックアップのアップロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

ローカルホストからアプライアンスにバックアップファイルをアップロードできます。この手順は、デバイスの Web インターフェイスを使用して実行する必要があります。

バックアップ ファイルに PKI オブジェクトが含まれている場合、アップロード時に、システムはランダム生成されたキーを使用して、内部 CA および内部証明書オブジェクトに関連付けられた秘密キーを再暗号化します。

はじめる前に

- [バックアップ管理（Backup Management）] ページ, （182 ページ）の説明に従って、ダウンロード機能を使用し、バックアップ ファイルをローカル ホストにダウンロードします。
- SCP を介してローカル ホストからリモート ホストに 4GB より大きいバックアップをコピーし、そこから Firepower Management Center に取り出します（Web ブラウザではその大きさのファイルのアップロードがサポートされていないため）。詳細については、リモート ストレージ管理, （582 ページ）を参照してください。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] を選択します。

ステップ 2 [バックアップのアップロード（Upload Backup）] をクリックします。

ステップ 3 [参照（Browse）] をクリックし、アップロードするバックアップ ファイルまで移動して選択します。

ステップ 4 [バックアップのアップロード（Upload Backup）] をクリックします。

ステップ 5 [バックアップ管理（Backup Management）] をクリックして、[バックアップ管理（Backup Management）] ページに戻ります。

次の作業

- アプライアンスによってファイルの整合性が確認された後、[バックアップ管理（Backup Management）] ページを更新し、詳細なファイル システム情報を表示します。

[バックアップ管理（Backup Management）] ページ

バックアップ ファイルに PKI オブジェクトが含まれている場合は、アップロード時に、内部 CA および内部証明書オブジェクトに関連付けられている秘密キーが、ランダムに生成されたキーで再暗号化されます。

ローカル ストレージを使用する場合、バックアップ ファイルは `/var/sf/backup` に保存されて、`/var` パーティションで使用されているディスク領域量と共に [バックアップ管理（Backup Management）] ページの下部にリストされます。Firepower Management Center で、[バックアップ管理（Backup Management）] ページの上部にある [リモート ストレージ（Remote Storage）] を選択して、リモート ストレージ オプションを設定します。その後、リモート ストレージを有効にするには [バックアップ管理（Backup Management）] ページの [バックアップ用にリモート ストレージを有効にする（Enable Remote Storage for Backups）] チェック ボックスをオンにします。リモート ストレージを使用している場合は、プロトコル、バックアップ システム、およびバックアップ ディレクトリがページの下部に表示されます。

次の表では、[バックアップ管理（Backup Management）] ページの各列とアイコンについて説明します。

表 *21*：バックアップ管理（*Backup Management*）

機能	説明
システム情報（System Information）	元のアプライアンスの名前、タイプ、バージョン。バックアップを復元できるのは、同一のアプライアンス タイプとバージョンに対してだけであることに注意してください。

機能	説明
作成日	バックアップ ファイルが作成された日時
ファイル名（File Name）	バックアップ ファイルのフルネーム
VDBバージョン（VDB Version）	バックアップ時にアプライアンスで実行されている脆弱性データベース（VDB）のビルド。
参照先	バックアップ ファイルの場所
サイズ（MB）（Size (MB)）	バックアップ ファイルのサイズ（メガバイト）
イベント?（Events?）	[はい（Yes）] は、バックアップにイベント データが含まれていることを示します
表示（View）	バックアップ ファイルの名前をクリックすると、圧縮されたバックアップ ファイルに含まれるファイルのリストが表示されます。
復元（Restore）	バックアップ ファイルを選択した状態でクリックすると、そのバックアップ ファイルがアプライアンスに復元されます。VDB バージョンがバックアップ ファイルの VDB のバージョンと一致しない場合、このオプションは無効になります。
ダウンロード（Download）	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルがローカル コンピュータに保存されます。
削除（Delete）	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルが削除されます。
[移動（Move）] をクリックします	Firepower Management Center で、以前に作成したローカル バックアップが選択された状態でクリックすると、そのバックアップが指定のリモート バックアップ ロケーションに送信されます。

バックアップ ファイルからのアプライアンスの復元

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

[バックアップ管理（Backup Management）]ページを使用して、バックアップ ファイルからアプライアンスを復元できます。この手順は、デバイスの Web インターフェイスを使用して実行する必要があります。

注意

- この操作により、すべてのコンフィギュレーション ファイルが上書きされ、管理対象デバイスでは、すべてのイベント データが上書きされます。
- 仮想 Firepower Management Center で作成されたバックアップを物理 Firepower Management Center に復元しないでください。これはシステム リソースに負荷をかける可能性があります。

（注） バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを（それらが使用されている場所をメモした上で）削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。

はじめる前に

- バックアップ ファイル内の VDB のバージョンが、アプライアンスの現在の VDB のバージョンと一致していることを確認します。詳細については、ダッシュボードの表示，（249 ページ）を参照してください。
- バックアップの完了後にアプライアンスに追加したライセンスは、リストア時の競合を避けるために、バックアップの復元前に削除します。詳細については、Firepower の機能ライセンスについて，（127 ページ）を参照してください。
- バックアップに保管されているものと同じ侵入イベント データがアプライアンスに存在しないことを確認します。これは、そのような状況下でバックアップを復元すると、重複するイベントが作成されるためです。詳細については、侵入イベントについて，（1959 ページ）を参照してください。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] を選択します。

ステップ 2 バックアップ ファイルをクリックして、そのコンテンツを表示します。詳細には、ファイルの所有者、ファイルの権限、ファイル サイズ、および日付が含まれています。

ステップ 3 [システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] を選択して、[バックアップ管理（Backup Management）] ページに戻ります。

ステップ 4 復元するバックアップ ファイルを選択します。

ステップ 5 [復元（Restore）] をクリックします。

（注） バックアップの VDB バージョンがアプライアンスに現在インストールされている VDB のバージョンと一致しない場合、[復元（Restore）] ボタンはグレー表示されます。

ステップ 6 ファイルを復元するには、次のいずれかまたは両方のオプションを選択します。

- 設定データの復元（Restore Configuration Data）

  （注） 管理対象デバイスの設定をバックアップ ファイルから復元すると、デバイスの管理用の Firepower Management Center から行われたデバイス設定の変更も復元されます。バックアップ ファイルを復元することで、バックアップ ファイルの作成後に行った変更は上書きされます。

- イベント データの復元（Restore Event Data）

ステップ 7 [復元（Restore）] をクリックします。

ステップ 8 アプライアンスを再起動します。

次の作業

- 最新のシスコ ルール アップデートをインポートします。侵入ルールのワンタイム手動更新, （160 ページ）を参照してください。インポートの一環としてポリシーを再展開する場合、設定の変更を展開する必要はありません（後述）。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。
- バックアップの復元前に、アプライアンスから削除したライセンスを追加して再設定します。
- 復元時にアプライアンスがライセンスの競合を示した場合は、サポートまでお問い合わせください。

第 8 章

コンフィギュレーションのインポートとエクスポート

次のトピックでは、インポート/エクスポート機能を使用する方法について説明します。

コンフィギュレーションのインポート/エクスポートについて

インポート/エクスポート機能を使用して、アプライアンス間で構成をコピーできます。インポート/エクスポートはバックアップ ツールではありませんが、展開に新しいアプライアンスを追加するプロセスを簡素化できます。

単一の設定をエクスポートすることや、（同じタイプまたは異なるタイプの）一連の設定を単一操作でエクスポートすることができます。後に別のアプライアンスにパッケージをインポートするとき、パッケージ内のどの設定をインポートするかを選択できます。

エクスポートされたパッケージには、その構成のリビジョン情報が含まれ、これにより、別のアプライアンスにその構成をインポートできるかどうかが決まります。アプライアンスに互換性があるものの、パッケージに重複構成が含まれていると、解決オプションが示されます。

（注） インポート側とエクスポート側のアプライアンスは、同じバージョンの Firepower システムを実行している必要があります。アクセス コントロールとそのサブポリシー（侵入ポリシーを含む）の場合、侵入ルールの更新バージョンも一致している必要があります。バージョンが一致しない場合、インポートは失敗します。インポート/エクスポート機能を使用して侵入ルールを更新することはできません。代わりに、最新バージョンのルール更新をダウンロードして適用します。

インポート/エクスポートをサポートする構成

インポート/エクスポートは、次の構成でサポートされます。

- アクセス コントロール ポリシーとそれが呼び出すポリシー：ネットワーク分析、侵入、SSL、ファイル
- 侵入ポリシー（アクセス コントロールとは無関係に）
- プラットフォーム設定
- 正常性ポリシー
- アラート応答
- アプリケーション ディテクタ（ユーザ定義および Cisco Professional サービスによって提供されるディテクタ）
- ダッシュボード
- カスタム テーブル
- カスタム ワークフロー
- 保存済み検索
- カスタム ユーザ ロール
- レポート テンプレート
- サードパーティ製品および脆弱性マッピング

設定のインポート/エクスポートに関する特別な考慮事項

構成をエクスポートすると、他の必要な構成もエクスポートされます。たとえば、アクセス コントロール ポリシーをエクスポートすると、そのポリシーが呼び出すサブポリシー、使用しているオブジェクトとオブジェクト グループ、先祖ポリシー（マルチドメイン展開の場合）などもエクスポートされます。別の例として、外部認証が有効になっているプラットフォーム設定ポリシーをエクスポートした場合は、認証オブジェクトもエクスポートされます。ただし、いくつかの例外があります。

- システム提供のデータベースとフィード：URL フィルタリング カテゴリとレピュテーション データ、シスコ インテリジェンス フィード データ、または地理位置情報データベース（GeoDB）はエクスポートされません。展開内のすべてのアプライアンスがシスコから最新情報を取得していることを確認してください。
- グローバルなセキュリティ インテリジェンスのリスト：エクスポートされた構成に関連するグローバルなセキュリティ インテリジェンスのブラックリストとホワイトリストがエクスポートされます（マルチドメイン展開では、これは現在のドメインに関係なく実行されます。子孫ドメインのリストはエクスポートされ**ません**）。インポート プロセスはこれらのブラックリストとホワイトリストをユーザ作成リストに変換してから、インポートされた構成でそれらの新しいリストを使用します。これにより、インポートされたリストが既存のグ

ローバルなブラックリストおよびホワイトリストと競合することはありません。インポートされた構成でインポート側の Firepower Management Center のグローバル リストを使用するには、これらを手動で追加します。

- 侵入ポリシー共有層：エクスポートプロセスにより、侵入ポリシー共有レイヤが切断されます。以前の共有レイヤはパッケージに含まれ、インポートされた侵入ポリシーには共有レイヤは含まれません。
- 侵入ポリシーのデフォルト変数セット：エクスポートパッケージには、カスタム変数とシステム提供の変数を含むデフォルト変数セットがユーザ定義値とともに含まれています。インポート プロセスでは、インポートされた値でインポート側の Firepower Management Center のデフォルト変数セットを更新します。ただし、インポートプロセスはエクスポートパッケージに存在しないカスタム変数を削除**しません**。また、エクスポートパッケージに設定されていない値については、インポート側の Firepower Management Center のユーザ定義値を元に戻しません。したがって、インポート側の Firepower Management Center で設定されているデフォルト変数が異なる場合は、インポートされた侵入ポリシーの動作が予想とは異なる可能性があります。

オブジェクトおよびオブジェクト グループをインポートする場合：

- インポートプロセスは、オブジェクトとグループを新規としてインポートします。既存のオブジェクトおよびグループを置き換えることはできません。
- インポートしたオブジェクトの名前がインポートする Firepower Management Center 上の既存のオブジェクトと一致する場合、システムはそれらの名前を一意にするため、インポートされたオブジェクトとグループの名前に自動生成した番号を付加します。
- インポートした設定で使用されているセキュリティ ゾーンを、インポート側の Firepower Management Center で管理されているタイプが一致するゾーンにマッピングする必要があります。
- 秘密キーを含む PKI オブジェクトを使用する構成をエクスポートすると、エクスポートの前に秘密キーが復号されます。インポート時に、キーはランダムに生成されたキーで暗号化されます。

設定のエクスポート

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

エクスポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、エクスポート プロセスに数分かかる場合があります。

ヒント

Firepowerシステムの多くのリストページには、リスト項目の横にエクスポートアイコン（）があります。このアイコンがある場合は、それを使用することにより、その後のエクスポート操作を簡単に代行させることができます。

はじめる前に

- インポートおよびエクスポートするアプライアンスが同じバージョンの Firepower システムを実行していることを確認します。アクセス制御とそのサブポリシー（侵入ポリシーを含む）の場合は、侵入ルールの更新バージョンも一致する必要があります。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [インポート/エクスポート（Import/Export）]を選択します。

折りたたむ（）アイコンか、展開する（）アイコンをクリックし、使用可能な設定のリストを折りたたんだり、展開したりします。

ステップ 2 エクスポートする構成をチェックして [エクスポート（Export）] をクリックします。

ステップ 3 Web ブラウザのプロンプトに従って、エクスポートされたパッケージをコンピュータに保存します。

設定のインポート

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

インポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、インポート プロセスに数分かかる場合があります。

はじめる前に

- インポートおよびエクスポートするアプライアンスが同じバージョンの Firepower システムを実行していることを確認します。アクセス制御とそのサブポリシー（侵入ポリシーを含む）の場合は、侵入ルールの更新バージョンも一致する必要があります。
- インポートされるアクセス コントロール ポリシーのゾーン タイプとタイプが一致するセキュリティ ゾーンをインポートする Firepower Management Center に作成します。詳細については、セキュリティ ゾーン, （392 ページ）を参照してください。

手順

ステップ 1 インポートするアプライアンスで、[システム（System）] > [ツール（Tools）] > [インポート/エクスポート（Import/Export）] を選択します。

ステップ 2 [パッケージのアップロード（Upload Package）] をクリックします。

ステップ 3 エクスポートしたパッケージへのパスを入力するか、そのパッケージの場所を参照して [アップロード（Upload）] をクリックします。

ステップ 4 バージョンが一致していないなどの問題がない場合は、インポートする設定を選択して、[インポート（Import）] をクリックします。
競合の解決やセキュリティ ゾーンのマッピングを実行する必要がない場合は、インポートが完了して、成功メッセージが表示されます。この手順の残りは省略してください。

ステップ 5 プロンプトが表示されたら、[アクセス制御インポートの解決（Access Control Import Resolution）] ページで、インポートする Firepower Management Center で管理されているインターフェイス タイプと一致するゾーンに、インポートした設定で使用されているセキュリティ ゾーンをマップします。

ステップ 6 [インポート（Import）] をクリックします。

ステップ 7 プロンプトが表示されたら、[インポートの解決（Import Resolution）] ページで、各設定を展開して適切なオプションを選択します。詳細については、インポート競合の解決, （191 ページ）を参照してください。

ステップ 8 [インポート（Import）] をクリックします。

インポート競合の解決

構成をインポートしようすると、同じ名前とタイプの構成がアプライアンスにすでに存在するかどうかがシステムによって確認されます。マルチドメイン展開では、構成が現在のドメイン、またはその先祖あるいは子孫ドメインのいずれかで定義されている構成の複製であるかどうかが確認されます。（子孫ドメインの構成は表示できませんが、重複する名前の構成が子孫ドメインに存在する場合は、システムにより競合が通知されます）。インポートに重複構成が含まれている場合、次の中から展開に適切な解決オプションが表示されます。

- 既存のものを維持する（Keep existing）

  その構成はインポートされません。

- 既存のものを置換する（Replace existing）

  インポート用に選択した構成で現在の構成が上書きされます。

- 最新バージョンを残す（Keep newest）

  選択した構成は、タイムスタンプがアプライアンスの現在の構成のタイムスタンプより新しい場合にのみインポートされます。

- 新たにインポート（Import as new）

選択した重複する構成はインポートされ、システム生成の番号が適用されて一意の構成になります。（インポートプロセスが完了する前にこの名前を変更できます）。アプライアンスの元の構成は変更されません。

表示される解決オプションは、展開でドメインを使用するかどうか、およびインポートされた構成が現在のドメインで定義されている構成の複製であるか、または現在のドメインの先祖あるいは子孫で定義された構成であるかどうかによって異なります。次の表に、どの場合に解決オプションが表示されるか表示されないかを示します。

解決オプション	Firepower Management Center		管理対象デバイス
	現在のドメインの複製	子孫または先祖ドメインの複製	
既存のものを維持する（Keep existing）	○	○	○
既存のものを置換する（Replace existing）	[はい（Yes）]	[いいえ（No）]	○
最新バージョンを残す（Keep newest）	[はい（Yes）]	[いいえ（No）]	○
新たにインポート（Import as new）	○	○	○

クリーンまたはカスタム定義ファイル リストを使用するファイル ポリシーとともにアクセス コントロール ポリシーをインポートし、ファイル リストに重複する名前競合が示されている場合、上記の表に示すように競合解決オプションが表示されますが、ポリシーおよびファイル リストに対して実行されるアクションは、次に表に示すように異なります。

解決オプション	システム アクション	
	アクセス コントロール ポリシーと関連ファイル ポリシーが新たにインポートされ、ファイル リストは統合される	既存のアクセス コントロール ポリシーと関連ファイル ポリシーおよびファイル リストは変更されない
既存のものを維持する（Keep existing）	なし	○
既存のものを置換する（Replace existing）	[はい（Yes）]	[いいえ（No）]
新たにインポート（Import as new）	[はい（Yes）]	[いいえ（No）]

解決オプション	システム アクション	
	アクセス コントロール ポリシーと関連ファイルポリシーが新たにインポートされ、ファイルリストは統合される	既存のアクセス コントロール ポリシーと関連ファイル ポリシーおよびファイル リストは変更されない
最新バージョンを残す（Keep newest）。インポートされるアクセス コントロール ポリシーが最新	[はい（Yes）]	[いいえ（No）]
最新バージョンを残す（Keep newest）。既存のアクセス コントロール ポリシーが最新	なし	○

アプライアンスにインポートされた構成を修正し、後で同じアプライアンスにその構成を再インポートする場合は、保持する構成のバージョンを選択する必要があります。

第 9 章

タスクのスケジューリング

ここでは、タスクをスケジュールする方法について説明します。

タスクのスケジューリングの概要

さまざまな種類の管理タスクを、指定した回数（1度または繰り返し）実行するようにスケジュールを設定できます。

（注） タスクによっては低帯域幅のネットワークに非常に負荷をかけることがあります（ソフトウェアの自動更新が含まれるタスクや、管理対象デバイスに更新をプッシュする必要があるタスクなど）。ネットワーク使用率が低い時間帯にこのようなタスクを実行するよう、スケジュールしてください。

定期タスクの設定

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

定期タスクの頻度を設定する際には、すべてのタイプのタスクで同じ手順に従います。

Web インターフェイスのほとんどのページに表示される時間はローカル時刻であり、ローカル設定で指定したタイム ゾーンに従ってそれが決定されます。さらに、Firepower Management Center は、該当する場合にはローカル時刻の表示を夏時間（DST）に合わせて自動的に調整します。ただし、DST から標準時への移行日および元に戻る移行日をまたがる定期タスクは、移行を考慮して調整されません。つまり、標準時の午前 2:00 にタスク スケジュールを作成すると、DST 期間中は午前 3:00 に実行されます。同様に、DST の午前 2:00 にタスク スケジュールを作成すると、標準時には午前 1:00 に実行されます。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] ドロップダウン リストから、スケジュールするタスクのタイプを選択します。

ステップ 4 [実行するタスクのスケジュール（Schedule task to run）] オプションの横にある [定期（Recurring）] オプション ボタンをクリックします。

ステップ 5 [開始日付（Start On）] フィールドに、定期タスクを開始する日付を指定します。

ステップ 6 [繰り返し設定（Repeat Every）] フィールドに、タスクを繰り返す頻度を指定します。
数値を入力するか、上矢印（▲）および下矢印（▼）アイコンをクリックして、間隔を指定できます。たとえば、2 日おきにタスクを実行するには、2 を入力して [日（Days）] オプション ボタンをクリックします。

ステップ 7 [実行時刻（Run At）] フィールドで、定期タスクを開始する時刻を指定します。

ステップ 8 週または月単位で実行するタスクの場合は、[繰り返す（オン）（Repeat On）] フィールドでタスクを実行する日付を選択します。

ステップ 9 作成するタスクのタイプについて残りのオプションを選択します。

- [バックアップ（Backup）]：Firepower Management Center のバックアップの自動化, （197 ページ）の説明に従って、バックアップ ジョブをスケジュールします。
- [CRL のダウンロード（Download CRL）]：証明書失効リストのダウンロードの設定, （199 ページ）の説明に従って、証明書失効リストのダウンロードをスケジュールします。
- [ポリシーの展開（Deploy Policies）]：ポリシー展開の自動化, （201 ページ）の説明に従って、ポリシーの展開をスケジュールします。
- [Nmap スキャン（Nmap Scan）]：Nmap スキャンのスケジュール, （202 ページ）の説明に従って、Nmap スキャンをスケジュールします。
- [レポート（Report）]：次の説明に従って、レポート生成をスケジュールします。 レポートの生成の自動化, （203 ページ）
- [Firepower 推奨ルール（Firepower Recommended Rules）]：次の説明に従って、Firepower 推奨ルールの自動更新をスケジュールします。 Firepower の推奨ルールの自動化, （205 ページ）

- [最新の更新のダウンロード（Download Latest Update）]：ソフトウェア ダウンロードの自動化，（207ページ）またはVDB 更新のダウンロードの自動化，（211ページ）の説明に従って、ソフトウェアまたは VDB の更新のダウンロードをスケジュールします。
- [最新の更新のインストール（Install Latest Update）]：ソフトウェア インストールの自動化，（209ページ）または次の説明に従って、Firepower Management Center または管理対象デバイスでのソフトウェアまたは VDB の更新のインストールをスケジュールします。 VDB 更新のインストールの自動化，（212 ページ）
- [最新の更新のプッシュ（Push Latest Update）]：ソフトウェア プッシュの自動化，（208 ページ）の説明に従って、管理対象デバイスへのソフトウェア更新のプッシュをスケジュールします。
- [URL フィルタリングデータベースの更新（Update URL Filtering Database）]：次の説明に従って、URL フィルタリング データの自動更新をスケジュールします。 URL フィルタリング更新の自動化，（214 ページ）

バックアップ タスクの自動化

スケジューラを使用して、Firepower Management Center や物理管理対象デバイスのバックアップを自動化することができます。

物理管理対象デバイスの設定データのスケジュール バックアップを実行するには、デバイス自体の Web インターフェイスを使用します。

Firepower Management Center で設定データとイベント データまたは設定データのみのスケジュール バックアップを実行するには、Firepower Management Center Web インターフェイスを使用します。タスクのスケジュール時に選択するバックアップ プロファイルによってデータのバックアップのタイプが決まります。

管理対象デバイスのバックアップを管理元の Firepower Management Center からスケジュールすることはできませんが、管理対象デバイスの一部のモデルについてはオンデマンド バックアップを Firepower Management Center から実行することができます。

関連トピック

バックアップと復元の概要，（173 ページ）

Firepower Management Center のバックアップの自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	グローバルだけ	Admin/Maint

はじめる前に

- バックアップ プロファイルを作成します。バックアップ プロファイルの作成, （180 ページ）を参照してください。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[バックアップ（Backup）] を選択します。

ステップ 4 バックアップをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定, （195 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [バックアップ プロファイル（Backup Profile）] リストから、適切なバックアップ プロファイルを選択します。

ステップ 7 必要に応じて、[コメント（Comment）] を追加します。
[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定, （596 ページ）

管理対象デバイスのバックアップの自動化

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

7000 または 8000 シリーズ デバイスのローカル Web インターフェイスを使用して、次の手順を実行する必要があります。

はじめる前に

バックアップ プロファイルを作成します。参照先 バックアップ プロファイルの作成, （180 ページ）

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[バックアップ（Backup）] を選択します。

ステップ 4 バックアップをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定, （195 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [バックアップ プロファイル（Backup Profile）] リストから、適切なバックアップ プロファイルを選択します。

ステップ 7 必要に応じて、[コメント（Comment）] を追加します。
[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定, （596 ページ）

証明書失効リストのダウンロードの設定

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

Firepower Management Center または 7000 または 8000 シリーズ デバイスのローカル Web インターフェイスを使用して、この手順を実行する必要があります。マルチドメイン展開では、このタスクは Firepower Management Center のグローバル ドメインでのみサポートされます。

アプライアンスのユーザ証明書または監査ログ証明書を有効にするアプライアンスのローカル設定で証明書失効リスト（CRL）のダウンロードを有効にすると、CRL のダウンロード タスクが自動的に作成されます。スケジューラを使用してタスクを編集し、更新の頻度を設定できます。

はじめる前に

- ユーザ証明書を有効にして設定し、CRL のダウンロード URL を設定します。詳細については、有効なユーザ証明書の強制，（559 ページ）を参照してください。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[CRL のダウンロード（Download CRL）] を選択します。

ステップ 4 CRL ダウンロードをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定，（195 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 タスクについてコメントするには、[コメント（Comment）] フィールドにコメントを入力します。[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 7 タスクのステータス メッセージを電子メールで送信する場合は、[ステータスの宛先電子メール：（Email Status To:）] フィールドに電子メール アドレス（またはカンマで区切った複数の電子メール アドレス）を入力します。ステータス メッセージを送信するには、Firepower Management Center で有効な電子メール中継サーバが設定されている必要があります。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定，（596 ページ）

ポリシー展開の自動化

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

Management Center の設定を変更した後は、影響を受けるデバイスへ変更を展開する必要があります。

マルチドメイン展開では、現在のドメインに限ってポリシーの展開をスケジュールできます。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[ポリシーの展開（Deploy Policies）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定, （195 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] フィールドで、ポリシーを展開するデバイスを選択します。

ステップ 7 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。
[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定, （596 ページ）
失効ポリシー, （334 ページ）

Nmap スキャンの自動化

ネットワーク上のターゲットに対する定期的な Nmap スキャンをスケジュールできます。スキャンを自動化すると、Nmap スキャンによって以前に提供された情報を更新できます。Firepower システムは Nmap から提供されるデータを更新できないため、このデータを最新に保つには定期的に再スキャンする必要があります。また、ネットワーク上のホストに識別不能なアプリケーションやサーバがあるかどうか自動的に検査するよう、スキャンをスケジュールすることもできます。

さらに、Discovery Administrator が修正用に Nmap スキャンを使用する場合があることにも注意してください。たとえば、ホストでオペレーティング システム競合が発生したために、Nmap スキャンがトリガーされることがあります。スキャンが実行されると、そのホストでのオペレーティング システムの更新済み情報が取得され、こうして競合が解決されます。

以前に Nmap スキャン機能を使用したことがない場合は、スケジュール スキャンを定義する前に、Nmap スキャンを設定します。

関連トピック

Nmap スキャン，（1479 ページ）

Nmap スキャンのスケジュール

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

システムで検出されたホストのオペレーティング システム、アプリケーション、またはサーバが Nmap スキャンの結果で置き換えられると、システムは、Nmap によって置換されたホストに関する情報を更新しなくなります。Nmap によって提供されるサービスやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、Nmap 提供のオペレーティング システム、アプリケーション、またはサーバを最新の状態に保つために、定期的なスキャン スケジュールをセットアップしてください。ネットワーク マップからホストが削除されて再び追加されると、Nmap スキャン結果はすべて破棄され、システムはホストに関するすべてのオペレーティング システムとサービスのデータのモニタリングを再開します。

マルチドメイン展開では、次のようになります。

- スキャンのスケジュールは、現在のドメインに対してのみ可能です。
- 選択する修正および Nmap ターゲットは、現在のドメインまたは先祖ドメインに存在している必要があります。
- 非リーフ ドメインでの Nmap スキャンの実行を選択すると、そのドメインの各子孫に含まれる同じターゲットをスキャンすることになります。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] リストから、[Nmap スキャン（Nmap Scan）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定, （195 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [Nmap 修復（Nmap Remediation）] フィールドで、Nmap 修復を選択します。

ステップ 7 [Nmap ターゲット（Nmap Target）] フィールドで、スキャン ターゲットを選択します。

ステップ 8 [ドメイン（Domain）] フィールドで、増補するネットワーク マップを持つドメインを選択します。

ステップ 9 タスクにコメントを付ける場合は、[コメント（Comment）] フィールドにコメントを入力します。

ヒント [コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 10 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 11 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定, （596 ページ）

レポートの生成の自動化

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

一定期間ごとにレポートを実行するよう自動化できます。

マルチドメイン展開では、現在のドメインに限ってレポートをスケジュールできます。

はじめる前に

- ：レポート デザイナを使用し、レポート テンプレートを作成します。詳細については、レポート テンプレート，（1712 ページ）を参照してください。
- スケジューラを使用してメール レポートを配布するには、メール リレーのホストを設定し、レポートの受信者およびメッセージ情報を指定します。メール リレー ホストおよび通知アドレスの設定，（596 ページ）と、レポートの生成時の電子メール配布，（1740 ページ）を参照してください。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] リストから、[レポート（Report）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定，（195 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [レポートテンプレート（Report Template）] フィールドで、レポートテンプレートを選択します。

ステップ 7 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。
[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

（注） このオプションを設定しても、レポートは配布されません。

ステップ 9 レポートのデータがない場合（たとえばレポート期間中に特定のタイプのイベントが発生しなかった場合）にレポート電子メール添付ファイルを受信しないようにするには、[空のレポートも添付（If report is empty, still attach to email）] チェックボックスを選択します。

ステップ 10 [保存（Save）] をクリックします。

Firepower の推奨ルールの自動化

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

カスタム侵入ポリシーで保存済みの最新の設定を使用し、ネットワークのディスカバリ データに基づいてルール状態の推奨を自動的に生成することができます。

（注） 変更が未保存のまま、侵入ポリシーに関するスケジュール済み推奨がシステムによって自動生成される場合、自動生成された推奨をポリシーに反映させるには、そのポリシー内の変更を破棄してポリシーをコミットする必要があります。

タスクを実行すると、推奨ルール状態が自動的に生成され、ポリシーの設定に基づいて侵入ルールの状態が変更されます。変更されたルール状態は、侵入ポリシーを次回に展開するときに有効になります。

マルチ ドメイン展開では、現在のドメインレベルの侵入ポリシーに関する推奨を自動化できます。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、先祖ドメインの侵入ポリシーでこの機能を有効にすると、システムはすべての子孫のリーフ ドメインからのデータを使用して、推奨事項を生成します。これにより、侵入ルールをすべてのリーフ ドメインに存在しない可能性があるアセットに調整することができ、パフォーマンスに影響を与えることができます。

はじめる前に

- 以下で説明されている、侵入ポリシーでの Firepower 推奨ルールを設定します。 Firepower の推奨事項の生成と適用, （1081 ページ）
- タスクのステータス メッセージをメールで送るには、有効なメール リレー サーバを設定します。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[Firepower 推奨ルール（Firepower Recommended Rules）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。

- 定期タスクの詳細については、定期タスクの設定，（195 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [ポリシー（Policies）] の横で、推奨を生成する 1 つ以上の侵入ポリシーを選択します。[すべてのポリシー（All Policies）] チェックボックスをオンにして、すべての侵入ポリシーを選択します。

ステップ 7 （任意）[コメント（Comments）] フィールドにコメントを入力します。
コメントは手短にします。コメントはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。

ステップ 8 （任意）タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー，（1011 ページ）
Firepower 推奨ルールについて，（1077 ページ）
メール リレー ホストおよび通知アドレスの設定，（596 ページ）

ソフトウェア更新の自動化

ほとんどのパッチや機能リリースは、自動的にダウンロードして Firepower システムに適用することができます。

ソフトウェア更新をインストールするためにどんなタスクをスケジュールする必要があるかは、Management Center を更新する場合と、Management Center を使用して管理対象デバイスを更新する場合とで異なります。

（注） シスコでは、Management Center を使用して管理対象デバイスを更新することを**強く**お勧めしています。

- Management Center を更新するには、Install Latest Update タスクを使用してソフトウェア インストールをスケジュールします。
- Management Center を使用して管理対象デバイスのソフトウェア更新を自動化するには、次の 2 つのタスクをスケジュールする必要があります。
  - Push Latest Update タスクを使用して、管理対象デバイスに更新をプッシュ（コピー）します。
  - Install Latest Update タスクを使用して、管理対象デバイスに更新をインストールします。

管理対象デバイスに更新をスケジュールする場合、push and install タスクが連続して発生するようにスケジュールします。更新をインストールする前に、最初にデバイスに更新をプッシュする必要があります。タスク間に、プロセスが完了するのに十分な時間があるようにします。タスクとタスクの間に 30 分以上の間隔をあけてスケジュールしてください。更新をインストールするようにタスクをスケジュールしても、Management Center からデバイスへの更新のコピーが終了していないと、インストール タスクは正しく実行されません。ただし、スケジュール済みインストール タスクが毎日繰り返される場合は、翌日の実行時に、すでにプッシュされた更新がインストールされます。

（注） 手動で更新をアップロードしてインストールする必要が生じる状況が 2 つあります。まず、Firepower システムへのメジャー アップデート（主要な更新）をスケジュールすることはできません。次に、サポート サイトにアクセスできない Management Center の更新や、そのアプライアンスからのプッシュをスケジュールすることはできません。Management Center がインターネットに直接接続しない場合、管理インターフェイスの設定を使用して、サポート サイトから更新をダウンロードできるようプロキシをセットアップする必要があります。

デバイス グループに更新プログラムをインストールするようにスケジュールされたタスクによって、デバイス グループ内の各デバイスにプッシュされた更新プログラムが同時にインストールされることに注意してください。デバイス グループ内の各デバイスについてスケジュールされたタスクが完了するだけの十分な時間を確保してください。

このプロセスをより確実に制御するには、更新がリリースされたことがわかった後、[1 回（Once）] オプションを使用してオフピーク時間帯に更新をダウンロードしインストールできます。

関連トピック

管理インターフェイス, （564 ページ）
システム ソフトウェア アップデートの概要, （139 ページ）

ソフトウェア ダウンロードの自動化

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

Cisco から最新のソフトウェア更新を自動的にダウンロードするスケジュール済みタスクを作成することができます。このタスクを使用すると、手動でインストールする予定の更新のダウンロードをスケジュールできます。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のダウンロード（Download Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定，（195 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [アップデート項目（Update Items）] の横の [ソフトウェア（Software）] チェックボックスをオンにします。

ステップ 7 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。
[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定，（596 ページ）

ソフトウェア プッシュの自動化

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

管理対象デバイスでのソフトウェア更新のインストールを自動化するには、インストールの前に、更新をデバイスにプッシュする必要があります。

ソフトウェア更新を管理対象デバイスにプッシュするタスクを作成する際には、更新がデバイスに確実にコピーされるよう、プッシュ タスクとスケジュール済みインストール タスクの間に十分な時間を確保してください。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] リストから、[最新の更新をプッシュ（Push Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定, （195 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] ドロップダウン リストから、更新するデバイスを選択します。

ステップ 7 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。
[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定, （596 ページ）

ソフトウェア インストールの自動化

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

管理対象デバイスへ更新をプッシュするタスクと、その更新をインストールするタスクの間に十分な時間を確保する必要があります。

注意 インストールする更新によっては、ソフトウェアのインストール後にアプライアンスがリブートする場合があります。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のインストール（Install Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定, （195 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] ドロップダウン リストから、更新をインストールするアプライアンス（Firepower Management Centerを含む）を選択します。

ステップ 7 [アップデート項目（Update Items）] の横の [ソフトウェア（Software）] チェックボックスをオンにします。

ステップ 8 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。
[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 9 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 10 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定, （596 ページ）

脆弱性データベースの更新の自動化

Cisco では脆弱性データベース（VDB）更新を使用して、Firepower システムで認識されるネットワーク アセット、トラフィック、および脆弱性のリストを拡張しています。スケジュール機能を

使用してVDBを更新できるため、常に最新の情報を使ってネットワーク上のホストを評価することができます。

VDB 更新を自動化する場合、次に示す 2 つの別個の手順を自動化する必要があります。

- VDB 更新のダウンロード。
- VDB 更新のインストール。

注意

VDB アップデートをインストールした後、初めて脆弱性データベース（VDB）アップデートをインストールするか、またはアクセス コントロール ポリシーを展開すると、すぐにSnortプロセスが再起動され、トラフィック インスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作，（326 ページ）を参照してください。

プロセスを完了させるには、タスクとタスクの間に十分な時間を確保してください。たとえば、更新のインストール タスクをスケジュールした場合、更新がまだ完全にダウンロードされていないと、インストールタスクは正しく実行されません。ただし、スケジュール済みインストールタスクが毎日繰り返される場合は、翌日のタスク実行時に、ダウンロード済みのVDB更新がインストールされます。

（注）

- サポートサイトにアクセスできないアプライアンスの更新をスケジュールすることはできません。Management Centerがインターネットに直接接続されていない場合、管理インターフェイスの設定を使用して、プロキシが更新をサポートサイトからダウンロードできるようにプロキシをセットアップする必要があります。
- このプロセスをより確実に制御するには、更新がリリースされたことがわかった後、[1 回（Once）] オプションを使用してオフピーク時間帯に VDB 更新をダウンロードしてインストールできます。
- マルチドメイン展開では、VDB 更新をスケジュールできるのはグローバル ドメインについてのみです。変更は、ポリシーを再度展開したときに有効になります。

関連トピック

管理インターフェイス，（564 ページ）

VDB 更新のダウンロードの自動化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	グローバルだけ	Admin/Maint

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のダウンロード（Download Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定，（195 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [アップデート項目（Update Items）] の横の [脆弱性データベース（Vulnerability Database）] チェックボックスをオンにします。

ステップ 7 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。
[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定，（596 ページ）

VDB 更新のインストールの自動化

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

VDB 更新をダウンロードするタスクと、その更新をインストールするタスクの間に十分な時間を確保してください。

注意 VDB アップデートをインストールした後、初めて脆弱性データベース（VDB）アップデートをインストールするか、またはアクセス コントロール ポリシーを展開すると、すぐに Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のインストール（Install Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定, （195 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] ドロップダウン リストから Management Center を選択します。

ステップ 7 [アップデート項目（Update Items）] の横の [脆弱性データベース（Vulnerability Database）] チェックボックスをオンにします。

ステップ 8 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。

ヒント コメント フィールドはページの [タスクの表示（View Tasks）] セクションに表示されるので、ある程度短くしてください。

ステップ 9 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 10 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定, （596 ページ）

URL フィルタリング更新の自動化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
URL フィルタリング（URL Filtering）	URL フィルタリング（URL Filtering）	任意（Any）	グローバルだけ	Admin/Maint

スケジューラを使用して、Cisco Collective Security Intelligence（CSI）からの URL フィルタリング データの更新を自動化できます。

また、URL フィルタリングを有効にする際に、自動更新を有効にできることに注意してください。その場合、URL フィルタリング データの更新を確認するために Management Center は必ず 30 分ごとに CSI と通信します。

（注） URL フィルタリングを有効にしたときに自動更新を有効にした場合は、URL フィルタリング データを更新するスケジュール済みタスクを作成**しないでください**。URL フィルタリングの更新を厳密に制御する場合のみタスクをスケジュールします。

通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL フィルタリング データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

はじめる前に

- Firepower Management Center にインターネット アクセス権があることを確認してください（セキュリティ、インターネットアクセス、および通信ポート，（2187 ページ） を参照）。
- URL フィルタリングをイネーブルにします。詳細については、集合型セキュリティ インテリジェンスとの通信の設定，（986 ページ）を参照してください。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[URL フィルタリング データベースの更新（Update URL Filtering Database）] を選択します。

ステップ 4 更新をスケジュールする頻度として、ワンタイム更新を示す [1 回（Once）] または定期更新を示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定，（195 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。
[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 7 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定, （596 ページ）

スケジュール済みタスクの確認

スケジュール済みタスクを追加した後、それらのタスクを表示したり、状態を評価したりできます。ページの [表示オプション（View Options）] セクションで、カレンダーやスケジュール済みタスク リストを使用してスケジュール済みタスクを表示できます。

カレンダー表示オプションを使用すると、どの日にどのスケジュール済みタスクが行われるかを表示できます。

タスク リストには、タスクとその状態のリストが表示されます。タスク リストは、カレンダーを開いたときにカレンダーの下に表示されます。また、カレンダーで 1 つの日付またはタスクを選択して表示することもできます。

以前に作成したスケジュール済みタスクを編集できます。この機能は、パラメータが正しいことを確認するために、スケジュール済みタスクを 1 度テストする場合に特に役立ちます。タスクが正常に完了したら、後で定期タスクに変更できます。

[スケジュール表示（Schedule View）] ページから 2 種類の削除操作を実行できます。まだ実行されていない特定のワンタイム タスク、または定期タスクのすべてのインスタンスを削除できます。定期タスクの 1 つのインスタンスを削除すると、そのタスクのすべてのインスタンスが削除されます。1 度だけ実行するようスケジュールされているタスクを削除すると、そのタスクだけが削除されます。

タスク一覧の詳細

表 *22*：タスク一覧のカラム

カラム（**Column**）	説明
[名前（Name）]	スケジュール済みタスクの名前と、関連付けられているコメントを表示します。
タイプ（Type）	スケジュール済みタスクのタイプを表示します。
開始時刻（Start Time）	スケジュールされている開始日時を表示します。
頻度（Frequency）	タスクの実行頻度を表示します。
前回の実行時間（Last Run Time）	実際の開始日時を表示します。 定期タスクの場合、これは最新の実行に適用されます。
最終実行ステータス（Last Run Status）	スケジュール済みタスクの現在の状態を次のように示します。 • チェック マーク アイコン（  ）は、タスクが正常に実行されたことを示します。 • 疑問符アイコン（  ）は、タスクの状態が不明であることを示します。 • 感嘆符アイコン（  ）は、タスクが失敗したことを示します。 定期タスクの場合、これは最新の実行に適用されます。
次回の実行時間（Next Run Time）	定期タスクの次の実行時間を表示します。 ワンタイム タスクの場合に「該当なし（N/A）」と表示します。
作成者（Creator）	スケジュール済みタスクを作成したユーザの名前を表示します。
編集（Edit）	スケジュール済みタスクを編集します。
削除（Delete）	スケジュール済みタスクを削除します。

カレンダーのスケジュール済みタスクの表示

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

マルチドメイン展開では、現在のドメインのスケジュール済みタスクのみを表示できます。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 カレンダー ビューを使用して、次のタスクを実行できます。

- 二重左矢印アイコン（«）をクリックすると、1 年戻ります。
- 単一の左矢印アイコン（‹）をクリックすると、1 ヵ月戻ります。
- 単一の右矢印アイコン（›）をクリックすると、1 ヵ月進みます。
- 二重右矢印アイコン（»）をクリックすると、1 年進みます。
- [今日（Today）] をクリックすると、現在の年月に戻ります。
- [タスクの追加（Add Task）] をクリックすると、新しいタスクをスケジュールできます。
- 1 つの日付をクリックすると、カレンダーの下にあるタスク リスト表に、特定の日付のスケジュール済みタスクがすべて表示されます。
- ある日付の特定のタスクをクリックすると、カレンダーの下にあるタスク リスト表にそのタスクが表示されます。

スケジュール済みタスクの編集

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

マルチドメイン展開では、現在のドメインのスケジュール済みタスクのみを編集できます。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 カレンダーで、編集するタスク、またはタスクが表示されている日付をクリックします。

ステップ 3 [タスクの詳細（Task Details）] テーブルで、編集するタスクの横にある編集アイコン（  ）をクリックします。

ステップ 4 タスクを編集します。

ステップ 5 [保存（Save）] をクリックします。

スケジュール済みタスクの削除

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

マルチドメイン導入では、現在のドメインのスケジュール済みタスクのみを削除できます。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

ステップ 2 カレンダーで、削除するタスクをクリックします。繰り返しタスクの場合は、タスクのインスタンスをクリックします。

ステップ 3 [タスク詳細（Task Details）] テーブルで、削除アイコン（  ）をクリックし、選択内容を確認します。

第 10 章

Management Center データベースの消去

以下のトピックでは、Management Center から検出データを消去する方法を示します。

Management Center データベースからのデータの消去

スマート ライセンス	従来のライセンス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	グローバルだけ	Admin/Security Analyst

データベース消去ページを使用すると、検出、アイデンティティ、接続、およびセキュリティ インテリジェンスのデータ ファイルを Management Center データベースから消去できます。データベースを消去すると、該当するプロセスが再起動される点に注意してください。

注意 データベースを消去すると、Firepower Management Center から指定したデータが削除されます。削除されたデータは復元できません。

手順

ステップ 1 [システム（System）] > [ツール（Tools）] > [データの削除（Data Purge）]を選択します。

ステップ 2 [ネットワーク検出（Network Discovery）] で、次のいずれかまたはすべてを実行します。

- [ネットワーク検出イベント（Network Discovery Events）] チェックボックスをオンにして、データベースからすべてのネットワーク検出イベントを削除します。
- [ホスト（Hosts）]チェックボックスをオンにして、データベースからすべてのホストと侵害の兆候フラグを削除します。

- [ユーザ アクティビティ（User Activity）] チェックボックスをオンにして、データベースからすべてのユーザ アクティビティ イベントを削除します。
- [ユーザ アイデンティティ（User Identities）] チェックボックスをオンにして、データベースからすべてのユーザ ログインとユーザ履歴データを削除します。

ステップ 3 [接続（Connections）] で、次のいずれかまたはすべてを実行します。

- [接続イベント（Connection Events）] チェックボックスをオンにして、データベースからすべての接続データを削除します。
- [接続の概要イベント（Connection Summary Events）] チェックボックスをオンにして、データベースからすべての接続の概要データを削除します。
- [セキュリティ インテリジェンス イベント（Security Intelligence Events）] チェックボックスをオンにして、データベースからすべてのセキュリティ インテリジェンス データを削除します。

（注） [接続イベント（Connection Events）] チェックボックスをオンにしても、セキュリティ インテリジェンス イベントは削除されません。セキュリティ インテリジェンス データとの接続は、セキュリティ インテリジェンス イベント ビューアに引き続き表示されます。同様に、[セキュリティ インテリジェンス イベント（Security Intelligence Events）] チェックボックスをオンにしても、セキュリティ インテリジェンス データに関連する接続イベントは削除されません。

ステップ 4 [選択したイベントの消去（Purge Selected Events）] をクリックします。
項目が消去され、該当するプロセスが再起動されます。

第 III 部

System Monitoring

第 11 章

ダッシュボード

次のトピックでは、Firepower システムでダッシュボードを使用する方法について説明します。

ダッシュボードについて

Firepower システム ダッシュボードは、システムによって収集および生成されたイベントに関するデータを含む、現在のシステムのステータスを概要的なビューとして提供します。またダッシュボードを使用して、展開のアプライアンスのステータスと全体の正常性に関する情報を表示することもできます。ダッシュボードが提供する情報はシステムのライセンス方法、設定方法、展開方法によって異なる点に注意してください。

ヒント ダッシュボードは網羅的なデータを提供する複雑で高度にカスタマイズ可能なモニタリング機能です。モニタ対象のネットワークについての広範、簡潔でカラフルな画像を得るには、Context Explorer を使ってください。ダッシュボードは、Firepower Management Center および 7000 & 8000 シリーズ デバイスで使用できます。

ダッシュボードはウィジェットの表示にタブを使用します。ウィジェットは小さな自己完結型のコンポーネントで、システムのさまざまな側面を理解するうえで役に立ちます。たとえば、定義済みの [アプライアンス情報（Appliance Information）] ウィジェットは、アプライアンスの名前、モデル、および Firepower システム ソフトウェアの現在実行中のバージョンを通知します。システムはダッシュボードの時間範囲によってウィジェットを制約します。この時間範囲は、最短で 1 時間前から、最長では 1 年前からの期間を反映するように変更できます。

システムには、いくつかの事前定義されたダッシュボード ウィジェットが付属していて、使用および変更できます。ユーザ ロールにダッシュボードへのアクセス権が付与されている（管理者、メンテナンスユーザ、セキュリティ アナリスト（読み取り専用）、およびダッシュボードの権限付きのカスタム ロール）場合、デフォルトでホームページは事前定義されたサマリ ダッシュボー

ドになっています。ただし、ダッシュボード以外を含む別のデフォルト ホーム ページを設定できます。デフォルトのダッシュボードを変更することもできます。ダッシュボードへのアクセス権がないユーザ ロールの場合、デフォルトのホームページはロールに関連するページです。たとえば、Discovery Admin ロールの場合はネットワーク検出ページが表示されます。

また、事前定義済みのダッシュボードをカスタム ダッシュボードのベースとして使用することもできます。これは共有することもプライベートとして制限することもできます。管理者アクセス権がない場合、他のユーザが作成したプライベート ダッシュボードは表示も変更もできません。

（注） イベントのドリルダウン ページとテーブル ビューには、[ダッシュボード（Dashboard）] ツールバーのリンクが含まれているものがあります。このリンクをクリックして、関連する事前定義されたダッシュボードを表示することができます。事前定義されたダッシュボードまたはタブを削除すると、関連付けられているツールバーのリンクが機能しなくなります。

マルチドメイン展開では、先祖ドメインのダッシュボードを表示することはできません。ただし、高位レベルのダッシュボードをコピーした新規のダッシュボードを作成することはできます。

Firepower システムのダッシュボード ウィジェット

ダッシュボードには 1 つ以上のタブがあり、それぞれのタブには、3 列のレイアウトで 1 つ以上のウィジェットを表示できます。Firepower システムには、事前定義された多数のダッシュボード ウィジェットが付属しています。それぞれのウィジェットは、Firepower システムのさまざまな側面を理解するうえで役に立ちます。ウィジェットは、次の 3 つのカテゴリに分類されます。

- [分析およびレポート（Analysis & Reporting）] ウィジェットは、Firepower システムで収集および生成されたイベントに関するデータを表示します。
- *[*その他（*Miscellaneous*）*]* ウィジェットは、イベント データもオペレーション データも表示しません。現時点では、このカテゴリのウィジェットのみが RSS フィードを表示します。
- [オペレーション（Operations）] ウィジェットは、Firepower システムのステータスおよび全体の正常性に関する情報を表示します。

表示されるダッシュボード ウィジェットは、次の項目に応じて異なります。

- 使用しているアプライアンスのタイプ
- ユーザ ロール
- 現在のドメイン（マルチドメイン展開内）

また、各ダッシュボードには、動作を決定する一連のプリファレンスがあります。

ユーザは、ウィジェットを最小化および最大化する、タブに対してウィジェットを追加および削除する、タブ上でウィジェットを再配置する、といったことができます。

（注） 所定の時間範囲でのイベント カウントを表示するウィジェットでは、イベント ビューアで利用できる詳細なデータのイベント数が、イベントの総数に反映されないことがあります。これは、ディスク領域の使用率を管理するために、古いイベントの詳細がシステムによってプルーニングされることがあるために発生します。イベント詳細のプルーニングを最小限にするために、対象の展開にとって最も重要なイベントだけを記録するようにイベント ロギングを調整できます。

ウィジェットの使用可能性

表示できるダッシュボード ウィジェットは、使用中のアプライアンスのタイプ、使用するユーザ ロール、および（マルチドメイン展開での）現在のドメインによって異なります。

マルチドメイン展開で、予期したウィジェットが表示されない場合、グローバル ドメインに切り替えます。Firepower Management Center のドメインの切り替え，（30 ページ）を参照してください。

次の点に注意してください。

- 無効なウィジェットとは、ユーザが誤ったタイプのアプライアンスを使用しているために表示できないウィジェットのことです。
- 不正なウィジェットとは、ユーザ アカウントに必要な権限がないために表示できないウィジェットのことです。

たとえば、[アプライアンスの状態（Appliance Status）] ウィジェットを使用できるのは、Management Center で、管理者（Administrator）、メンテナンス ユーザ（Maintenance User）、セキュリティ アナリスト（Security Analyst）、またはセキュリティ アナリスト（読み取り専用）（Security Analyst（Read Only））のアカウント権限を持つユーザだけです。

不正なウィジェットまたは無効なウィジェットはダッシュボードに追加できませんが、インポートしたダッシュボードに不正なウィジェットまたは無効なウィジェットが含まれていることがあります。たとえば、インポートしたダッシュボードが次の場合に、このようなウィジェットが含まれている可能性があります。

- 各種アクセス権限を持つユーザによって作成された場合、または
- 先祖ドメインに属している場合。

使用できないウィジェットは無効になり、それらのウィジェットを表示できない理由を示すエラー メッセージが表示されます。

これらのウィジェットがタイムアウトした場合、またはそれ以外で問題が発生した場合には、個々のウィジェットでもエラー メッセージが表示されます。

（注） 不正なウィジェットと無効なウィジェット、および表示するデータがないウィジェットは、削除または最小化できます。共有されているダッシュボード上でウィジェットを変更すると、アプライアンスのすべてのユーザのウィジェットも変更されることに注意してください。

ユーザ ロール別のダッシュボード ウィジェットの可用性

次の表に、各ウィジェットを表示するために必要なユーザ アカウントの権限を示します。Administrator、Maintenance User、Security Analyst、または Security Analyst（読み取り専用）のアクセス権を持つユーザ アカウントのみがダッシュボードを使用できます。

カスタム ロールを持つユーザは、自身のユーザ ロールの許可によって、ウィジェットのいずれかの組み合わせにアクセスできる場合もあれば、どのウィジェットにもアクセスできない場合もあります。

表 *23*：ユーザ ロールとダッシュボード ウィジェットの可用性

ウィジェット	管理者（**Administrator**）	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（**RO**）
アプライアンス情報（Appliance Information）	Yes	Yes	Yes	Yes
アプライアンス ステータス（Appliance Status）	Yes	Yes	Yes	No
相関イベント（Correlation Events）	Yes	No	Yes	Yes
現在のインターフェイス ステータス（Current Interface Status）	Yes	Yes	Yes	Yes
現在のセッション（Current Sessions）	Yes	No	No	No
カスタム分析（Custom Analysis）	Yes	No	Yes	Yes
ディスク使用量	Yes	Yes	Yes	Yes
インターフェイス トラフィック（Interface Traffic）	Yes	Yes	Yes	Yes

ウィジェット	管理者（Administrator）	メンテナンス ユーザ	セキュリティ アナリスト	セキュリティ アナリスト（RO）
侵入イベント	Yes	No	Yes	Yes
ネットワーク コンプライアンス（Network Compliance）	Yes	No	Yes	Yes
製品ライセンスの認証（Product Licensing）	Yes	Yes	No	No
製品アップデート（Product Updates）	Yes	Yes	No	No
RSS フィード（RSS Feed）	Yes	Yes	Yes	Yes
システム ロード（System Load）	Yes	Yes	Yes	Yes
システム タイム（System Time）	Yes	Yes	Yes	Yes
ホワイトリスト イベント（White List Events）	Yes	No	Yes	Yes

定義済みダッシュボード ウィジェット

Firepowerシステムには、いくつかの定義済みウィジェットが付属しています。これらのウィジェットをダッシュボード上で使用することで、現在のシステム ステータスを一目で確認できます。ウィジェットのビューには、以下の情報が表示されます。

- システムが収集および生成したイベントに関するデータ
- 使用している導入のアプライアンスのステータスと全体的なヘルスに関する情報

（注） 表示できるダッシュボード ウィジェットは、使用しているアプライアンスのタイプとユーザ ロール、およびマルチドメイン展開の場合は現在のドメインによって異なります。

[アプライアンス情報（Appliance Information）] ウィジェット

[アプライアンス情報（Appliance Information）] ウィジェットは、アプライアンスのスナップショットを提供します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。このウィジェットは以下の情報を提供します。

- アプライアンスの名前、IPv4 アドレス、IPv6 アドレス、およびモデル
- ダッシュボードでアプライアンスにインストールされている、Firepower システム ソフトウェア、オペレーティング システム、Snort、ルール アップデート、ルール パック、モジュール パック、脆弱性データベース（VDB）、および地理情報のアップデートのバージョン（仮想 Firepower Management Center は除く）
- 管理対象アプライアンスの場合は、管理アプライアンスとの通信リンクの名前とステータス

単純なビューまたは高度なビューを表示するようにウィジェットのプリファレンスを変更することで、ウィジェットで表示する情報量を調整できます。プリファレンスでは、ウィジェットをアップデートする頻度を調整することもできます。

[アプライアンス ステータス（Appliance Status）] ウィジェット

[アプライアンス ステータス（Appliance Status）] ウィジェットは、アプライアンスの正常性、およびそのアプライアンスが管理しているアプライアンスの正常性を示します。Firepower Management Center は、管理対象のデバイスに対して自動的に正常性ポリシーを適用しないため、ユーザは正常性ポリシーをデバイスへ手動で適用する必要があります。このようにしないと、デバイスのステータスは `Disabled` として示されます。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

ウィジェットの設定を変更して、アプライアンスのステータスを円グラフまたは表で表示するように設定できます。

プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

円グラフの一部、またはアプライアンス ステータス表のいずれかの数字をクリックすると、[ヘルス モニタ（Health Monitor）] ページが表示され、対象のアプライアンス、およびそのアプライアンスが管理しているすべてのアプライアンスのコンパイル済みの正常性ステータスを参照することができます。

[相関イベント（Correlation Events）] ウィジェット

[相関イベント（Correlation Events）] ウィジェットは、ダッシュボードの時間範囲における 1 秒あたりの相関イベントの平均数を、優先度ごとに示します。このウィジェットは、詳細ダッシュボードの [相関（Correlation）] タブにデフォルトで表示されます。

ウィジェットを設定して、線形（増分）や対数（10 の倍数）のスケールを選択するだけでなく、ウィジェットの設定を変更してさまざまな優先度の相関イベントを表示することができます。

優先度を持たないイベントも含めて、特定の優先度のイベントに対して別のグラフを表示するには、1 つ以上の [優先順位（Priorities）] チェックボックスをオンにします。優先度に関係なくすべ

ての相関イベントに対して追加のグラフを表示するには、[すべて表示（Show All）] を選択します。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

グラフをクリックして特定の優先度の相関イベントを表示することも、[すべて（All）] グラフをクリックしてすべての相関イベントを表示することもできます。いずれの場合も、イベントはダッシュボードの時間範囲に制限されます。ダッシュボードを介して相関イベントにアクセスすると、そのアプライアンスに対するイベント（またはグローバル）の期間が変わります。

[現在のインターフェイス ステータス（Current Interface Status）] ウィジェット

[現在のインターフェイス ステータス（Current Interface Status）] ウィジェットは、有効になっているか未使用のアプライアンスのすべてのインターフェイスのステータスを示します。Firepower Management Center では、管理（`eth0`、`eth1` など）インターフェイスを表示できます。管理対象デバイスでは、センシング（`s1p1` など）インターフェイスのみを表示するか、または管理インターフェイスとセンシング インターフェイスの両方を表示するかを選択できます。インターフェイスは、タイプ（管理、インライン、パッシブ、スイッチド、ルーテッド、スタック、未使用）別にグループ化されます。

ウィジェットは、各インターフェイスに対して次の情報を提供します。

- インターフェイスの名前
- インターフェイスのリンク状態
- インターフェイスのリンク モード（100Mb 全二重、または 10Mb 半二重など）
- インターフェイスのタイプ（銅線または光ファイバ）
- インターフェイスで受け取ったデータ量（Rx）および送信したデータ量（Tx）

リンク状態を表すボールの色は、次のように現在のステータスを示します。

- 緑色：リンクがフル スピードでアップ状態になっています
- 黄色：リンクはアップ状態ですがフル スピードではありません
- 赤色：リンクはアップ状態ではありません
- 灰色：リンクは管理上無効になっています
- 青色：リンク ステート情報は使用できません（たとえば ASA）

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。

[現在のセッション（Current Sessions）] ウィジェット

[現在のセッション（Current Sessions）] ウィジェットは、アプライアンスに現在ログインしているユーザ、セッションが生じたマシンに関連付けられている IP アドレス、各ユーザがアプライアンス上のページにアクセスした最後の（アプライアンスのローカル時間に基づいた）時間を示します。自分を表すユーザ（現在ウィジェットを表示しているユーザ）には、ユーザアイコン（  ）のマークが付けられ、太字で示されます。ログオフするか非アクティブになってから 1 時間以内

に、セッションはこのウィジェットのデータからプルーニングされます。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

[現在のセッション（Current Sessions）] ウィジェットでは、次のことができます。

- いずれかのユーザ名をクリックして、[ユーザ管理（User Management）] ページでユーザ アカウントを管理します。
- ホスト アイコン（）、または IP アドレスの隣の侵害されたホスト アイコン（  ）をクリックして、関連付けられているマシンのホスト プロファイルを表示します。
- いずれかの IP アドレスまたはアクセス時間をクリックして、その IP アドレスおよびその IP アドレスに関連付けられているユーザが Web インターフェイスにログオンした時間によって制約される監査ログを表示します。

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。

[カスタム分析（Custom Analysis）] ウィジェット

[カスタム分析（Custom Analysis）] ウィジェットは高度にカスタマイズ可能なウィジェットで、これを使用すると、Firepower システムで収集および生成されたイベントの詳細情報を表示できます。

このウィジェットには複数のプリセットが用意されており、導入に関する情報にすばやくアクセスできます。事前定義済みのダッシュボードから、これらのプリセットを幅広く使用できます。これらのプリセットを使用することも、カスタム設定を作成することもできます。カスタム構成では少なくとも、関心のあるデータ（表とフィールド）とそのデータの集計方法を指定します。イベントの相対的な発生数を表示するのか（棒グラフ）、一定期間のイベント数を表示するのか（折れ線グラフ）など、その他の表示関連の設定を適用することもできます。

このウィジェットは、ローカル時間に基づいて、最後にアップデートされた時間を表示します。ウィジェットのアップデートは、ダッシュボードの時間範囲に基づいた頻度で実行されます。たとえば、ダッシュボードの時間範囲を 1 時間に設定すると、ウィジェットは 5 分ごとにアップデートされます。また、ダッシュボードの時間範囲を 1 年に設定すると、ウィジェットは 1 週間ごとにアップデートされます。ダッシュボードが次にアップデートされるタイミングを設定するには、ウィジェットの左下にある [最終更新日（Last updated）] の通知にポインタを移動します。

（注） [カスタム分析（Custom Analysis）] ウィジェットに赤い影が付いている場合は、そのウィジェットの使用がシステムのパフォーマンスに悪影響を及ぼしています。ウィジェットが長時間赤い状態のままになっている場合は、そのウィジェットを削除してください。また、システム構成（[システム（System）] > [設定（Configuration）] > [ダッシュボード（Dashboard）]）のダッシュボード設定で、すべての [カスタム分析（Custom Analysis）] ウィジェットを無効にすることもできます。

イベントの相対的な発生数の表示（棒グラフ）

[カスタム分析（Custom Analysis）] ウィジェットの棒グラフでは、ウィジェットの背景の色付きバーが、各イベントの相対的な発生数を示します。バーは右から順にお読みください。

矢印のアイコン（）は、表示のソート順を示して、制御しています。下向きのアイコンは降順を表し、上向きのアイコンは昇順を表します。ソート順を変更するには、アイコンをクリックします。

最新の結果以降何らかの変更点があることを示すために、ウィジェットでは、各イベントの横に次の 3 つのアイコンのうちの 1 つを表示します。

- 新しいイベントアイコン（  ）は、イベントが、最新の結果以降のものであることを示します。
- 上向き矢印のアイコン（）は、ウィジェットが最後にアップデートされた後で、イベントがこの場所に上がってきたことを示します。イベントが何段階上がってきたかを表す数字が、アイコンの横に示されます。
- 下向き矢印のアイコン（）は、ウィジェットが最後にアップデートされた後で、イベントがこの場所に下がってきたことを示します。イベントが何段階下がってきたかを表す数字が、アイコンの横に示されます。

一定期間のイベントの表示（折れ線グラフ）

一定期間のイベントまたは収集されたその他のデータに関する情報が必要な場合は、対象の展開で、一定期間に発生した侵入イベントの合計数を表示するような線グラフを表示するように[カスタム分析（Custom Analysis）] ウィジェットを設定することができます。

[カスタム分析（Custom Analysis）] ウィジェットの制限

[カスタム分析（Custom Analysis）] ウィジェットは、表示するように設定されたデータを表示する権限がないことを示すことがあります。たとえば、メンテナンス ユーザには検出イベントを表示する権限がありません。また、このウィジェットは、ライセンスされていない機能に関連する情報を表示しません。ただし、そのユーザ（およびダッシュボードを共有している他のユーザ）は、ウィジェットの設定を変更して、自分が表示できるデータを表示することも、ウィジェットを削除することもできます。これを防ぐには、ダッシュボードをプライベート（非公開）で保存します。

ユーザ データを表示した場合は、権限のあるユーザのみが表示されます。

URL カテゴリ情報を表示した場合、分類されていない URL は表示されません。

[カウント（Count）] で集約した侵入イベントを表示した場合、この数には、侵入イベントについてレビューされたイベントが含まれています。イベント数をイベント ビューアで表示する場合は、レビューされたイベントは含まれません。

（注） マルチドメイン展開では、システムは、各リーフ ドメインに個別のネットワーク マップを作成します。その結果、リーフ ドメインには、ネットワーク内で一意である IP アドレスを含めることができますが、別のリーフ ドメイン内の IP アドレスと同じにすることができます。先祖ドメインで[カスタム分析（Custom Analysis）]ウィジェットを表示すると、繰り返し使用される IP アドレスの複数のインスタンスを表示できます。一見すると、エントリが重複しているように見えることがあります。ただし、各 IP アドレスのホスト プロファイル情報までドリル ダウンすると、それらが異なるリーフ ドメインに属していることがわかります。

例：カスタム構成

最近の侵入イベントのリストを表示するように[カスタム分析（Custom Analysis）]ウィジェットを設定するには、[侵入イベント（Intrusion Events）]テーブルのデータを表示するようにウィジェットを設定します。[分類（Classification）]フィールドを選択し、このデータを[カウント（Count）]で集約すると、各タイプのイベントがいくつ生成されたかが通知されます。

一方、[一意のイベント（Unique Events）]で集約すると、各タイプで一意の侵入イベントがいくつ発生したかが通知されます（たとえばネットワークの Trojan、企業ポリシーの潜在的な違反、行われたサービス妨害攻撃の検出個数など）。

ウィジェットをさらに制約するには、保存されている検索（アプライアンスに付属している事前定義の検索、またはユーザが作成したカスタム検索のいずれか）を使用します。たとえば、最初の例（[分類（Classification）]フィールドを使用して[カウント（Count）]で集約する）を、[ドロップされたイベント（Dropped Events）]の検索を使用して制約すると、各タイプの侵入イベントがいくつドロップされたかが通知されます。

関連トピック

ダッシュボードの時刻設定の変更，（247 ページ）

*[カスタム分析（Custom Analysis）]*ウィジェットのプリファレンス

次の表に、[カスタム分析（Custom Analysis）]ウィジェットで設定できるプリファレンスについて示します。

さまざまなプリファレンスは、ウィジェットを設定する方法に応じて表示されます。たとえば、イベントの相対頻度（棒グラフ）を表示する場合と、時系列のグラフ（線グラフ）を表示する場合とでは、ウィジェットの設定時に異なるプリファレンス セットが表示されます。フィルタなど、一部のプリファレンスは、表示するデータが存在する特定のテーブルを選択する場合にのみ表示されます。

表 *24*：*[カスタム分析（Custom Analysis）]*ウィジェットのプリファレンス

設定	詳細（Details）
役職（Title）	ウィジェットのタイトルを指定しない場合、システムは、設定済みのイベント タイプをタイトルとして使用します。

設定	詳細（Details）
プリセット（Preset）	[カスタム分析（Custom Analysis）]のプリセットによって、展開に関する情報に簡単にアクセスできます。事前定義済みのダッシュボードから、これらのプリセットを幅広く使用できます。これらのプリセットを使用することも、カスタム設定を作成することもできます。
テーブル（Table）（必須）	ウィジェットが表示するデータを含むイベントまたはアセットのテーブル。
フィールド（Field）（必須）	表示するイベントタイプの特定のフィールド。時系列でデータ（線グラフ）を表示するには、[時間（Time）] を選択します。イベントの相対頻度（棒グラフ）を表示するには、もう一方のオプションを選択します。
集約（Aggregate）（必須）	集約方法は、表示するデータをウィジェットがどのようにグループ化するかを設定します。ほとんどのイベント タイプのデフォルト オプションは [カウント（Count）] です。
フィルタ	[アプリケーション統計（Application Statistics）] および [アプリケーション別の侵入イベント統計（Intrusion Event Statistics by Application）] テーブルのデータを制約するには、アプリケーション フィルタを使用できます。
検索（Search）	保存した検索を使用して、ウィジェットが表示するデータを制約することができます。検索を指定する必要はありませんが、プリセットの中には事前定義された検索が使用されるものがあります。 ユーザがアクセスできる検索は、プライベートで保存した検索だけです。共有ダッシュボード上にウィジェットを設定し、プライベートの検索を使用してイベントを制約すると、ウィジェットは、他のユーザがログインしたときにその検索を使用しないようにリセットされます。ウィジェットのビューにも影響します。これを防ぐには、ダッシュボードをプライベート（非公開）で保存します。 接続イベントに基づいて [カスタム分析（Custom Analysis）] ダッシュボード ウィジェットを制約できるのは、接続サマリーを制限しているフィールドだけです。保存した無効な検索はグレー表示されます。 保存されている検索を使用して [カスタム分析（Custom Analysis）] ウィジェットを制約し、その後で検索を編集すると、次にアップデートされるまでウィジェットには変更が反映されません。
表示（Show）	最も高い（[最上位（Top）]）または最も低い（[最下位（Bottom）]）頻度で発生するイベントを表示するかどうかを選択します。
結果（Results）	表示する結果の行数を選択します。
Mover の表示（Show Movers）	最新の結果以降の変更を示すアイコンを表示するかどうかを選択します。
タイム ゾーン	結果の表示に使用するタイム ゾーンを選択します。

設定	詳細（Details）
カラー（Color）	ウィジェットの棒グラフのバーの色を変更できます。

関連トピック

ウィジェットの設定, （243 ページ）

Custom Analysis ウィジェットから関連付けられているイベントを表示する

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

Custom Analysis ウィジェットから、ウィジェットに表示されるイベントに関する詳細情報を提供するイベント ビュー（ワークフロー）を起動することができます。イベントは、ダッシュボードの時間範囲によって制限されて、そのイベント タイプのデフォルトのワークフローで表示されます。設定した時間枠の数やイベント タイプに応じて、Firepower Management Center の時間枠が適宜変更されます。

次に例を示します。

- 複数の期間が設定されている場合に、Custom Analysis ウィジェットからヘルス イベントにアクセスすると、デフォルトのヘルス イベント ワークフローにイベントが表示され、ヘルス モニタリング期間はダッシュボードの時間範囲に変更されます。
- 1 つの時間枠を設定していて Custom Analysis ウィジェットから任意のタイプのイベントにアクセスすると、イベントはそのイベント タイプのデフォルト ワークフローに表示され、グローバル期間がダッシュボードの時間範囲に変更されます。

手順

次の選択肢があります。

- Custom Analysis ウィジェットの右下にあるすべて表示のアイコン（  ）をクリックして、ウィジェットの設定で制約して、すべての関連イベントを表示することができます。
- 関連するイベントの発生数（棒グラフ）を表示するように設定された Custom Analysis ウィジェットで、任意のイベントをクリックして、ウィジェットの設定、およびそのイベントで制約して、関連イベントを表示します。

[ディスク使用量（Disk Usage）] ウィジェット

[ディスク使用量（Disk Usage）] ウィジェットは、ディスク使用率のカテゴリに基づいて、ハードドライブで使用される領域のパーセンテージを表示します。また、アプライアンスのハード ドライブの各パーティションで使用される領域のパーセンテージおよび容量も示します。[ディスク使用量（Disk Usage）] ウィジェットがデバイスにインストールされている場合、または Firepower Management Center が、マルウェア ストレージ パックが含まれているデバイスを管理している場合、[ディスク使用量（Disk Usage）] ウィジェットはマルウェア ストレージ パックについて同じ情報を表示します。このウィジェットは、デフォルト ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

[カテゴリ別（By Category）] スタック バーは、各ディスク使用率のカテゴリを、使用可能な合計ディスク領域に対する使用量の割合として表示します。次の表で、使用可能なカテゴリについて説明します。

表 *25*：ディスク使用率のカテゴリ

ディスク使用率のカテゴリ	説明
イベント	システムで記録されたすべてのイベント
ファイル（Files）	システムに格納されたすべてのファイル
バックアップ	すべてのバックアップ ファイル
変更点	ルールのアップデートやシステムのアップデートなど、アップデートに関連するすべてのファイル
その他	システムのトラブルシューティング ファイルおよびその他のファイル
未使用	アプライアンス上の残りの空き領域

[カテゴリ別（By Category）] スタック バーのディスク使用率カテゴリにポインタを合わせると、使用可能なディスク領域のうち、そのカテゴリで使用された領域の割合、ディスク上の実際のストレージ領域、およびそのカテゴリで使用可能なディスク領域の合計を表示することができます。マルウェア ストレージ パックがインストールされている場合、[ファイル（Files）] カテゴリで使用できるディスク領域の合計は、マルウェア ストレージ パックで使用できるディスク領域になることに注意してください。

マルウェア ストレージ パックがインストールされている場合は、ウィジェットのプリファレンスを変更して、[カテゴリ別（By Category）] スタック バーのみを表示したり、スタック バーと admin（/）、`/Volume`、および `/boot` パーティションの使用率、および `/var/storage` パーティションを表示したりするようにウィジェットを設定できます。

ウィジェットのプリファレンスは、ウィジェットのアップデート頻度、およびダッシュボードの時間範囲で現在のディスク使用率または収集したディスク使用率の統計のいずれかを表示するかも制御します。

[インターフェイス トラフィック（Interface Traffic）] ウィジェット

[インターフェイス トラフィック（Interface Traffic）] ウィジェットには、アプライアンスのインターフェイスで送受信された受信（Rx）トラフィックと送信（Tx）トラフィックの割合が示されます。7000 & 8000 シリーズ デバイスの場合、ウィジェットにはセンシング インターフェイスに関する情報も表示されます。このウィジェットは、事前定義されたダッシュボードにデフォルトでは表示されません。

アウトバウンド（送信）トラフィックには、フロー制御パケットが含まれます。そのため、7000 & 8000 シリーズ デバイス上のパッシブ センシング インターフェイスには、送信トラフィックが表示されることがあり、これは想定されている動作です。マルウェア ライセンスが有効になっているデバイスは、動的分析を設定していない場合でも、定期的にAMPクラウドへの接続を試行します。そのため、これらのデバイスには送信トラフィックが表示されます。これもまた想定されている動作です。

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。7000 & 8000シリーズデバイスでは、設定によって、使用されていないインターフェイスのトラフィック レートをウィジェットに表示するかどうかも制御します（デフォルトでは、ウィジェットにはアクティブなインターフェイスのトラフィック レートのみが表示されます）。

[侵入イベント（Intrusion Events）] ウィジェット

[侵入イベント（Intrusion Events）] ウィジェットは、ダッシュボードの時間範囲で発生した侵入イベントを、優先度ごとに表示します。これには、ドロップされたパケットおよびさまざまな影響を含む、侵入イベントの統計が含まれています。このウィジェットは、サマリ ダッシュボードの [侵入イベント（Intrusion Events）] タブにデフォルトで表示されます。

ウィジェットの設定では、次のことができます。

- [イベント フラグ（Event Flags）] には、パケットが欠落したイベント、パケットが欠落した可能性のあるイベント、または特定の影響を示すグラフが個別に表示されます。影響やルールの状態に関係なくすべての侵入イベントに対して追加のグラフを表示するには、[すべて（All）] を選択します。
- [表示（Show）] では、[1 秒あたりの平均イベント数（Average Events Per Second）] または [イベントの合計数（Total Events）] を選択できます。
- [縦方向スケール（Vertical Scale）] では、[線形（Linear）]（増分）または [対数（Logarithmic）]（10 の倍数）のスケールを選択できます。
- ウィジェットの更新頻度。

ウィジェットでは次のことができます。

- ドロップされたパケット、ドロップされた可能性のあるパケット、または特定の影響に対応するグラフをクリックして、そのタイプの侵入イベントを表示します。

- ドロップされたイベントに対応するグラフをクリックして、ドロップされたイベントを表示します。
- ドロップされたと考えられるイベントに対応するグラフをクリックして、ドロップされたと考えられるイベントを表示します。
- [すべて（All）] グラフをクリックして、すべての侵入イベントを表示します。

結果のイベント ビューは、ダッシュボードの時間範囲に制約されます。ダッシュボードを介して侵入イベントにアクセスすると、そのアプライアンスに対するイベント（またはグローバル）の期間が変わります。侵入ルールの状態または侵入ポリシーのインライン ドロップ動作に関係なく、パッシブな配置のパケットはドロップされないことに注意してください。

[ネットワーク コンプライアンス（Network Compliance）] ウィジェット

[ネットワーク コンプライアンス（Network Compliance）] ウィジェットは、ユーザが設定したホワイト リストに対するホストのコンプライアンスを要約します。デフォルトではこのウィジェットに、アクティブな相関ポリシーにおけるすべてのコンプライアンス ホワイトリストに対して準拠しているホスト、準拠していないホスト、および評価されなかったホストの数を示す円グラフが表示されます。このウィジェットは、詳細ダッシュボードの [相関（Correlation）] タブにデフォルトで表示されます。

ウィジェットの設定を変更して、すべてのホワイトリスト、または特定のホワイトリストのいずれかについてネットワーク コンプライアンスを表示するようにウィジェットを設定できます。

すべてのホワイトリストに対してネットワーク コンプライアンスを表示するよう選択すると、あるホストが、アクティブな相関ポリシーのいずれのホワイト リストにも準拠していない場合、ウィジェットはそのホストが非準拠であるとみなします。

また、このウィジェットの設定を使用すると、ネットワーク コンプライアンスの表示で次の 3 つのスタイルのうちどれを使用するかを指定することができます。

[ネットワーク コンプライアンス（Network Compliance）] スタイル（デフォルト）は、準拠しているホスト、準拠していないホスト、および評価されなかったホストの数を示す円グラフを表示します。ホストの違反の件数を表示するには、円グラフをクリックします。このようにすると、少なくとも 1 つのホワイト リストに違反しているホストが表示されます。

[一定期間のネットワーク コンプライアンス（%）（Network Compliance over Time (%)）] スタイルは、ダッシュボードの時間範囲において準拠しているホスト、準拠していないホスト、およびまだ評価されていないホストの相対的な割合を示す積み重ね面積グラフを表示します。

[一定期間のネットワーク コンプライアンス（Network Compliance over Time）] スタイルは、ダッシュボードの時間範囲において準拠しているホスト、準拠していないホスト、およびまだ評価されていないホストの数を示す線グラフを表示します。

ウィジェットをアップデートする頻度は、設定で調整します。まだ評価されていないイベントを非表示にするには、[未評価を表示（Show Not Evaluated）] ボックスをオンにします。

[製品ライセンス（Product Licensing）] ウィジェット

[製品ライセンス（Product Licensing）] ウィジェットは、Firepower Management Center に現在インストールされているデバイスおよび機能のライセンスを示します。また、ライセンス契約されているアイテムの数、許可される残りのライセンス契約アイテム数も示します。これは、事前定義されたどのダッシュボードにおいてもデフォルトでは表示されません。

このウィジェットの上部のセクションには、一時的なライセンスも含めて、Firepower Management Center にインストールされているすべてのデバイスおよび機能のライセンスが表示されますが、[期限の切れたライセンス（Expiring Licenses）] セクションには、一時的なライセンスおよび期限の切れたライセンスのみが表示されます。

ウィジェットの背景のバーは、使用中のライセンスのそれぞれのタイプの割合を示しています。このバーは右から左へ読みます。期限の切れたライセンスには、取り消し線が付けられています。

ウィジェットのプリファレンスを変更して、現在ライセンス契約されている機能を表示するか、またはライセンス契約が可能なすべての機能を表示するようにウィジェットを設定することができます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

任意のライセンス タイプをクリックすると、ローカル設定の [ライセンス（License）] ページに移動して、機能ライセンスを追加または削除することができます。

[製品更新（Product Updates）] ウィジェット

[製品更新（Product Updates）] ウィジェットは、アプライアンスに現在インストールされているソフトウェアの概要、およびダウンロード済みだがまだインストールしていない更新プログラムの情報を提供します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

このウィジェットは、スケジュールされたタスクを使用して最新バージョンを判別するため、更新プログラムをダウンロード、プッシュ、またはインストールするようにスケジュールされたタスクを構成するまで、Unknown と表示されます。
ウィジェットのプリファレンスを変更して、最新のバージョンを非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

このウィジェットには、ソフトウェアを更新できるページへのリンクもあります。次の操作を実行できます。

- 現在のバージョンをクリックして、アプライアンスを手動で更新します。
- 最新バージョンをクリックして、更新プログラムをダウンロードするタスクをスケジュールします。

[RSS フィード（RSS Feed）] ウィジェット

[RSS フィード（RSS Feed）] ウィジェットは、ダッシュボードに RSS フィードを追加します。デフォルトでは、ウィジェットはシスコのセキュリティ ニュースのフィードを示します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

また、企業ニュース、Snort.org ブログ、または Cisco 脅威調査ブログの事前設定済みのフィードを表示するようウィジェットを設定することができます。ウィジェットの設定で URL を指定して、他の RSS フィードに対するカスタム接続を作成することもできます。

フィードは 24 時間ごとに更新されます（ただしユーザはフィードを手動で更新できます）。また、ウィジェットはアプライアンスのローカル時間に基づいて、フィードが最後に更新された時間を表示します。アプライアンスは、（事前設定された 2 つのフィードについて）Web サイトに対するアクセス権を持っている、または設定したいずれかのカスタム フィードに対するアクセス権を持っている必要があります。

ウィジェットを設定する場合には、フィードからいくつのストーリーをウィジェットに表示するか、およびヘッドラインとともにストーリーの説明を表示するかどうかを選択することができます。ただしすべての RSS フィードで説明が使用できるわけではないことに注意してください。

[RSS フィード（RSS Feed）] ウィジェットでは、次のことができます。

- フィード内のストーリーのいずれかをクリックして、ストーリーを表示します
- [さらに表示（more）] リンクをクリックして、フィードの Web サイトへ移動します
- 更新アイコン（）をクリックして、フィードを手動で更新します

[システム負荷（System Load）] ウィジェット

[システム負荷（System Load）] ウィジェットは、アプライアンス上の（各 CPU についての）CPU の使用率、メモリ（RAM）の使用率、およびシステムの負荷（実行を待機しているプロセスの数によって測定され、負荷平均とも呼ばれる）を現在、およびダッシュボードの時間範囲について表示します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

ウィジェットのプリファレンスを変更して、負荷平均を表示または非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

[システム時刻（System Time）] ウィジェット

[システム時刻（System Time）] ウィジェットは、アプライアンスのローカル システム時間、稼動時間、およびブート時間を表示します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

ウィジェットのプリファレンスを変更して、ブート時間を非表示にするようウィジェットを設定できます。プリファレンスは、ウィジェットがアプライアンスの時計と同期する頻度も調整します。

[ホワイト リスト イベント（White List Events）] ウィジェット

[ホワイト リスト イベント（White List Events）] ウィジェットは、ダッシュボードの時間範囲における 1 秒あたりの平均イベント数を、優先度別に表示します。このウィジェットは、デフォルト ダッシュボードの [相関（Correlation）] タブにデフォルトで表示されます。

ウィジェットの設定を変更して、さまざまな優先度のホワイト リスト イベントを表示するようウィジェットを設定できます。

ウィジェットの設定では、次のことができます。

- 優先度を持たないイベントも含めて、特定の優先度のイベントに対して別のグラフを表示するには、1 つ以上の [優先順位（Priorities）] チェックボックスをオンにします。
- 優先度に関係なくすべてのホワイトリストイベントに対して追加のグラフを表示するには、[すべて表示（Show All）] を選択します。
- [縦方向スケール（Vertical Scale）] を選択して、[線形（Linear）]（増分）または [対数（Logarithmic）]（10 の倍数）のスケールを選択します。

プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

グラフをクリックして特定の優先度のホワイトリストイベントを表示することも、[すべて（All）] グラフをクリックしてすべてのホワイトリストイベントを表示することもできます。いずれの場合も、イベントは、ダッシュボードの時間範囲によって制約されます。ダッシュボードを介してホワイト リスト イベントにアクセスすると、Firepower Management Center に対するイベント（またはグローバル）の期間が変わります。

ダッシュボードの管理

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

手順

ステップ 1 [概要（Overview）] > [ダッシュボード（Dashboards）] を選択して、変更するダッシュボードをメニューから選択します。

ステップ 2 ダッシュボードを管理します。

- ダッシュボードの作成：カスタム ダッシュボードを作成します。カスタム ダッシュボードの作成, （244 ページ）を参照してください。
- ダッシュボードの削除：ダッシュボードを削除するには、削除するダッシュボードの横にある削除アイコン（）をクリックします。デフォルトのダッシュボードを削除する場合は、新しいデフォルトを定義する必要があります。そうしない場合、ダッシュボードを表示しようとするたびに、アプライアンスからダッシュボードを選択するように要求されます。

- オプションの編集：カスタムのダッシュボード オプションを編集します。ダッシュボード オプションの編集, （247 ページ）を参照してください。
- 時間の制約の変更：ダッシュボードの表示時間または一時停止/一時停止解除の時間を変更します。詳細は、ダッシュボードの時刻設定の変更, （247 ページ）を参照してください。

ステップ 3 ダッシュボードのタブを管理します。

- タブの追加：ダッシュボードにタブを追加します。ダッシュボード タブの追加, （242 ページ）を参照してください。
- タブの削除：ダッシュボードのタブを削除するには、タブの右上隅にある閉じるアイコン（ ）をクリックし、[OK] をクリックして確認します。ダッシュボードから最後のタブを削除することはできません。各ダッシュボードには少なくとも 1 つのタブが必要です。
- タブの名前変更：ダッシュボードのタブの名前を変更します。ダッシュボードタブの名前の変更, （248 ページ）を参照してください。

（注） ダッシュボードのタブの順序は変更できません。

ステップ 4 ダッシュボード ウィジェットを管理します。

- ウィジェットの追加：ダッシュボードにウィジェットを追加します。ダッシュボードへのウィジェットの追加, （242 ページ）を参照してください。
- プリファレンスの設定：ウィジェットのプリファレンスを設定します。ウィジェットの設定, （243 ページ）を参照してください。
- 表示のカスタマイズ：ウィジェットの表示をカスタマイズします。ウィジェット表示のカスタマイズ, （246 ページ）を参照してください。
- イベントの表示：カスタム分析ウィジェットから関連するイベントを表示します。Custom Analysis ウィジェットから関連付けられているイベントを表示する, （234 ページ）を参照してください。

ヒント シスコの事前定義のダッシュボード内のカスタム分析ウィジェットのすべての設定が、ウィジェットのシステム プリセットに対応しています。これらのウィジェットの 1 つを変更または削除した場合は、適切なプリセットをベースにして新しいカスタム分析ウィジェットを作成して復元することができます。

ダッシュボード タブの追加

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

手順

ステップ 1 変更するダッシュボードを表示します（ダッシュボードの表示, （249 ページ）を参照）。

ステップ 2 最後の既存のタブの横にある追加アイコン（＋）をクリックします。

ステップ 3 タブの名前を入力します。

ステップ 4 [OK] をクリックします。

ダッシュボードへのウィジェットの追加

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

各タブには、3列のレイアウトで1つ以上のウィジェットを表示できます。ダッシュボードにウィジェットを追加するには、ウィジェットを追加するタブを選択します。ウィジェットは、自動的にウィジェットが最も少ない列に追加されます。すべてのカラムに同じ数のウィジェットがある場合、新しいウィジェットは最も左のカラムに追加されます。ダッシュボード タブには最大 15 個のウィジェットを追加できます。

ヒント 追加したウィジェットは、タブの任意の場所に移動できます。ただし、別のタブにはウィジェットを移動できません。

表示されるダッシュボードウィジェットは、使用しているアプライアンスのタイプ、ユーザ ロールと（マルチドメイン環境では）現在のドメインにより異なります。すべてのユーザ ロールがすべてのダッシュボード ウィジェットに対してアクセス権を持っているわけではないため、多くの権限を持つユーザが作成したダッシュボードを、それよりも少ない権限を持つユーザが参照する

場合、ダッシュボードのすべてのウィジェットを使用できないことがあることに注意してください。ダッシュボード上に、許可されていないウィジェットが表示されることがありますが、これらのウィジェットは無効です。

手順

ステップ 1 ウィジェットを追加するダッシュボードを表示します。ダッシュボードの表示, （249ページ） を参照してください。

ステップ 2 ウィジェットを追加するタブをクリックします。

ステップ 3 [ウィジェットの追加（Add Widgets）] をクリックします。カテゴリ名をクリックして各カテゴリのウィジェットを表示することも、[すべてのカテゴリ（All Categories）] をクリックしてすべてのウィジェットを表示することもできます。

ステップ 4 追加するウィジェットの横にある [追加（Add）] をクリックします。[ウィジェットの追加（Add Widgets）] ページには、追加するものも含め、各タブにあるウィジェットの数がタイプごとに表示されます。

ヒント （複数の RSS Feed ウィジェット、または複数の Custom Analysis ウィジェットを追加する場合など）同じタイプの複数のウィジェットを追加するには、[追加（Add）] をもう一度クリックします。

ステップ 5 ウィジェットの追加が終了したら、[完了（Done）] をクリックしてダッシュボードに戻ります。

次の作業

- カスタム分析ウィジェットを追加した場合は、ウィジェットの設定が必要です。ウィジェットの設定, （243 ページ） を参照してください。

関連トピック

ウィジェットの使用可能性, （225 ページ）

ウィジェットの設定

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

各ウィジェットには、動作を決定する一連のプリファレンスがあります。

手順

ステップ 1 プリファレンスを変更するウィジェットのタイトルバーで、プリファレンスの表示アイコン（⌄）をクリックします。

ステップ 2 必要に応じて変更を加えます。

ステップ 3 プリファレンスのセクションを非表示にするには、ウィジェットのタイトル バーで、プリファレンスの非表示アイコン（⌃）をクリックします。

カスタム ダッシュボードの作成

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

ヒント 新しいダッシュボードを作成する代わりに、別のアプライアンスからダッシュボードをエクスポートし、それを自分のアプライアンスへインポートすることができます。その後でニーズに合わせて、インポートしたダッシュボードを編集することができます。

手順

ステップ 1 [概要（Overview）] > [ダッシュボード（Dashboards）] > [管理（Management）]を選択します。

ステップ 2 [ダッシュボードの作成（Create Dashboard）] をクリックします。

ステップ 3 カスタム ダッシュボード オプション, （244 ページ）の説明に従って、カスタム ダッシュボード オプションを変更します。

ステップ 4 [保存（Save）] をクリックします。

カスタム ダッシュボード オプション

次の表に、カスタム ダッシュボードを作成または編集するときに使用できるオプションを示します。

表 *26*：カスタム ダッシュボード オプション

オプション	説明
ダッシュボードのコピー（Copy Dashboard）	カスタムダッシュボードを作成する場合は、ユーザが作成した、またはシステムで事前定義されている既存のダッシュボードをベースとして使用するよう選択できます。このオプションは、ニーズに合わせて変更できる、既存のダッシュボードのコピーを取ります。必要に応じて、[なし（None）] を選択することで、空白の新規ダッシュボードを作成できます。このオプションは、新しいダッシュボードを作成する場合のみ使用可能になります。 マルチドメイン展開では、先祖ドメインのプライベート以外のダッシュボードはコピーできます。
[名前（Name）]	カスタム ダッシュボードの固有名。
説明	カスタム ダッシュボードの簡単な説明。
タブを変更する間隔（Change Tabs Every）	ダッシュボードがそれぞれのタブを自動変更する頻度（分単位）を指定します。ダッシュボードを一時停止した場合や、ダッシュボードのタブが 1 つのみの場合を除き、この設定により、指定した間隔で次のタブが表示されます。タブの自動変更を無効にするには、[タブを変更する間隔（Change Tabs Every）] フィールドに 0 を入力します。
ページを更新する間隔（Refresh Page Every）	現在のダッシュボードのタブを新しいデータで更新する頻度（分単位）を指定します。この値は、[タブを変更する間隔（Change Tabs Every）] の設定より大きい値にする必要があります。ダッシュボードを一時停止しない限り、この設定より、指定した間隔でダッシュボード全体が更新されます。定期的なページ更新を無効にするには、[ページを更新する間隔（Refresh Page Every）] フィールドに 0 を入力します。ダッシュボードのページ全体を自動的に更新する頻度を決定します。 ダッシュボード全体を更新すると、共有のダッシュボードに対して他のユーザが行ったプリファレンスまたはレイアウトの変更や、他のコンピュータ上のプライベート ダッシュボードに対して、ダッシュボードが最後に更新された後で自分が行った変更を確認できます。ダッシュボードが常に表示されているネットワーク オペレーション センター（NOC）などでは、頻繁な更新が有効です。ローカル コンピュータでダッシュボードの変更を行なえば、ユーザが指定する間隔でNOCのダッシュボードが自動的に更新されるため、手動による更新は必要ありません。データのアップデートを確認するためにダッシュボード全体を更新する必要はありません。個々のウィジェットはプリファレンスに従ってアップデートされます。 （注） この設定は、個々のウィジェットの多くで使用可能なアップデート間隔とは異なります。ダッシュボードのページを更新すると個々のウィジェットのアップデート間隔はリセットされますが、[ページを更新する間隔（Refresh Page Every）] 設定を無効にしていても、ウィジェットはそれ自身のプリファレンスに従ってアップデートされます。

オプション	説明
プライベートとして保存（Save As Private）	カスタムダッシュボードは、アプライアンスのすべてのユーザが表示および変更可能か、またはユーザアカウントに関連付けて、独自の使用に限り予約可能かを決定します。ロールに関係なく、ダッシュボードへアクセスできるすべてのユーザは、共有ダッシュボードを変更できることに注意してください。特定のダッシュボードを自分のみが変更できるようにするには、そのダッシュボードをプライベートとして保存します。

ウィジェット表示のカスタマイズ

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

ウィジェットは、タブ上で最小化、最大化、および再配置することができます。

手順

ステップ 1 ダッシュボードを表示します（ダッシュボードの表示, （249 ページ）を参照）。

ステップ 2 次のように、ウィジェット表示をカスタマイズします。

- タブ上でウィジェットを再配置するには、移動するウィジェットのタイトルバーをクリックし、新しい場所へドラッグします。

  （注） 別のタブにウィジェットを移動することはできません。ウィジェットを別のタブに表示する場合は、現在のタブからいったん削除してから新しいタブに追加する必要があります。

- ダッシュボードでウィジェットを最小化または最大化するには、ウィジェットのタイトルバーにある最小化（−）アイコンまたは最大化（□）アイコンをクリックします。
- ウィジェットをタブ上に表示する必要がなくなった場合にそのウィジェットを削除するには、ウィジェットのタイトル バーにある閉じるアイコン（✖）をクリックします。

ダッシュボード オプションの編集

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

手順

ステップ 1 編集するダッシュボードを表示します（ダッシュボードの表示，（249 ページ）を参照）。

ステップ 2 変更するダッシュボードの横にある編集アイコン（  ）をクリックします。

ステップ 3 カスタム ダッシュボード オプション，（244 ページ）の説明に従ってオプションを変更します。

ステップ 4 [保存（Save）] をクリックします。

ダッシュボードの時刻設定の変更

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

最短で 1 時間前（デフォルト）から、最長では 1 年前からの期間を反映するように時間範囲を変更できます。時間範囲を変更する場合は、時間によって制約される可能性のあるウィジェットが自動でアップデートされ、新しい時間範囲が反映されます。

すべてのウィジェットを時間で制約できるわけではないことに注意してください。たとえば、ダッシュボードの時間範囲は [アプライアンス情報（Appliance Information）] ウィジェットには影響を与えません。このウィジェットは、アプライアンスの名前、モデル、および Firepower システム ソフトウェアの現在のバージョンが含まれている情報を提供します。

企業による Firepower システムの展開では、新しいイベントが古いイベントを置き換える頻度によっては、時間範囲を長期に変更しても、[カスタム分析（Custom Analysis）] ウィジェットなどのウィジェットでは役立たない場合があることに注意してください。

また、ダッシュボードを一時停止することもできます。これにより変更を表示したり、分析を中断したりせずに、ウィジェットで提供されたデータを調べることができます。ダッシュボードを一時停止すると、次のような影響があります。

- [更新間隔（Update Every）] ウィジェット プリファレンスに関係なく、個々のウィジェットでアップデートが停止します。
- ダッシュボード プロパティの [タブのサイクル間隔（Cycle Tabs Every）] 設定に関係なく、ダッシュボードのタブの自動変更が停止します。
- ダッシュボード プロパティの [ページの更新間隔（Refresh Page Every）] 設定に関係なく、ダッシュボードのページの更新が停止します。
- 時間範囲を変更しても影響はありません。

分析が完了したら、ダッシュボードの一時停止を解除できます。ダッシュボードの一時停止を解除すると、ページ上で該当するすべてのウィジェットが更新され、最新の時間範囲が反映されます。また、ダッシュボードのプロパティで指定した設定に従って、ダッシュボード タブの自動変更が再開され、ダッシュボード ページの更新が再開されます。

ダッシュボードに対するシステム情報のフローを中断するような接続の問題、または他の問題が発生した場合、ダッシュボードは自動的に一時停止し、問題が解決するまでエラー通知を表示します。

（注） ダッシュボードが一時停止しているかどうかに関係なく、セッションは通常、非アクティブな状態が1時間（または設定した他の時間）続いた場合、ユーザをログアウトします。ダッシュボードを長期間パッシブにモニタリングする場合は、一部のユーザをセッション タイムアウトしないよう設定したり、システムのタイムアウト設定を変更することを検討してください。

手順

ステップ 1 ウィジェットを追加するダッシュボードを表示します。ダッシュボードの表示, （249 ページ）を参照してください。

ステップ 2 必要に応じて、ダッシュボードの時間範囲を変更するには、[表示経過時間（Show the Last）] ドロップダウンリストから時間範囲を選択します。

ステップ 3 必要に応じて、一時停止（⏸）または再生アイコン（▶）を使用して、時間範囲コントロールでダッシュボードを一時停止または一時停止解除します。

ダッシュボード タブの名前の変更

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

手順

ステップ 1 変更するダッシュボードを表示します（ダッシュボードの表示, （249 ページ）を参照）。
ステップ 2 名前を変更するタブのタイトルをクリックします。
ステップ 3 タブの名前を入力します。
ステップ 4 [OK] をクリックします。

ダッシュボードの表示

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

デフォルトでは、アプライアンスのホーム ページにデフォルトのダッシュボードが表示されます。デフォルトのダッシュボードを定義していない場合は、ホーム ページに [ダッシュボードの管理（Dashboard Management）] ページが示され、ここで表示するダッシュボードを選択できます。

手順

いつでも次のいずれかの方法で操作できます。

- アプライアンスのデフォルト ダッシュボードを表示するには、[概要（Overview）] > [ダッシュボード（Dashboards）] を選択します。
- 特定のダッシュボードを表示するには、[概要（Overview）]>[ダッシュボード（Dashboards）] を選択し、メニューからダッシュボードを選択します。
- 利用可能なすべてのダッシュボードを表示するには、[概要（Overview）] > [ダッシュボード（Dashboards）]>[管理（Management）] を選択します。個々のダッシュボードの横にある表示アイコン（  ）を選択すると、そのダッシュボードを表示できます。

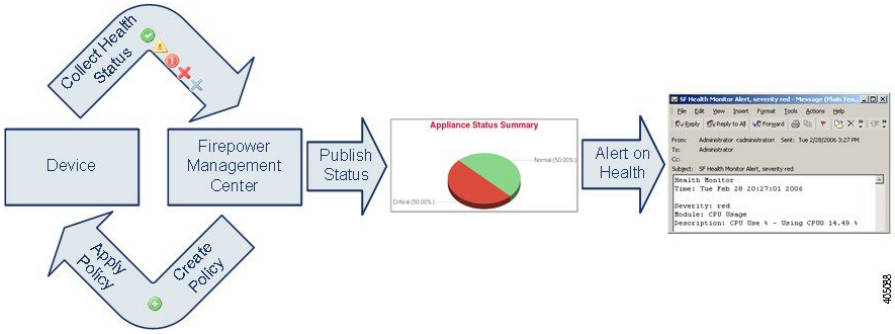
第 12 章

ヘルス モニタリング

次のトピックでは、Firepower システムでヘルス モニタリングを使用する方法について説明します。

ヘルス モニタリングについて

Firepower Management Center のヘルス モニタでは、さまざまなヘルス インジケータを追跡して Firepower システムのハードウェアとソフトウェアが正常に動作することを確認します。ヘルス モニタを使用して、Firepower システム展開全体の重要な機能のステータスを確認できます。



ヘルス モニタを使用すれば、正常性ポリシーとも呼ばれるテストのコレクションを作成し、正常性ポリシーを 1 つ以上のアプライアンスに適用できます。ヘルス モジュールとも呼ばれるテストは、指定された基準に照らしてテストするスクリプトです。テストを有効または無効にするか、テスト設定を変更することによって、正常性ポリシーを変更したり、不要になった正常性ポリシーを削除したりできます。アプライアンスをブラックリストに登録することによって、選択したアプライアンスからのメッセージを抑制することもできます。

正常性ポリシー内のテストは設定された時間間隔で自動的に実行されます。すべてのテストを実行することも、オンデマンドで特定のテストを実行することもできます。ヘルスモニタは設定されたテスト条件に基づいてヘルス イベントを収集します。

（注） すべてのアプライアンスはハードウェア アラームのヘルス モジュール経由でハードウェアのステータスを自動的に報告します。また、Firepower Management Center はデフォルトの正常性ポリシーで設定されているモジュールを使用して自動的にステータスを報告します。アプライアンス ハートビートなどの一部の正常性モジュールは、Firepower Management Center 上で実行され Firepower Management Center の管理対象デバイスのステータスを報告します。ヘルス モジュールによっては、そのモジュールが設定されている正常性ポリシーをデバイスに適用しない限り管理対象デバイスのステータスを報告しないものもあります。

ヘルス モニタを使用してシステム全体、特定のアプライアンス、または特定のドメイン（マルチドメイン展開の場合）に関するヘルス ステータス情報にアクセスできます。[ヘルス モニタ（Health Monitor）] ページの円グラフとステータス テーブルには、Firepower Management Center を含むネットワーク上のすべてのアプライアンスのステータスの視覚的なサマリが示されます。個々のアプライアンスのヘルス モニタを使用すれば、特定のアプライアンスのヘルス詳細にドリルダウンできます。

完全にカスタマイズ可能なイベント ビューを使用すれば、ヘルスモニタによって収集されたヘルス ステータス イベントを迅速かつ容易に分析できます。このイベント ビューでは、イベント データを検索して表示したり、調査中のイベントに関係する他の情報にアクセスしたりできます。たとえば、特定のパーセンテージの CPU 使用率の全記録を表示する場合は、CPU 使用率モジュールを検索して、パーセンテージ値を入力できます。

ヘルス イベントに対応した電子メール、SNMP、または syslog アラートを設定することもできます。ヘルス アラートは、標準アラートとヘルス ステータス レベルを関連付けたものです。たとえば、アプライアンスでハードウェアの過負荷が原因で障害が発生することは絶対ないことを確認する必要がある場合は、電子メール アラートをセットアップできます。その後で、CPU、ディスク、またはメモリの使用率がそのアプライアンスに適用される正常性ポリシーで設定された警告レベルに達するたびにその電子メールアラートをトリガーとして使用するヘルスアラートを作成できます。アラートしきい値を、受け取る反復アラートの数が最小になるように設定できます。

サポートから依頼された場合に、アプライアンスのトラブルシューティング ファイルを作成することもできます。

ヘルスモニタリングは管理活動であるため、管理者ユーザ ロール特権を持っているユーザのみがシステム ヘルス データにアクセスできます。

ヘルス モジュール

ヘルス モジュールまたはヘルス テストは、正常性ポリシーに指定した条件でテストします。

表 *27*：ヘルス モジュール

モジュール	適用可能なアプライアンス	説明
AMP for Endpoint のステータス	Management Center	このモジュールは、最初に接続に成功した後 Firepower Management Center が AMP クラウドまたは Cisco AMP Private Cloud (AMPv) に接続できない場合、または AMPv が AMP クラウドに接続できない場合、アラートを出します。また、AMP for Endpoints 管理コンソールを使用して AMP クラウド接続の登録が解除された場合にもアラートを出します。
AMP for Firepower のステータス	Management Center	このモジュールは、以下の場合にアラートを出します。 • Firepower Management Center が AMP クラウド、Cisco AMP Private Cloud (AMPv)、AMP Threat Grid クラウド、AMP Threat Grid オンプレミス アプライアンスに接続できない、または AMPv が AMP クラウドに接続できない。 • 接続に使用する暗号化キーが無効である。 • デバイスが AMP Threat Grid クラウドまたは AMP Threat Grid オンプレミス アプライアンスに接続して動的分析用のファイルを送信できない。 • ファイル ポリシー設定に基づいてネットワーク トラフィックで過剰な数のファイルが検出された。 Firepower Management Center のインターネット接続が切断された場合、AMP for Firepower ステータス ヘルス アラートの生成に最大 30 分かかることがあります。
アプライアンス ハートビート	任意（Any）	このモジュールは、アプライアンス ハートビートがアプライアンスから届いているかどうかを確認し、アプライアンスのハートビート ステータスに基づいてアラートを出します。
自動アプリケーション バイパス ステータス	7000 & 8000 シリーズ	このモジュールは、アプライアンスがバイパスしきい値で設定された秒数以内に応答しなかったためにバイパスされたかどうかを確認し、バイパスが発生した場合にアラートを出します。

モジュール	適用可能なアプライアンス	説明
クラシック ライセンス モニタ	Management Center	このモジュールは、制御、保護、URL フィルタリング、マルウェア、および VPN 用の十分なクラシック ライセンスが残っているかどうかを確認します。また、スタック内のデバイスに適合しないライセンス セットが含まれている場合にアラートを出します。モジュールに自動的に設定された警告レベルに基づいてアラートを出します。このモジュールの設定は変更できません。
CPU 使用率	任意（Any）	このモジュールは、アプライアンス上の CPU が過負荷になっていないことを確認し、CPU 使用率がモジュールに設定されたパーセンテージを超えた場合にアラートを出します。
カード リセット	任意（Any）	このモジュールは、リセット時に、ハードウェア障害原因で再起動されたネットワーク カードをチェックし、アラートを出します。
ディスク ステータス	任意（Any）	このモジュールは、ハードディスクと、アプライアンス上のマルウェア ストレージ パック（設置されている場合）のパフォーマンスを調査します。このモジュールは、ハードディスクと RAID コントローラ（設置されている場合）で障害が発生する恐れがある場合、または、マルウェア ストレージ パックではない追加のハードドライブが設置されている場合に、警告（黄色）ヘルス アラートを生成します。また、設置されているマルウェア ストレージ パックを検出できなかった場合はアラート（赤色）ヘルス アラートを生成します。
ディスク使用量	任意（Any）	このモジュールは、アプライアンスのハードドライブとマルウェア ストレージパック上のディスク使用率をモジュールに設定された制限と比較し、その使用率がモジュールに設定されたパーセンテージを超えた時点でアラートを出します。また、モジュールしきい値に基づいて、システムが監視対象のディスク使用カテゴリ内のファイルを過剰に削除する場合、または、これらのカテゴリを除くディスク使用率が過剰なレベルに達した場合にもアラートを出します。ディスク使用率ヘルス ステータス モジュールは、アプライアンス上の `/` パーティションと `/volume` パーティションのディスク使用率を監視して、ドレイン頻度を追跡するために使用します。ディスク使用率モジュールは `/boot` パーティションを監視対象パーティションとして列挙しますが、そのパーティションのサイズが固定のため、このモジュールはブート パーティションに基づいてアラートを出すことはしません。
FireSIGHT ホスト制限	Management Center	このモジュールは、Firepower Management Center がモニタできるホスト数が制限に近づいているかどうかを確認し、モジュールに設定された警告レベルに基づいてアラートを出します。詳細については、Firepower システムのホスト制限, （1449 ページ）を参照してください。

モジュール	適用可能なアプライアンス	説明
ハードウェアアラーム	7000 & 8000 シリーズ	このモジュールは、物理管理対象デバイス上のハードウェアを交換する必要があるかどうかを確認し、ハードウェア ステータスに基づいてアラートを出します。また、ハードウェア関連デーモンのステータスと高可用性展開の 7000 および 8000 シリーズ デバイスのステータスについてレポートします。
ヘルス モニタ プロセス	任意（Any）	このモジュールは、ヘルス モニタ自体のステータスを監視し、Firepower Management Center で受信された最後のステータス イベント以降の分数が警告制限または重大制限を超えた場合にアラートを出します。
インライン リンク不一致アラーム	ASA FirePOWER を除くすべての管理対象デバイス	このモジュールは、インライン セットに関連付けられたポートを監視し、インライン ペアの 2 つのインターフェイスが別々の速度をネゴシエートした場合にアラートを出します。
侵入およびファイル イベント レート	すべての管理対象デバイス	このモジュールは、1 秒あたりの侵入イベント数をこのモジュールに設定された制限と比較し、制限を超えた場合にアラートを出します。侵入およびファイル イベント レートが 0 の場合は、侵入プロセスがダウンしているか、管理対象デバイスがイベントを送信していない可能性があります。イベントがデバイスから送られているかどうかをチェックするには、[分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）] の順に選択します。 一般に、ネットワーク セグメントのイベント レートは平均で 1 秒あたり 20 イベントです。この平均レートのネットワーク セグメントでは、[1 秒あたりのイベント（重大）（Events per second (Critical)）] を 50 に設定し、[1 秒あたりのイベント（警告）（Events per second (Warning)）] を 30 に設定する必要があります。システムの制限を決定するには、デバイスの [統計情報（Statistics）] ページ（[システム（System）] > [モニタリング（Monitoring）] > [統計（Statistics）]）で [イベント/秒（Events/Sec）] 値を探してから、次の式を使用して制限を計算します。 • 1 秒あたりのイベント（重大）= イベント/秒 * 2.5 • 1 秒あたりのイベント（警告）= イベント/秒 * 1.5 両方の制限に設定可能な最大イベント数は 999 であり、重大制限は警告制限より大きくする必要があります。

モジュール	適用可能なアプライアンス	説明
インターフェイス ステータス	任意（Any）	このモジュールは、デバイスが現在トラフィックを収集しているかどうかを確認して、物理インターフェイスおよび集約インターフェイスのトラフィック ステータスに基づいてアラートを出します。物理インターフェイスの情報には、インターフェイス名、リンク ステート、および帯域幅が含まれます。集約インターフェイスの情報には、インターフェイス名、アクティブ リンクの数、および総集約帯域幅が含まれます。 ASA FirePOWER の場合、DataPlaneInterfacex というラベルの付いたインターフェイス（ここで、xは数値）は、内部インターフェイス（ユーザ定義ではない）で、システム内部のパケット フローに関与します。
リンク ステート伝達	NGIPSv と ASA FirePOWER を除くすべて	このモジュールは、ペア化されたインライン セット内のリンクで障害が発生した時点を特定して、リンク ステート伝達モードをトリガーとして使用します。 リンク ステートがペアに伝達した場合は、そのモジュールのステータス分類が [重大（Critical）] に変更され、状態が次のように表示されます。 `Module Link State Propagation: ethx_ethy is Triggered` ここで、`x` と `y` はペア化されたインターフェイス番号です。
ローカルマルウェア分析	任意（Any）	このモジュールは、デバイスがローカル マルウェア分析用に設定され、AMP クラウドからローカルマルウェア分析エンジンのシグネチャの更新をダウンロードできなかった場合、アラートを出します。

モジュール	適用可能なアプライアンス	説明
メモリ使用率	任意（Any）	このモジュールは、アプライアンス上のメモリ使用率をモジュールに設定された制限と比較し、使用率がモジュールに設定されたレベルを超えるとアラートを出します。 メモリが 4 GB を超えるアプライアンスの場合、プリセットされたアラートしきい値は、システム問題を引き起こす可能性のあるメモリ空き容量の割合を求める式に基づいています。4 GB 未満のアプライアンスでは、警告しきい値と重大しきい値の時間間隔が非常に狭いため、[警告しきい値 %（Warning Threshold %）] の値を手動で 50 に設定することを推奨します。これにより、時間内にアプライアンスのメモリ アラートを受け取って問題を解決できる可能性がさらに高まります。 複雑なアクセス コントロール ポリシーやルールは、重要なリソースを消費し、パフォーマンスに悪影響を与える可能性があります。FirePOWER サービス ソフトウェア を含む一部のよりローエンドの ASA デバイスでは、デバイスのメモリ割り当てが最大限に使用されているため、断続的なメモリ使用率の警告が生成されることがあります。
電源モジュール	物理 Management Center、7000 & 8000 シリーズ	このモジュールは、デバイスの電源が交換が必要かどうかを確認し、電源ステータスに基づいてアラートを出します。 （注） 8000 シリーズ 管理対象デバイスで電源障害が発生した場合、アラートを生成するために最大 20 分かかることがあります。
Process Status	任意（Any）	このモジュールは、アプライアンス上のプロセスがプロセス マネージャの外部で停止または終了したかを確認します。プロセスが故意にプロセス マネージャの外部で停止された場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが [警告（Warning）] に変更され、ヘルス イベント メッセージが停止されたプロセスを示します。プロセスがプロセス マネージャの外部で異常終了またはクラッシュした場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが [重大（Critical）] に変更され、ヘルス イベント メッセージが終了したプロセスを示します。
検出の再設定	すべての管理対象デバイス	このモジュールは、デバイスの再設定が失敗した場合、アラートを出します。

モジュール	適用可能なアプライアンス	説明
RRD サーバ プロセス	Management Center	このモジュールは、時系列データを格納するラウンド ロビン サーバが正常に機能しているかどうかを確認します。このモジュールは、RRD サーバが前回の更新以降に再起動した場合にアラートを出します。また、RRDサーバの再起動を伴う連続更新回数がモジュール設定で指定された数値に達した場合に [重大（Critical）] または [警告（Warning）] ステータスに遷移します。
セキュリティインテリジェンス（Security Intelligence）	Management Center	このモジュールは、セキュリティ インテリジェンス フィルタリングに関するさまざまな状況でアラートを出します。このモジュールは、セキュリティインテリジェンスが使用中で次の場合にアラートを出します。 • Firepower Management Center がフィードを更新できないか、フィード データが破損している、または認識可能な IP アドレスが含まれていない。 • 管理対象デバイスが Firepower Management Center から更新されたセキュリティ インテリジェンス データを受信できない。 • 管理対象デバイスが、メモリ問題のために、Firepower Management Center から提供されたすべてのセキュリティ インテリジェンス データをロードできない。 セキュリティ インテリジェンス メモリ警告がヘルス モニタに表示された場合は、影響を受けるデバイスのアクセス コントロール ポリシーを再適用して、セキュリティインテリジェンスに割り当てるメモリを増やすことができます。
時系列データ モニタ	Management Center	このモジュールは、時系列データ（相関イベント カウントなど）が保存されるディレクトリ内の破損ファイルの存在を追跡して、ファイルが破損としてフラグが付けられ、削除された段階でアラートを出します。
時刻同期ステータス	任意（Any）	このモジュールは、NTP を使用して時刻を取得するデバイス クロックと NTP サーバ上のクロックの同期を追跡して、クロックの差が 10 秒を超えた場合にアラートを出します。

モジュール	適用可能なアプライアンス	説明
URL フィルタリング モニタ	Management Center	このモジュールは、Firepower Management Center と管理対象デバイス間の通信、およびシステムがよくアクセスされる URL の脅威インテリジェンスを取得する Cisco Collective Security Intelligence（CSI）との通信を追跡します。Firepower Management Center が Cisco CSI との通信または Cisco CSI からの更新の取得に失敗した場合にアラートを出します。 このモジュールは、Firepower Management Center が管理対象デバイスに URL データをプッシュできない場合にもアラートを出します。
ユーザ エージェント ステータス モニタ	Management Center	このモジュールは、Firepower Management Center に接続されたユーザ エージェントでハートビートが検出されない場合にアラートを出します。
VPN ステータス	Management Center	このモジュールは、Firepower システム デバイス間の 1 つ以上の VPN トンネルがダウンしているときにアラートを出します。

ヘルス モニタリングの設定

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

手順

ステップ 1 ヘルス モジュール, （253 ページ）で説明されているように、モニタするヘルス モジュールを決定します。
Firepower システムで使用しているアプライアンスの種類ごとに固有のポリシーをセットアップして、そのアプライアンスに適切なテストだけを有効にすることができます。

ヒント モニタリング動作をカスタマイズすることなくすぐにヘルス モニタリングを有効にするには、そのために用意されたデフォルト ポリシーを適用できます。

ステップ 2 正常性ポリシーの作成, （260 ページ）で説明されているように、ヘルス ステータスを追跡するアプライアンスごとに正常性ポリシーを適用します。

ステップ 3 （オプション）ヘルス モニタ アラートの作成, （268 ページ）で説明されているように、ヘルス モニタ アラートを設定します。
ヘルス ステータス レベルが特定のヘルス モジュールの特定の重大度レベルに達した段階でトリガーされる電子メール、Syslog、または SNMP アラートをセットアップできます。

正常性ポリシー

正常性ポリシーには、複数のモジュールに対して設定されたヘルス テスト基準が含まれます。アプライアンスごとにどのヘルス モジュールを実行するかを制御したり、モジュールごとに実行するテストで使用される特定の制限を設定したりできます。

正常性ポリシーを設定するときに、そのポリシーに対して各ヘルス モジュールを有効にするかどうかを決定します。また、有効にした各モジュールが、プロセスの正常性を評価するたびに報告するヘルス ステータスを制御するための基準を選択することもできます。

システム内のすべてのアプライアンスに適用可能な 1 つの正常性ポリシーを作成することも、適用を計画している特定のアプライアンス用に正常性ポリシーをカスタマイズすることも、付属のデフォルト正常性ポリシーを使用することもできます。マルチドメイン展開では、先祖ドメインの管理者が子孫ドメインのデバイスに正常性ポリシーを適用できます。子孫ドメインではそのポリシーを使用するか、またはカスタマイズされたローカル ポリシーと置き換えることができます。

デフォルトの正常性ポリシー

Firepower Management Center のヘルス モニタでは、アプライアンスのヘルス モニタリングを迅速に実行できるように、デフォルトの正常性ポリシーが提供されます。デフォルト正常性ポリシーでは、実行中のプラットフォーム上で使用可能なヘルス モジュールのほとんどが自動的に有効になります。デフォルト正常性ポリシーを編集することはできませんが、コピーしてその設定に基づくカスタム ポリシーを作成することができます。デフォルト正常性ポリシーは自動的にFirepower Management Centerに適用されますが、正常性をモニタするすべての管理対象デバイスに適用する必要があります。

正常性ポリシーの作成

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

アプライアンスで使用する正常性ポリシーをカスタマイズすることによって、新しいポリシーを作成できます。ポリシー内の設定は、最初に、新しいポリシーの基準として選択した正常性ポリシー内の設定を使用して生成されます。必要に応じて、ポリシー内のモジュールを有効または無効にし、各モジュールのアラート基準を変更できます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。先祖ドメインの管理者

は、子孫ドメインのデバイスに正常性ポリシーを適用できます。子孫ドメインではこのポリシーを使用することも、カスタマイズしたローカル ポリシーで置き換えることもできます。

手順

ステップ 1 [システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）]を選択します。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 3 [コピー ポリシー（Copy Policy）] ドロップダウン リストから、新しいポリシーの基準として使用する既存のポリシーを選択します。

ステップ 4 ポリシーの名前を入力します。

ステップ 5 ポリシーの説明を入力します。

ステップ 6 [保存（Save）] を選択して、ポリシー情報を保存します。

ステップ 7 使用するモジュールを選択します。

ステップ 8 [有効（Enabled）] オプションに対して [オン（On）] を選択して、ヘルス ステータス テストのモジュールの使用を有効化します。

ステップ 9 該当する場合は、[重大（Critical）] および [警告（Warning）] 基準を設定します。

ステップ 10 モジュールの追加設定を行います。各モジュールで手順 7 ～ 10 を繰り返します。

ステップ 11 次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[正常性ポリシー（Health Policy）]ページに戻るには、[ポリシーを保存して終了（Save Policy and Exit）] をクリックします。
- このモジュールの設定を保存せずに、[正常性ポリシー（Health Policy）]ページに戻るには、[キャンセル（Cancel）] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって[ポリシーを保存して終了（Save Policy and Exit）] をクリックすると、加えたすべての変更が保存されます。[キャンセル（Cancel）] をクリックすると、すべての変更が破棄されます。

次の作業

- 正常性ポリシーの適用, （262 ページ）の説明に従って、各アプライアンスに正常性ポリシーを適用します。これにより変更が適用され、影響を受けるすべてのポリシーのポリシー ステータスが更新されます。

正常性ポリシーの適用

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

正常性ポリシーをアプライアンスに適用すると、ポリシー内で有効にしたすべてのモジュールのヘルス テストが、アプライアンス上のプロセスとハードウェアの正常性を自動的に監視します。その後、ヘルス テストは、ポリシー内で設定された時間間隔で実行を続け、アプライアンスのヘルス データを収集し、そのデータを Firepower Management Centerに転送します。

正常性ポリシーでモジュールを有効にしてから、ヘルス テストが必要ないアプライアンスにポリシーを適用した場合、ヘルスモニタはそのヘルスモジュールのステータスを無効として報告します。

すべてのモジュールが無効になっているポリシーをアプライアンスに適用すると、適用されたすべての正常性ポリシーがアプライアンスから削除されるため、どの正常性ポリシーも適用されません。

すでにポリシーが適用されているアプライアンスに別のポリシーを適用した場合は、新しく適用されたテストに基づく新しいデータの表示が少し遅れる可能性があります。

先祖ドメインの マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。管理者は子孫ドメインのデバイスに正常性ポリシーを適用できます。子孫ドメインはこれを使用でき、またはこれをカスタマイズされたローカル ポリシーと置き換えることができます。

手順

ステップ 1 [システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）]を選択します。

ステップ 2 適用するポリシーの横にある適用アイコン（）をクリックします。

ヒント [正常性ポリシー（Health Policy）] 列の横にあるステータス アイコン（）は、アプライアンスの現在のヘルス ステータスを示します。[システムポリシー（System Policy）] 列の横にあるステータスアイコン（）は、Firepower Management Center とデバイス間の通信ステータスを示します。削除アイコン（）をクリックすることによって、現在適用されているポリシーを削除できることに注意してください。

ステップ 3 正常性ポリシーを適用するアプライアンスを選択します。

ステップ 4 [適用（Apply）] をクリックして、選択したアプライアンスにポリシーを適用します。

次の作業

- 必要に応じて、タスクのステータスをモニタします（タスク メッセージの表示, （303 ページ） を参照）。

  アプライアンスのモニタリングは、ポリシーが正常に適用された直後に開始されます。

正常性ポリシーの編集

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

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。先祖ドメインの管理者は、子孫ドメインのデバイスに正常性ポリシーを適用でき、子孫ドメインはこれを使用するか、またはカスタマイズしたローカル ポリシーに置き換えることができます。

手順

ステップ 1 [システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）]を選択します。

ステップ 2 変更するポリシーの横にある編集アイコン（  ）をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドまたは [ポリシーの説明（Policy Description）] フィールドを必要に応じて編集します。

ステップ 4 変更するヘルス モジュールをクリックします。

ステップ 5 ヘルス モジュール, （253 ページ）の説明に従って、設定を変更します。

ステップ 6 次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[正常性ポリシー（Health Policy）]ページに戻るには、[ポリシーを保存して終了（Save Policy and Exit）] をクリックします。
- このモジュールの設定を保存せずに、[正常性ポリシー（Health Policy）]ページに戻るには、[キャンセル（Cancel）] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって[ポリシーを保存して終了（Save Policy and Exit）] をクリックすると、加えたすべての変更が保存されます。[キャンセル（Cancel）] をクリックすると、すべての変更が破棄されます。

次の作業

- 正常性ポリシーの適用, （262 ページ）の説明に従って、正常性ポリシーを再適用します。これにより変更が適用され、影響を受けるすべてのポリシーのポリシー ステータスが更新されます。

正常性ポリシーの削除

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

不要になった正常性ポリシーを削除できます。アプライアンスに適用されているポリシーを削除した場合は、別のポリシーを適用するまでそのポリシー設定が有効のままになります。加えて、デバイスに適用されている正常性ポリシーを削除した場合、元となる関連アラート応答を無効にするまでは、そのデバイスに対して有効になっているヘルス モニタリング アラートがアクティブなままになります。

マルチドメイン導入では、現在のドメインで作成された正常性ポリシーのみを削除できます。

ヒント　アプライアンスのヘルス モニタリングを停止するには、すべてのモジュールが無効になっている正常性ポリシーを作成し、それをアプライアンスに適用します。

手順

ステップ 1　[システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）]を選択します。

ステップ 2　削除するポリシーの横にある削除アイコン（）をクリックします。
削除が成功したかどうかを示すメッセージが表示されます。

ヘルス モニタ ブラックリスト

通常のネットワーク メンテナンスの一環として、アプライアンスを無効にしたり、一時的に使用不能にしたりすることがあります。このような機能停止は意図したものであり、アプライアンスからのヘルス ステータスに Firepower Management Center 上のサマリー ヘルス ステータスを反映させる必要はありません。

ヘルス モニタ ブラックリスト機能を使用して、アプライアンスまたはモジュールに関するヘルス モニタリング ステータス レポートを無効にすることができます。たとえば、ネットワークのあるセグメントが使用できなくなることがわかっている場合は、そのセグメント上の管理対象デバイ

スのヘルス モニタリングを一時的に無効にして、Firepower Management Center 上のヘルス ステータスにデバイスへの接続がダウンしたことによる警告状態または重大状態が表示されないようにできます。

ヘルス モニタリング ステータスを無効にしても、ヘルス イベントは生成されますが、そのステータスが無効になっているため、ヘルス モニタのヘルス ステータスには影響しません。ブラックリストからアプライアンスまたはモジュールを削除しても、ブラックリストに登録中に生成されたイベントのステータスは [無効（Disabled）] のままです。

アプライアンスからのヘルス イベントを一時的に無効にするには、ブラックリスト設定ページに移動して、アプライアンスをブラックリストに追加します。設定が有効になると、システムは全体のヘルス ステータスを計算するときにブラックリストに登録されているアプライアンスを含めません。[ヘルス モニタ アプライアンス ステータスの概要（Health Monitor Appliance Status Summary）] にはこのアプライアンスが [無効（Disabled）] としてリストされます。

アプライアンス上の個別のヘルス モニタリング モジュールをブラックリストに登録する方が実用的な場合があります。たとえば、Firepower Management Center 上でホスト制限に達した場合、FireSIGHT ホスト制限ステータス メッセージをブラックリストに登録できます。

メインの [ヘルス モニタ（Health Monitor）] ページで、ステータス行内の矢印をクリックして特定のステータスを持つアプライアンスのリストを展開表示すれば、ブラックリストに登録されたアプライアンスを区別できることに注意してください。

ブラックリストに登録されたアプライアンスまたは部分的にブラックリストに登録されたアプライアンスのビューを展開すると、ブラックリスト アイコン（）と注記が表示されます。

（注） Firepower Management Center では、ヘルス モニタのブラックリスト設定はローカル コンフィギュレーション設定です。そのため、Firepower Management Center 上でデバイスをブラックリストに登録してから削除しても、後で再登録すれば、ブラックリスト設定は元どおりになります。新たに再登録したデバイスはブラックリストに登録されたままです。

マルチドメイン導入では、先祖ドメインの管理者が子孫ドメインのアプライアンスやヘルス モジュールをブラックリストに登録できます。ただし、子孫ドメインの管理者は、先祖のコンフィギュレーションをオーバーライドして、自身のドメインのデバイスのブラックリストをクリアすることができます。

アプライアンスのブラックリスト登録

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

アプライアンスは個別に、またはグループ、モデル、関連付けられている正常性ポリシーにより、ブラックリストに登録できます。

ブラックリスト設定が有効になると、[正常性モニタアプライアンスモジュールの概要（Health Monitor Appliance Module Summary）] と [デバイス管理（Device Management）] ページでアプライアンスが [無効（Disabled）] として表示されます。アプライアンスのヘルス イベントのステータスは [無効（Disabled）] です。

個別のアプライアンスのイベントとヘルス ステータスを [無効（Disabled）] に設定する必要がある場合、アプライアンスをブラックリストに登録できます。ブラックリスト設定が有効になると、アプライアンスが [正常性モニタアプライアンスモジュールの概要（Health Monitor Appliance Module Summary）] に [無効（Disabled）] として表示され、アプライアンスのヘルス イベントのステータスが [無効（Disabled）] になります。

マルチドメイン展開では、アプライアンスを先祖ドメインのブラックリストに登録すると、子孫ドメインもすべてブラックリストに登録されたことになります。子孫ドメインは、この設定の継承をオーバーライドし、ブラックリスト指定を解除できます。Firepower Management Center はグローバル レベルでのみブラックリスト指定できます。

手順

ステップ 1 [システム（System）] > [ヘルス（Health）] > [ブラックリスト（Blacklist）]を選択します。

ステップ 2 アプライアンス グループ、モデル、またはポリシーでリストをソートするには、右側にあるドロップダウンリストを使用します。

ヒント [正常性ポリシー（Health Policy）] 列の横にあるステータス アイコン（）は、アプライアンスの現在のヘルス ステータスを示します。[システムポリシー（System Policy）] 列の横にあるステータス アイコン（）は、Firepower Management Center とデバイス間の通信ステータスを示します。

ステップ 3 次の 2 つの選択肢があります。

- グループ、モデル、またはポリシー カテゴリ内のすべてのアプライアンスをブラックリストに登録するには、カテゴリのチェックボックスをオンにしてから、[選択したデバイスをブラックリストに登録（Blacklist Selected Devices）] をクリックします。
- グループ、モデル、またはポリシー カテゴリ内のすべてのアプライアンスをブラックリストから除外するには、カテゴリのチェックボックスをオンにしてから、[選択したデバイスのブラックリスト指定を解除（Clear Blacklist on Selected Devices）] をクリックします。

正常性ポリシー モジュールのブラックリスト登録

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

アプライアンス上の個別の正常性ポリシー モジュールをブラックリストに登録できます。この操作により、モジュールからのイベントによってアプライアンスのステータスが Warning または Critical に変更されないようにすることができます。

ブラックリスト設定が有効になると、アプライアンスが [ブラックリスト（Blacklist）] ページと [アプライアンス正常性モニタモジュールステータスの概要（Appliance Health Monitor Module Status Summary）] で [部分的なブラックリスト指定（Partially Blacklisted）] または [すべてのモジュールがブラックリスト指定（All Modules Blacklisted）] として表示されますが、メインの [アプライアンスのステータスの概要（Appliance Status Summary）] ページでは展開されたビューにだけ表示されます。

ヒント 個別にブラックリストに登録したモジュールを追跡して、必要に応じてそれらを再アクティブ化できるようにしてください。誤ってモジュールを無効にすると、必要な警告または重大メッセージを見逃す可能性があります。

マルチドメイン展開では、先祖ドメインの管理者は子孫ドメインの正常性モジュールをブラックリストに登録できます。しかし、子孫ドメインの管理者は、この先祖の設定をオーバーライドし、ドメインに適用されるポリシーのブラックリスト指定を解除できます。Firepower Management Center 正常性モジュールはグローバル レベルでのみブラックリスト指定できます。

手順

ステップ 1 [システム（System）] > [ヘルス（Health）] > [ブラックリスト（Blacklist）]を選択します。

ステップ 2 変更するアプライアンスの横にある編集アイコン（ ）をクリックします。

ステップ 3 ブラックリスト指定する正常性ポリシーモジュールの横にあるチェックボックスをオンにします。一部のモジュールは特定のデバイスにのみ適用できます。詳細は ヘルス モジュール, （253 ページ）を参照してください。

ステップ 4 [保存（Save）] をクリックします。

ヘルス モニタ アラート

正常性ポリシー内のモジュールのステータスが変更された場合に電子メール、SNMP、またはシステム ログ経由で通知するアラートをセットアップできます。特定のレベルのヘルス イベントが発生したときにトリガーとして使用して警告するヘルス イベント レベルと既存のアラート応答を関連付けることができます。

たとえば、アプライアンスがハード ディスク スペースを使い果たす可能性を懸念している場合は、残りのディスク スペースが警告レベルに達したときに自動的に電子メールをシステム管理者に送信できます。ハード ドライブがさらにいっぱいになる場合、ハード ドライブが重大レベルに達したときに 2 つ目の電子メールを送信できます。

マルチドメイン展開では、現在のドメインで作成されたヘルス モニタのアラートのみを表示、および変更できます。

ヘルス モニタ アラート情報

ヘルス モニタによって生成されるアラートには次の情報が含まれます。

- アラートの重大度レベルを示す [重大度（Severity）]。
- テスト結果がアラートをトリガーとして使用したヘルス モジュールを示す [モジュール（Module）]。
- アラートをトリガーとして使用したヘルス テスト結果を含む [説明（Description）]。

次の表で、これらの重大度レベルについて説明します。

表 *28*：アラートの重大度

重大度（Severity）	説明
クリティカル（Critical）	ヘルス テスト結果がクリティカル アラート ステータスをトリガーとして使用する基準を満たしました。
警告	ヘルス テスト結果が警告アラート ステータスをトリガーとして使用する基準を満たしました。
標準	ヘルス テスト結果が通常のアラート ステータスをトリガーとして使用する基準を満たしました。
エラー（Error）	ヘルス テストが実行されませんでした。
回復済み（Recovered）	ヘルス テスト結果がクリティカルまたは警告のアラート ステータスから通常のアラート ステータスに戻るための基準を満たしました。

ヘルス モニタ アラートの作成

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

ヘルス モニタ アラートを作成するときに、重大度レベル、ヘルス モジュール、およびアラート応答の関連付けを作成します。既存のアラートを使用することも、新しいアラートをシステム へ

ルスの報告専用に設定することもできます。選択したモジュールが重大度レベルに達すると、アラートがトリガーされます。

既存のしきい値と重複するようにしきい値を作成または更新すると、競合が通知されます。重複したしきい値が存在する場合、ヘルス モニタは最も少ないアラートを生成するしきい値を使用し、その他のしきい値を無視します。しきい値のタイムアウト値は、5 ～ 4,294,967,295 分の間にする必要があります。

マルチドメイン導入では、現在のドメインで作成されたヘルスモニタアラートのみを表示および変更できます。

はじめる前に

- ヘルス アラートを送信する SNMP、syslog、電子メール サーバと Firepower Management Center との通信を制御するアラート応答を設定します。Firepower Management Center アラート応答, （1747 ページ）を参照してください。

手順

ステップ 1 [システム（System）] > [ヘルス（Health）] > [モニタ アラート（Monitor Alerts）]を選択します。

ステップ 2 [ヘルス アラート名（Health Alert Name）] フィールドに、ヘルス アラートの名前を入力します。

ステップ 3 [重大度（Severity）] リストから、アラートをトリガーするために使用する重大度レベルを選択します。

ステップ 4 [モジュール（Module）] リストから、アラートを適用する正常性ポリシー モジュールを選択します。

ステップ 5 [アラート（Alert）] リストから、指定した重大度レベルに達したときにトリガーするアラート応答を選択します。

ステップ 6 オプションで、[しきい値タイムアウト（Threshold Timeout）] フィールドに、それぞれのしきい値期間が終了してしきい値がリセットされるまでの分数を入力します。
ポリシーの実行時間間隔の値がしきい値タイムアウトの値より小さい場合でも、特定のモジュールから報告される 2 つのヘルス イベント間の間隔のほうが常に大きくなります。たとえば、しきい値タイムアウトを 8 分に変更し、ポリシーの実行時間間隔が 5 分である場合、報告されるイベント間の間隔は 10 分（5 × 2）になります。

ステップ 7 [保存（Save）] をクリックして、ヘルス アラートを保存します。

ヘルス モニタ アラートの編集

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

既存のヘルス モニタ アラートを編集して、ヘルス モニタ アラートに関連付けられた重大度レベル、ヘルス モジュール、またはアラート応答を変更できます。

マルチドメイン展開では、現在のドメインで作成されたヘルスモニタアラートのみを表示および変更できます。

手順

ステップ 1 [システム（System）] > [ヘルス（Health）] > [モニタ アラート（Monitor Alerts）]を選択します。

ステップ 2 [アクティブ ヘルス アラート（Active Health Alerts）] リストから、変更するアラートを選択します。

ステップ 3 [ロード（Load）] をクリックして、選択したアラートの構成済みの設定をロードします。

ステップ 4 必要に応じて設定を変更します。

ステップ 5 [保存（Save）] をクリックして、変更したヘルス アラートを保存します。
アラート設定が正常に保存されたかどうかを示すメッセージが表示されます。

ヘルス モニタ アラートの削除

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

マルチドメイン導入では、現在のドメインで作成されたヘルスモニタアラートのみを表示および変更できます。

手順

ステップ 1 [システム（System）] > [ヘルス（Health）] > [モニタ アラート（Monitor Alerts）]を選択します。

ステップ 2 削除するアクティブなヘルス アラートを選択してから、[削除（Delete）] をクリックします。

次の作業

- アラートが継続しないようにするには、元になるアラート応答を無効にするか、または削除します。Firepower Management Center アラート応答, （1747 ページ）を参照してください。

ヘルス モニタの使用

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

ヘルス モニタには、Firepower Management Center によって管理されているすべてのデバイスに加えて、Firepower Management Center に関して収集されたヘルス ステータスが表示されます。ヘルス モニタは以下で構成されています。

- ステータス テーブル：この Firepower Management Center の管理対象アプライアンスの台数が全体のヘルス ステータス別に表示されます。
- 円グラフ：それぞれのヘルス ステータス カテゴリにおけるアプライアンスの現在のパーセンテージを示します。
- アプライアンス リスト：管理対象デバイスのヘルス状態の詳細が表示されます。

マルチドメイン展開では、先祖ドメインのヘルス モニタに、すべての子孫ドメインからのデータが表示されます。子孫ドメインには、現在のドメインからのデータのみが表示されます。

手順

ステップ 1 [システム（System）] > [ヘルス（Health）] > [モニタ（Monitor）]を選択します。

ステップ 2 テーブルの [ステータス（Status）] カラム内の該当するステータスまたは円グラフの該当する部分を選択して、そのステータスを持つアプライアンスをリストします。

ヒント ステータス レベルに関する行内の矢印が下向きの場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右向きの場合、アプライアンス リストは非表示です。

ステップ 3 次の選択肢があります。

- アプライアンスのヘルス モニタを表示します（アプライアンス ヘルス モニタの表示, （272 ページ）を参照）。
- ヘルス ポリシーを作成します（正常性ポリシーの作成, （260 ページ）を参照）。
- ヘルス モニタ アラートを作成します（ヘルス モニタ アラートの作成, （268 ページ）を参照）。

ヘルス モニタ ステータスのカテゴリ

使用可能なステータス カテゴリを、重大度別に次の表に示します。

表 *29*：ヘルス ステータス インジケータ

ステータス レベル	ステータス アイコン	円グラフのステータスの色	説明
エラー（Error）		黒色	アプライアンス上の 1 つ以上のヘルス モニタリング モジュールで障害が発生し、それ以降、正常に再実行していないことを示します。テクニカル サポート担当者に連絡して、ヘルス モニタリング モジュールの更新プログラムを入手してください。
クリティカル（Critical）		赤	アプライアンス上の 1 つ以上のヘルス モジュールが重大制限を超え、問題が解決されていないことを示します。
警告		黄色	アプライアンス上の 1 つ以上のヘルス モジュールが警告制限を超え、問題が解決されていないことを示します。
標準		グリーン	アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作していることを示します。
回復済み（Recovered）		グリーン	アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作していることを示します。これには、前にクリティカルまたは警告状態だったモジュールも含まれます。
無効		青	アプライアンスが無効またはブラックリストに登録されている、アプライアンスに正常性ポリシーが適用されていない、またはアプライアンスが現在到達不能になっていることを示します。

アプライアンス ヘルス モニタの表示

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

アプライアンス ヘルス モニタは、アプライアンスのヘルス ステータスの詳細ビューを提供します。

マルチドメイン展開では、子孫ドメインのアプライアンスのヘルス ステータスを表示できます。

ヒント 通常は、非活動状態が1時間（または設定された他の時間間隔）続くと、ユーザはセッションからログアウトされます。ヘルス ステータスを長期間受動的に監視する予定の場合は、一部のユーザのセッション タイムアウトの免除、またはシステム タイムアウト設定の変更を検討してください。詳細については、ユーザ アカウント ログイン オプション，（81 ページ）とセッション タイムアウトの設定，（609 ページ）を参照してください。

手順

ステップ 1 [システム（System）] > [ヘルス（Health）] > [モニタ（Monitor）]を選択します。

ステップ 2 アプライアンス リストを展開します。特定のステータスを持つアプライアンスを表示するには、そのステータス行内の矢印をクリックします。または、[アプライアンス ステータスの概要（Appliance Status Summary）] グラフで、表示するアプライアンス ステータス カテゴリの色をクリックします。

ヒント ステータス レベルに関する行内の矢印が下向きの場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右向きの場合、アプライアンス リストは非表示です。

ステップ 3 アプライアンス リストの[アプライアンス（Appliance）]列で、詳細を表示するアプライアンスの名前をクリックします。

ステップ 4 オプションで、[モジュール ステータスの概要（Module Status Summary）] グラフで、表示するイベント ステータス カテゴリの色をクリックします。
[アラート詳細（Alert Detail）] リストで、表示を切り替えてイベントを表示または非表示にします。

アプライアンスのすべてのモジュールの実行

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

ヘルス モジュール テストは、正常性ポリシーの作成時に設定されたポリシー実行時間間隔で自動的に実行されます。ただし、アプライアンスの最新の正常性情報を収集するためにすべてのヘルス モジュール テストをオンデマンドで実行することもできます。

マルチドメイン展開では、現在のドメイン内のアプライアンスと、子孫ドメイン内のアプライアンスに対してヘルス モジュール テストを実行できます。

手順

ステップ 1 アプライアンスのヘルス モニタを表示します。アプライアンス ヘルス モニタの表示, （272 ページ）を参照してください。

ステップ 2 [すべてのモジュールの実行（Run All Modules）] をクリックします。ステータス バーにテストの進捗状況が表示されてから、[ヘルス モニタ アプライアンス（Health Monitor Appliance）] ページが更新されます。

（注） ヘルス モジュールを手動で実行した場合は、自動的に発生する最初の更新に、手動で実行したテストの結果が反映されないことがあります。手動で直前に実行したモジュールの値が変更されていない場合は、数秒待ってから、デバイス名をクリックしてページを更新してください。ページが自動的に再び更新されるまで待機していてもかまいません。

特定のヘルス モジュールの実行

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

ヘルス モジュール テストは、正常性ポリシーの作成時に設定されたポリシー実行時間間隔で自動的に実行されます。ただし、そのモジュールの最新のヘルス情報を収集するためにヘルス モジュール テストをオンデマンドで実行することもできます。

マルチドメイン展開では、現在のドメイン内のアプライアンスと、子孫ドメイン内のアプライアンスに対してヘルス モジュール テストを実行できます。

手順

ステップ 1 アプライアンスのヘルス モニタを表示します。アプライアンス ヘルス モニタの表示, （272 ページ）を参照してください。

ステップ 2 [モジュール ステータスの概要] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

ステップ 3 イベントのリストを表示するアラートの [アラート詳細（Alert Detail）] 行で、[実行（Run）] をクリックします。
ステータス バーにテストの進捗状況が表示されてから、[ヘルス モニタ アプライアンス（Health Monitor Appliance）] ページが更新されます。

（注） ヘルス モジュールを手動で実行した場合は、自動的に発生する最初の更新に、手動で実行したテストの結果が反映されないことがあります。直前に手動で実行したモジュールの値が変更されていない場合は、数秒待ってから、デバイス名をクリックしてページを更新してください。ページが再び自動的に更新されるまで待機していてもかまいません。

ヘルス モジュール アラート グラフの生成

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

特定のアプライアンスの特定のヘルス テストの一定期間にわたる結果をグラフ化できます。

手順

ステップ 1 アプライアンスのヘルス モニタを表示します（アプライアンス ヘルス モニタの表示, （272 ページ）を参照）。

ステップ 2 [ヘルス モニタ アプライアンス（Health Monitor Appliance）] ページの [モジュール ステータスの概要（Module Status Summary）] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

ステップ 3 イベントのリストを表示するアラートの [アラート詳細（Alert Detail）] 行で、[グラフ（Graph）] をクリックします。

ヒント イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。

トラブルシューティング用のヘルス モニタ レポート

アプライアンスで問題が発生したときに、問題の診断に役立つように、サポートからトラブルシューティング ファイルを生成するように依頼されることがあります。次の表に示すオプションのいずれかを選択して、ヘルス モニタから報告されるトラブルシューティング データをカスタマイズすることができます。

一部のオプションは報告対象のデータの点で重複していますが、トラブルシューティング ファイルには、オプションの選択に関係なく冗長コピーは含まれません。

表 *30* : 選択可能なトラブルシュート オプション

オプション	報告内容
Snort のパフォーマンスと設定（Snort Performance and Configuration）	アプライアンス上の Snort に関連するデータと構成設定
ハードウェア パフォーマンスとログ（Hardware Performance and Logs）	アプライアンス ハードウェアのパフォーマンスに関連するデータとログ
システムの設定、ポリシー、ログ（System Configuration, Policy, and Logs）	アプライアンスの現在のシステム設定に関連する構成設定、データ、およびログ
検知機能の構成、ポリシー、ログ（Detection Configuration, Policy, and Logs）	アプライアンス上の検知機能に関連する構成設定、データ、およびログ
インターフェイスとネットワーク関連データ（Interface and Network Related Data）	アプライアンスのインラインセットとネットワーク設定に関連する構成設定、データ、およびログ
検知、認識、VDB データ、およびログ（Discovery, Awareness, VDB Data, and Logs）	アプライアンス上の現在の検出設定と認識設定に関連する構成設定、データ、およびログ
データおよびログのアップグレード（Upgrade Data and Logs）	アプライアンスの以前のアップグレードに関連するデータおよびログ
全データベースのデータ（All Database Data）	トラブルシュート レポートに含まれるすべてのデータベース関連データ
全ログのデータ（All Log Data）	アプライアンス データベースによって収集されたすべてのログ
ネットワーク マップ情報（Network Map Information）	現在のネットワーク トポロジ データ

アプライアンス トラブルシューティング ファイルの生成

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

カスタマイズしたトラブルシューティング ファイルを生成して、そのファイルをサポートに送信できます。

マルチドメイン展開では、子孫ドメイン内のデバイスに対するトラブルシューティング ファイルを生成できます。

手順

ステップ 1 アプライアンスのヘルス モニタを表示します。アプライアンス ヘルス モニタの表示, （272 ページ）を参照してください。

ステップ 2 [トラブルシューティング ファイルの生成（Generate Troubleshooting Files）] をクリックします。

ステップ 3 [全データ（All Data）] を選択して入手可能なすべてのトラブルシューティング データを生成することも、個別のチェックボックスをオンにしてレポートをカスタマイズすることもできます。

ステップ 4 [OK] をクリックします。

次の作業

- 必要に応じて、タスクのステータスをモニタします（タスク メッセージの表示, （303 ページ） を参照）。
- トラブルシューティング ファイルをダウンロードします。手順については、トラブルシューティング ファイルのダウンロード, （277 ページ）を参照してください。

トラブルシューティング ファイルのダウンロード

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

マルチドメイン導入では、子孫ドメインのデバイス用のトラブルシューティング ファイルをダウンロードできます。

手順

ステップ 1 Message Center でタスク メッセージを表示します。タスク メッセージの表示, （303 ページ）を参照してください。

ステップ 2 生成されたトラブルシューティング ファイルに対応するタスクを探します。

ステップ 3 アプライアンスがトラブルシューティング ファイルを生成し、タスク ステータスが [完了（Completed）] に変ったら、[クリックして生成されたファイルを取得（Click to retrieve generated files）] をクリックします。

ステップ 4 ブラウザのプロンプトに従ってファイルをダウンロードします。

（注） 管理対象デバイスでは、システムはファイル名の前にデバイス名を付加してファイル名を変更します。

ステップ 5 サポートの指示に従って、トラブルシューティング ファイルを Cisco に送信してください。

ヘルス イベント ビュー

[ヘルス イベント ビュー（Health Event View）] ページでは、ヘルス モニタがログに記録したヘルス イベントを、Firepower Management Center ログ ヘルス イベントで表示できます。完全にカスタマイズ可能なイベント ビューを使用すれば、ヘルス モニタによって収集されたヘルス ステータス イベントを迅速かつ容易に分析できます。イベントデータを検索して、調査中のイベントに関係する可能性のある他の情報に簡単にアクセスしたりできます。ヘルス モジュールごとにテストされる条件を理解していれば、ヘルス イベントに対するアラートをより効率的に設定できます。

ヘルス イベント ビュー ページで多くの標準イベント ビュー機能を実行できます。

ヘルス イベントの表示

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

[ヘルス イベントのテーブル ビュー（Table View of Health Events）] ページには、指定したアプライアンス上のすべてのヘルス イベントのリストが表示されます。

Firepower Management Center 上の [ヘルス モニタ（Health Monitor）] ページからヘルス イベントにアクセスした場合は、すべての管理対象アプライアンスのすべてのヘルス イベントが表示されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ヒント このビューをブックマークすれば、イベントの [ヘルス イベント（Health Events）] テーブルを含むヘルス イベント ワークフロー内のページに戻ることができます。ブックマークしたビューには、現在見ている時間範囲内のイベントが表示されますが、必要に応じて時間範囲を変更してテーブルを最新情報で更新することができます。

手順

[システム（System）] > [ヘルス（Health）] > [イベント（Events）]を選択します。

ヒント　ヘルス イベントのテーブル ビューが含まれていないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。[ワークフローの選択（Select Workflow）] ページで、[ヘルス イベント（Health Events）] をクリックします。

（注）　イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。

モジュールとアプライアンス別のヘルス イベントの表示

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

手順

ステップ 1　アプライアンスのヘルス モニタを表示します（アプライアンス ヘルス モニタの表示, （272 ページ）を参照）。

ステップ 2　[モジュール ステータスの概要（Appliance Status Summary）] グラフで、表示するイベント ステータス カテゴリの色をクリックします。
[アラート詳細（Alert Detail）] リストで、表示を切り替えてイベントを表示または非表示にします。

ステップ 3　イベントのリストを表示するアラートの [アラート詳細（Alert Detail）] 行で、[イベント（Events）] をクリックします。
[ヘルス イベント（Health Events）] ページが開いて、制限としてアプライアンスの名前と指定したヘルス アラート モジュールの名前を含むクエリーの結果が表示されます。イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。

ステップ 4　指定したアプライアンスのすべてのステータス イベントを表示する場合は、[検索制約（Search Constraints）] を展開し、[モジュール名（Module Name）] 制限をクリックして削除します。

ヘルス イベント テーブルの表示

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

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [システム（System）] > [ヘルス（Health）] > [イベント（Events）]を選択します。

ステップ 2 次の選択肢があります。

- ブックマーク：すぐに現在のページに戻れるように、現在のページをブックマークするには、[このページのブックマーク（Bookmark This Page）]をクリックしてブックマークの名前を指定し、[保存（Save）] をクリックします。
- ワークフローの変更：別のヘルス イベント ワークフローを選択するには、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。
- イベントの削除：ヘルス イベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして、[削除（Delete）] をクリックします。現在の制約されているビューですべてのイベントを削除するには、[すべて削除（Delete All）] をクリックしてから、すべてのイベントを削除することを確認します。
- レポートの生成：テーブル ビューのデータに基づいてレポートを生成するには、[レポート デザイナ（Report Designer）] をクリックします。
- 変更：ヘルス テーブル ビューに表示されるイベントの時刻と日付範囲を変更します。イベント ビューを時間によって制約している場合は、（グローバルかイベントに固有かに関係なく）アプライアンスに設定されている時間枠の範囲外で生成されたイベントがイベント ビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。
- 移動：イベント ビュー ページを使用して移動します。
- ブックマークの移動：ブックマーク管理ページに移動するには、任意のイベント ビューから [ブックマークの表示（View Bookmarks）] をクリックします。
- その他に移動：他のイベント テーブルに移動して関連イベントを表示します。
- ソート：表示されたイベントをソートする、イベント テーブルに表示するカラムを変更する、または表示するイベントを制約します。
- すべて表示：すべてのイベントのイベントの詳細をビューに表示するには、[すべて表示（View All）] をクリックします。
- 詳細の表示：単一のヘルス イベントに関連付けられる詳細を表示するには、イベントの左側にある下矢印のリンクをクリックします。
- 複数表示：複数のヘルス イベントのイベント詳細を表示するには、詳細を表示するイベントに対応する行の横にあるチェックボックスをオンにして、[表示（View）] をクリックします。

- ステータスの表示：特定のステータスのすべてのイベントを表示するには、そのステータスのイベントの [ステータス（Status）] カラムのステータス アイコンをクリックします。

7000 および 8000 シリーズ デバイスのハードウェア アラートの詳細

（注） 8350 ハードウェア プラットフォームには 6 つのファンがあり、FAN2 ～ FAN7 と表示されています。これは想定されている動作です。8350 プラットフォームで FAN1 またはファンの番号付けに関するハードウェア アラートを受け取った場合は、アラートを無視できます。

表 *31* : *7000* および *8000* シリーズ デバイスの監視対象条件

監視対象条件	黄色または赤色エラー状態の原因
デバイスの高可用性ステータス	高可用性ペアの 7000 または 8000 シリーズ デバイスが相互に通信していない（ケーブル配線の問題などで）場合は、ハードウェア アラーム モジュールが赤色に変化します。
`ftwo` デーモン ステータス	`ftwo` デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
検出された NFE カード	システム上で検出された NFE カードの枚数を示します。この値がアプライアンスの予想NFEカウントと一致しない場合は、ハードウェア アラーム モジュールが赤色に変化します。
NFE ハードウェア ステータス	1 つ以上の NFE カードが通信していない場合は、ハードウェア アラームモジュールが赤色に変化し、該当するカードがメッセージ詳細に表示されます。
NFE ハートビート	システムが NFE ハートビートを検出しなかった場合は、ハードウェア アラーム モジュールが赤色に変化し、メッセージ詳細に関連カードへの参照が追加されます。
NFE 内部リンク ステータス	NMSB カードと NFE カード間のリンクがダウンした場合は、ハードウェア アラーム モジュールが赤色に変化し、メッセージ詳細に関連ポートへの参照が追加されます。

監視対象条件	黄色または赤色エラー状態の原因
NFE メッセージ デーモン	NFE メッセージ デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
NFE 温度	NFE 温度が 97 □を超えると、ハードウェア アラーム モジュールのヘルス ステータスが黄色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。 NFE 温度が 102 □を超えると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。
NFE 温度ステータス	特定の NFE カードの現在の温度ステータスを示します。OK の場合ハードウェア アラーム モジュールは緑色を、警告の場合は黄色を、クリティカルの場合は赤色（および該当する場合はNFE カード番号）を示します。
NFE TCAM デーモン	NFE TCAM デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
nfm_ipfragd（ホスト フラグ）デーモン	nfm_ipfragd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合はNFE カード番号）が追加されます。
NFE プラットフォーム デーモン	NFE プラットフォーム デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合はNFE カード番号）が追加されます。
NMSB コミュニケーション	メディア アセンブリが存在しないか、通信していない場合は、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。
psls デーモン ステータス	psls デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。

監視対象条件	黄色または赤色エラー状態の原因
Rulesd（ホスト ルール）デーモン	Rulesdデーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが黄色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
scmd デーモン ステータス	scmd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。

[ヘルス イベント（Health Events）] テーブル

正常性ポリシー内で有効にされたヘルス モニタ モジュールが、さまざまなテストを実行してアプライアンスのヘルス ステータスを特定します。ヘルス ステータスが指定された基準を満たしている場合は、ヘルス イベントが生成されます。

次の表で、ヘルス イベント テーブルで表示および検索できるフィールドについて説明します。

表 *32*：ヘルス イベント フィールド

フィールド	説明
モジュール名（Module Name）	表示するヘルス イベントを生成したモジュールの名前を指定します。たとえば、CPU パフォーマンスを測定するイベントを表示するには、「CPU」と入力します。検索によって、該当する CPU 使用率イベントと CPU 温度イベントが取得されます。
テスト名（Test Name） （検索専用）	イベントを生成したヘルス モジュールの名前。
時刻（Time） （検索専用）	ヘルス イベントのタイムスタンプ。
説明	イベントを生成したヘルス モジュールの説明。たとえば、プロセスが実行できない場合に生成されるヘルス イベントには「Unable to Execute」というラベルが付けられます。
値	イベントが生成されたヘルス テストから得られた結果の値（単位数）。 たとえば、監視対象デバイスが 80% 以上の CPU リソースを使用しているときに生成されるヘルス イベントを Firepower Management Center が生成した場合の値は 80 ～ 100 です。

フィールド	説明
単位	結果の単位記述子。アスタリスク（*）を使用してワイルドカード検索を作成できます。 たとえば、監視対象デバイスが 80% 以上の CPU リソースを使用しているときに生成されるヘルス イベントを Firepower Management Center が生成した場合の単位記述子はパーセント記号（%）です。
ステータス（Status）	アプライアンスに報告されるステータス（[クリティカル（Critical）]、[黄色（Yellow）]、[緑色（Green）]、または [無効（Disabled）]）。
ドメイン（Domain）	管理対象デバイスによって報告されたヘルス イベントの場合は、ヘルス イベントを報告したデバイスのドメイン。Firepower Management Center によって報告されたヘルス イベントの場合は、`Global`。このフィールドは、マルチドメイン展開の場合にのみ存在します。
Device	ヘルス イベントが報告されたアプライアンス。

第 13 章

システムのモニタリング

以下のトピックでは、Firepower システムをモニタする方法を示します。

- システム統計，285 ページ
- システム メッセージ，297 ページ
- システム メッセージの管理，300 ページ

システム統計

Firepower システム Web インターフェイスの [統計情報（Statistics）] ページには、アプライアンスの現在の一般的ステータスに関する統計情報（ディスク使用量とシステム プロセス）、データ コリレータ統計情報、侵入イベント情報が表示されます。

Firepower Management Center と 7000 & 8000 シリーズ デバイスの両方に関するシステム統計情報を確認できます。

システム統計が使用できるアプライアンス

Web インターフェイスにシステム統計が用意されているアプライアンスは以下の通りです。

統計情報の種類	統計ページのセクション	Management Center	7000 & 8000 シリーズ デバイス
ホスト統計情報	[ホスト統計情報（Host Statistics）] セクション，（286 ページ）	Yes	Yes
システム ステータスとディスク使用量	[ディスク使用量（Disk Usage）] セクション，（287 ページ）	Yes	Yes
システム プロセス ステータス	[プロセス（Processes）] セクション，（287 ページ）	Yes	Yes

統計情報の種類	統計ページのセクション	Management Center	7000 & 8000 シリーズ デバイス
データ コリレータ統計	[SFDataCorrelator プロセス統計情報（SFDataCorrelator Process Statistics）] セクション，（294 ページ）	Yes	No
侵入イベント統計	[侵入イベント情報（Intrusion Event Information）] セクション，（295 ページ）	Yes	No

[ホスト統計情報（Host Statistics）] セクション

次の表に、[統計情報（Statistics）] ページにリストされるホスト統計情報を示します。

表 *33*：ホスト統計情報（*Host Statistics*）

カテゴリ（Category）	説明
時刻（Time）	システムの現在の時刻。
Uptime（アップタイム）	システムが前回起動してから経過した日数（該当する場合）、時間数、および分数。
メモリ使用率（Memory Usage）	使用中のシステム メモリの割合。
負荷平均（Load Average）	直前の 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数。
ディスク使用率（Disk Usage）	使用中のディスクの割合。詳細なホスト統計情報を表示するには、矢印をクリックします。
プロセス（Processes）	システムで実行されているプロセスの概要。

関連トピック

システム統計情報の表示，（296 ページ）

[ディスク使用量（Disk Usage）] セクション

[統計情報（Statistics）] ページの [ディスク使用率（Disk Usage）] セクションは、カテゴリ別およびパーティション ステータス別に、ディスク使用量のクイック概要を示します。マルウェア ストレージパックがデバイスにインストールされている場合、そのパーティション ステータスも確認できます。このページを定期的にモニタして、システム プロセスおよびデータベースで十分なディスク領域が使用可能であることを確認できます。

ヒント　Firepower Management Center で、ヘルス モニタを使用して、ディスク使用状況を監視し、ディスク容量不足の状態をアラートすることもできます。

[プロセス（Processes）] セクション

[統計情報（Statistics）] ページの [プロセス（Processes）] セクションでは、アプライアンスで現在実行中のプロセスを表示できます。これは、一般的なプロセス情報と、実行中の各プロセスに固有の情報を提供します。Firepower Management Center の Web インターフェイスを使用すると、管理対象デバイスのプロセスのステータスを表示できます。

アプライアンスで実行されるプロセスには、デーモンと実行可能ファイルの 2 種類があることに注意してください。デーモンは常に実行され、実行可能ファイルは必要に応じて実行されます。

プロセス使用状況フィールド

統計情報ページのプロセス セクションを展開すると、以下を表示できます。

[CPU（Cpu(s)）]

次の CPU 使用状況情報がリストされます：

- ユーザ プロセスの使用状況の割合
- システム プロセスの使用状況の割合
- nice 使用状況の割合（高い優先度を示す、負の nice 値を持つプロセスの CPU 使用状況）。nice 値は、システム プロセスのスケジュールされた優先度を示しており、-20（最も高い優先度）から 19（最も低い優先度）の範囲の値になります。
- アイドル状態の使用状況の割合

[メモリ（Mem）]

以下のメモリ使用状況情報がリストされます。

- メモリ内の合計キロバイト数
- メモリ内の使用キロバイト数の合計

- メモリ内の空きキロバイト数の合計
- メモリ内のバッファに書き出されたキロバイト数の合計

[切替（Swap）]

以下のスワップ使用状況情報がリストされます。

- スワップ内の合計キロバイト数
- スワップ内の使用キロバイト数の合計
- スワップ内の空きキロバイト数の合計
- スワップ内のキャッシュされたキロバイト数の合計

次の表に、プロセス セクションに表示される各列を示します。

表 *34*：プロセス リスト カラム

カラム（Column）	説明
Pid	プロセス ID 番号
[ユーザ名（Username）]	プロセスを実行しているユーザまたはグループの名前
Pri	プロセスの優先度
Nice	*nice* 値。プロセスのスケジューリング優先度を示す値です。値は -20（最も高い優先度）から 19（最も低い優先度）までの範囲になります。
Size	プロセスで使用されるメモリ サイズ（値の後ろにメガバイトを表す m がない場合はキロバイト単位）
Res	メモリ内の常駐ページング ファイルの量（値の後ろにメガバイトを表す m がない場合はキロバイト単位）

カラム（Column）	説明
State	プロセスの状態： • D：プロセスが中断不能スリープ状態（通常は入出力）にある • N：プロセスの nice 値が正の値 • R：プロセスが実行可能である（実行するキュー上で） • S：プロセスがスリープ モードにある • T：プロセスがトレースまたは停止されている • W：プロセスがページングしている • X：プロセスがデッド状態である • Z：プロセスが機能していない • <：プロセスの nice 値が負の値
時刻（Time）	プロセスが実行されてきた時間の長さ（時間数:分数:秒数）
Cpu	プロセスが使用している CPU の割合
コマンド（Command）	プロセスの実行可能ファイル名

関連トピック

システム デーモン，（289 ページ）
実行可能ファイルおよびシステム ユーティリティ，（291 ページ）

システム デーモン

デーモンは、アプライアンスで継続的に実行されます。これにより、サービスが使用可能になり、必要に応じてプロセスが生成されるようになります。次の表では、[プロセスのステータス（Process Status）] ページに表示されるデーモンをリストし、その機能について簡単に説明しています。

（注） 次の表は、アプライアンスで実行される可能性があるすべてのプロセスの包括的なリストではありません。

表 *35*：システム デーモン

デーモン	説明
crond	スケジュールされたコマンド（cron ジョブ）の実行を管理します
dhclient	ダイナミック ホスト IP アドレッシングを管理します
fpcollect	クライアントとサーバのフィンガープリントの収集を管理します
httpd	HTTP（Apache Web サーバ）プロセスを管理します
httpsd	HTTPS（SSL を使用した Apache Web サーバ）サービスを管理し、SSL および有効な証明書の認証が機能しているかチェックし、アプライアンスへの安全な Web アクセスを提供するためにバックグラウンドで実行します
keventd	Linux カーネルのイベント通知メッセージを管理します
klogd	Linux カーネル メッセージのインターセプションおよびロギングを管理します
kswapd	Linux カーネルのスワップ メモリを管理します
kupdated	ディスクの同期を実行する、Linux カーネルの更新プロセスを管理します
mysqld	データベース プロセスを管理します
ntpd	Network Time Protocol（NTP）プロセスを管理します
午後	すべての Firepower システム プロセスを管理し、必要なプロセスを始動し、予期せずに失敗したプロセスをすべて再始動します
reportd	レポートを管理します
safe_mysqld	データベースのセーフ モード運用を管理し、エラーが発生した場合にはデータベース デーモンを再始動し、ランタイム情報をファイルに記録します
SFDataCorrelator	データ転送を管理します
sfestreamer（Management Center のみ）	Event Streamer を使用するサードパーティ製クライアント アプリケーションへの接続を管理します
sfmgr	アプライアンスへの sftunnel 接続を使用して、リモートでアプライアンスを管理および設定するための RPC サービスを提供します

デーモン	説明
SFRemediateD（Management Center のみ）	修復応答を管理します
sftimeserviced（Management Center のみ）	時間同期メッセージを管理対象デバイスに転送します
sfmbservice	アプライアンスへの sftunnel 接続を使用して、リモートアプライアンスで実行されている sfmb メッセージブローカ プロセスへのアクセスを提供します。現在、ヘルス モニタリングでのみ使用されており、管理対象デバイスから Firepower Management Center へ正常なイベントやアラートを送信します。
sftroughd	着信ソケットで接続をリッスンしてから、正しい実行可能ファイル（通常は、Cisco メッセージ ブローカ sfmb）を呼び出して要求を処理します
sftunnel	リモートアプライアンスとの通信を必要とするすべてのプロセスに対し、安全な通信チャネルを提供します。
sshd	セキュア シェル（SSH）プロセスを管理し、アプライアンスへの SSH アクセスを提供するためにバックグラウンドで実行します
syslogd	システム ロギング（syslog）プロセスを管理します

実行可能ファイルおよびシステム ユーティリティ

システム上には、他のプロセスまたはユーザ操作によって実行される実行可能ファイルが数多く存在します。次の表に、[プロセス ステータス（Process Status）]ページで表示される実行可能ファイルについて説明します。

表 *36*：システムの実行可能ファイルおよびユーティリティ

実行可能ファイル	説明
awk	`awk` プログラミング言語で作成されたプログラムを実行するユーティリティ
bash	GNU Bourne-Again シェル
cat	ファイルを読み取り、コンテンツを標準出力に書き込むユーティリティ
chown	ユーザおよびグループのファイル権限を変更するユーティリティ

実行可能ファイル	説明
chsh	デフォルトのログイン シェルを変更するユーティリティ
SFDataCorrelator（Management Center のみ）	システムで作成されるバイナリ ファイルを分析し、イベント、接続データ、およびネットワーク マップを生成します。
cp	ファイルをコピーするユーティリティ
df	アプライアンスの空き領域の量をリストするユーティリティ
エコー	コンテンツを標準出力に書き込むユーティリティ
egrep	指定された入力を、ファイルおよびフォルダで検索するユーティリティ。標準 grep でサポートされていない正規表現の拡張セットをサポートします
検索	指定された入力のディレクトリを再帰的に検索するユーティリティ
grep	指定された入力をファイルとディレクトリで検索するユーティリティ
halt	サーバを停止するユーティリティ
httpsdctl	セキュアな Apache Web プロセスを処理する
hwclock	ハードウェア クロックへのアクセスを許可するユーティリティ
ifconfig	ネットワーク構成実行可能ファイルを示します。MACアドレスが常に一定になるようにします
iptables	[アクセス権の設定（Access Configuration）]ページに加えられた変更に基づいてアクセス制限を処理します。
iptables-restore	iptables ファイルの復元を処理します
iptables-save	iptables に対する保存済みの変更を処理します
kill	セッションおよびプロセスを終了するために使用できるユーティリティ
killall	すべてのセッションおよびプロセスを終了するために使用できるユーティリティ
ksh	Korn シェルのパブリック ドメイン バージョン
ロガー	コマンドラインからsyslogデーモンにアクセスする方法を提供するユーティリティ

実行可能ファイル	説明
md5sum	指定したファイルのチェックサムとブロック数を印刷するユーティリティ
mv	ファイルを移動（名前変更）するユーティリティ
myisamchk	データベース テーブルの検査および修復を示します
mysql	データベース プロセスを示します。複数のインスタンスが表示されることがあります
openssl	認証証明書の作成を示します
perl	perl プロセスを示します
ps	標準出力にプロセス情報を書き込むユーティリティ
sed	1 つ以上のテキスト ファイルの編集に使用されるユーティリティ
sfheartbeat	アプライアンスがアクティブであることを示す、ハートビート ブロードキャストを識別します。ハートビートはデバイスと Firepower Management Center の間の接続を維持するのに使用されます
sfmb	メッセージ ブローカ プロセスを示します。Firepower Management Center とデバイスとの間の通信を処理します。
sh	Korn シェルのパブリック ドメイン バージョン
shutdown	アプライアンスをシャットダウンするユーティリティ
sleep	指定された秒数のあいだプロセスを中断するユーティリティ
smtpclient	電子メール イベント通知機能が有効な場合に、電子メール送信を処理するメール クライアント
snmptrap	SNMP 通知機能が有効な場合に、指定された SNMP トラップ サーバに SNMP トラップ データを転送します
snort	Snort が動作していることを示します
ssh	アプライアンスへのセキュア シェル（SSH）接続を示します
sudo	sudo プロセスを示します。これにより、admin 以外のユーザが実行可能ファイルを実行できるようになります
top	上位の CPU プロセスに関する情報を表示するユーティリティ

実行可能ファイル	説明
touch	指定したファイルへのアクセス時刻や変更時刻を変更するために使用できるユーティリティ
vim	テキスト ファイルの編集に使用されるユーティリティ
wc	指定したファイルの行、ワード、バイトのカウントを実行するユーティリティ

関連トピック

システムのアクセス リストの設定, （590 ページ）

[SFDataCorrelator プロセス統計情報（SFDataCorrelator Process Statistics）] セクション

Firepower Management Center では、現在の日付のデータ コリレータとネットワーク検出プロセスに関する統計情報を表示できます。管理対象デバイスがデータの取得、復号化、および分析を実行する際に、ネットワーク検出プロセスはデータをフィンガープリントおよび脆弱性データベースと関連付けてから、Firepower Management Center で実行中のデータ コリレータで処理されるバイナリ ファイルを生成します。データ コリレータはバイナリ ファイルの情報を分析し、イベントを生成し、ネットワーク マップを作成します。

ネットワーク検出とデータ コリレータに表示される統計情報は、デバイスごとに 0:00 から 23:59 までの間に収集された統計情報を使用した、当日の平均です。

次の表に、データ コリレータ プロセスに表示される統計情報を示します。

表 *37*：データ コリレータ プロセスの統計情報

カテゴリ（**Category**）	説明
イベント/秒（Events/Sec）	データ コリレータが受信し処理する検出イベントの 1 秒当たりの数
接続/秒（Connections/Sec）	データ コリレータが受信し処理する接続の 1 秒当たりの数
CPU 使用率 — ユーザ（%）（CPU Usage — User (%)）	当日のユーザ プロセスで使用される CPU 時間の平均割合
CPU 使用率 — システム（%）（CPU Usage — System (%)）	当日のシステム プロセスで使用される CPU 時間の平均割合

カテゴリ（**Category**）	説明
VmSize（KB）	当日のデータ コリレータに割り当てられたメモリの平均サイズ（キロバイト単位）
VmRSS（KB）	当日のデータ コリレータで使用されるメモリの平均量（キロバイト単位）

[侵入イベント情報（Intrusion Event Information）] セクション

Firepower Management Center デバイスと管理対象デバイスのどちらでも、[統計情報（Statistics）] ページで、侵入イベントに関するサマリ情報を確認できます。表示される情報には、前回の侵入イベントの日時、過去 1 時間および過去 1 日に発生したイベントの合計数、データベース内のイベントの合計数などがあります。

（注） [統計情報（Statistics）] ページの [侵入イベント情報（Intrusion Event Information）] セクションにある情報は、Firepower Management Center に送信された侵入イベントではなく、管理対象デバイスに保存されている侵入イベントに基づいています。管理対象デバイスが侵入イベントをローカルに格納できない（または格納しないように設定されている）場合、侵入イベント情報はこのページに表示されません。

次の表に、[統計情報（Statistics）] ページの [侵入イベント情報（Intrusion Event Information）] セクションに表示される統計情報を示します。

表 *38*：侵入イベント情報（*Intrusion Event Information*）

統計	説明
前回のアラート（Last Alert Was）	前回のイベントが発生した日時
過去 1 時間のイベントの合計（Total Events Last Hour）	過去 1 時間に発生したイベントの合計数
過去 1 日のイベントの合計（Total Events Last Day）	過去 24 時間に発生したイベントの合計数
データベース内のイベントの合計（Total Events in Database）	イベント データベース内のイベントの合計数

システム統計情報の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any） 脅威（侵入イベント データ用）	任意（Any） 保護（侵入イベント データ用）	任意（Any）	グローバルだけ	Admin/Maint

Firepower Management Center では、Web インターフェイスはアプライアンスとその管理対象となるすべてのデバイスの統計情報を表示します。7000 および 8000 シリーズ デバイスでは、システムはそのデバイスの統計情報のみを表示します。

手順

ステップ 1 [システム（System）] > [モニタリング（Monitoring）] > [統計（Statistics）]を選択します。

ステップ 2 必要に応じ、Firepower Management Center で、[デバイスの選択（Select Device(s)）] リストからデバイスを選択し、[デバイスの選択（Select Devices）] をクリックします。

ステップ 3 使用可能な統計を表示します（システム統計が使用できるアプライアンス, （285 ページ）を参照）。

ステップ 4 オプションで、[ディスク使用率（Disk Usage）] セクションで以下を実行できます。

- [カテゴリ別（By Category）] 積み上げ横棒で、ディスク使用量カテゴリの上にポインタを移動すると、以下が（順番に）表示されます。
  - そのカテゴリが使用する使用可能なディスク領域の割合
  - ディスク上の実際のストレージ領域
  - そのカテゴリで使用可能なディスク領域の合計
- [パーティション別（By Partion）]の横にある下矢印をクリックして展開します。マルウェア ストレージパックがインストールされている場合は、`/var/storage`パーティションの使用状況が表示されます。

ステップ 5 オプションで、[プロセス（Processes）] の横にある矢印をクリックすると、プロセス使用状況フィールド, （287 ページ）で説明されている情報が表示されます。

システム メッセージ

Firepower システムで発生した問題を突き止める必要がある場合、調査の出発点となるのはメッセージセンターです。メッセージセンターでは、Firepower システムがシステムのアクティビティとステータスに関して継続的に生成するメッセージを表示できます。

メッセージ センターを開くには、メイン メニューの [展開（Deploy）] ボタンの右隣にある [システム ステータス（System Status）] アイコンをクリックします。このアイコンは、システムのステータスによって以下のように表示されます。

- ：1 つ以上のエラーと任意の数の警告がシステム上に存在することを示します。
- ：1 つ以上の警告がシステム上に存在することを示します。エラーは発生していません。
- ：警告とエラーはいずれもシステム上に存在していないことを示します。

アイコンに数字が表示されている場合、その数字は現在のエラー メッセージまたは警告メッセージの数を示します。

メッセージ センターを閉じるには、Firepower システム Web インターフェイス内でメッセージ センターの外側をクリックします。

メッセージ センターに加え、Web インターフェイスには、ユーザのアクティビティおよび進行中のシステム アクティビティに応じて即時にポップアップ通知が表示されます。ポップアップ通知のなかには 5 秒経過すると自動的に非表示になるものや、非表示アイコン（×）をクリックして明示的に表示を消さなければならない「スティッキー」通知もあります。通知リストの最上部にある [表示を消す（Dismiss）] リンクをクリックすると、すべての通知をまとめて非表示にすることができます。

ヒント スティッキー以外のポップアップ通知の上にマウスのカーソルを合わせると、その通知はスティッキーになります。

システムはユーザのライセンス、ドメイン、アクセス ロールに基づいて、どのメッセージをポップアップ通知やメッセージ センターに表示するか決定します。

メッセージ タイプ

Message Center では、システムのアクティビティとステータスをレポートするメッセージが 3 つのタブに編成されて表示されます。

展開（Deployments）

このタブには、システムの各アプライアンスの設定展開に関連する現在のステータスがドメイン別にグループ化されて表示されます。Firepower システムでは、次の展開ステータス値がこのタブでレポートされます。

- [実行中（Running）]（ の表示が回転中）：設定は展開の処理中です。
- [成功（Success）]（）：設定は正常に展開されました。
- [警告（Warning）]（）：警告展開ステータスは、警告システム ステータス アイコン（）とともに表示されるメッセージ数に含まれます。
- [失敗（Failure）]（）：設定は展開に失敗しました。失効ポリシー，（334 ページ）を参照してください。失敗した展開は、エラー システム ステータス アイコン（）とともに表示されるメッセージ数に含まれます。

ヘルス（Health）

このタブには、システムの各アプライアンスの現在のヘルス ステータス情報がドメイン別にグループ化されて表示されます。ヘルス ステータスは、ヘルス モニタリングについて，（251 ページ）に記載されているように、ヘルス モジュールによって生成されます。Firepower システムでは、次のヘルス ステータス値がこのタブでレポートされます。

- [警告（Warning）]（）：アプライアンス上のヘルス モジュールが警告制限を超え、問題が解決されていないことを示します。[ヘルス モニタリング（Health Monitoring）] ページには、これらの状態が黄色い三角形のアイコン（）で示されます。警告ステータスは、警告システム ステータス アイコン（）とともに表示されるメッセージ数に含まれます。
- [重大（Critical）]（）：アプライアンス上のヘルス モジュールが重大制限を超え、問題が解決されていないことを示します。[ヘルス モニタリング（Health Monitoring）] ページには、これらの状態が アイコンで示されます。重大ステータスは、エラー システム ステータス アイコン（）とともに表示されるメッセージ数に含まれます。
- [エラー（Error）]（）：アプライアンス上のヘルス モニタリング モジュールに障害が発生し、それ以降、正常に再実行されていないことを示します。[ヘルス モニタリング（Health Monitoring）] ページには、これらの状態が アイコンで示されます。エラー ステータスは、エラー システム ステータス アイコン（）とともに表示されるメッセージ数に含まれます。

[ヘルス（Health）] タブのリンクをクリックして、[ヘルス モニタリング（Health Monitoring）] ページで関連の詳細情報を表示できます。現在のヘルス ステータス状態がない場合、[ヘルス（Health）] タブにメッセージは表示されません。

タスク

Firepowerシステムでは、完了するまで時間がかかる可能性がある特定のタスク（構成のバックアップやインストールの更新など）を実行できます。このタブには、これらの長時間実行タスクのステータスが表示され、自分が開始したタスクや、適切なアクセス権がある場合は、システムの他のユーザが開始したタスクが含まれることがあります。このタブには、各メッセージの最新の更新時間に基づいて時系列の逆順にメッセージが表示されます。一部のタスク ステータス メッセージには、問題となっているタスクについての詳細情報へのリンクが含まれています。Firepower システムでは、次のタスク ステータス値がこのタブでレポートされます。

- [待機中（Waiting）]（）：別の進行中のタスクが完了するまで実行を待機しているタスクを示します。このメッセージ タイプでは、更新の経過表示バーが表示されます。
- [実行中（Running）]（の表示が回転中）：進行中のタスクを示します。このメッセージ タイプでは、更新の経過表示バーが表示されます。
- [再試行中（Retrying）]（）：自動的に再試行しているタスクを示します。なお、すべてのタスクの再試行が許可されるわけではありません。このメッセージタイプでは、更新の経過表示バーが表示されます。
- [成功（Success）]（）：正常に完了したタスクを示します。
- [失敗（Failure）]（）：正常に完了しなかったタスクを示します。失敗したタスクは、エラー システム ステータス アイコン（）とともに表示されるメッセージ数に含まれます。
- [停止（Stopped）]（）：システム アップデートのために中断されたタスクを示します。停止したタスクを再開することはできません。

新しいタスクが開始されると、新しいメッセージがこのタブに表示されます。タスクが完了すると（成功、失敗、または停止のステータス）、タスクを削除するまで、このタブには最終ステータスを示すメッセージが引き続き表示されます。[タスク（Tasks）]タブおよびメッセージ データベースがいっぱいにならないように、メッセージを削除することをお勧めします。

メッセージ管理

メッセージ センターから、以下を実行できます。

- ポップアップ通知の動作を設定します（これらを表示するかどうかを選択します）。
- システム データベースの追加のタスクのステータス メッセージを表示します（削除されていないもので利用可能なものがある場合）。
- 個々のタスクのステータス メッセージを削除します。（これは、削除されたメッセージを確認できるすべてのユーザに影響します）。

- タスクのステータス メッセージを一括で削除します。（これは、削除されたメッセージを確認できるすべてのユーザに影響します）。

ヒント　シスコは、表示に加えてデータベースの不要なデータを削除するために、累積されたタスクのステータス メッセージを[タスク（Task）]タブから定期的に削除することを推奨します。データベースのメッセージ数が100,000に到達すると、削除したタスクのステータス メッセージが自動的に削除されます。

システム メッセージの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	展開（Deployment）：管理者/[設定をデバイスに展開する（Deploy Configuration to Devices）] 権限を持つカスタム ユーザ ロール [ヘルス（Health）]：管理者/[ヘルス（Health）] 権限を持つカスタム ユーザ ロール 他人によって開始されたタスク：管理者/[他のユーザのタスクを確認する（View Other Users' Tasks）] 権限があるカスタム ユーザ ロール 自分が開始したタスク：任意

手順

ステップ 1 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 2 次の選択肢があります。

- [展開（Deployments）] タブをクリックして、設定の展開に関連するメッセージを表示します。展開メッセージの表示, （301 ページ）を参照してください。
- [ヘルス（Health）] タブをクリックして、Firepower Management Center とそれに登録したデバイスの状況に関連するメッセージを表示します。ヘルス メッセージの表示, （302 ページ）を参照してください。
- [タスク（Tasks）] タブをクリックして、長時間実行タスクに関連するメッセージを表示または管理します。タスク メッセージの表示, （303 ページ）またはタスク メッセージの管理, （304 ページ）を参照してください。
- Message Center の右上隅にある歯車アイコン（  ）をクリックして、ポップアップ通知の動作を設定します。通知動作の設定, （305 ページ）を参照してください。

展開メッセージの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	[設定をデバイスに展開する（Deploy Configuration to Devices）] 権限を持つ管理者/ユーザ ロール

手順

ステップ 1 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 2 [展開（Deployments）] タブをクリックします。

ステップ 3 次の選択肢があります。

- 現在のすべての展開ステータスを表示するには、[合計（total）] をクリックします。
- 任意の展開ステータスに関するメッセージのみを表示するには、そのステータスの値をクリックします。
- 展開の経過時間、開始時刻および停止時刻を表示するには、メッセージの時間経過インジケータ（たとえば、[1分5秒（1m 5s）]）の上にカーソルを置きます。

関連トピック

設定変更の導入, （320 ページ）

ヘルス メッセージの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	[ヘルス（Health）] の権限を持つ管理者/ユーザ ロール

手順

ステップ 1 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 2 [ヘルス（Health）] タブをクリックします。

ステップ 3 次の選択肢があります。

- 現在のすべてのヘルス ステータスを表示するには、[合計（total）] をクリックします。
- 任意のステータスに関するメッセージのみを表示するには、そのステータスの値をクリックします。
- メッセージが最も最近更新された時刻を表示するには、そのメッセージの相対時間インジケータ（たとえば [3 日前（3 day(s) ago）]）の上にカーソルを置きます。
- 特定のメッセージの詳細なヘルス ステータス情報を表示するには、メッセージをクリックします。
- [ヘルス モニタリング（Health Monitoring）] ページの完全なヘルス ステータスを表示するには、タブの下部にある [ヘルス モニタ（Health Monitor）] をクリックします。

関連トピック

ヘルス モニタリングについて，（251 ページ）

タスク メッセージの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	他人によって開始されたタスク：[他のユーザのタスクを確認する（View Other Users' Tasks）] 権限がある管理/カスタム ユーザ ロール 自分が開始したタスク：任意

手順

ステップ 1 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 2 [タスク（Tasks）] タブをクリックします。

ステップ 3 次の選択肢があります。

- 現在のすべてのタスクのステータスを表示するには、[合計（total）] をクリックします。
- 任意のステータスのタスクに関するメッセージのみを表示するには、そのステータスの値をクリックします。

  （注） 停止したタスクのメッセージは、タスクのステータス メッセージの合計リストにのみ表示されます。停止したタスクではフィルタリングできません。

- メッセージが最も最近更新された時刻を表示するには、そのメッセージの相対時間インジケータ（たとえば [3 日前（3 day(s) ago）]）の上にカーソルを置きます。
- タスクに関する詳細を表示するには、メッセージ内のリンクをクリックします。

- さらにタスクのステータス メッセージが表示可能な場合は、メッセージ リストの下部にある [さらにメッセージを取得する（Fetch more messages）] をクリックして取得します。

タスク メッセージの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	他人によって開始されたタスク：[他のユーザのタスクを確認する（View Other Users' Tasks）] 権限がある管理/カスタム ユーザ ロール 自分が開始したタスク：任意

手順

ステップ 1 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 2 [タスク（Tasks）] タブをクリックします。

ステップ 3 次の選択肢があります。

- さらにタスクのステータス メッセージが表示可能な場合は、メッセージ リストの下部にある [さらにメッセージを取得する（Fetch more messages）] をクリックして取得します。
- 完了したタスク（ステータスが停止、成功、または失敗のタスク）に関する 1 つのメッセージを削除するには、メッセージの横にある削除アイコン（✖）をクリックします。
- すべての完了しているタスク（ステータスが停止、成功、または失敗のタスク）に関するメッセージをすべて削除するには、[総数（total）] でメッセージをフィルタリングして、[すべての完了タスクの削除（Remove all completed tasks）] をクリックします。
- すべての正常に完了したタスクに関するメッセージをすべて削除するには、[成功（success）] でメッセージをフィルタリングして、[すべての成功タスクの削除（Remove all successful tasks）] をクリックします。

- すべての失敗したタスクに関するメッセージをすべて削除するには、[失敗（failure）] でメッセージをフィルタリングして、[すべての失敗タスクの削除（Remove all failed tasks）] をクリックします。

通知動作の設定

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

（注） この設定は、すべてのポップアップ通知に影響を及ぼし、ログイン セッション間で保持されます。

手順

ステップ 1 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 2 メッセージ センターの右上にある歯車アイコン（⚙）をクリックします。

ステップ 3 ポップアップ通知の表示を有効または無効にするには、[通知を表示（Show notifications）] スライダをクリックします。

ステップ 4 スライダを非表示にするには、歯車アイコン（⚙）を再度クリックします。

ステップ 5 [システム ステータス（System Status）] アイコンを再度クリックして、メッセージ センターを閉じます。

第 IV 部

導入管理

第 14 章

ドメイン管理

次のトピックでは、ドメインを使用してマルチテナンシーを管理する方法について説明します。

ドメインを使用したマルチテナンシーの概要

Firepower システムでは、ドメインを使用したマルチテナンシーを実装できます。ドメインは、管理対象デバイス、構成、およびイベントへのユーザ アクセスをセグメント化します。最上位の [グローバル（Global）] ドメインの下に、2 つまたは 3 つのレベルで最大 50 個のサブドメインを作成できます。

Firepower Management Center にログインすると、現在のドメインと呼ばれる単一ドメインにログインします。ユーザ アカウントによっては、他のドメインに切り替えることができる場合があります。

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

その他のタスクは、サブドメインがないドメインであるリーフ ドメインに制限されます。たとえば、各管理対象デバイスをリーフ ドメインと関連付け、そのリーフ ドメインのコンテキストからデバイス管理タスクを実行する必要があります。

ヒント このガイドの各タスク トピックには、タスクを実行できるドメイン レベルを示すサポートされるドメイン数という値があります。

各リーフ ドメインは、そのリーフ ドメインのデバイスで集められた検出データに基づいて独自のネットワーク マップを作成します。管理対象デバイスによって報告されたイベント（接続、侵入、マルウェアなど）もデバイスのリーフ ドメインに関連付けられます。

1 ドメイン レベル：グローバル

マルチテナンシーを設定しない場合、すべてのデバイス、構成、およびイベントはグローバル ドメインに属します。グローバル ドメインは、このシナリオの場合はリーフ ドメインでもあります。ドメイン管理を除き、サブドメインを追加するまでは、ドメイン固有の構成および分析オプションは非表示になります。

2 ドメイン レベル：グローバル、セカンドレベル

2 レベルのマルチドメイン展開では、グローバル ドメインには直接の子孫ドメインのみがあります。たとえば、マネージド セキュリティ サービス プロバイダー（MSSP）は、1 つの Firepower Management Center を使用して複数の顧客のネットワーク セキュリティを管理できます。

- MSSP の管理者は、グローバル ドメインにログインして、すべての顧客の展開を管理できます。
- 各顧客の管理者は、サブドメインと呼ばれるセカンドレベルにログインして、その組織に適用されるデバイス、構成、およびイベントのみを管理できます。これらのローカル管理者は、MSSP の他の顧客の展開を表示したり、その環境に影響を与えることはできません。

3 ドメイン レベル：グローバル、セカンドレベル、サードレベル

3 レベルのマルチドメイン展開では、グローバル ドメインにはサブドメインがあり、そのうち少なくとも 1 つに独自のサブドメインがあります。前の例を拡張するには、MSSP 顧客（すでにサブドメインに制限されている）がその展開をさらにセグメント化しようとしているシナリオを考えてみます。この顧客は、2 つのクラスのデバイス（ネットワーク エッジに配置されているデバイスと内部に配置されているデバイス）を個別に管理しようとしています。

- 顧客の管理者はセカンドレベルのサブドメインにログインして、顧客の展開全体を管理できます。
- 顧客のエッジ ネットワークの管理者は、サードレベル（リーフ）ドメインにログインして、ネットワーク エッジに展開されているデバイスに適用されるデバイス、構成、およびイベントのみを管理できます。同様に、顧客の内部ネットワークの管理者は、別のサードレベル ドメインにログインして、内部のデバイス、構成、およびイベントを管理できます。エッジと内部の管理者は、互いの展開を表示できません。

ドメインの用語

このマニュアルでは、ドメインおよびマルチドメイン展開を説明する際に次の用語を使用します。

グローバル ドメイン

マルチドメイン展開でのトップレベル ドメイン。マルチテナンシーを設定しない場合、すべてのデバイス、設定、およびイベントはグローバル ドメインに属します。グローバル ドメインの Administrators は、Firepower システム全体の導入を管理できます。

サブドメイン

第 2 または第 3 レベルのドメイン。

第 2 レベル ドメイン

グローバル ドメインの子。第 2 レベル ドメインは、リーフ ドメインにするか、サブドメインを持つことができます。

第 3 レベル ドメイン

第 2 レベル ドメインの子。第 3 レベル ドメインは常にリーフ ドメインです。

リーフ ドメイン

サブドメインを持たないドメイン。各デバイスはリーフ ドメインに属している必要があります。

子孫ドメイン

階層の現在のドメインから下のドメイン。

子ドメイン

ドメインの直接子孫。

先祖ドメイン

現在のドメインより上にある同じ系統のドメイン。

親ドメイン

ドメインの直接先祖。

兄弟ドメイン

同じ親を持つドメイン。

現在のドメイン

現在ログインしているドメイン。システムでは、Web インターフェイスの右上のユーザ名の前に現在のドメイン名が表示されます。ユーザ ロールが制限されている場合を除き、現在のドメインの設定を編集できます。

ドメインのプロパティ

ドメインのプロパティを変更するには、そのドメインの親ドメインの Administrator アクセス権が必要です。

名前（Name）と説明（Description）

各ドメインには、その階層内に一意の名前が必要です。説明は任意です。

親ドメイン（Parent Domain）

第2および第3レベルのドメインには親ドメインがあります。ドメインを作成した後にドメインの親を変更することはできません。

デバイス

リーフ ドメインにのみデバイスを含めることができます。つまり、1つのドメインにはサブドメインまたはデバイスを含めることができますが、両方を含めることはできません。非リーフ ドメインが直接デバイスを制御している展開を保存することはできません。

ドメイン エディタで、ドメイン階層の現在の場所に応じて、Web インターフェイスに使用可能な選択されたデバイスが表示されます。

ホスト制限（Host Limit）

Firepower Management Center がモニタでき、ネットワーク マップに保存できるホストの数。モデルによって異なります。マルチドメイン展開では、リーフ ドメインは使用可能なモニタされたホストのプールを共有しますが、個別のネットワーク マップを持っています。

各リーフ ドメインがネットワーク マップに値を入力できるように、ホスト制限を各サブドメイン レベルで設定できます。ドメインのホスト制限を 0 に設定すると、ドメインは一般的なプールで共有します。

ホスト制限を設定すると、各ドメイン レベルで異なる効果があります。

- リーフ：リーフ ドメインの場合、ホスト制限は単に、リーフ ドメインがモニタできるホスト数の制限です。
- 第 2 レベル：第 3 レベルのリーフ ドメインを管理する第 2 レベルのドメインの場合、ホスト制限は、リーフ ドメインがモニタできるホストの総数を表します。リーフ ドメインは、使用可能なホストのプールを共有します。
- グローバル：グローバル ドメインの場合、ホスト制限は、Firepower Management Center がモニタできるホストの総数に等しくなります。変更することはできません。

サブドメインのホスト制限の合計を、親ドメインのホスト制限より多くすることができます。たとえば、グローバル ドメインのホスト制限が 150,000 の場合、複数のサブドメインを設定して、それぞれのホスト制限を 100,000 にすることができます。これらのドメインのいずれか（すべてではない）が 100,000 のホストをモニタできます。

ホスト制限に到達した後に新しいホストを検出すると、ネットワーク検出ポリシーが制御を行います。新しいホストをドロップするか、または長期間非アクティブになっているホストを置換することができます。各リーフ ドメインには独自のネットワーク検出ポリシーがあるため、各リーフ ドメインは、システムが新しいホストを検出すると、独自の動作を制御します。

ドメインのホスト制限を軽減した場合に、そのネットワーク マップに新しい制限より多くのホストが含まれている場合、システムは最も長い間非アクティブになっているホストを削除します。

ドメインの管理

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

ドメインのプロパティを変更するには、そのドメインの親ドメインへの管理者アクセス権が必要です。

手順

ステップ 1 [システム（System）] > [ドメイン（Domains）]を選択します。

ステップ 2 次のようにドメインを管理します。

- 追加：[ドメインの追加（Add Domain）] をクリックするか、または親ドメインの横にある [サブドメインの追加（Add Subdomain）] アイコンをクリックします（新しいドメインの作成, （314 ページ） を参照）。
- 編集：変更するドメインの横にある編集アイコン（  ）をクリックします（ドメインのプロパティ, （312 ページ） を参照）。
- 削除：削除する空のドメインの横にある削除アイコン（  ）をクリックして、選択内容を確認します。宛先ドメインを編集することによって、削除するドメインからデバイスを移動します。

ステップ 3 ドメイン構造への変更を行い、すべてのデバイスをリーフ ドメインに関連付けたら、[保存（Save）] をクリックして変更を実行します。

ステップ 4 プロンプトが表示されたら、追加の変更を行います。

- リーフ ドメインを親ドメインに変更した場合は、古いネットワーク マップを移動または削除します（ドメイン間のデータの移動, （316 ページ） を参照）。
- ドメイン間でデバイスを移動し、新しいポリシーおよびセキュリティ ゾーンを割り当てる必要がある場合は、ドメイン間のデバイスの移動, （317 ページ） を参照してください。

次の作業

- 新しいドメインのユーザ ロールとポリシー（アクセス制御、ネットワーク検出など）を設定します。必要に応じてデバイスのプロパティを更新します。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

新しいドメインの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバルおよびセカンドレベル	Admin

最上位の [グローバル（Global）] ドメインの下に、2 つまたは 3 つのレベルで最大 50 個のサブドメインを作成できます。

ドメイン設定を実装する前に、リーフ ドメインにすべてのデバイスを割り当てる必要があります。リーフ ドメインにサブドメインを追加すると、ドメインはリーフ ドメインではなくなるので、デバイスを再度割り当てる必要があります。

手順

ステップ 1 グローバルまたはセカンドレベル ドメインで、[システム（System）]>[ドメイン（Domains）] を選択します。

ステップ 2 [ドメインの追加（Add Domain）] をクリックするか、または親ドメインの横にある [サブドメインの追加（Add Subdomain）] アイコンをクリックします。

ステップ 3 [名前（Name）] と [説明（Description）] に入力します。

ステップ 4 [親ドメイン（Parent Domain）] を選択します。

ステップ 5 [デバイス（Devices）] タブで、ドメインに追加する [使用可能なデバイス（Available Devices）] を選択し、[ドメインに追加（Add to Domain）] をクリックするか、または [選択されたデバイス（Selected Devices）] のリストにドラッグ アンド ドロップします。

ステップ 6 必要に応じて、[詳細設定（Advanced）] タブをクリックして、新しいドメインがモニタできるホスト数を制限します（ドメインのプロパティ, （312 ページ） を参照）。

ステップ 7 [保存（Save）] をクリックして、ドメイン管理ページに戻ります。
デバイスが非リーフ ドメインに割り当てられている場合は、システムによって警告が表示されます。これらのデバイスに新しいドメインを作成するには、[新しいドメインの作成（Create New Domain）] をクリックします。デバイスを既存のドメインに移動する予定がある場合は、[未割り当てのままにする（Keep Unassigned）] をクリックします。

ステップ 8 ドメイン構造への変更を行い、すべてのデバイスをリーフ ドメインに関連付けたら、[保存（Save）] をクリックして変更を実行します。

ステップ 9 プロンプトが表示されたら、追加の変更を行います。

- リーフ ドメインを親ドメインに変更した場合は、古いネットワーク マップを移動または削除します（ドメイン間のデータの移動, （316 ページ） を参照）。
- ドメイン間でデバイスを移動し、新しいポリシーおよびセキュリティ ゾーンを割り当てる必要がある場合は、ドメイン間のデバイスの移動, （317 ページ） を参照してください。

次の作業

- 新しいドメインのユーザ ロールとポリシー（アクセス制御、ネットワーク検出など）を設定します。必要に応じてデバイスのプロパティを更新します。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ドメイン間のデータの移動

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

イベントおよびネットワーク マップがリーフ ドメインに関連付けられているため、リーフ ドメインを親ドメインに変更する場合は、2 つの選択肢があります。

- ネットワーク マップおよび関連付けられているイベントを新しいリーフ ドメインに移動します。
- ネットワーク マップは削除しますが、イベントは保持します。この場合、システムが必要に応じてまたは設定されているようにイベントをプルーニングするまで、イベントは親ドメインに関連付けられたままとなります。または、古いイベントを手動で削除できます。

はじめる前に

- 以前のリーフ ドメインが現在の親ドメインになるドメイン設定を実行します（ドメインの管理, （313 ページ） を参照）。

手順

ステップ 1 現在親ドメインである以前のリーフ ドメインそれぞれに対し、2 つの選択肢があります。

- 親ドメインのイベントおよびネットワーク マップを継承するには、新しいリーフ ドメインを選択します。
- 親ドメインのネットワーク マップを削除するが、古いイベントは保持する場合は、[なし（None）] を選択します。

ステップ 2 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ドメイン間のデバイスの移動

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバルおよびセカンドレベル	Admin

ドメイン間でデバイスを移動すると、デバイスに適用された設定とポリシーに影響する可能性があります。システムは実行できる内容を自動的に保持および更新し、実行できない内容を削除します。

デバイスを移動すると、システムによって、次の新しい必要な設定を選択するようにプロンプトが表示される場合があります。

- [アクセス コントロール ポリシー（Access Control Policy）]：移動したデバイスに割り当てられたアクセス コントロール ポリシーが有効でない場合、または新しいドメインでアクセスできない場合は、新しいポリシーを選択します。すべてのデバイスに、割り当てられたアクセス コントロール ポリシーが必要です。
- [正常性ポリシー（Health Policy）]：移動したデバイスに割り当てられた正常性ポリシーが新しいドメインでアクセス不能の場合、新しい正常性ポリシーを選択できます。
- [セキュリティ ゾーン（Security Zones）]：移動したデバイス上のインターフェイスが、新しいドメインでアクセスできないセキュリティ ゾーンに属している場合は、新しいゾーンを選択できます。

デバイスでポリシーの更新が必要だが、ゾーン間でインターフェイスを移動する必要がない場合は、ゾーン設定が最新であることを示すメッセージが表示されます。たとえば、デバイスのインターフェイスが共通の先祖ドメインに設定されているセキュリティ ゾーンに属している場合は、サブドメインからサブドメインにデバイスを移動する場合はゾーン設定を更新する必要はありません。

はじめる前に

- デバイスをドメインからドメインに移動し、次に新しいポリシーとセキュリティ ゾーンを割り当てる必要があるドメイン構成を実装します（ドメインの管理, （313 ページ） を参照）。

手順

ステップ 1 [デバイスの移動（Move Devices）] ダイアログボックスの [設定するデバイスの選択（Select Device(s) to Configure）] の下で、設定するデバイスをオンにします。
同じ正常性ポリシーとアクセス コントロール ポリシーを割り当てるには、複数のデバイスをオンにします。

ステップ 2 デバイスに適用する [アクセス コントロール ポリシー（Access Control Policy）] を選択するか、または新しいポリシーを作成するには [新しいポリシー（New Policy）] を選択します。

ステップ 3 デバイスに適用する [正常性ポリシー（Health Policy）] を選択するか、またはデバイスに正常性ポリシーを適用しないままにするには [なし（None）] を選択します。

ステップ 4 インターフェイスを新しいゾーンに割り当てるようにプロンプトが表示された場合は、リストされている各インターフェイスに [新しいセキュリティ ゾーン（New Security Zone）] を選択するか、または後で割り当てるには [なし（None）] を選択します。

ステップ 5 すべての影響を受けるデバイスを設定した後、[保存（Save）] をクリックしてポリシーとゾーンの割り当てを保存します。

ステップ 6 [保存（Save）] をクリックして、ドメイン構成を実装します。

次の作業

- 移動の影響を受けた移動済みデバイスでその他の設定を更新します。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 15 章

ポリシー管理

ここでは、Firepower Management Center でさまざまなポリシーを管理する方法について説明します。

ポリシーの導入

導入を設定した後、およびその設定を変更したときは、影響を受けるデバイスにその変更を導入する必要があります。導入のステータスは、メッセージ センターで確認できます。

導入を行うと、以下のコンポーネントが更新されます。

- デバイスとインターフェイスの設定
- デバイス関連のポリシー：NAT、VPN、プラットフォームの設定
- アクセス コントロールおよび関連するポリシー：DNS、ファイル、アイデンティティ、侵入、ネットワーク分析、SSL
- ネットワーク検出ポリシー
- 侵入ルールの更新
- これらの要素のいずれかに関連付けられている設定とオブジェクト

システムにポリシーを自動的に導入させるには、導入タスクをスケジュールするか、あるいは侵入ルールの更新をインポートする際に導入するようにシステムを設定します。特に、侵入ポリシーの更新によって侵入およびネットワーク分析に関するシステム定義の基本ポリシーを変更できるようにしている場合は、ポリシーの導入を自動化すると役立ちます。侵入ルール更新によって、

アクセス コントロール ポリシーの前処理およびパフォーマンスの詳細設定オプションのデフォルト値が変更されることもあります。

マルチドメイン展開では、ユーザ アカウントが属するいずれのドメインにも変更を導入できます。

- 導入先を先祖ドメインに切り替えると、変更がすべてのサブドメインに同時に導入されます。
- 導入先をリーフ ドメインに切り替えると、変更はそのドメインだけに導入されます。

設定変更の導入

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

展開を設定した後、およびその設定を変更したときは、その変更を影響を受けるデバイスに展開します。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。このインスペクション中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。 Firepower 7010、7020、および 7030 の管理対象デバイスでは、設定変更の展開に最大 5 分かかる場合があります。利用できない時間を最小限にするために、導入は変更時間帯に実行します。

はじめる前に

- 設定変更の展開に関するガイドラインを確認してください（設定変更の展開に関する注意事項, （323 ページ）を参照）。
- すべての管理対象デバイスが同じバージョンのセキュリティ ゾーン オブジェクトを使用していることを確認してください。セキュリティ ゾーン オブジェクトを編集している場合：同期させるすべてのデバイスでインターフェイスのゾーン設定を編集するまでは、デバイスに設定変更を展開しないでください。すべての管理対象デバイスに同時に展開する必要があります。（セキュリティ ゾーン オブジェクトのリビジョンの同期, （496 ページ）を参照してください。）

手順

ステップ 1 Firepower Management Center メニュー バーで、[展開（Deploy）] をクリックします。
[ポリシーの展開（Deploy Policies）] ダイアログに、設定の期限が切れているデバイスがリストされます。ダイアログの上部の [バージョン（Version）] は、最後に設定変更を行った時期を示します。デバイス テーブルの [現在のバージョン（Current Version）] 列は、変更を各デバイスに最後に展開した時期を示します。

ステップ 2 設定変更を展開するデバイスを特定して選択します。

- [ソート（Sort）] : 列ヘッダーをクリックすることで、デバイス リストをソートします。
- [展開（Expand）] : デバイス リストを展開して展開される設定変更を表示するには、プラス アイコン（ ）をクリックします。システムは、期限切れのポリシーをインデックス（ ）アイコンでマーキングします。
- [フィルタ（Filter）] : デバイス リストをフィルタリングします。ディスプレイの列ヘッダーの右上隅にある矢印をクリックし、[フィルタ（Filter）]テキスト ボックスにテキストを入力し、Enter を押します。

ステップ 3 [展開（Deploy）] をクリックします。

ステップ 4 変更の展開時にエラーまたは警告が出された場合には、次の選択肢があります。

- [続行（Proceed）] : 警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [キャンセル（Cancel）] : 展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

次の作業

- 必要に応じて、展開のステータスをモニタします（展開メッセージの表示, （301 ページ） を参照）。
- 設定の展開に失敗した場合は、解決策について 設定変更の展開に関する注意事項, （323 ページ） を参照してください。

関連トピック

Snort® の再起動シナリオ , （324 ページ）

デバイスへの強制導入

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

通常は設定を変更すると構成設定に失効のマークが付きますが、そのようにしなくてもデバイスに設定を導入できます。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。このインスペクション中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort® の再起動によるトラフィックの動作，（326 ページ）を参照してください。 Firepower 7010、7020、および 7030 の管理対象デバイスでは、設定変更の展開に最大 5 分かかる場合があります。利用できない時間を最小限にするために、導入は変更時間帯に実行します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2 強制導入するデバイスの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [全般（General）] セクション見出しの横にある編集アイコン（）をクリックします。

ステップ 5 [強制導入（Force Deploy）] 矢印（）をクリックします。

ステップ 6 必要に応じてデバイス リストを展開して、導入される構成設定を表示します。
システムは、期限切れのポリシーをインデックス（）アイコンでマーキングします。

ステップ 7 [展開（Deploy）] をクリックします。

ステップ 8 構成設定の展開時にエラーまたは警告が出された場合には、次の選択肢があります。

- [続行（Proceed）] をクリックして、エラーまたは警告条件を解決しないで導入を続行します。このボタンは、システムが導入の警告のみを特定した場合に有効になります。システムが導入のエラーを特定した場合には無効になります。

- [キャンセル（Cancel）] をクリックして、展開を実行せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

次の作業

- 必要に応じて、展開のステータスをモニタします（展開メッセージの表示, （301 ページ） を参照）。
- 設定の展開に失敗した場合は、解決策について設定変更の展開に関する注意事項, （323 ページ） を参照してください。

関連トピック

Snort® の再起動シナリオ , （324 ページ）

設定変更の展開に関する注意事項

設定変更を管理対象デバイスに展開する際は、次の点に留意してください。

重要 利用できない時間を最小限にするために、展開は変更時間帯に実行します。

展開の結果

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。このインスペクション中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。 Firepower 7010、7020、および 7030 の管理対象デバイスでは、設定変更の展開に最大 5 分かかる場合があります。

- デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。
- アプリケーション制御の実行時に必要なディテクタが無効になっている場合、システムは、ポリシーの展開時にシステムによって提供される適切なディテクタを自動的に有効にしま

す。何もない場合、システムは、アプリケーションに対し直近で変更されたユーザ定義のディテクタを有効にします。

- ネットワーク検出ポリシーに変更を展開する場合、システムは、監視対象ネットワーク内のホストのネットワークマップからMACアドレス、TTL、およびホップ情報を削除してから、再検出を行います。また、影響を受ける管理対象デバイスは、まだ Firepower Management Center に送信されていない検出データを破棄します。

トラブルシューティング

- インライン設定をパッシブに展開されたデバイスに適用しないでください。またその逆も同様です。
- デバイスの機能を超えないように注意してください。

  複雑なアクセス コントロール ポリシーやルールは、重要なリソースを消費し、パフォーマンスに悪影響を与える可能性があります。アクセス コントロール ポリシーを展開すると、システムはすべてのルールをまとめて評価し、ネットワーク トラフィックを評価するためにターゲット デバイスが使用する拡張基準セットを作成します。

  ターゲット デバイスでサポートされるアクセス コントロール ルールまたは呼び出し侵入ポリシーの最大数を超えると、システムが警告を表示します。この最大数は、ポリシーの複雑性、物理メモリ、デバイスのプロセッサ数などの、さまざまな要因によって異なります。
- デバイスが設定した機能に対して正しいモデルであり、正しいライセンスと最小バージョンの Firepower システムを使用していることを確認します。たとえば、異なるバージョンの Firepower システムを実行しているスタック構成の 7000 または 8000 シリーズ デバイスをターゲットにすることはできません。

自動展開

次のように自動的に展開するようにシステムを設定できます。

- 侵入ルール更新の完了後
- スケジュールされたタスクの使用

関連トピック

Snort® の再起動シナリオ，（324 ページ）

Snort® の再起動シナリオ

管理対象デバイス上の侵入検知および防御エンジンは、*Snort* プロセスと呼ばれます。Snort プロセスがトラフィック インスペクション中に再起動すると、プロセスが再開するまでインスペクションが中断されます。この中断中に、トラフィックがドロップされるか、追加の検査なしで受け渡されるかは、Snort® の再起動によるトラフィックの動作，（326 ページ） で説明されているように、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。また、Snort

プロセスが再起動するかどうかに関係なく、展開時にリソース需要が高まった結果、いくつかのパケットがインスペクションを実行せずにドロップされることがあります。

次の表に示すいずれかのシナリオでは、Snort プロセスが再起動されます。

表 *39*：*Snort* 再起動のシナリオ

再起動のシナリオ	詳細情報の参照先
Snort プロセスの再起動が必要な特定の設定を展開した場合。	展開またはアクティブ化された際に Snort プロセスを再起動する設定，（327 ページ）
Snort プロセスを直ちに再起動するように設定を変更した場合。	変更により Snort プロセスがただちに再起動する場合，（330 ページ）
現在展開されている自動アプリケーションバイパス（AAB）設定のトラフィックをアクティブにした場合。	自動アプリケーション バイパスの設定，（474 ページ）

関連トピック

アクセス コントロール ポリシーの詳細設定，（796 ページ）
展開またはアクティブ化された際に Snort プロセスを再起動する設定，（327 ページ）

ポリシー適用中のトラフィックの検査

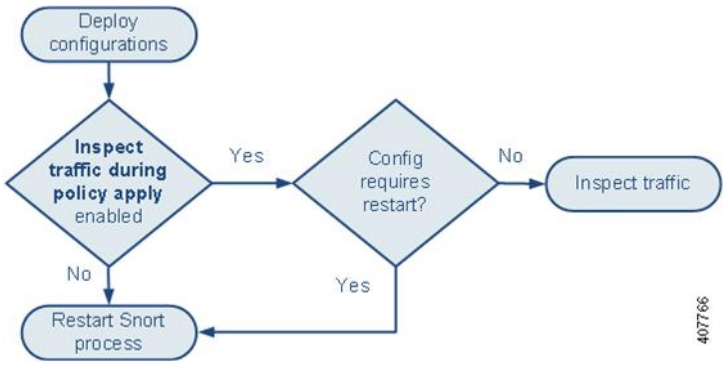
アクセス コントロール ポリシー全般の [ポリシー適用時にトラフィックを検査（Inspect traffic during policy apply）] 詳細設定を使用すると、設定変更の展開時でもトラフィックを検査できます。これは、展開する設定で Snort プロセスの再起動が不要な場合に限ります。このオプションは、次のように設定できます。

- [有効（Enabled）]：特定の設定で Snort 処理を再起動する必要な場合を除き、トラフィックは展開時に検査されます。

  展開する設定に Snort の再起動が必要でなければ、システムは現在展開されているアクセス コントロール ポリシーを使用してトラフィックを検査し、導入中に、展開しているアクセス コントロール ポリシーに切り替えます。

- [無効（Disabled）]：展開時にトラフィックは検査されません。Snort プロセスは展開時に必ず再起動されます。

次の図に、[ポリシー適用時にトラフィックを検査（Inspect traffic during policy apply）] を有効にした場合と無効にした場合の Snort の再起動の仕組みを示します。



注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。このインスペクション中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

Snort® の再起動によるトラフィックの動作

次の表に、Snort プロセスが再起動した場合のさまざまなデバイスのトラフィックの処理方法を示します。

表 *40*：再起動によるトラフィックへの影響（管理対象デバイスのモデル別）

デバイス モデル	インターフェイスの設定	再起動によるトラフィックの動作
7000 および 8000 シリーズ、NGIPSv	インライン、[フェールセーフ（Failsafe）] が有効または無効	インスペクションなしで受け渡される [フェールセーフ（Failsafe）] が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
	インライン、タップ モード	すぐにパケットを出力し、バイパス Snort をコピーする
	パッシブ	中断なし、インスペクションなし

デバイス モデル	インターフェイスの設定	再起動によるトラフィックの動作
7000 および 8000 シリーズ	ルーテッド、スイッチド、トランスペアレント	ドロップされる
ASA FirePOWER	フェールオープン（[トラフィック許可（Permit Traffic）]）状態のルーテッドまたはトランスペアレント	インスペクションなしで受け渡される
	フェールクローズ（[トラフィック クローズ（Close Traffic）]）状態のルーテッドまたはトランスペアレント	ドロップされる

（注） 再起動中に Snort プロセスがダウンした場合のトラフィック処理に加え、フェールセーフ オプションの設定に応じて、トラフィックをインスペクションなしで通過させたり、または Snort プロセスがビジーのときにトラフィックをドロップしたりすることもできます。Firepower システムのインライン セット，（505 ページ）を参照してください。

展開またはアクティブ化された際に Snort プロセスを再起動する設定

AAB 以外の構成を展開すると、常に Snort プロセスが再起動されます。AAB の展開自体には再起動が伴いませんが、パケットの遅延が大きすぎると、現在展開されている AAB 設定がアクティブになり、Snort プロセスが部分的に再起動されます。

アクセス コントロール ポリシー（Access Control Policy）

- アクセス コントロール ルールの URL カテゴリ/レピュテーションの最初の条件を追加または最後の条件を削除します。
- 現在使用されていない侵入ポリシーを追加するか、または侵入ポリシーの最後のインスタンスを削除することで、アクティブな侵入ポリシーの総数を変更します。アクセス コントロール ルールで侵入ポリシーをデフォルトのアクションまたはデフォルトの侵入ポリシーとして使用できます。

アクセス コントロール ポリシーの詳細設定

- [ポリシー適用時にトラフィックのインスペクションを実行する（Inspect traffic during policy apply）] が無効な場合に展開します。

- [ファイルとマルウェアの設定（Files and Malware Settings）] で、デフォルト以外の値を設定します。
- SSL ポリシーを追加または削除します。
- アダプティブ プロファイルを有効または無効にします。
- [ログ セッション/プロトコル配信（Log Session/Protocol Distribution）] トラブルシューティング オプションを有効または無効にします。

セキュリティ インテリジェンス（Security Intelligence）

- アクセス コントロール ポリシーの [セキュリティ インテリジェンス（Security Intelligence）] タブからホワイトリストまたはブラックリストに複数のオブジェクトを追加したり、複数のオブジェクトを削除したりします。Snortプロセスが再起動するかどうかは、インスペクションに使用できるメモリに応じて、デバイスごとに異なります。

SSL ポリシー（SSL Policy）

- SSL ルールのカテゴリ/レピュテーションの最初の条件を追加または最後の条件を削除します。

ファイル ポリシー（File Policy）

- [アーカイブを検査する（Inspect Archives）] を有効または無効にします。
- ファイル ルールで [ファイルを検出（Detect Files）] または [ファイルをブロック（Block Files）] を選択します。
- [ファイルを検出（Detect Files）] または [ファイルをブロック（Block Files）] ルールで、[ストア ファイル（Store files）] を有効または無効にします。
- [マルウェア クラウドのルックアップ（Malware Cloud Lookup）] または [マルウェアをブロック（Block Malware）] ルール アクションと、分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[ダイナミック分析（Dynamic Analysis）] または [ローカル マルウェア分析（Local Malware Analysis）]）またはストア ファイル オプション（[マルウェア（Malware）]、[不明（Unknown）]、[クリーン（Clean）] または [カスタム（Custom）]）を組み合わせた最初のアクティブ ファイル ルールを追加するか、または最後のアクティブ ファイル ルールを削除します。

アイデンティティ ポリシー（Identity Policy）

- SSL 復号化が無効になっている場合（つまり、アクセス コントロール ポリシーに SSL ポリシーが含まれていない場合）は、最初のアクティブ認証ルールを追加するか、または最後のルールを削除します。

  アクティブな認証ルールに [アクティブ認証（Active Authentication）] ルール アクションが含まれるか、[パッシブ認証でユーザを識別できない場合にアクティブ認証を使用（Use active

authentication if passive authentication cannot identify user）] が選択された [パッシブ認証（Passive Authentication）] ルール アクションが含まれます。

ネットワーク分析ポリシー

- 現在使用されていないネットワーク分析ポリシーを追加するか、またはネットワーク分析ポリシーの最後のインスタンスを削除することで、ネットワーク分析ポリシーの総数を変更します。ネットワーク分析ポリシーは、ネットワーク分析ルールと一緒に使用することもできれば、デフォルトのネットワーク分析ポリシーとして使用することもできます。
- IMAP、POP または SMTP プリプロセッサの値を変更します。値は、[Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth] または [Unix-to-Unix Decoding Depth] のいずれかです。

ネットワーク ディスカバリ（Network Discovery）

- ネットワーク検出ポリシーを使用して、HTTP、FTP、または MDNS プロトコル経由で権限のないトラフィックベースのユーザ検出を有効または無効にします。

デバイス管理

- ルーティング：7000 または 8000 シリーズ デバイスにルーテッド インターフェイス ペアまたは仮想ルータを追加します。
- VPN：7000 または 8000 シリーズ デバイスで VPN を追加または削除します。

注意 システムは、7000 または 8000 シリーズ デバイスの VPN を追加または削除したときに Snort プロセスが再起動することを警告しません。

- MTU：デバイス上のすべての非管理インターフェイスのうちの最大 MTU 値を変更します。
- 従来型デバイスの高可用性：高可用性状態共有オプションを変更します。
- 自動アプリケーション バイパス（AAB）：現在展開されている AAB 構成は、Snort プロセスの誤動作またはデバイスの誤設定により、単一のパケットが過度の処理時間を使用した場合にアクティブになります。その結果、Snort プロセスが部分的に再起動され、非常に大きい遅延が緩和されるか、または完全なトラフィックの停止が防止されます。この部分的な再起動により、デバイスがトラフィックをどのように処理するかに応じて、いくつかのパケットがインスペクションなしで通過するか、またはドロップされます。

侵入ルールの更新

- 侵入ルールの更新をインポートした後に展開します。

システムの更新プログラム

- まれに、システムの更新プログラムが再起動は不要だが、Snortバイナリを更新する場合に、Snort プロセスが再起動されます。
- 脆弱性データベース（VDB）更新をインストールするか、VDB更新のインストール後にアクセス コントロール ポリシーを初めて展開します。

関連トピック

設定変更の導入，（320 ページ）
Snort® の再起動シナリオ，（324 ページ）

変更により Snort プロセスがただちに再起動する場合

以下の変更を行うと、展開プロセスを経ることなくSnortプロセスが直ちに再起動されます。再起動がトラフィックにどのように影響するかは、管理対象デバイスのモデルおよびトラフィックの処理方法によって異なります。詳細については、Snort® の再起動によるトラフィックの動作，（326 ページ）を参照してください。

- アプリケーションまたはアプリケーションディテクタに関する次の操作のいずれかを実行します。
  - システムまたはカスタム アプリケーション ディテクタを有効または無効にします。
  - アクティブ化されたカスタム ディテクタを削除します。
  - アクティブ化されたカスタム ディテクタを保存して再アクティブ化します。
  - ユーザ定義のアプリケーションを作成します。

  すべての管理対象デバイスで Snort プロセスが再起動します。
- 脆弱性データベース（VDB）更新をインストールするか、VDB更新のインストール後にアクセス コントロール ポリシーを初めて展開します。
- 7000 または 8000 シリーズ ユーザ インターフェイスで Snort プロセスを再起動します（[システム（System）]>[設定（Configuration）]>[プロセス（Process）]）。確認メッセージが表示され、キャンセルすることができます。

ポリシーの比較

変更後のポリシーが組織の標準に準拠することを確かめたり、システム パフォーマンスを最適化したりする目的で、2つのファイル ポリシーの間の違いや、保存済みポリシーと実行中のポリシーの間の違いを調べることができます。

比較できるポリシーのタイプは次のとおりです。

- DNS
- ファイル

- ヘルス
- アイデンティティ
- 侵入
- ネットワーク分析
- SSL

比較ビューには、両方のポリシーが並べて表示されます。2 つのポリシー間の差異は、次のように強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーで異なることを示し、差異は赤色で示されます。
- 緑色は強調表示された設定が一方のポリシーには存在するが、他方には存在しないことを示します。

ポリシーの比較

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

手順

ステップ 1 比較するポリシーの管理ページにアクセスします。

- [DNS]：[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [DNS]
- [ファイル（File）]：[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [マルウェアとファイル（Malware & File）]
- [状況（Health）]：[システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）]
- [ID（Identity）]：[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [ID（Identity）]
- [侵入（Intrusion）]：[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]
- [ネットワーク分析（Network Analysis）]：[ポリシー（Policies）] > [アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

- [SSL]：[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [SSL]

ステップ 2 [ポリシーの比較（Compare Policies）] をクリックします。

ステップ 3 [比較対象（Compare Against）] ドロップダウン リストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[他のポリシー（Other Policy）] を選択します。
- 同じポリシーの 2 つのリビジョンを比較するには、[その他のリビジョン（Other Revision）] を選択します。
- 現在のアクティブ ポリシーを他のポリシーに対して比較するには、[実行中の設定（Running Configuration）] を選択します。

ステップ 4 選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較する場合、[ポリシー A（Policy A）] ドロップダウン リストと [ポリシー B（Policy B）] ドロップダウン リストから比較するポリシーを選択します。
- 実行中の設定を別のポリシーと比較する場合、[ポリシー B（Policy B）] ドロップダウン リストから 2 番目のポリシーを選択します。

ステップ 5 [OK] をクリックします。

ステップ 6 比較の結果を確認します。

- [比較ビューア（Comparison Viewer）]：比較ビューアを使用して、ポリシーの違いを個別に検索するには、タイトル バーの上にある [前へ（Previous）] または [次へ（Next）] をクリックします。
- [比較レポート（Comparison Report）]：2 つのポリシーの違いを示す PDF レポートを生成するには、[比較レポート（Comparison Report）] をクリックします。

ポリシー レポート

ほとんどのポリシーには、2 種類のレポートを生成することができます。単一のポリシーに関するレポートには、現在保存されているポリシー設定の詳細が記載されます。一方、比較レポートには、2 つのポリシー間の違いだけがリストされます。単一ポリシー レポートは、ヘルス ポリシーを除くすべてのポリシー タイプについて生成できます。

（注） 侵入ポリシー レポートには基本ポリシーの設定とポリシー階層の設定が結合され、どちらが基本ポリシーまたはポリシー レイヤのどちらに基づく設定であるかは区別されません。

現在のポリシー レポートの生成

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

手順

ステップ 1 レポートを生成するポリシーの管理ページにアクセスします。

- [アクセス制御（Access Control）]：[ポリシー（Policies）]>[アクセス コントロール（Access Control）]
- [DNS]：[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[DNS]
- [ファイル（File）]：[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[マルウェアとファイル（Malware & File）]
- [ヘルス（Health）]：[システム（System）]>[ヘルス（Health）]>[ポリシー（Policy）]
- [ID（Identity）]：[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[ID（Identity）]
- [侵入（Intrusion）]：[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]
- [デバイスの NAT（NAT for 7000 & 8000 シリーズ devices）]：[デバイス（Devices）]>[NAT]
- [ネットワーク分析（Network Analysis）]：[ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。

  （注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

- [SSL]：[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[SSL]

ステップ 2 レポートの生成対象とするポリシーの横にあるレポート アイコン（  ）をクリックします。

失効ポリシー

Firepowerシステムは、失効したポリシーに赤色のステータステキストでマークを付けます。このテキストには、ポリシーの更新を必要とするターゲットデバイスの数が示されます。失効ステータスをクリアするには、ポリシーをデバイスに再展開する必要があります。

ポリシーの再展開が必要な設定変更には次のものがあります。

- アクセスコントロールポリシー自体の変更：アクセスコントロールルール、デフォルトアクション、ポリシーターゲット、セキュリティインテリジェンスフィルタリング、前処理などの詳細オプションの変更。
- アクセスコントロールポリシーが呼び出すポリシーの変更：SSLポリシー、ネットワーク分析ポリシー、侵入ポリシー、ファイルポリシー、アイデンティティポリシー、またはDNSポリシー。
- 呼び出されるアクセスコントロールポリシーで使用される再利用可能オブジェクトまたは設定の変更：
  - ネットワーク、ポート、VLANタグ、URL、地理位置情報オブジェクト
  - セキュリティインテリジェンスリストおよびフィード
  - アプリケーションフィルタまたはディテクタ
  - 侵入ポリシーの変数セット
  - ファイルリスト
  - 復号関連のオブジェクトとセキュリティゾーン
- システムソフトウェア、侵入ルール、または脆弱性データベース（VDB）の更新。

Webインターフェイスの複数の場所からこれらの設定の一部を変更できることに留意してください。たとえば、オブジェクトマネージャ（[オブジェクト（Objects）]>[オブジェクト管理（Object Management）]）を使用してセキュリティゾーンを変更できますが、デバイスの設定（[デバイス（Devices）]>[デバイス管理（Device Management）]）でインターフェイスのタイプを変更すると、ゾーンも変更され、ポリシーの再展開が必要になります。

次の更新では、ポリシーの再展開は必要ありません。

- セキュリティインテリジェンスフィードへの自動更新およびコンテキストメニューを使用したセキュリティインテリジェンスのグローバルブラックリストおよびホワイトリストへの追加
- URLフィルタリングデータへの自動更新
- スケジュールされた位置情報データベース（GeoDB）の更新

限定的な導入のパフォーマンスに関する考慮事項

システムはホスト、アプリケーション、ユーザ検出データを使用することで、ネットワークの完全な最新プロファイルを作成できます。また、システムが侵入検知および防御システム（IPS）として機能して、ネットワーク トラフィックを分析して侵入およびエクスプロイトを検出し、オプションで問題のあるパケットをドロップすることもできます。

検出と IPS を組み合わせることで、ネットワーク アクティビティにコンテンツが提供され、次のような多くの機能を利用することができます。

- 侵害の影響フラグと表示。これによって、どのホストが特定のエクスプロイト、攻撃、またはマルウェアに対して脆弱であるかが示されます。
- アダプティブ プロファイルと Firepower の推奨事項。これによって、宛先ホストに応じてトラフィックを個別に検査できます。
- 相関。これによって、影響を受けるホストに応じて別々に侵入（およびその他のイベント）に応答できます。

ただし、組織がIPSまたは検出のみを実行することを目的としている場合は、システムのパフォーマンスを最適化できる設定がいくつかあります。

侵入防御のない検出

検出機能では、ネットワーク トラフィックをモニタして、ネットワーク上のホストの数とタイプ（ネットワークデバイスを含む）だけでなく、それらのホスト上のオペレーティング システム、アクティブなアプリケーション、およびオープン ポートを判断できます。管理対象デバイスをネットワークのユーザ アクティビティをモニタするように設定することもできます。検出データを使用して、トラフィック プロファイリングを実行し、ネットワーク コンプライアンスを評価し、ポリシー違反に応答できます。

基本的な展開（検出と単純なネットワークベースのアクセス制御のみ）では、アクセス コントロール ポリシーの設定時にいくつかの重要なガイドラインに従うことで、デバイスのパフォーマンスを向上させることができます。

（注） それが単にすべてのトラフィックを許可する場合であっても、アクセスコントロールポリシーを使用する必要があります。ネットワーク検出ポリシーが実行できるのは、アクセス コントロール ポリシーが通過を許可したトラフィックを検査する**のみ**です。

最初に、アクセスコントロールポリシーは複雑な処理を必要とせず、単純なネットワークベースの基準のみを使用してネットワーク トラフィックを処理することを確認します。次の**すべての**ガイドラインを実装する必要があります。これらのオプションのいずれかを誤って設定すると、パフォーマンス上の利点がなくなります。

- セキュリティ インテリジェンス機能を使用**しないで**ください。入力されたグローバル ホワイトリストまたはブラックリストをポリシーのセキュリティインテリジェンスの設定から削除します。
- モニタ アクションまたはインタラクティブ ブロック アクションにアクセス コントロール ルールを含め**ない**でください。許可、信頼、およびブロック ルールのみを使用します。許可されたトラフィックは検出によって検査できますが、信頼されたトラフィックとブロックされたトラフィックは検査できないことに留意してください。
- アプリケーション、ユーザ、URL、ISE 属性、または位置情報ベースのネットワーク条件にアクセス コントロール ルールを含め**ない**でください。単純なネットワークベースの条件（ゾーン、IP アドレス、VLAN タグ、およびポート）のみを使用します。
- ファイル、マルウェア、または侵入インスペクションを実行するアクセス コントロール ルールを含め**ない**でください。つまり、ファイル ポリシーまたは侵入ポリシーをアクセス コントロール ルールに関連付けないでください。
- アクセス コントロール ポリシーのデフォルトの侵入ポリシーが [アクティブなルールなし（No Rules Active）] に設定されていることを確認します。
- ポリシーのデフォルト アクションとして [ネットワーク検出のみ（Network Discovery Only）] を選択します。侵入インスペクションを実行するポリシーのデフォルト アクションを選択**しない**でください。

アクセス コントロール ポリシーと組み合わせて、ネットワーク検出ポリシーを設定して適用できます。このポリシーは、システムが検出データについて検査をするネットワーク セグメント、ポート、およびゾーンを指定し、ホスト、アプリケーション、およびユーザがセグメント、ポート、およびゾーンで検出されるかどうかを指定します。

関連トピック

デフォルトの侵入ポリシー, （1259 ページ）

ディスカバリのない侵入防御

侵入検知および防御機能によって、侵入とエクスプロイトの有無についてネットワーク トラフィックを分析できます。またオプションで違反パケットをドロップできます。侵入インスペクションを実行するがディスカバリ（検出）データを利用する必要がない場合は、ディスカバリを無効にして、デバイスのパフォーマンスを向上させることができます。

（注） アプリケーション、ユーザ、または URL の制御を実行する場合は、パフォーマンス上の利点を得るためにディスカバリを無効にすることは**できません**。システムがディスカバリ データを保存しないようにすることはできますが、システムはそれらの機能を実行するためにディスカバリ データを収集して検査する**必要があります**。

ディスカバリを無効にするには、次の**すべての**ガイドラインを実行します。いずれかでも誤って設定すると、パフォーマンス上の利点がなくなります。

- アクセス コントロール ポリシーでは、デバイスが適切にライセンス済みであっても、アプリケーション条件、ユーザ条件、URL 条件、ISE 属性条件、または地理位置情報ベースのネットワーク条件を持つルールを含め**ない**でください。単純なネットワークベースの条件（ゾーン、IP アドレス、VLAN タグ、およびポート）のみを使用します。
- ネットワーク検出ポリシーからすべてのルールを削除します。

アクセスコントロールポリシーとネットワーク検出ポリシーを展開すると、新しいディスカバリがターゲットデバイスで停止します。システムは、ネットワーク検出ポリシーで指定されたタイムアウト期間に応じて、ネットワーク マップ内の情報を段階的に削除します。また、すべてのディスカバリ データを即座に消去することもできます。

第 16 章

ルール管理：共通の特性

以下のトピックでは、Firepower Management Center でさまざまなポリシーのルールの共通特性を管理する方法について説明します。

ルールの概要

さまざまなポリシー内のルールで、ネットワーク トラフィックをきめ細かく制御できます。システムは最初の一致のアルゴリズムを使用して、指定した順番でルールに照らし合わせてトラフィックを評価します。

これらのルールはポリシー全体で一貫していない他の設定を含んでいる場合もありますが、次のような多くの基本的な特性や設定メカニズムは共通です。

- 条件：ルールの条件は各ルールが処理するトラフィックを指定します。各ルールには複数の条件を設定できます。トラフィックがルールに一致するには、すべての条件に一致する必要があります。
- アクション：ルールのアクションによって、一致するトラフィックの処理方法が決まります。選択できる [アクション（Action）] リストがルールにない場合でも、ルールには関連付けられたアクションが 1 つある点に注意してください。たとえば、カスタム ネットワーク分析ルールはそのルールの「アクション」としてネットワーク分析ポリシーを使用します。
- 位置：ルールの位置は評価の順番を決定します。ポリシーを使ってトラフィックを評価すると、システムは指定した順序でトラフィックとルールを照合します。通常は、システムによ

るトラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初のルールに従って行われます（トラフィック フローの追跡と記録を行うがトラフィック フローには影響しないモニタ ルールは例外です）。適切なルールの順序を指定することで、ネットワークトラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

- カテゴリ：いくつかのルール タイプを整理するために、各親ポリシーでカスタムのルールカテゴリを作成できます。
- ロギング：多くのルールでは、ルールが処理する接続をシステムがロギングするかどうか、およびロギングの処理方法は、ロギングの設定によって制御されます。一部のルール（IDルールやネットワーク分析ルールなど）にはロギング設定は含まれません。これは、ルールが接続の最終的な性質を決定するわけではなく、またそのルールが接続をロギングするために特別に設計されているわけではないためです。
- コメント：一部のルール タイプでは、変更を保存するたびにコメントを追加できます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。

ヒント 多くのポリシーエディタでは、右クリック メニューで編集、削除、移動、有効化、無効化など、数多くのルール管理オプションへのショートカットを提供しています。

共通の特性を持つルール

この章では、以下のルールや設定に見られる多くの共通の側面について説明しています。共通していない設定の情報については、以下を参照してください。

- アクセス コントロール ルール：アクセス コントロール ルール, （801 ページ）
- SSL ルール：SSL ルールの作成および変更, （900 ページ）
- DNS ルール：DNS ルールの作成および編集, （845 ページ）
- ID ルール：アイデンティティ ルールの作成, （1595 ページ）
- ネットワーク分析ルール：ネットワーク分析ルールの設定, （1264 ページ）
- インテリジェントアプリケーションバイパス（IAB）：インテリジェントアプリケーションバイパス, （855 ページ）
- アプリケーション フィルタ：アプリケーション フィルタ, （393 ページ）

共通の特性のないルール

次のルールの設定は、この章では説明していません。

- 侵入ルール：ルールを使用した侵入ポリシーの調整, （1043 ページ）
- ファイル ルール：ファイル ルール, （967 ページ）

- 相関ルール：相関ルールの設定, （1638 ページ）
- NAT ルール（クラシック）：7000 および 8000 シリーズ デバイス用の NAT, （653 ページ）
- 8000 シリーズ ファスト パス ルール：高速パス ルールの設定（8000 シリーズ）, （476 ページ）

ルール条件タイプ

次の表は、この章に記述している一般的なルールの条件について説明し、使用設定を列挙します。

条件	トラフィック制御方法	対応しているルール/設定
セキュリティ ゾーンの条件, （343 ページ）	送信元と宛先のセキュリティ ゾーン	アクセス コントロール ルール SSL ルール DNS ルール アイデンティティ ルール ネットワーク分析ルール
ネットワーク条件, （345 ページ）	送信元 IP アドレスと宛先 IP アドレス、対応している場合には地理的な場所や発信側のクライアント	アクセス コントロール ルール SSL ルール DNS ルール アイデンティティ ルール ネットワーク分析ルール
VLAN 条件, （347 ページ）	VLAN タグ	アクセス コントロール ルール SSL ルール DNS ルール アイデンティティ ルール ネットワーク分析ルール
ポートおよびICMP コードの条件, （347 ページ）	送信元ポート、宛先ポート、プロトコル、ICMP コード	アクセス コントロール ルール SSL ルール アイデンティティ ルール

条件	トラフィック制御方法	対応しているルール/設定
アプリケーション条件（アプリケーション制御），（350 ページ）	アプリケーションまたはアプリケーション特性（タイプ、リスク、ビジネスの関連性、カテゴリ、タグ）	アクセス コントロール ルール SSL ルール アイデンティティ ルール アプリケーション フィルタ インテリジェント アプリケーション バイパス（IAB）
URL 条件（URL フィルタリング），（356 ページ）	URL、対応している場合には、URL の特性（カテゴリおよびレピュテーション）	アクセス コントロール ルール SSL ルール
ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御），（363 ページ）	ホストのログイン権限のあるユーザまたはそのユーザのレルム、グループ、または ISE 属性	アクセス コントロール ルール SSL ルール（ISE 属性なし）

ルール条件の仕組み

ルール条件では、各ルールで処理するトラフィックを指定します。各ルールに複数の条件を設定し、トラフィックがルールに一致するにはすべての条件を満たす必要があります。使用可能な条件タイプは、ルール タイプによって異なります。

ルール エディタには、条件タイプごとに独自のタブがあります。一致させるトラフィック特性を選択して条件を作成します。一般に、左側の使用可能な項目のリスト（1 つまたは 2 つ）から基準を選択し、それらの基準を右側の選択済み項目のリスト（1 つまたは 2 つ）に追加します。たとえば、アクセス コントロール ルールの URL 条件では、URL カテゴリとレピュテーション基準を組み合わせて、ブロックする Web サイトのグループを 1 つ作成できます。

条件を作成しやすくするために、レルム、ISE 属性、さまざまなタイプのオブジェクトやオブジェクト グループなど、さまざまなシステム提供の構成やカスタム構成を使用して、トラフィックを照合できます。多くの場合、ルール基準は手動で指定できます。

送信元と宛先の基準

ルールに送信元と宛先の基準（ゾーン、ネットワーク、ポート）が含まれる場合、通常は一方または両方の基準を制約として使用できます。両方を使用する場合、一致するトラフィックの発信元は、指定した送信元のゾーン、ネットワーク、またはポートのいずれかであり、宛先のゾーン、ネットワーク、またはポートのいずれかから送出される必要があります。

条件ごとの項目

最大50個の項目を各条件に追加できます。送信元と宛先の基準を含むルールでは、それぞれ最大 50 個使用できます。選択した項目のいずれかに一致するトラフィックが条件に一致します。

単純なルールの仕組み

ルール エディタには、次の一般的な選択肢があります。条件の作成の詳細な手順については、各条件タイプのトピックを参照してください。

- 項目の選択（Choose Item）：項目をクリックするか、そのチェックボックスにマークを付けます。多くの場合、Ctrl または Shift キーを使用して複数の項目を選択するか、右クリックして [すべて選択（Select All）] を選択できます。
- 検索（Search）：検索フィールドに基準を入力します。入力するとリストが更新されます。項目名が検索され、オブジェクトとオブジェクト グループについては、その値が検索されます。リロード（  ）またはクリア（  ）をクリックして検索をクリアします。
- 事前定義された項目の追加（Add Predefined Item）：1 つ以上の使用可能な項目を選択し、[追加（Add）] ボタンをクリックするか、ドラッグアンドドロップします。無効な項目（重複、無効な組み合わせなど）は追加できません。
- 手動項目の追加（Add Manual Item）：[選択済み（Selected）] 項目リストの下のフィールドをクリックし、有効な値を入力して [追加（Add）] をクリックします。ポートを追加すると、ドロップダウン リストからプロトコルも選択できます。
- オブジェクトの作成（Create Object）：追加アイコン（  ）をクリックし、作成する条件ですぐに使用できる新しい再利用可能オブジェクトを作成し、オブジェクト マネージャで管理できます。この方法を使用してアプリケーション フィルタをその場で追加した場合、別のユーザ作成フィルタが含まれるフィルタを保存することはできません。
- 削除（Delete）：項目の削除アイコン（  ）をクリックするか、1 つ以上の項目を選択し、右クリックして [選択項目の削除（Delete Selected）] を選択します。

セキュリティ ゾーンの条件

セキュリティ ゾーンを利用すると、ネットワークをセグメント化し、複数のデバイスでインターフェイスをグループ化して、トラフィック フローを管理および分類する上で助けになります。

ゾーンのルール条件では、トラフィックをその送信元と宛先のセキュリティ ゾーンで制御します。送信元ゾーンと宛先ゾーンの両方をゾーン条件に追加すると、送信元ゾーンのいずれかにあるインターフェイスから発信され、宛先ゾーンのいずれかにあるインターフェイスを通過するトラフィックだけが一致することになります。

ゾーン内のすべてのインターフェイスは同じタイプ（すべてインライン、パッシブ、スイッチド、ルーテッドまたは ASA FirePOWER）でなければならないのと同じく、ゾーン条件で使用するすべてのゾーンも同じタイプでなければなりません。パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブ インターフェイスのあるゾーンを宛先ゾーンとして使用することはできません。

ヒント　ゾーンによってルールを制限することは、システムのパフォーマンスを向上させる最適な手段の 1 つです。ルールがデバイスのインターフェイスを通過するトラフィックに適用しなければ、ルールがそのデバイスのパフォーマンスに影響することはありません。

セキュリティ ゾーン条件とマルチテナンシー

マルチドメイン導入では、先祖ドメイン内に作成されるゾーンに、別のドメイン内にあるデバイス上のインターフェイスを含めることができます。子孫ドメイン内のゾーン条件を設定すると、その設定は表示可能なインターフェイスだけに適用されます。

セキュリティ ゾーン条件を使用したルール

次のルールは、セキュリティ ゾーン条件をサポートします。

- アクセス コントロール
- SSL
- DNS（送信元ゾーンの制約のみ）
- アイデンティティ
- ネットワーク分析

例：セキュリティ ゾーンを使用したアクセス制御

ホストにインターネットへの無制限接続を提供しつつ、それでも着信トラフィックで侵入およびマルウェアの有無を検査することでホストを保護したいという展開を想定します。

最初に、内部と外部の 2 つのセキュリティ ゾーンを作成します。次に、1 つ以上のデバイスでインターフェイスのペアをこれらのゾーンに割り当てます。この際、1 つのインターフェイスは内部ゾーンの各ペアに割り当て、1 つは外部ゾーンに割り当てます。内部側のネットワークに接続されたホストは、保護されている資産を表します。

（注）　内部（または外部）のすべてのインターフェイスを1つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティ ポリシーが意味をなすグループ化を選択します。

次に、宛先ゾーンの条件が内部に設定されているアクセス コントロール ルールを設定します。この単純なルールでは、内部ゾーンのいずれかのインターフェイスからデバイスを離れるトラフィックが照合されます。一致するトラフィックを侵入やマルウェアについて検査するには、ルール アクションとして [許可（Allow）] を選択し、そのルールを侵入ポリシーとファイル ポリシーに関連付けます。

ネットワーク条件

ネットワークルールの条件では、内部ヘッダーを使用して、送信元と宛先のIPアドレスを基準にトラフィックを制御します。外部ヘッダーを使用するトンネル ルールでは、ネットワーク条件の代わりにトンネル エンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々のIPアドレスまたはアドレス ブロックを手動で指定することもできます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ネットワーク条件での地理位置情報

ルールによっては、送信元または宛先の地理的位置を使用してトラフィックを照合することもできます。ルールのタイプが地理位置情報をサポートするものであれば、ネットワーク条件と地理位置情報条件を混在させることができます。トラフィックのフィルタリングに最新の地理位置情報データが使用されるよう、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

ネットワーク条件を使用したルール

ルール タイプ	地理位置情報による制約のサポート
アクセス コントロール	Yes
SSL	Yes
DNS（送信元ネットワークのみ）	No
ID（Identity）	Yes
ネットワーク分析	No

ネットワーク条件の設定

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

手順

ステップ 1 ルール エディタで、[ネットワーク（Networks）] タブをクリックします。

ステップ 2 [利用可能なネットワーク（Available Networks）] リストから追加する定義済みネットワークを見つけて選択します。
ルールが地理位置情報をサポートしている場合は、ネットワークと地理位置情報の基準を同じルールに混在させることができます。

- [ネットワーク（Networks）] : [ネットワーク（Networks）] サブタブをクリックして、ネットワークを選択します。
- [地理位置情報（Geolocation）] : [地理位置情報（Geolocation）] サブタブをクリックして、地理位置情報オブジェクトを選択します。

ステップ 3 [送信元に追加（Add to Source）]、[元のクライアントに追加（Add to Original Client）]、または [宛先に追加（Add to Destination）] をクリックするか、またはドラッグ アンド ドロップします。

ステップ 4 手動で指定するネットワークを追加します。送信元または宛先 IP アドレスかアドレスブロックを入力し、[追加（Add）] をクリックします。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ステップ 5 ルールを保存するか、編集を続けます。

例：アクセス コントロール ルールのネットワーク条件

次の図は、内部ネットワークから発生し、北朝鮮または 93.184.216.119（example.com）のリソースにアクセスしようとする接続をブロックするアクセス コントロール ルールのネットワーク条件を示しています。

この例で、「Private Networks」と呼ばれるネットワーク オブジェクト グループ（図に示されていない IPv4 および IPv6 プライベート ネットワークのネットワーク オブジェクトから構成されます）は、内部ネットワークを表します。また、example.com の IP アドレスを手動で指定し、システムが提供する北朝鮮の地理位置情報オブジェクトを使用して北朝鮮の IP アドレスを表しています。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

VLAN 条件

VLAN ルール条件によって、VLAN タグ付きトラフィックが制御されます。システムでは、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

事前定義のオブジェクトを使用して VLAN 条件を作成でき、また 1 ～ 4094 の VLAN タグを手動で入力することもできます。VLAN タグの範囲を指定するには、ハイフンを使用します。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の VLAN タグを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

VLAN 条件が含まれたルール

次のルール タイプでは、VLAN 条件がサポートされます。

- アクセス コントロール
- SSL
- DNS
- アイデンティティ
- ネットワーク分析

ポートおよび ICMP コードの条件

ポート条件を使用することで、トラフィックの送信元および宛先のポートに応じてそのトラフィックを制御できます。ルールのタイプによって、「ポート」は次のいずれかを表します。

- TCP と UDP：TCP および UDP トラフィックは、トランスポート層プロトコルに基づいて制御できます。システムは、カッコ内に記載されたプロトコル番号＋オプションの関連ポートまたはポート範囲を使用してこの設定を表します。例：TCP(6)/22。
- ICMP：ICMP および ICMPv6（IPv6 ICMP）トラフィックは、そのインターネット層プロトコルと、オプションでタイプおよびコードに基づいて制御できます。例：ICMP(1):3:3
- ポートなし：ポートを使用しない他のプロトコルを使用してトラフィックを制御できます。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポートプロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポート プロトコルを使用するポートを追加できます。たとえば、DNS over TCP および DNS over UDP の両方を 1 つのアクセス コントロール ルールの送信元ポート条件として追加できます。

ポート条件を使用した非 TCP トラフィックの照合

非 TCP トラフィックを照合するためのポート条件を設定することはできますが、いくつかの制約事項があります。

- アクセス コントロール ルール：GRE でカプセル化されたトラフィックをアクセス コントロール ルールに照合するには、宛先ポート条件として GRE（47）プロトコルを使用します。GRE 制約ルールには、ネットワーク ベースの条件（ゾーン、IP アドレス、ポート、VLAN タグ）のみを追加できます。また、GRE 制約ルールが設定されたアクセス コントロール ポリシーでは、システムが外側のヘッダーを使用して**すべての**トラフィックを照合します。
- SSL ルール：SSL ルールは TCP ポート条件のみをサポートします。
- アイデンティティ ルール：システムは非 TCP トラフィックに対してアクティブ認証を適用できません。アイデンティティ ルールのアクションが [アクティブ認証（Active Authentication）] の場合、あるいは [パッシブ認証でユーザを識別できない場合はアクティブ認証を使用する（Use active authentication if passive authentication cannot identify user）] オプションをオンにする場合は、TCP ポート制約のみを使用してください。アイデンティティ ルール アクションが [パッシブ認証（Passive Authentication）] または [認証なし（No Authentication）] である場合、非 TCP トラフィックに基づいてポート条件を作成できます。

注意 SSL 復号が無効の場合（つまりアクセス コントロール ポリシーに SSL ポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。
アクティブ認証ルールには [アクティブ認証（Active Authentication）] ルール アクションが含まれているか、または [パッシブ認証でユーザを識別できない場合はアクティブ認証を使用する（Use active authentication if passive authentication cannot identify user）] が選択された [パッシブ認証（Passive Authentication）] ルール アクションが含まれています。

- IMCP エコー：タイプ 0 が設定された宛先 ICMP ポート、またはタイプ 129 が設定された宛先 ICMPv6 ポートは、要求されていないエコー応答だけと照合されます。ICMP エコー要求への応答として送信される ICMP エコー応答は無視されます。ルールですべての ICMP エコーに一致させるには、ICMP タイプ 8 または ICMPv6 タイプ 128 を使用してください。

ポート条件を使用したルール

次のルールは、ポート条件をサポートします。

- アクセス コントロール
- SSL（TCP トラフィックのみをサポート）
- アイデンティティ（アクティブ認証は TCP トラフィックのみをサポート）

ポート条件の設定

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

手順

ステップ 1 ルール エディタで、[ポート（Ports）] タブをクリックします。

ステップ 2 [利用可能なポート（Available Ports）] リストから追加する定義済みポートを見つけて選択します。

ステップ 3 [送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックするか、またはドラッグ アンド ドロップします。

ステップ 4 手動で指定する送信元ポートまたは宛先ポートを追加します。

- [送信元（Source）]：プロトコルを選択し、0 から 65535 までのポートを 1 つ入力して [追加（Add）] をクリックします。
- [宛先（ICMP 以外）（Destination (non-ICMP)）]：プロトコルを選択または入力します。プロトコルを指定しない場合、または [TCP] か [UDP] を選択した場合は、0 から 65535 までのポートを 1 つ入力します。[追加（Add）] をクリックします。
- [宛先（ICMP）（Destination (ICMP)）]：[プロトコル（Protocol）] ドロップダウン リストから [ICMP] または [IPv6-ICMP] を選択し、表示されるポップアップ ウィンドウでタイプおよ

び関連するコードを選択します。ICMP タイプとコードの詳細については、Internet Assigned Numbers Authority（IANA）の Web サイトを参照してください。

ステップ 5 ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

アプリケーション条件（アプリケーション制御）

システムは IP トラフィックを分析する際、ネットワークで一般的に使用されているアプリケーションを識別および分類できます。このディスカバリベースのアプリケーション認識は、アプリケーション制御、つまりアプリケーション トラフィック制御機能の基本です。

システム提供のアプリケーション フィルタは、アプリケーションの基本特性（タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ）にしたがってアプリケーションを整理することで、アプリケーション制御に役立ちます。システム提供のフィルタの組み合わせやアプリケーションの任意の組み合わせをもとに、ユーザ定義の再利用可能フィルタを作成できます。

アプリケーション フィルタと個別に指定されたアプリケーションの両方を使用することで、完全なカバレッジを確保できます。

アプリケーション フィルタの利点

アプリケーション フィルタにより、迅速にアプリケーション制御を設定できます。たとえば、システム提供のフィルタを使って、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを簡単に作成できます。ユーザがそれらのアプリケーションの 1 つを使用しようとすると、システムがセッションをブロックします。

アプリケーション フィルタを使用することで、ポリシーの作成と管理は簡単になります。この方法によりアプリケーション トラフィックが期待どおりに制御されます。シスコは、システムと脆弱性データベース（VDB）の更新を通して、頻繁にアプリケーション ディテクタを更新しています。このため、アプリケーション トラフィックは常に最新のディテクタによってモニタされます。また、独自のディテクタを作成し、どのような特性のアプリケーションを検出するかを割り当て、既存のフィルタを自動的に追加することもできます。

アプリケーション条件の設定

次の表に示す設定を行い、アプリケーション制御を実行します。この表には、設定する内容により、アプリケーション制御にどのような制約を設けることができるかも示します。

設定（Configuration）	タイプ、リスク、関連性、カテゴリ	タグ	ユーザ定義のフィルタ
アクセス コントロール ルール	Yes	Yes	Yes

設定（Configuration）	タイプ、リスク、関連性、カテゴリ	タグ	ユーザ定義のフィルタ
SSL ルール	Yes	No：SSL プロトコル タグによって、自動的に暗号化アプリケーション トラフィックに制約される	No
ID ルール（アクティブ認証からアプリケーションを免除）	Yes	No：ユーザ エージェント除外タグによって、自動的に制約される	No
オブジェクト マネージャ内のユーザ定義のアプリケーション フィルタ	Yes	Yes	No：ユーザ定義のフィルタのネストは不可
インテリジェント アプリケーション バイパス（IAB）	Yes	Yes	Yes

関連トピック

概要：アプリケーション検出, （1507 ページ）

アプリケーション条件とフィルタの設定

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

アプリケーションの条件またはフィルタを作成するには、使用可能なアプリケーションのリストから、トラフィックを制御するアプリケーションを選択します。オプションとして（推奨）、フィルタを使用して使用可能なアプリケーションを抑制します。フィルタと個別に指定されたアプリケーションを同じ条件で使用できます。

はじめる前に

- アクセス コントロール ルールでアプリケーション制御を実行するためには、適応型プロファイルの設定, （1431 ページ） で説明されているように、アダプティブ プロファイルを有効にする**必要があります**。

手順

ステップ 1 ルール エディタまたは設定エディタを起動します。

- アクセス コントロール、SSL ルール条件：ルール エディタで [アプリケーション（Applications）] タブをクリックします。
- アイデンティティ ルール条件：ルール エディタで [レルムおよび設定（Realms & Settings）] タブをクリックし、アクティブ認証を有効にします。アイデンティティ ルールとレルムの関連付け，（1603 ページ）を参照してください。
- アプリケーション フィルタ：オブジェクト マネージャの [アプリケーション フィルタ（Application Filters）] ページで、アプリケーション フィルタを追加または編集します。フィルタの一意の名前を指定します。
- インテリジェント アプリケーション バイパス（IAB）：アクセス コントロール ポリシー エディタで [詳細（Advanced）] タブをクリックし、IAB の設定を編集して、[バイパス可能なアプリケーションおよびフィルタ（Bypassable Applications and Filters）] をクリックします。

ステップ 2 [使用可能なアプリケーション（Available Applications）] リストから追加するアプリケーションを見つけて選択します。
[使用可能なアプリケーション（Available Applications）] に表示されるアプリケーションを抑制するには、1 つ以上のアプリケーション フィルタを選択するか、個別のアプリケーションを検索します。使用可能なアプリケーションを抑制した後に、フィルタに一致するすべてのアプリケーションを追加したり、個別のアプリケーションを選択および追加したりできます。

ヒント サマリー情報とインターネットの検索リンクを表示するには、アプリケーションの横の情報アイコン（）をクリックします。ロック解除アイコン（）は、システムが復号されたトラフィックでのみ識別できるアプリケーションを示します。

フィルタを単独または組み合わせて選択すると、[使用可能なアプリケーション（Available Applications）] リストが更新され、条件を満たすアプリケーションのみが表示されます。システムによって提供されるフィルタは組み合わせて選択できますが、ユーザ定義フィルタはできません。

- 同じ特性（リスク、ビジネス関連性など）の複数のフィルタ：アプリケーション トラフィックは 1 つのフィルタのみに一致する必要があります。たとえば、中リスク フィルタと高リスク フィルタの両方を選択すると、[使用可能なアプリケーション（Available Applications）] リストにすべての中リスク アプリケーションと高リスク アプリケーションが表示されます。
- 異なるアプリケーション特性のフィルタ：アプリケーション トラフィックは、両方のフィルタ タイプに一致する必要があります。たとえば、高リスク フィルタとビジネスとの関連性が低いフィルタの両方を選択すると、[使用可能なアプリケーション（Available Applications）] リストに両方の条件を満たすアプリケーションのみが表示されます。

ステップ 3 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

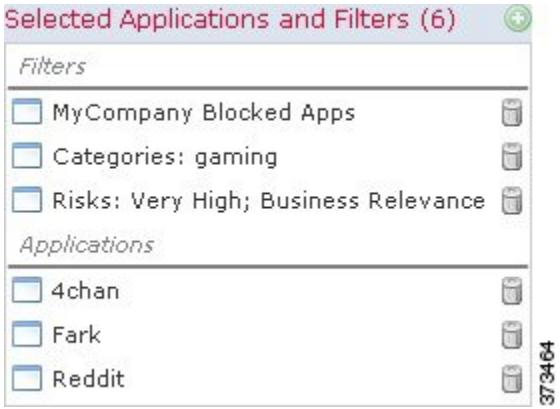
ヒント フィルタとアプリケーションをさらに追加する前に、[フィルタのクリア（Clear Filters）] をクリックして現在の選択をクリアします。

Web インターフェイスでは、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。

ステップ 4 ルールまたは設定を保存するか、編集を続けます。

例：アクセス コントロール ルールのアプリケーション条件

次の図は、MyCompany のユーザ定義アプリケーション フィルタ、リスクが高くビジネスとの関連性が低いすべてのアプリケーション、ゲーム アプリケーション、および個々に選択されたいくつかのアプリケーションをブロックするアクセス コントロール ルールのアプリケーション条件を示しています。



次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

アプリケーションの特性

システムは、次の表に示す基準を使用して、検出された各アプリケーションの特性を判別します。これらの特性をアプリケーション フィルタとして使用します。

表 41：アプリケーションの特性

特性	説明	例
タイプ（Type）	アプリケーション プロトコルは、ホスト間の通信を意味します。 クライアントは、ホスト上で動作しているソフトウェアを意味します。 Web アプリケーションは、HTTP トラフィックの内容または要求された URL を意味します。	HTTP と SSH はアプリケーション プロトコルです。 Web ブラウザと電子メール クライアントはクライアントです。 MPEG ビデオと Facebook は Web アプリケーションです。

特性	説明	例
リスク（Risk）	アプリケーションが組織のセキュリティ ポリシーに違反することがある目的で使用される可能性。	ピアツーピア アプリケーションはリスクが極めて高いと見なされます。
ビジネスとの関連性（Business Relevance）	アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。	ゲーム アプリケーションはビジネスとの関連性が極めて低いと見なされます。
カテゴリ（Category）	アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも1つのカテゴリに属します。	Facebook はソーシャル ネットワーキングのカテゴリに含まれます。
タグ	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。	ビデオ ストリーミング Web アプリケーションには、ほとんどの場合、`high bandwidth` と `displays ads` というタグが付けられます。

アプリケーション制御の制限

アプリケーション ディテクタの自動有効化

ディテクタが検出対象のアプリケーションに対して有効でない場合、システムは、そのアプリケーションに対応するシステム提供のすべてのディテクタを自動的に有効にします。存在しない場合、システムはそのアプリケーション対応で最近変更されたユーザ定義のディテクタを有効にします。

アプリケーション識別の速度

システムは、次が実行されるまで、インテリジェント アプリケーション バイパス（IAB）アプリケーション制御を実行できません。

- モニタ対象の接続がクライアントとサーバの間で確立され、
- システムがセッションでアプリケーションを識別する

この識別は 3 ～ 5 パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に行われる必要があります。

早期のトラフィックがその他のすべての基準に一致するが、アプリケーション識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、SSL ハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッション トラフィックに適切なアクションを適用します。

アクセス コントロールの場合、これらの受け渡されたパケットは、アクセス コントロール ポリシーのデフォルトの侵入ポリシー（デフォルト アクション侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもない）によりインスペクションが実行されます。

暗号化および復号トラフィックのアプリケーション制御

システムは暗号化トラフィックと復号トラフィックを識別し、フィルタ処理することができます。

- 暗号化トラフィック：システムは、SMTPS、POPS、FTPS、TelnetS、IMAPS を含む StartTLS で暗号化されたアプリケーション トラフィックを検出できます。さらに、TLS ClientHello メッセージの Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。これらのアプリケーションに `SSL Protocol` タグが付けられます。SSL ルールでは、これらのアプリケーションのみを選択できます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。
- 復号トラフィック：システムは、復号されたトラフィック（暗号化されたまたは暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに `decrypted traffic` タグを割り当てます。

アプリケーションのアクティブ認証の免除

アイデンティティ ポリシーでは、特定のアプリケーションのアクティブ認証を免除し、トラフィックにアクセス コントロールの続行を許可できます。これらのアプリケーションには、`User-Agent Exclusion` タグが付けられます。アイデンティティ ルールでは、これらのアプリケーションのみを選択できます。

ペイロードのないアプリケーション トラフィック パケットの処理

アクセス コントロールを実行している場合、システムは、アプリケーションが識別された接続内にペイロードがないパケットに対してデフォルト ポリシー アクションを適用します。

参照されるアプリケーション トラフィックの処理

アドバタイズメント トラフィックなどの Web サーバによって参照されるトラフィックを処理するには、参照しているアプリケーションではなく、参照されるアプリケーションを照合します。

複数のプロトコルを使用するアプリケーション トラフィックの制御（Skype）

システムは、Skype の複数のタイプの アプリケーション トラフィックを検出できます。Skype のトラフィックを制御するには、個々のアプリケーションを選択するのではなく、[アプリケーション フィルタ（Application Filters）] リストから [Skype] タグを選択します。これにより、システムは同じ方法で Skype のすべてのトラフィックを検出してコントロールできるようになります。

コンテンツ制限機能用にサポートされる検索エンジン

システムは、特定の検索エンジンの場合のみ、セーフサーチフィルタリングをサポートします。システムは、これらの検索エンジンからのアプリケーション トラフィックに `safesearch supported` タグを割り当てます。

関連トピック

デフォルトの侵入ポリシー, （1259 ページ）
アプリケーション検出に関する特殊な考慮事項, （1512 ページ）

URL 条件（URL フィルタリング）

URL 条件は、ネットワークのユーザがアクセスできる Web サイトを制御します。この機能は、*URL* フィルタリングと呼ばれます。

- カテゴリおよびレピュテーションベースの URL フィルタリング：URL フィルタリング ライセンスでは、URL の一般的な分類（カテゴリ）とリスク レベル（レピュテーション）に基づいて Web サイトへのアクセスを制御することができます。
- 手動 URL フィルタリング：任意のライセンスで、個々の URL、URL のグループおよび URL リストとフィードを手動で指定し、Web トラフィックのきめ細かいカスタム制御を実現できます。

Web サイトをブロックするときは、ユーザのブラウザにデフォルト動作を許可するか、またはシステムによって提供される一般的なページまたはカスタム *HTTP* 応答ページを表示できます。インタラクティブ ブロッキングは、警告ページをクリック スルーすることで Web サイトのブロックをバイパスする機会をユーザに与えます。詳細については、HTTP応答ページとインタラクティブ ブロッキング，（825 ページ）を参照してください。

URL 条件を伴うルール

次の表に、URL条件をサポートするルールと、各ルールタイプがサポートするフィルタリングのタイプを一覧します。

ルール タイプ	カテゴリとレピュテーションのサポートフィルタリングの有無	手動フィルタリングのサポート
アクセス コントロール	Yes	Yes
SSL	Yes	なし。代わりに識別名条件を使用

レピュテーションベースの URL フィルタリング

URL フィルタリング ライセンスでは、要求された URL のカテゴリおよびレピュテーションに基づいて、Web サイトへのアクセスを制御できます。

- カテゴリ：URL の一般的な分類。たとえば ebay.com はオークション カテゴリ、monster.com は求職カテゴリに属します。1 つの URL は複数のカテゴリに属することができます。
- レピュテーション：この URL が、組織のセキュリティ ポリシーに違反するかもしれない目的で使用される可能性がどの程度であるか。レピュテーションは、高リスク（レベル 1）からウェルノウン（レベル 5）の範囲です。

（注） イベントで URL カテゴリおよびレピュテーション情報を表示するには、URL 条件を使用して少なくとも 1 つのルールを作成する必要があります。また、Cisco Collective Security Intelligence（CSI）との通信を有効にして、最新の脅威インテリジェンスを取得する必要もあります。

レピュテーションベースの URL フィルタリングの利点

URL カテゴリとレピュテーションによって、URL フィルタリングをすぐに設定できます。たとえば、アクセス コントロールを使用して、乱用薬物カテゴリの高リスク URL をブロックできます。

カテゴリおよびレピュテーション データを使用すると、ポリシーの作成と管理がより簡単になります。この方法では、システムが Web トラフィックを期待どおりに確実に制御します。脅威インテリジェンスは、新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは確実に最新の情報を使用して要求された URL をフィルタ処理します。セキュリティに対する脅威を表すサイトや望ましくないコンテンツが表示されるサイトは、ユーザが新しいポリシーを更新したり展開したりするペースを上回って次々と現れては消える可能性があります。

システムはどのように適応するのか、いくつかの例を示します。

- アクセス コントロール ルールですべてのゲーム サイトをブロックする場合、新しいドメインが登録されてゲームに分類されると、これらのサイトをシステムで自動的にブロックできます。
- アクセス コントロール ルールですべてのマルウェア サイトをブロックし、あるブログ ページがマルウェアに感染すると、システムはその URL をブログからマルウェアに再分類して、そのサイトをブロックすることができます。
- アクセス コントロール ルールでリスクの高いソーシャル ネットワーキング サイトをブロックし、だれかがプロファイル ページに悪意のあるペイロードへのリンクが含まれるリンクを掲載すると、システムはそのページのレピュテーションを無害なサイトから高リスクに変更してブロックすることができます。

関連トピック

集合型セキュリティ インテリジェンスの通信設定オプション，（984 ページ）
Snort® の再起動シナリオ，（324 ページ）

手動 URL フィルタリング

アクセス コントロール ルール ルールでは、個々の URL、URL のグループ、または URL のリストとフィードを手動でフィルタリングすることで、カテゴリとレピュテーション ベースの URL のフィルタリングを補足したり、選択的にオーバーライドしたりできます。

（注） 多数のURLをフィルタリングする場合、個別の、またはグループ化されたURLオブジェクトを使用する代わりに、URLリストを使用します。詳細については、セキュリティインテリジェンスのリストとフィード，（418ページ）を参照してください。

特殊なライセンスなしでこのタイプのURLフィルタリングを実行することができます。手動URLフィルタリングはSSLルールではサポートされません。その代わりに、識別名の条件を使用します。

たとえば、アクセスコントロールを使用して組織に適していないWebサイトのカテゴリをブロックできます。ただし、カテゴリに適切なWebサイトが含まれていて、そこにアクセスを提供する必要がある場合は、そのサイトに手動で許可ルールを作成し、カテゴリのブロックルールの前に配置できます。

特定のURLを手動でフィルタリングする場合、影響を受ける可能性のある他のトラフィックについて慎重に検討してください。ネットワークトラフィックがURL条件に一致するかどうか判別するために、システムは単純な部分文字列マッチングを実行します。要求されたURLが文字列の一部に一致すると、URLが一致したと見なされます。

たとえばexample.comへのすべてのトラフィックを許可する場合、ユーザは次のURLを含むサイトを参照できます。

- http://example.com/
- http://example.com/newexample
- http://www.example.com/

別の例として、ign.com（ゲームサイト）を明示的にブロックする場合を考えてください。部分文字列マッチングによりign.com自体だけでなくverisign.comもブロックされることになり、意図しない動作が生じる可能性があります。

関連トピック

セキュリティインテリジェンスのリストとフィード，（418ページ）

URL条件の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
URLフィルタリング（カテゴリ/レピュテーション）任意（手動）	URLフィルタリング（カテゴリ/レピュテーション）任意（手動）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

URL条件を作成するときに、トラフィックを制御するURLカテゴリを選択します。必要に応じて、URLカテゴリをレピュテーションで制約できます。

アクセス コントロール ルールでは、事前定義された URL オブジェクト、URL リストとフィード、および手動のルールごとの URL を使用して個々の URL をフィルタ処理することもできます。これらの URL はレピュテーションで制約できません。手動 URL フィルタリングは SSL ルールではサポートされません。その代わりに、識別名の条件を使用します。

注意 アクセス コントロールまたは SSL ルールの URL またはカテゴリ/レピュテーションの最初の条件を追加するかまたは最後の条件を削除すると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

手順

ステップ 1 ルール エディタで、URL 条件のタブをクリックします。

- アクセス コントロールまたは ：[URL（URLs）] タブをクリックします。
- SSL：[カテゴリ（Categoy）] タブをクリックします。

ステップ 2 制御する URL を見つけて選択します。

- カテゴリ：URL の URL カテゴリを選択するか、デフォルトの [任意（Any）] のままにします。アクセス コントロール ルールでは、[カテゴリ（Categoy）] サブタブをクリックしてカテゴリを選択します。
- URL オブジェクト、リスト、およびフィード：定義済みの URL オブジェクトおよび URL リストとフィードを選択します。アクセス コントロール ルールでは、[URL（URLs）] サブタブをクリックして URL を選択します。

ステップ 3 （オプション）レピュテーションを選択して URL カテゴリを制約します。
レピュテーション レベルを選択すると、ルール アクションに応じて、選択したレベルよりも重大または重大でない他のレピュテーションも含められます。ルール アクションを変更すると、URL 条件のレピュテーション レベルが自動的に変更されます。

- [より重大でないレピュテーションを含める（Includes less severe reputations）]：ルールで Web トラフィックを許可または信頼する場合。たとえば、無害なサイト（レベル 4）を許可するようアクセス コントロール ルールを設定した場合、有名（レベル 5）サイトも自動的に許可されます。
- [より重大なレピュテーションを含める（Includes more severe reputations）]：ルールで Web トラフィックを、復号、ブロック、またはモニタする場合。たとえば、疑わしいサイト（レベル 2）をブロックするようアクセス コントロール ルールを設定した場合、高リスク（レベル 1）のサイトも自動的にブロックされます。

ステップ 4 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5 （オプション）アクセス コントロール ルールでは、URL を入力し、[追加（Add）] をクリックして、手動で指定する URL を追加します。
URL またはIPアドレスを入力できます。このフィールドでは、ワイルドカードはサポートされません。

ステップ 6 ルールを保存するか、編集を続けます。

例：アクセス コントロール ルールの URL 条件

次の図は、すべてのマルウェア サイト、すべての高リスク サイト、およびすべての有害なソーシャル ネットワーキング サイトをブロックするアクセス コントロール ルールの URL 条件を示しています。また、単一サイト example.com（URL オブジェクトによって表されます）もブロックされます。

次の表では、条件を作成する方法を要約します。

ブロックする URL	カテゴリまたはURLオブジェクト	レピュテーション
マルウェアサイト（レピュテーションに関係なく）	マルウェア サイト（Malware Sites）	任意（Any）
高リスクの URL（レベル 1）	任意（Any）	1 - 高リスク（High Risk）
無害（benign）よりも大きいリスクがあるソーシャル ネットワーキング サイト（レベル 1 ～ 3）	ソーシャル ネットワーク（Social Network）	3 - セキュリティ リスクのある無害なサイト（Benign sites with security risks）
example.com	example.com という名前の URL オブジェクト	none

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

HTTPS トラフィックのフィルタリング

暗号化されたトラフィックをフィルタリングするには、システムは SSL ハンドシェイク時に渡される情報（トラフィックを暗号化するために使用される公開キー証明書のサブジェクト共通名）に基づいて、要求された URL を決定します。

HTTPS フィルタリングは、HTTP フィルタリングとは異なり、サブジェクト共通名内のサブドメインを無視します。アクセス コントロール ポリシーで HTTPS URL を手動でフィルタリングする場合は、サブドメイン情報を含めないでください。たとえば、www.example.com ではなく、example.com を使用します。

また、HTTPS フィルタリングは URL リストもサポートしていません。代わりに、URL オブジェクトとグループを使用する必要があります。

ヒント

SSL ポリシーでは、特定の URL に対するトラフィックの処理と復号は、識別名の SSL ルール条件を定義することで行えます。証明書のサブジェクト識別名にある共通名属性には、サイトの URL が含まれています。HTTPS トラフィックを復号すると、アクセス コントロール ルールが復号されたセッションを評価できるようになるため、URL フィルタリングが改善します。

暗号化プロトコルによるトラフィックの制御

アクセス コントロール ポリシー内で URL フィルタリングを実行する場合、暗号化プロトコル（HTTP または HTTPS）は無視されます。これは、手動およびレピュテーションベース両方の URL 条件で発生します。つまり、URL フィルタリングは、次の Web サイトへのトラフィックを同じように扱います。

- http://example.com/
- https://example.com/

HTTP または HTTPS トラフィックのみに一致するルールを設定するには、アプリケーション条件をルールに追加します。たとえば、あるサイトへの HTTPS アクセスを許可する一方で、HTTP アクセスを許可しないようにできます。そのためには、2 つのアクセス コントロール ルールを作成し、それぞれにアプリケーションと URL の条件を割り当てます。

最初のルールは Web サイトへの HTTPS トラフィックを許可します。

Action: Allow
Application: HTTPS
URL: example.com

2 番目のルールは同じ Web サイトへの HTTP アクセスをブロックします。

Action: Block
Application: HTTP
URL: example.com

URL フィルタリングの制限

URL 識別の速度

システムは以下の動作の前に URL をフィルタリングできません。

- モニタ対象の接続がクライアントとサーバの間で確立される。
- システムがセッションで HTTP または HTTPS アプリケーションを識別する。
- システムが要求された URL を識別する（ClientHello メッセージまたはサーバ証明書からの暗号化されたセッションの場合）。

この識別は 3 ～ 5 パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に行われる必要があります。

早期のトラフィックがその他のすべてのルール条件に一致するが、識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、SSL ハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッショントラフィックに適切なルールアクションを適用します。

アクセス制御の場合、これらの受け渡されたパケットは、デフォルト アクション侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもなく、アクセス制御ポリシーのデフォルトの侵入ポリシーによりインスペクションが実行されます。

カテゴリまたはレピュテーションが不明な URL

URL のカテゴリまたはレピュテーションが不明な場合、Web サイトの閲覧は、カテゴリまたはレピュテーションベースの URL 条件を持つルールには一致しません。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

手動 URL フィルタリング

特定のURLを手動でフィルタリングする場合は、影響を受ける可能性のある他のトラフィックを慎重に考慮してください。ネットワーク トラフィックが URL 条件に一致するかどうか判別するために、システムは単純な部分文字列マッチングを実行します。要求されたURLが文字列の任意の部分に一致する場合、URL は一致するとみなされます。

暗号化された Web トラフィックの URL フィルタリング

暗号化された Web トラフィックに対して URL フィルタリングを実行すると、システムは次のように動作します。

- 暗号化プロトコルを無視します。ルールに URL 条件はあるがプロトコルを指定するアプリケーション条件がない場合、ルールは HTTPS および HTTP 両方のトラフィックを照合します。
- URL リストを使用しません。代わりに、URL オブジェクトとグループを使用する必要があります。

- トラフィックを暗号化するために使用する公開キー証明書のサブジェクト共通名に基づいてHTTPSトラフィックを照合し、サブジェクト共通名に含まれるサブドメインを無視します。
- アクセス制御ルール（または、その他の設定）によってブロックされている暗号化されたまたは復号された接続の場合はHTTP応答ページを表示しません。HTTP 応答ページの制限,（826 ページ）を参照してください。

URL での検索クエリ パラメータ

システムでは、URL条件の照合にURL内の検索クエリ パラメータを使用しません。たとえば、すべてのショッピング トラフィックをブロックする場合を考えます。amazon.comを探すためにWeb検索を使用してもブロックされませんが、amazon.comを閲覧しようとするとブロックされます。

選択したデバイス モデルのメモリ制限

メモリの制約上、一部のモデルでは、小規模でそれほど細分化されていないカテゴリとレピュテーションによってURLフィルタリングが実行されます。たとえば、親URLのサブサイトがそれぞれ異なるURLカテゴリとレピュテーションを持っている場合、一部のデバイスでは、すべてのサブサイトに対して親URLのデータが使用されます。具体的な例として、システムはgoogle.comカテゴリとレピュテーションを使用してmail.google.comを評価します。

メモリが少ないデバイスには、7100ファミリと次のASAモデルが含まれます：ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X。NGIPSvで、カテゴリおよびレピュテーション ベースのURLフィルタリングを実行するための正しいメモリ量を割り当てる方法ついて、詳しくは*Firepower System Virtual Installation Guide*を参照してください。

関連トピック

デフォルトの侵入ポリシー,（1259 ページ）

ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御）

Firepowerシステムによって収集された権限のあるユーザ アイデンティティ データを使用してユーザ制御を実行することができます。

アイデンティティ ソースはユーザがログインまたはログアウトする際、またはMicrosoft Active Directory（AD）またはLDAPのクレデンシャルを使用して認証する際にユーザをモニタします。次に、この収集されたアイデンティティ データを使用して、モニタ対象ホストに関連付けられているログインしている権限のあるユーザに基づいてトラフィックを処理するルールを設定できます。ユーザは、そのユーザがログオフする（アイデンティティ ソースによって報告される）か、レルムがセッションをタイムアウトするか、システムのデータベースからそのユーザ データが削除されるまで、ホストに関連付けられたままになります。

Firepowerシステムのご使用のバージョンでサポートされる権限のあるユーザ アイデンティティ ソースについては、ユーザ アイデンティティ ソースについて,（1531 ページ）を参照してください。

ユーザ制御を実行するために、次のルール条件を使用できます。

- ユーザ条件およびレルム条件：ホストのログインしている権限のあるユーザに基づいてトラフィックを照合します。トラフィックは、レルム、個々のユーザ、またはそれらのユーザが属しているグループに基づいて制御できます。
- ISE 属性条件：ユーザの、ISE が割り当てたセキュリティ グループ タグ（SGT）、デバイス タイプ（エンドポイント プロファイルとも呼ばれる）、またはロケーション IP（エンドポイント ロケーションとも呼ばれる）に基づいてトラフィックを照合します。ISE をアイデンティティ ソースとして設定する必要があります。

ユーザ条件を持つルール

ルール タイプ	ユーザ条件およびレルム条件のサポート	ISE 属性条件のサポート
アクセス コントロール	Yes	Yes
SSL	Yes	No

関連トピック

ユーザ エージェントのアイデンティティ ソース, （1533 ページ）
ISE アイデンティティ ソース, （1535 ページ）
キャプティブ ポータルのアイデンティティ ソース, （1540 ページ）

ユーザ制御の前提条件

アイデンティティ ソース/認証方式の設定

実行する認証タイプのアイデンティティ ソースを設定します。詳細については、ユーザアイデンティティ ソースについて, （1531 ページ）を参照してください。

ユーザ エージェントまたは ISE デバイスのモニタ対象に多くのユーザ グループを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、Firepower Management Center のユーザ制限が原因で、システムがグループに基づいてユーザ マッピングをドロップすることがあります。その結果、レルム、ユーザ、またはユーザ グループの条件のルールが、一致することが想定されているトラフィックと一致しなくなる可能性があります。

レルムの設定

監視対象の各 AD または LDAP サーバ（ISE またはユーザ エージェント サーバを含む）のレルムを設定し、ユーザのダウンロードを実行します。詳細については、レルムの作成, （1586 ページ）を参照してください。

レルムを設定するときには、アクティビティを監視するユーザおよびユーザ・グループを指定します。ユーザ グループを含めると、自動的に、すべてのセカンダリ グループのメンバーを含む、そのグループのすべてのメンバーが含まれます。ただし、セカンダリ グループをルール条件として使用する場合は、セカンダリ グループをレルム構成に明示的に含める必要があります。

レルムごとに、ユーザデータの自動ダウンロードを有効にすると、ユーザおよびユーザ グループの信頼できるデータを更新することができます。

アイデンティティ ポリシーの作成

レルムを認証方式に関連付けるアイデンティティ ポリシーを作成し、そのポリシーをアクセス制御に関連付けます。詳細については、アイデンティティ ポリシーの作成, （1594 ページ）を参照してください。

デバイスのユーザ制御（アクセス制御、SSL）を実行するポリシーは、アイデンティティ ポリシーを共有します。そのアイデンティティ ポリシーによって、それらのデバイス上のトラフィックに影響するルールで使用できるレルム、ユーザ、およびグループが決まります。

ユーザおよびレルム条件の設定

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

レルム、またはそのレルム内のユーザとユーザ グループでルールを制約できます。

はじめる前に

- ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御）, （363 ページ）で説明されているユーザ制御の前提条件を満たしてください。

手順

ステップ 1 ルール エディタで、[ユーザ（Users）] タブをクリックします。

ステップ 2 （オプション）[利用可能なレルム（Available Realms）] リストから使用するレルムを見つけて選択します。

ステップ 3 （オプション）[有効なユーザ（Available Users）] リストからユーザとグループを選択して、ルールをさらに制約します。

ステップ 4 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5 ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

ISE 属性条件の設定

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

はじめる前に

- ユーザ条件、レルム条件、およびISE属性条件（ユーザ制御），（363ページ）に記載されているユーザ制御の前提条件を満たします。

手順

ステップ 1 ルール エディタで、[ISE 属性（ISE Attributes）] タブをクリックします。

ステップ 2 [使用可能な属性（Available Attributes）] リストから、使用する ISE 属性を見つけて選択します。

- [セキュリティ グループ タグ（SGT）（Security Group Tag (SGT)）]
- [デバイス タイプ（Device Type）]（エンドポイント プロファイルとも呼ばれます）
- [ロケーション IP（Location IP）]（エンドポイント ロケーションとも呼ばれます）

ステップ 3 [使用可能なメタデータ（Available Metadata）] リストから属性メタデータを選択して、さらにルールを制約します。または、デフォルトの [すべて（any）] のままにします:。

ステップ 4 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5 （オプション）[ロケーション IP アドレスの追加（Add a Location IP Address）] フィールドで、IP アドレスによりルールを制約し、[追加（Add）] をクリックします。
システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 6 ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

ユーザ制御のトラブルシューティング

ユーザルールの予期しない動作に気付いたら、ルール、アイデンティティ ソース、またはレルムの設定を調整することを検討してください。その他の関連するトラブルシューティング情報については、以下を参照してください。

- ユーザ エージェント アイデンティティ ソースのトラブルシューティング，（1535 ページ）
- ISE アイデンティティ ソースのトラブルシューティング，（1539 ページ）
- キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング，（1546 ページ）
- レルムとユーザのダウンロードのトラブルシューティング，（1583 ページ）

レルム、ユーザ、またはユーザ グループを対象とするルールがトラフィックと一致しない

ユーザ エージェントまたはISEデバイスのモニタ対象に多くのユーザ グループを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、Firepower Management Center のユーザ制限が原因で、システムがユーザ レコードをドロップすることがあります。その結果、ユーザ条件のルールが、一致することが想定されているトラフィックと一致しない可能性があります。

ユーザ グループまたはユーザ グループ内のユーザを対象とするルールが、一致することが想定されているトラフィックと一致しない

ユーザ グループ条件を含むルールを設定する場合は、LDAP または Active Directory サーバでユーザ グループを設定している必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、システムはユーザ グループ制御を実行できません。

セカンダリ グループ内のユーザを対象とするルールが、一致することが想定されているトラフィックと一致しない

Active Directory サーバのセカンダリ グループのメンバーであるユーザを含めるか除外するユーザ グループ条件を含むルールを設定する場合、サーバは報告するユーザの数を制限していることがあります。

デフォルトでは、Active Directory サーバはセカンダリ グループから報告するユーザの数を制限します。この制限は、セカンダリ グループ内のすべてのユーザが Firepower Management Center に報告され、ユーザ条件を含むルールでの使用に適するようにカスタマイズする必要があります。

ルールが、初めて表示されたユーザと一致しない

システムは、以前に表示されていないユーザからのアクティビティを検出すると、サーバからそれらのユーザに関する情報を取得します。システムがこの情報を正常に取得するまで、このユーザに表示されるアクティビティは、一致するルールによって**処理されません**。代わりに、ユーザ セッションが、一致する次のルール（または該当する場合はポリシーのデフォルト アクション）によって処理されます。

たとえば、次のような状況が考えられます。

- ユーザ グループのメンバーであるユーザが、ユーザ グループ条件を含むルールに一致しない。
- ユーザ データの取得に使用されたサーバが Active Directory サーバである場合、ユーザ エージェントまたは ISE デバイスによって報告されたユーザがルールと一致しない。

これにより、システムがユーザデータをイベント ビューおよび分析ツールに表示するのが遅れる可能性があることに注意してください。

ルールがすべての ISE ユーザと一致しない

これは想定されている動作です。Active Directory ドメイン コントローラで認証された ISE ユーザに対してユーザ制御を実行することができます。LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE ユーザに対するユーザ制御は実行できません。

ルールの検索

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

多くのポリシーでは、ルールとルール内の検索が可能です。システムは、入力内容をルールの名前および条件値と照合します。これには、オブジェクトとオブジェクト グループが含まれます。

セキュリティ インテリジェンスまたは URL のリストまたはフィードに含まれる値は検索できません。

手順

ステップ 1 ポリシー エディタで、[ルール（Rules）] タブをクリックします。

ステップ 2 [ルールの検索（Search Rules）] プロンプトをクリックし、検索文字列のすべてまたは一部を入力してから Enter キーを押します。
照合ルールごとに、一致する値のカラムが強調表示されます。ステータス メッセージには、現行の一致および合計一致数が表示されます。

ステップ 3 目的のルールを見つけます。
照合ルールの間を移動する場合は、次の一致アイコン（▼）または前の一致アイコン（▲）をクリックします。

次の作業

- 新しい検索を開始する前に、クリアアイコン（✖）をクリックして、検索と強調表示をクリアします。

デバイス別のフィルタリング ルール

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

一部のポリシー エディタでは、該当デバイスによってルールの表示をフィルタ処理することができます。

システムは、ルールがそのデバイスに影響するかどうかを判断するために、ルールのインターフェイス制約を使用します。インターフェイス（セキュリティゾーン条件）でルールを制約すると、インターフェイスが置かれている場所のデバイスがそのルールの影響を受けます。インターフェイス制約のないルールは、すべてのインターフェイスに適用されるので、すべてのデバイスに適用されることになります。

手順

ステップ 1 ポリシー エディタで、[ルール（Rules）] タブをクリックし、[デバイスでフィルタ処理（Filter by Device）] をクリックします。
ターゲット デバイスとデバイス グループのリストが表示されます。

ステップ 2 1 つまたは複数のチェック ボックスをオンにして、これらのデバイスまたはグループに適用されるルールだけを表示します。または、[すべて（All）] をオンにしてリセットし、すべてのルールを表示します。

ヒント ポインタをルール基準に合わせると、その値が表示されます。基準がデバイス特有のオーバーライドを持つオブジェクトを表し、そのデバイスだけでルール リストをフィルタ処理する場合、システムはオーバーライド値を表示します。基準がドメイン特有のオーバーライドを持つオブジェクトを表し、そのドメインのデバイスでルール リストをフィルタ処理する場合、システムはオーバーライド値を表示します。

ステップ 3 [OK] をクリックします。

関連トピック

アクセス コントロール ルールの作成および編集, （807 ページ）

ルールとその他のポリシーの警告

ポリシーおよびルール エディタでは、トラフィックの分析やフローに悪影響を与える可能性のある設定をアイコンで示します。問題に応じて、システムはユーザがそのようなポリシーを展開しようとするときに警告するか、導入を完全に阻止します。

ヒント　警告、エラー、または情報のテキストを確認するには、マウスのポインタをアイコンの上に置きます。

表 *42*：ポリシーのエラー アイコン

アイコン	説明	例
error	ルールまたは設定にエラーがある場合、影響を受けるルールを無効にしても、問題を修正するまではポリシーを展開できません。	カテゴリおよびレピュテーションベースのURLフィルタリングを実行するルールは、URLフィルタリング ライセンスのないデバイスをターゲットにする時点まで有効です。その時点で、ルールの横にエラーアイコンが表示され、ポリシーを展開できなくなります。ポリシーを展開するには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、URLフィルタリングライセンスを有効にする必要があります。
警告	ルールに関する警告またはその他の警告が表示されていても、ポリシーを展開することはできます。しかし、警告でマークされている誤った設定は有効になりません。 警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。	プリエンプトされるルール、または誤った設定によりトラフィックを照合できないルールは有効になりません。誤った設定には、空のオブジェクトグループ、一致するアプリケーションがないアプリケーションフィルタ、除外されたLDAPユーザ、無効なポートなどを使用した条件が含まれます。 一方、警告アイコンがライセンスエラーまたはモデルの不一致を示している場合は、問題を修正するまでそのポリシーを展開することはできません。

アイコン	説明	例
情報	情報アイコンは、トラフィックのフローに影響する可能性がある設定に関する有用な情報を表示します。これらの問題によってポリシーの展開が阻止されることはありません。	アプリケーション制御およびURL フィルタリングが適用されている場合、システムは接続でアプリケーション トラフィックまたは Web トラフィックを識別するまで、その接続の最初の数パケットと一部のルールとの照合をスキップすることがあります。これにより接続を確立することができ、アプリケーションと HTTP 要求を識別できるようになります。

関連トピック

アプリケーション制御の制限, （354 ページ）
URL フィルタリングの制限, （362 ページ）

ルールのパフォーマンスに関するガイドライン

Firepowerシステムでは、さまざまなポリシーに含まれるルールが、ネットワーク トラフィックをきめ細かく制御します。ルールを適切に設定して順序付けることは、効果的な導入を確立する上で不可欠な要素です。それぞれの組織と導入に固有のポリシーとルール セットがありますが、ニーズに対処しながらもパフォーマンスを最適化するために従うべき一般的なガイドラインがいくつかあります。

パフォーマンスの最適化は、リソースを大量に消費する分析を実行する場合は特に重要です。複雑なポリシーやルールは、重要なリソースを消費し、パフォーマンスに悪影響を与える可能性があります。設定の変更を展開すると、システムはすべてのルールをまとめて評価し、ターゲット デバイスでネットワーク トラフィックを評価するために使用する拡張基準セットを作成します。それらの基準がターゲット デバイスのリソース（物理メモリ、プロセッサなど）を上回っている場合、そのデバイスに展開することはできません。

（注）

常に、ルールを組織のニーズに適した順序に配置する必要があります。すべてのトラフィックに適用する必要がある最優先順位のルールをポリシーの先頭近くに配置します。ただし、ルールに優先順位を付けなければ、アプリケーション条件または URL 条件を設定したルールが一致する可能性が高くなります。これは、システムは接続においてアプリケーション トラフィックまたは Web トラフィックを識別するまで、その接続の最初の数パケットと一部のルールとの照合をスキップすることがあるためです。これにより接続を確立することができ、アプリケーションと HTTP 要求を識別できるようになります。

関連トピック

アプリケーション制御の制限, （354 ページ）
URL フィルタリングの制限, （362 ページ）

ルールの簡素化および絞り込みのガイドライン

簡素化：設定しすぎない

処理するトラフィックの照合が 1 つの条件で十分な場合には、2 つの条件を使用しないでください。

個々のルール条件を最小化します。できる限り少ない個々の要素をルールの条件に使用します。たとえば、ネットワーク条件では、個々の IP アドレスではなく IP アドレス ブロックを使用します。ポート条件では、ポート範囲を使用します。アプリケーション制御およびURLフィルタリングを実行する場合はアプリケーション フィルタと URL カテゴリおよびレピュテーションを使用し、ユーザ制御を実行する場合は LDAP ユーザ グループを使用します。

要素をオブジェクトに組み合わせても、パフォーマンスは向上**しません**。たとえば、50 個の IP アドレスを 1 つのネットワーク オブジェクトに含めて使用することにパフォーマンス的なメリットはなく、条件にこれらの IP アドレスを個別に含めるよりも単に構成上のメリットがあるだけです。

絞り込み：特にインターフェイスによってリソース消費ルールを絞り込んで制約する

できる限り、ルールの条件を使用してリソース消費ルールが処理するトラフィックを絞り込んで定義します。絞り込まれたルールは、広範な条件を持つルールが多様なタイプのトラフィックを照合し、後でより多くの特定のルールをプリエンプション処理できるという理由からも重要です。以下は、リソース消費ルールの例です。

- トラフィックを復号する SSL ルール：復号だけでなく、復号されたトラフィックの更なる分析にもリソースが必要です。絞り込みを細かくし、また可能な場合は、暗号化トラフィックをブロックするか、復号しないようにします。
- ディープ インスペクションを呼び出すアクセス コントロール ルール：特に複数のカスタム侵入ポリシーと変数セットを使用している場合、侵入ファイルやマルウェアのインスペクションにはリソースが必要です。ディープインスペクションは必要な場所でのみ呼び出されることを確認してください。

最大のパフォーマンスによるメリットを得るため、インターフェイスによってルールを制約します。ルールがデバイスのすべてのインターフェイスを除外する場合、そのルールはそのデバイスのパフォーマンスに影響しません。

ルールの順序指定のガイドライン

ルールのプリエンプション

ルールのプリエンプションが発生するのは、評価する順番が前のルールがトラフィックと一致するために、その後のルールが全くトラフィックと一致しない場合です。ルールの条件により、そのルールが他のルールをプリエンプション処理するかどうかが決まります。次の例では、最初の

ルールが管理トラフィックを許可するため、2 番目のルールがそのトラフィックをブロックできません。

アクセス コントロール ルール 1：管理ユーザを許可
アクセス コントロール ルール 2：管理ユーザをブロック

どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。次の例では、最初の SSL ルールでの VLAN 範囲に 2 番目のルールでの VLAN が含まれるため、最初のルールが 2 番目のルールをプリエンプション処理します。

SSL ルール 1：VLAN 22 ～ 33 を復号しない
SSL ルール 2：VLAN 27 をブロック

次の例では、VLAN が設定されていないルール 1 はあらゆる VLAN と一致します。そのため、ルール 1 がルール 2 をプリエンプション処理し、ルール 2 での VLAN 2 の照合は行われません。

アクセス コントロール ルール 1：送信元ネットワーク 10.4.0.0/16 を許可
アクセス コントロール ルール 2：送信元ネットワーク 10.4.0.0/16、VLAN 2 を許可

あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールがプリエンプション処理されます。

アクセス コントロール ルール 1：VLAN 1 URL www.example.com を許可
アクセス コントロール ルール 2：VLAN 1 URL www.example.com を許可

条件が 1 つでも異なる場合は、後続のルールがプリエンプション処理されることはありません。

アクセス コントロール ルール 1：VLAN 1 URL www.example.com を許可
アクセス コントロール ルール 2：VLAN 2 URL www.example.com を許可

例：プリエンプションを避けるための SSL ルールの順序付け

ここで1つのシナリオとして、信頼できるCA（GoodCA）が悪意のあるエンティティ（BadCA）に間違って CA 証明書を発行してしまい、その証明書を取り消していない状況を考えてみましょう。信頼できない CA によって発行された証明書で暗号化されたトラフィックは SSL ポリシーを使用してブロックしたいものの、信頼できる CA の信頼チェーン内にあるそれ以外のトラフィックは許可したいとします。CA 証明書とすべての中間CA 証明書をアップロードした後、ルールを以下の順序で設定した SSL ポリシーを構成します。

SSL ルール 1：発行元 CN=www.badca.com をブロック
SSL ルール 2：発行元 CN=www.goodca.com を復号しない

上記のルールを逆の順序にすると、不正な CA で信頼されたトラフィックを含め、正当な CA で信頼されたすべてのトラフィックが最初に一致することになります。どのトラフィックも後続の不正な CA ルールに一致しないため、悪意のあるトラフィックはブロックされずに許可される可能性があります。

ルールのアクションとルールの順序

ルールのアクションによって、一致したトラフィックの処理方法が決まります。パフォーマンスを向上させるには、リソースを集約的に使用するルールを実行する前に、トラフィックの追加処理を実行または保証しないルールを配置してください。これにより、システムはさらに検査する必要のあるトラフィックだけを転送できます。

以下の例は、一連のルールがすべて同等に重要であり、プリエンプションが問題にならない場合に、さまざまなポリシーでルールを順序付ける方法を示しています。

最適な順序：SSL ルール

復号にはリソースが必要になるだけでなく、復号後のトラフィックの分析も必要になります。したがって、トラフィックを復号する SSL ルールを最後に配置します。

1. [モニタ（Monitor）]：一致する接続をログに記録するだけで、トラフィックに対して他のアクションは実行しないルール。
2. [ブロック（Block）]、[リセットしてブロック（Block with reset）]：それ以上のインスペクションを行わずにトラフィックをブロックするルール。
3. [復号しない（Do not decrypt）]：暗号化トラフィックを復号しないまま、暗号化セッションをアクセス コントロール ルールに渡すルール。これらのセッションのペイロードにディープ インスペクションは適用されません。
4. [復号 - 既知のキー（Decrypt - Known Key）]：既知の秘密キーを使用して着信トラフィックを復号するルール。
5. [復号 - 再署名（Decrypt - Resign）]：サーバ証明書に再署名することによって発信トラフィックを復号するルール。

最適な順序：アクセス コントロール ルール

複数のカスタム侵入ポリシーと変数セットを使用している場合は特に、侵入、ファイル、マルウェアのインスペクションにリソースが必要です。したがって、ディープ インスペクションを呼び出すアクセス コントロール ルールを最後に配置します。

1. [モニタ（Monitor）]：一致する接続をログに記録するだけで、トラフィックに対して他のアクションは実行しないルール。
2. [信頼（Trust）]、[ブロック（Block）]、[リセットしてブロック（Block with reset）]：それ以上のインスペクションを行わずにトラフィックを処理するルール。信頼できるトラフィックは、アイデンティティ ポリシーが課す認証要件の対象となることに注意してください。
3. [許可（Allow）]、[インタラクティブ ブロック（ディープ インスペクションなし）（Interactive Block (no deep inspection)）]：それ以上のインスペクションを行わずにトラフィックのディスカバリを許可するルール。許可されるトラフィックは、アイデンティティ ポリシーが課す認証要件の対象となることに注意してください。
4. [許可（Allow）]、[インタラクティブ ブロック（ディープ インスペクションあり）（Interactive Block (deep inspection)）]：禁止されているファイル、マルウェア、エクスプロイトのディープ

インスペクションを実行するファイルポリシーまたは侵入ポリシーに関連付けられているルール。

コンテンツ規制ルールの順序

SSL とアクセス コントロール ポリシーの両方でルールのプリエンプションを避けるため、YouTube 規制を制御するルールは、セーフサーチ規制を制御するルールの上に配置します。

アクセス コントロール ルールに対してセーフサーチを有効にする場合、システムは検索エンジンのカテゴリを [選択したアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加します。このアプリケーション カテゴリには YouTube が含まれます。そのため、YouTube トラフィックは、評価の優先順位が上のルールで YouTube EDU が有効にされていない限り、セーフサーチ ルールに一致します。

同様のルールのプリエンプションは、セーフサーチ サポート フィルタを持つ SSL ルールを、評価順序内で特定の YouTube アプリケーション条件を持つ SSL ルールよりも高い順序に配置した場合に生じます。

SSL ルールの順序

証明書がピニングされたサイトからのトラフィックの許可

証明書のピニングを行うと、SSL セッションが確立される前に、サーバの公開キー証明書が、サーバにすでに関連付けられているブラウザの証明書と一致しているかどうかを、クライアントのブラウザが強制的に確認します。[復号 - 再署名（Decrypt - Resign）] アクションにはサーバ証明書を変更してからクライアントに渡すという動作が含まれているため、ブラウザがすでにその証明書をピニングしている場合は、変更された証明書が拒否されます。

たとえば、クライアント ブラウザが、証明書ピニングを使用するサイト windowsupdate.microsoft.com に接続されており、そのトラフィックと一致する SSL ルールを [復号 - 再署名（Decrypt - Resign）] アクションを使用して設定すると、システムはサーバ証明書に再署名してから、クライアント サーバに渡します。この変更されたサーバ証明書は、ブラウザでピニングした windowsupdate.microsoft.com の証明書と一致しないため、クライアント ブラウザは接続を拒否します。

このトラフィックを許可するには、サーバ証明書の共通名または識別名と一致させるために、[復号しない（Do not decrypt）] アクションを使用して SSL ルールを設定します。SSL ポリシーでは、このルールを、トラフィックと一致するすべての [復号 - 再署名（Decrypt - Resign）] ルールの前に配置してください。Web サイトに正常に接続された後で、クライアント ブラウザから、ピニングされた証明書を取得できます。また、接続が成功したか失敗したかに関わらず、ログに記録された接続イベントから証明書を表示できます。

侵入ポリシーの急増を回避するためのガイドライン

アクセス コントロール ポリシーでは、1 つの侵入ポリシーを各許可ルール、インタラクティブ ブロック ルール、およびデフォルト アクションと関連付けることができます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。

ただし、ターゲット デバイスでサポートされるアクセス コントロール ルールや侵入ポリシーには最大数があります。この最大数は、ポリシーの複雑性、物理メモリ、デバイスのプロセッサ数などの、さまざまな要因によって異なります。

デバイスでサポートされる最大を超えるとアクセスコントロールポリシーは展開できず、再評価する必要があります。いくつかの侵入ポリシーまたは変数セットを統合すると、複数のアクセス コントロール ルールに 1 つの侵入ポリシーと変数セットのペアを関連付けることができます。一部のデバイスでは、すべての侵入ポリシーに関して 1 つの変数セットだけを使用できる場合や、デバイス全体でただ 1 つの侵入ポリシー/変数セット ペアだけを使用できる場合があります。

第 17 章

再利用可能なオブジェクト

以下のトピックでは、Firepower システムで再利用可能オブジェクトを管理する方法について説明します。

再利用可能オブジェクトの概要

柔軟性と Web インターフェイスの使いやすさを向上させるために、Firepower システムでは、名前を値に関連付ける再利用可能な構成である名前付きオブジェクトを使用します。その値を使用する場合は、代わりに名前付きオブジェクトを使用します。多くのポリシーとルール、イベント

検索、レポート、ダッシュボードなど、Web インターフェイスのさまざまな場所でのオブジェクトの使用がサポートされています。よく使用される構成を表す多くの事前定義されたオブジェクトが提供されています。

オブジェクトを作成および管理するには、オブジェクト マネージャを使用します。オブジェクトを使用する多くの構成では、必要に応じて、その場でオブジェクトを作成することもできます。オブジェクト マネージャを使用して、次の操作も実行できます。

- 単一の構成で複数のオブジェクトを参照するための、オブジェクトのグループ化。オブジェクト グループ，（382 ページ）を参照してください。
- 選択したデバイス、またはマルチドメイン展開の場合は選択したドメインのオブジェクト値のオーバーライド。オブジェクトのオーバーライド，（384 ページ）を参照してください。

アクティブなポリシーで使用されるオブジェクトを編集した後に、変更を有効にするには、変更した構成を再展開する必要があります。アクティブなポリシーで使用されているオブジェクトは削除できません。

オブジェクト タイプ

次の表に、Firepower システムで作成できるオブジェクト、各オブジェクト タイプがグループ化可能かどうか、およびオーバーライドを許可するように構成できるかどうかを示します。

オブジェクト タイプ（Object Type）	グループ化可能	オーバーライドを許可
ネットワーク	Yes	Yes
[ポート（Port）]	Yes	Yes
セキュリティ ゾーン	No	No
アプリケーション フィルタ	No	No
VLAN タグ	Yes	Yes
URL	Yes	Yes
位置情報（GeoLocation）	No	No
変数セット	No	No
セキュリティ インテリジェンス：ネットワーク、DNS、URL のリストとフィード	No	No
シンクホール	No	No
ファイル リスト	No	No

オブジェクト タイプ（**Object Type**）	グループ化可能	オーバーライドを許可
暗号スイート リスト	No	No
識別名（Distinguished Name）	Yes	No
公開キー インフラストラクチャ（PKI）： • 内部および信頼できる CA • 内部および外部証明書	Yes	No

オブジェクトおよびマルチテナンシー

マルチドメイン展開では、グローバルおよび子孫ドメインでオブジェクトを作成できます。現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。また、編集できない先祖ドメインで作成されたオブジェクトも表示されますが、セキュリティ ゾーンを除きます。

（注） セキュリティ ゾーンは、リーフ レベルで設定したデバイス インターフェイスに関連するため、子孫ドメイン内の管理者は、先祖ドメインで作成されたセキュリティ ゾーンを表示および編集できます。サブドメインのユーザは、先祖ゾーンからインターフェイスを追加および削除できますが、ゾーンを削除または名前変更することはできません。

オブジェクト名は、ドメイン階層内で一意である必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

グループ化をサポートするオブジェクトの場合、現在のドメインのオブジェクトを先祖ドメインから継承されたオブジェクトとグループ化できます。

オブジェクトのオーバーライドにより、ネットワーク、ポート、VLAN タグ、URL などの特定のオブジェクト タイプのデバイス固有またはドメイン固有の値を定義できます。マルチドメイン展開では、先祖ドメイン内のオブジェクトのデフォルト値を定義できますが、子孫ドメイン内の管理者は、そのオブジェクトのオーバーライドの値を追加できます。

オブジェクト マネージャ

オブジェクトマネージャを使用すると、オブジェクトおよびオブジェクト グループを作成、管理することができます。

オブジェクトマネージャには、ページあたり 20 のオブジェクトまたはグループが表示されます。オブジェクトまたはグループのタイプが 20 を超える場合は、ページ下部のナビゲーション リンクを使用して追加ページを表示します。特定のページにアクセスしたり、更新アイコン（）にアクセスしてビューを更新したりすることもできます。

デフォルトでは、オブジェクトとグループはページで、アルファベット順に名前でリストされます。ただし、表示されている任意の列でオブジェクトまたはグループの各タイプをソートできます。ページのオブジェクトは、名前または値でフィルタすることもできます。

オブジェクトの編集

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 リストからオブジェクトタイプを選択します（再利用可能オブジェクトの概要, （377ページ）を参照）。

ステップ 3 編集するオブジェクトの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、オブジェクトは先祖ドメインに属しており、上書きを許可しないように設定されており、オブジェクトを変更する権限がありません。

ステップ 4 必要に応じてオブジェクト設定を変更します。

ステップ 5 変数セットを編集する場合は、セット内の変数を管理します（変数の管理, （414 ページ）を参照）。

ステップ 6 オーバーライドを許可するように設定できるオブジェクトの場合、次の操作をします。

- このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可, （386 ページ）を参照）。現在のドメインに属しているオブジェクトに対してのみ、この設定を変更できます。

- このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド（Override）]セクションを展開し、[追加（Add）]をクリックします（オブジェクトのオーバーライドの追加, （387 ページ） を参照）。

ステップ 7 [保存（Save）]をクリックします。

ステップ 8 変数セットを編集するときにそのセットがアクセス コントロール ポリシーで使用されている場合、[はい（Yes）]をクリックして変更の保存を確認します。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入, （320 ページ） を参照）。

オブジェクトまたはオブジェクト グループのフィルタ処理

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

マルチドメインの導入環境では、現在ドメインと親ドメインで作成されたオブジェクトが表示され、それらをフィルタ処理できます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [フィルタ処理（Filter）]フィールドのフィルタ条件を入力します。
ページは入力に従って更新され、一致する項目が表示されます。

次のメタ文字を使用できます。

- アスタリスク（*）文字は、ある文字の 0 回以上のオカレンスに一致します。
- キャレット記号（^）は文字列の先頭部分と一致します。
- ドル記号（$）は文字列の末尾と一致します。

オブジェクトのソート

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 列の見出しをクリックします。反対方向でソートするには、見出しを再度クリックします。

オブジェクト グループ

オブジェクトをグループ化すると、複数のオブジェクトを 1 つの設定で参照できます。システムでは、Web インターフェイスでオブジェクトおよびオブジェクト グループを交互に使用することができます。たとえば、ポート オブジェクトを使用する場合はいつでも、ポート オブジェクト グループも使用できます。

ネットワーク、ポート、VLAN タグ、URL、および PKI オブジェクトをグループ化できます。

同じタイプのオブジェクトおよびオブジェクト グループには、同じ名前を付けることはできません。マルチドメイン展開では、オブジェクト グループの名前をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ポリシーで使用されるオブジェクト グループ（たとえば、アクセス コントロール ポリシーで使用されるネットワーク オブジェクト グループ）を編集する場合、変更を適用するためには、変更後の設定を再展開する必要があります。

グループを削除しても、グループ内のオブジェクトは削除されず、相互の関連性だけが削除されます。さらに、アクティブ ポリシーで使用中のグループは削除できません。たとえば、保存されたアクセス コントロール ポリシーの VLAN 条件で使用している VLAN タグのグループは削除できません。

再利用可能オブジェクトのグループ化

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

先祖ドメインから継承したオブジェクトを持つ現在のドメイン内のオブジェクトをグループ化できます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 グループ化するオブジェクトタイプが、[ネットワーク（Network）]、[ポート（Port）]、[URL]、[VLAN タグ（VLAN Tag）] の場合は、次のように操作します。

a) オブジェクト タイプのリストからオブジェクト タイプを選択します。

b) [追加 [オブジェクト タイプ]（Add [Object Type]）] ドロップダウンリストから [グループの追加（Add Group）] を選択します。

ステップ 3 グループ化するオブジェクトタイプが [識別名（Distinguished Name）] の場合は、次のように操作します。

a) [識別名（Distinguished Name）] ノードを展開します。

b) [オブジェクト グループ（Object Groups）] を選択します。

c) [識別名グループの追加（Add Distinguished Name Group）] をクリックします。

ステップ 4 グループ化するオブジェクト タイプが [PKI] の場合は、次のように操作します。

a) [PKI] ノードを展開します。

b) 次のいずれかを実行します。

- 内部 CA グループ（Internal CA Groups）
- 信頼できる CA グループ（Trusted CA Groups）
- 内部証明書グループ（Internal Cert Groups）
- 外部証明書グループ（External Cert Groups）

c) [[オブジェクト タイプ] グループの追加（Add [Object Type] Group）] ボタンをクリックします。

ステップ 5 一意の [名前（Name）] を入力します。

ステップ 6 リストから 1 つ以上のオブジェクトを選択して、[追加（Add）] をクリックします。
次のことも実行できます。

- 含める既存のオブジェクトを検索するには、フィルタ フィールド（）を使用します。これは入力に従って更新され、一致する項目を表示します。検索文字列をクリアするには、検索フィールドの上にある再ロードアイコン（）をクリックするか、検索フィールド内のクリア アイコン（）をクリックします。
- 既存のオブジェクトがニーズを満たさない場合、すぐにオブジェクトを作成するには、追加アイコン（）をクリックします。

ステップ 7 必要に応じて、[ネットワーク（Network）]、[ポート（Port）]、[URL]、および [VLAN タグ（VLAN Tag）] グループに対し、次の操作を実行します。

- [説明（Description）] を入力します。
- [オーバーライドを許可する（Allow Overrides）] チェックボックスをオンにして、このオブジェクト グループのオーバーライドを許可します。オブジェクトのオーバーライドの許可, （386 ページ）を参照してください。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクト グループを参照する場合は、設定の変更を展開します。設定変更の導入, （320 ページ）を参照してください。

オブジェクトのオーバーライド

オブジェクトをオーバーライドすることにより、オブジェクトの代替値を定義できます。指定したデバイスに対して、システムはこの代替値を使用します。

ほとんどのデバイスに有効な定義を設定したオブジェクトを作成した後、異なる定義を必要とする少数のデバイスについて、オーバーライドを使用してオブジェクトに対する変更内容を指定できます。また、すべてのデバイスに対してオーバーライドする必要があるオブジェクトを作成し、そのオブジェクトを使用してすべてのデバイスに適用する単一のポリシーを作成することもできます。オブジェクト オーバーライドでは、デバイス全体で使用する共有ポリシーの小さなセットを作成し、個々のデバイスの必要に応じてポリシーを変更できます。

たとえば、社内のさまざまな部門への ICMP トラフィックを拒否する場合があります。それぞれの部門は、異なるネットワークに接続されています。これを実行するには、Departmental Network という名前のネットワーク オブジェクトを含むルールを使用して、アクセス コントロール ポリシーを定義します。このオブジェクトのオーバーライドを許可することによって、関連する各デ

バイスで、デバイスが接続されている実際のネットワークを指定するオーバーライドを作成できます。

マルチドメイン展開では、先祖ドメインのオブジェクトのデフォルト値を定義して、子孫ドメインの管理者がそのオブジェクトのオーバーライド値を追加できるようにすることができます。たとえば、マネージド セキュリティ サービス プロバイダー（MSSP）では、単一の Firepower Management Center を使用して複数の顧客のネットワーク セキュリティを管理する場合があります。この場合、MSSP の管理者は、すべての顧客の導入で使用するオブジェクトをグローバル ドメインに定義できます。各顧客の管理者は子孫ドメインにログインして、それぞれの組織に応じてそのオブジェクトをオーバーライドできます。これらのローカル管理者が MSSP の他の顧客のオーバーライド値を表示したり、影響を与えたりすることはできません。

オブジェクト オーバーライドのターゲットを特定のドメインに絞ることもできます。その場合、ユーザがデバイス レベルで値をオーバーライドしない限り、システムはターゲット ドメインのすべてのデバイスにオブジェクト オーバーライド値を使用します。

オブジェクト マネージャで、オーバーライド可能なオブジェクトを選択し、そのオブジェクトに対するデバイスレベルまたはドメインレベルのオーバーライドのリストを定義できます。

オブジェクト オーバーライドを使用できるオブジェクト タイプは以下に限られます。

- ネットワーク
- [ポート（Port）]
- VLAN タグ
- URL

オブジェクト マネージャでは、オーバーライド可能なオブジェクトのオブジェクト タイプには [オーバーライド（Override）] 列が表示されます。この列の有効な値は以下のとおりです。

- 緑のチェックマーク：このオブジェクトにはオーバーライドを作成できます。オーバーライドはまだ追加されていません。
- 赤の X：このオブジェクトにはオーバーライドを作成できません。
- 数値：このオブジェクトに追加されているオーバーライドの数を表します（たとえば、「2」は 2 つのオーバーライドが追加されていることを意味します）。

オブジェクト オーバーライドの管理

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 オブジェクトタイプのリストから選択します（再利用可能オブジェクトの概要, （377 ページ）を参照）。

ステップ 3 編集するオブジェクトの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（）が表示される場合、オブジェクトは先祖ドメインに属しており、上書きを許可しないように設定されており、オブジェクトを変更する権限がありません。

ステップ 4 オブジェクト オーバーライドを管理します。

- 追加：オブジェクト オーバーライドを追加します（オブジェクトのオーバーライドの追加, （387 ページ）を参照）。
- 許可：オブジェクト オーバーライドを許可します（オブジェクトのオーバーライドの許可, （386 ページ） を参照）。
- 削除：オブジェクトエディタで、削除するオーバーライドの横にある削除アイコン（  ）をクリックします。
- 編集：オブジェクト オーバーライドを編集します（オブジェクト オーバーライドの編集, （388 ページ）を参照）。

オブジェクトのオーバーライドの許可

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

手順

ステップ 1 オブジェクト エディタで、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします。

ステップ 2 [保存（Save）] をクリックします。

次の作業

- オブジェクトのオーバーライド値を追加します（オブジェクトのオーバーライドの追加, （387 ページ） を参照）。

オブジェクトのオーバーライドの追加

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

はじめる前に

- オブジェクトのオーバーライドを許可します（オブジェクトのオーバーライドの許可, （386 ページ） を参照）。

手順

ステップ 1 オブジェクト エディタで、[オーバーライド（Override）] セクションを展開します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ターゲット（Targets）] タブで、[使用可能なデバイスとドメイン（Available Devices and Domains）] リストからドメインまたはデバイスを選択し、[追加（Add）] をクリックします。

ステップ 4 [オーバーライド（Override）] タブで、[名前（Name）] を入力します。

ステップ 5 必要に応じて、[説明（Description）] を入力します。

ステップ 6 オーバーライド値を入力します。

例：
ネットワーク オブジェクトについては、ネットワーク値を入力します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入, （320 ページ） を参照）。

オブジェクト オーバーライドの編集

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

既存のオーバーライドの説明と値を変更できます。ただし、既存のターゲット リストは変更できません。代わりに、既存のオーバーライドを置き換える、新しいターゲットに対する新しいオーバーライドを追加する必要があります。

手順

ステップ 1 オブジェクト エディタで、[オーバーライド（Override）] セクションを展開します。

ステップ 2 変更するオーバーライドの横にある編集アイコン（  ）をクリックします。

ステップ 3 必要に応じて、[説明（Description）] を変更します。

ステップ 4 オーバーライド値を変更します。

ステップ 5 [保存（Save）] をクリックして、オーバーライドを保存します。

ステップ 6 [保存（Save）] をクリックして、オブジェクトを保存します。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入，（320 ページ） を参照）。

ネットワーク オブジェクト

ネットワーク オブジェクトは、個別に、またはアドレス ブロックとして指定できる 1 つ以上の IP アドレスを表します。ネットワーク オブジェクトおよびグループを、アクセス コントロール ポリシー、ネットワーク変数、侵入ルール、アイデンティティ ルール、ネットワーク検出ルール、イベント検索、レポートなど、システムの Web インターフェイスのさまざまな場所で使用できます。

ネットワーク オブジェクトの作成

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 オブジェクト タイプのリストから [ネットワーク（Network）] を選択します。

ステップ 3 [ネットワークを追加（Add Network）] ドロップダウン メニューで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 名前を入力します。
マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 必要に応じて、[説明（Description）] を入力します。

ステップ 6 [ネットワーク（Network）] フィールドに、オブジェクトに追加する IP アドレスまたはアドレス ブロックを入力します。

ステップ 7 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可, （386 ページ） を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド（Override）]セクションを展開し、[追加（Add）] をクリックします（オブジェクトのオーバーライドの追加, （387 ページ） を参照）。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入, （320 ページ） を参照）。

ポート オブジェクト

ポート オブジェクトは、異なるプロトコルをそれぞれ少し異なる方法で表します。

TCP および UDP

ポート オブジェクトは、カッコ内にプロトコル番号が記載されたトランスポート層プロトコルと、オプションの関連ポートまたはポート範囲を表します。例：`TCP(6)/22`。

ICMP および ICMPv6（IPv6-ICMP）

ポート オブジェクトはインターネット層プロトコルと、オプションでタイプおよびコードを表します。例：`ICMP(1):3:3`

ICMP または IPV6-ICMP ポート オブジェクトは、タイプ、および該当する場合はコードを基準に制限できます。ICMP のタイプとコードの詳細については、次の URL を参照してください。

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

その他

ポート オブジェクトは、ポートを使用しない他のプロトコルを表します。

Firepower システムには、ウェルノウン ポート用にデフォルトのポート オブジェクトが用意されています。これらのデフォルト オブジェクトを変更または削除することはできません。デフォルト オブジェクトに加え、カスタム ポート オブジェクトを作成できます。

ポート オブジェクトおよびグループは、アクセス コントロール ポリシー、アイデンティティ ルール、ネットワーク検出ルール、ポート変数、イベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、組織が特定のポート範囲を使用するカスタム クライアントを使用していて、システムで過剰なイベントや誤解を与えるイベントが発生した場合、それらのポートをモニタ対象から除外するようネットワーク検出ポリシーを設定できます。

ポート オブジェクトを使用する際は、次のガイドラインに従ってください。

- アクセス コントロール ルールの送信元ポート条件には TCP/UDP 以外のプロトコルを追加できません。さらに、送信元ポートと宛先ポートの両方のポート条件をルールで設定する場合、トランスポート プロトコルを混在させることはできません。
- 送信元ポート条件で使用されるポート オブジェクト グループにサポート対象外のプロトコルを追加した場合、設定を展開しても、その条件が使用されているルールは管理対象デバイスで適用されません。
- TCP と UDP の両方のポートを含むポート オブジェクトを作成してから、ルールの送信元ポート条件としてそのポート オブジェクトを追加した場合、宛先ポートを追加することはできません。その逆もまた同様です。

ポート オブジェクトの作成

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 オブジェクト タイプのリストから [ポート（Port）] を選択します。

ステップ 3 [ポートの追加（Add Port）] ドロップダウン リストで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 名前を入力します。

ステップ 5 [プロトコル（Protocol）] を選択します。

ステップ 6 選択したプロトコルに応じて、[ポート（Port）] で制限するか、または ICMP の [タイプ（Type）] および [コード（Code）] を選択します。
1 から 65535 のポートを入力できます。ポート範囲を指定するには、ハイフンを使用します。[すべて（All）] のプロトコルと一致させることを選択した場合は、[その他（Other）] ドロップダウン リストを使用して、ポートでオブジェクトを制限する必要があります。

ステップ 7 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可, （386 ページ） を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド（Override）] セクションを展開し、[追加（Add）] をクリックします（オブジェクトのオーバーライドの追加, （387 ページ） を参照）。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入, （320 ページ） を参照）。

セキュリティ ゾーン

セキュリティゾーンは、ネットワークをセグメント化してトラフィック フローを制御し、分類しやすくします。セキュリティ ゾーンは単にインターフェイスをグループ化します。これらのグループは複数のデバイスにまたがることがあります。また、単一のデバイスに複数のゾーンを設定することもできます。

セキュリティ ゾーン 内のすべてのインターフェイスが同じタイプ（すべてインライン、パッシブ、スイッチド、ルーテッド、または ASA FirePOWER）である必要があります。セキュリティ ゾーン を作成した後、それに含まれるインターフェイスのタイプを変更することはできません。インターフェイスは 1 つのゾーンだけに属することができます。

オブジェクト マネージャのセキュリティ ゾーンのページでは、管理対象デバイスで設定されているゾーンの一覧が表示されます。また、このページには、各ゾーンのタイプも表示され、各ゾーンを展開すると、どのデバイスのどのインターフェイスが各ゾーンに属するかを表示できます。

モデル固有の注意事項および警告

7000 または 8000 シリーズ デバイスの初期設定時に、システムはデバイス用に選択した検出モードに基づいてセキュリティ ゾーンを作成します。たとえば、パッシブ展開ではシステムはパッシブ ゾーンを作成し、インライン展開では外部ゾーンと内部ゾーンを作成します。Firepower Management Center にデバイスを登録すると、これらのセキュリティ ゾーンが Management Center に追加されます。

ASA FirePOWER セキュリティ コンテキストの変更（シングル コンテキスト モードからマルチ コンテキスト モードへの変更、またはその逆の変更）をすると、割り当てられているセキュリティ ゾーンからデバイスのすべてのインターフェイスがシステムによって削除されます。

ゾーンとマルチテナンシー

マルチドメイン展開では、どのレベルでもセキュリティ ゾーンを作成できます。先祖ドメインで作成されたゾーン には別のドメインのデバイスに存在するインターフェイスが含まれる場合があります。この状況において、オブジェクト マネージャ内の先祖のゾーン の設定を表示するサブドメイン ユーザには、当該ドメインのインターフェイスのみが確認できます。

ロールによって制限されない限り、サブドメインのユーザは先祖ドメインで作成されたゾーン を表示**および**編集できます。サブドメインのユーザは、これらのゾーン にインターフェイスの追加や削除を行えます。ただし、ゾーン の削除や名称変更はできません。子孫ドメインで作成されたゾーン の表示や編集はできません。

セキュリティ ゾーン オブジェクトの作成

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

ヒント　空のセキュリティ ゾーンを作成し、後からインターフェイスを追加できます。インターフェイスを追加するには、インターフェイスに名前が付いている必要があります。[デバイス（Devices）] > [デバイス管理（Device Management）] でインターフェイスを設定しているときに、セキュリティ ゾーンを作成することもできます。

はじめる前に

- 各種セキュリティ ゾーンの使用要件および制限を理解します。セキュリティ ゾーン, （392 ページ）を参照してください。

手順

ステップ 1　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2　オブジェクト タイプのリストから、[セキュリティ ゾーン（Security Zones）] を選択します。

ステップ 3　[セキュリティ ゾーンの追加（Add Security Zone）] をクリックします。

ステップ 4　名前を入力します。

ステップ 5　[インターフェイス タイプ（Interface Type）] を選択します。

ステップ 6　[デバイス（Device）]>[インターフェイス（Interfaces）] ドロップダウン リストから、追加するインターフェイスを含むデバイスを選択します。

ステップ 7　1 つ以上のインターフェイスを選択します。

ステップ 8　[追加（Add）]をクリックして、デバイス別にグループ化された、選択したインターフェイスを追加します。

ステップ 9　[保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入, （320 ページ） を参照）。

アプリケーション フィルタ

システム提供のアプリケーション フィルタは、アプリケーションの基本特性（タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ）にしたがってアプリケーションを整理することで、アプリケーション制御に役立ちます。オブジェクト マネージャで、システム提供のフィルタの組み合わせやアプリケーションの任意の組み合わせをもとに、ユーザ定義の再利用可能アプリケーション フィルタを作成、管理できます。詳細については、アプリケーション条件（アプリケーション制御）, （350 ページ）を参照してください。

VLAN タグ オブジェクト

設定した個々の VLAN タグ オブジェクトは、1 つの VLAN タグまたはタグの範囲を表します。

複数の VLAN タグ オブジェクトをグループ化できます。グループは複数のオブジェクトを表します。つまり、1 つのオブジェクトで VLAN タグの範囲を使用することは、この意味ではグループとはみなされません。

VLAN タグ オブジェクトとグループは、ルールやイベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、特定の VLAN だけに適用されるアクセス コントロール ルールを作成することができます。

VLAN タグ オブジェクトの作成

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2 オブジェクト タイプのリストから [VLAN タグ（VLAN Tag）] を選択します。

ステップ 3 [VLAN タグの追加（Add VLAN Tag）] ドロップダウン リストで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 [名前（Name）] を入力します。

ステップ 5 [説明（Description）] を入力します。

ステップ 6 [VLAN タグ（VLAN Tag）] フィールドに値を入力します。VLAN タグの範囲を指定するには、ハイフンを使用します。

ステップ 7 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可, （386 ページ） を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド（Override）] セクションを展開し、[追加（Add）] をクリックします（オブジェクトのオーバーライドの追加, （387 ページ） を参照）。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入，（320 ページ） を参照）。

URL オブジェクト

設定した各 URL オブジェクトは、単一の URL または IP アドレスを表します。URL オブジェクトとグループは、アクセス コントロール ポリシーやイベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、特定の Web サイトをブロックするアクセス コントロール ルールを作成することができます。

URL オブジェクトを作成する際に、特に暗号化トラフィックを復号またはブロックする SSL インスペクションを設定しない場合は、次の事項に留意してください。

- アクセス コントロール ルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は含めないでください。たとえば、www.example.com ではなく、example.com を使用します。
- URL 条件を含むアクセス コントロール ルールを使用して Web トラフィックを照合する場合、システムは暗号化プロトコル（HTTP 対 HTTPS）を無視します。つまり、アプリケーション条件を使用してルールを調整しない限り、Web サイトをブロックすると、その Web サイトへの HTTP と HTTPS の両方のトラフィックがブロックされます。URL オブジェクトを作成する場合は、オブジェクトの作成時にプロトコルを指定する必要はありません。たとえば、`http://example.com/` ではなく、`example.com` を使用します。

URL オブジェクトの作成

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 オブジェクト タイプのリストから [URL] を選択します。

ステップ 3 [URL の追加（Add URL）] ドロップダウン リストで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 名前を入力します。
マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 必要に応じて、[説明（Description）] を入力します。

ステップ 6 [URL] に、URL または IP アドレスを入力します。

ステップ 7 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可, （386 ページ） を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド（Override）]セクションを展開し、[追加（Add）] をクリックします（オブジェクトのオーバーライドの追加, （387 ページ） を参照）。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入, （320 ページ） を参照）。

地理位置情報オブジェクト

設定済みの位置情報（ジオロケーション）オブジェクトは、モニタ対象ネットワーク上のトラフィックの送信元または宛先としてシステムで識別された 1 つ以上の国または大陸を表します。アクセス コントロール ポリシー、SSL ポリシー、イベント検索など、システムの Web インターフェイスのさまざまな場所で地理位置情報オブジェクトを使用できます。たとえば、特定の国が送信元/宛先であるトラフィックをブロックするアクセス コントロール ルールを作成できます。

常に最新の情報を使用してネットワーク トラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

地理位置情報オブジェクトの作成

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 オブジェクト タイプのリストから [地理位置情報（Geolocation）] を選択します。

ステップ 3 [位置情報の追加（Add Geolocation）] をクリックします。

ステップ 4 名前を入力します。
マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 地理位置情報オブジェクトに含める国および大陸のチェック ボックスを選択します。大陸を選択すると、その大陸内のすべての国、およびGeoDB 更新によってその大陸に今後追加されるすべての国が選択されます。大陸の下でいずれかの国を選択解除すると、その大陸が選択解除されます。国と大陸を任意に組み合わせて選択できます。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入, （320 ページ） を参照）。

変数セット

変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーで変数を使用して、ルール抑制、アダプティブ プロファイル、および動的（ダイナミック）ルール状態で IP アドレスを表すこともできます。

ヒント プリプロセッサ ルールは、侵入ルールで使用されるネットワーク変数で定義されたホストにかかわらず、イベントをトリガーできます。

変数セットを使用して、変数を管理、カスタマイズ、およびグループ化します。システム提供のデフォルトの変数セットを使用することも、独自のカスタム セットを作成することもできます。いずれのセット内でも、定義済みのデフォルト変数を変更したり、ユーザ定義変数を追加および変更したりできます。

Firepower システムで提供する共有オブジェクト ルールと標準テキスト ルールのほとんどで、定義済みのデフォルト変数を使用してネットワークとポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 `$HOME_NET` を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 `$EXTERNAL_NET` を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Web サーバに対するエクスプロイトを検出するルールは、`$HTTP_SERVERS` 変数および `$HTTP_PORTS` 変数を使用します。

ルールがより効率的なのは、変数がユーザのネットワーク環境をより正確に反映する場合です。少なくとも、デフォルト セットにあるデフォルト変数は変更する必要があります。`$HOME_NET` などの変数がネットワークを正しく定義し、`$HTTP_SERVERS` にネットワーク上のすべての Web サーバが含まれていれば、処理は最適化され、疑わしいアクティビティがないかどうかすべての関連システムがモニタされます。

変数を使用するには、変数セットをアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに関連付けられている侵入ポリシーにリンクします。デフォルトでは、デフォルトの変数セットは、アクセスコントロールポリシーによって使用されるすべての侵入ポリシーにリンクされています。

変数を任意のセットに追加すると、それはすべてのセットに追加されます。つまり、各変数セットは、システムで現在設定されているすべての変数のコレクションになります。どの変数セット内でも、ユーザ定義変数を追加し、任意の変数の値をカスタマイズすることができます。

Firepower システムでは、初めに定義済みのデフォルト値で構成された単一のデフォルトの変数セットを提供します。デフォルト セット内の各変数は、最初はそのデフォルト値に設定されています。定義済みの変数の場合、このデフォルト値は Cisco Talos Security Intelligence and Research Group（Talos） によって設定され、ルール更新で提供される値です。

定義済みのデフォルト変数は、そのデフォルト値に設定されたままにすることもできますが、定義済みの変数のサブセットを変更することを推奨します。

変数はデフォルトセットでのみ使用できますが、多くの場合、1つ以上のカスタム設定を追加し、異なるセットで異なる変数の値を設定し、場合によっては新しい変数を追加することによって、最大限に活用できます。

複数のセットを使用する場合は、デフォルトのセットにある任意の変数の現在値によって、他のすべてのセットの変数のデフォルト値が決まることに注意してください。

[オブジェクト マネージャ（Object Manager）] ページで [変数セット（Variable Sets）] を選択した場合、オブジェクト マネージャには、デフォルトの変数セットと、作成したすべてのカスタム セットがリストされます。

新しくインストールされたシステムでは、デフォルトの変数セットは、Cisco で定義済みのデフォルト変数だけで構成されています。

各変数セットには、システムによって提供されるデフォルト変数と、任意の変数セットから追加したすべてのカスタム変数が含まれます。デフォルト設定は編集できますが、デフォルト セットの名前を変更したり、削除したりすることはできないことに注意してください。

マルチドメイン展開では、システムはサブドメインごとにデフォルトの変数セットを生成します。

注意 アクセス コントロールまたは侵入ポリシーをインポートすると、デフォルトの変数セットにある既存のデフォルト変数が、インポートされたデフォルト変数でオーバーライドされます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。

関連トピック

変数の管理, （414 ページ）
変数セットの管理, （412 ページ）

侵入ポリシー内の変数セット

Firepower システムは、デフォルトではアクセス コントロール ポリシーで使用されるすべての侵入ポリシーにデフォルトの変数セットをリンクします。侵入ポリシーを使用するアクセス コントロール ポリシーを展開すると、その侵入ポリシー内で有効にした侵入ルールでは、リンクされた変数セットの変数値が使用されます。

アクセス コントロール ポリシー内の侵入ポリシーで使用されるカスタム変数セットを変更すると、システムの [アクセス コントロール ポリシー（Access Control Policy）] ページで、そのポリシーのステータスが「失効（out-of-date）」と表示されます。変数セットの変更内容を実装するには、アクセス コントロール ポリシーを再度展開する必要があります。デフォルト セットを変更すると、侵入ポリシーを使用するすべてのアクセス コントロール ポリシーのステータスが「失効（out-of-date）」と表示され、変更内容を実装するにはすべてのアクセス コントロール ポリシーを再度展開する必要があります。

変数

変数は、次のカテゴリのいずれかに属します。

デフォルト変数

Firepower システムから提供される変数。デフォルト変数の名前変更または削除はできません。また、デフォルト値を変更することもできません。ただし、デフォルト変数のカスタマイズしたバージョンを作成できます。

カスタマイズされた変数

作成した変数。この変数には、次の変数があります。

- カスタマイズされたデフォルト変数

  デフォルト変数の値を編集すると、システムはその変数を [デフォルトの変数（Default Variables）] 領域から [カスタマイズされた変数（Customized Variables）] 領域に移動します。デフォルト セットの変数値によってカスタム セットの変数のデフォルト値が決まるため、デフォルト セットのデフォルト変数をカスタマイズすると、他のすべてのセットの変数のデフォルト値が変更されます。

- ユーザ定義変数

  独自の変数を追加および削除したり、異なる変数セット内の値をカスタマイズしたり、カスタマイズされた変数をそのデフォルト値にリセットしたりできます。ユーザ定義変数をリセットすると、それは [カスタマイズされた変数（Customized Variables）] 領域に残ります。

  ユーザ定義変数は、次のいずれかのタイプにできます。

  - ネットワーク変数は、ネットワーク トラフィックのホストの IP アドレスを指定します。
  - ポート 変数は、ネットワーク トラフィックの TCP または UDP ポートを指定するもので、いずれかのタイプを意味する値 `any` を指定することもできます。

たとえば、カスタム標準テキスト ルールを作成する場合、独自のユーザ定義変数を追加して、トラフィックをより正確に反映したり、ショートカットとしてルール作成プロセスを単純化したりすることもできます。また、「緩衝地帯」（つまり DMZ）でのみトラフィックを検査するルールを作成する場合、公開されているサーバの IP アドレスが値にリストされる `$DMZ` という変数を作成することもできます。こうして、この地帯で作成された任意のルールで `$DMZ` 変数を使用できます。

拡張変数

特定の条件下で Firepower システムから提供される変数。この変数が含まれる展開は非常に限定的です。

定義済みデフォルト変数

デフォルトでは、Firepower System は、1 つのデフォルト変数セットを提供します。このセットは、定義済みのデフォルト変数から構成されています。Cisco Talos Security Intelligence and Research Group（Talos） では、ルール更新を使用し、新しい侵入ルールや更新された侵入ルール、他の侵入ポリシー エレメント（デフォルト変数など）を提供します。

システムが提供する侵入ルールの多くが定義済みのデフォルト変数を使用していることから、これらの変数に関する適切な値を設定します。変数セットを使用してネットワーク上のトラフィックを特定する方法によっては、任意またはすべての変数セットにあるこれらのデフォルト変数の値を変更できます。

注意 アクセス コントロールまたは侵入ポリシーをインポートすると、デフォルトの変数セットにある既存のデフォルト変数が、インポートされたデフォルト変数でオーバーライドされます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。

次の表では、システムによって提供される変数について説明し、通常、いずれの変数が変更されるかを示します。変数をご使用のネットワークに合わせて調整する方法を決定するには、プロフェッショナル サービスまたはサポートに問い合わせてください。

表 *43*：システム提供変数

変数名	説明	変更しますか
$AIM_SERVERS	既知の AOL インスタント メッセンジャ（AIM）サーバを定義し、これらはチャット ベースのルールや AIM エクスプロイトを検索するルールで使用されます。	不要。
$DNS_SERVERS	ドメイン ネーム サービス（DNS）サーバを定義します。DNS サーバに特に影響するルールを作成する場合、$DNS_SERVERS 変数を宛先または送信元 IP アドレスとして使用できます。	現在のルール セットでは不要です。
$EXTERNAL_NET	Firepower System が非保護ネットワークとして表示されるネットワークを定義し、外部ネットワークを定義する多くのルールで使用されます。	はい。$HOME_NET を適切に定義してから、$EXTERNAL_NET の値として $HOME_NET を除外する必要があります。
$FILE_DATA_PORTS	ネットワーク ストリームでファイルを検出する侵入ルールで使用される非暗号化ポートを定義します。	不要。
$FTP_PORTS	ネットワーク上の FTP サーバのポートを定義し、FTP サーバのエクスプロイト ルールに使用されます。	はい。FTP サーバがデフォルト ポート以外のポートを使用する場合（web インターフェイスのデフォルト ポートを表示できます）。
$GTP_PORTS	パケット デコーダが GTP（General Packet Radio Service（GPRS）トンネリング プロトコル）PDU 内部でペイロードを取得するデータ チャネル ポートを定義します。	不要。
$HOME_NET	関連した侵入ポリシーがモニタするネットワークを定義し、内部ネットワークを定義するために多くのルールで使用されます。	内部ネットワークの IP アドレスを指定する場合は変更します。
$HTTP_PORTS	ネットワーク上の Web サーバのポートを定義し、Web サーバのエクスプロイト ルールに使用されます。	はい。web サーバがデフォルト ポート以外のポートを使用する場合（web インターフェイスのデフォルト ポートを表示できます）。
$HTTP_SERVERS	ネットワーク上の Web サーバを定義します。Web サーバのエクスプロイト ルールで使用されます。	HTTP サーバを実行する場合は変更します。
$ORACLE_PORTS	ネットワーク上で Oracle データベース サーバのポートを定義し、Oracle データベースでの攻撃をスキャンするルールで使用されます。	Oracle サーバを実行する場合は変更します。

変数名	説明	変更しますか
$SHELLCODE_PORTS	システムにシェル コードのエクスプロイトをスキャンさせるポートを定義し、シェル コードを使用するエクスプロイトを検出するルールで使用されます。	不要。
$SIP_PORTS	ネットワーク上の SIP サーバのポートを定義し、SIP のエクスプロイト ルールに使用されます。	不要。
$SIP_SERVERS	ネットワーク上の SIP サーバを定義し、SIP 対象エクスプロイトを指定するルールで使用されます。	はい。SIP サーバを実行している場合は、$HOME_NET を適切に定義してから、$SIP_SERVERS の値として $HOME_NET を含める必要があります。
$SMTP_SERVERS	ネットワーク上でSMTPサーバを定義し、メール サーバをターゲットとするエクスプロイトを解決するルールで使用されます。	SMTPサーバを実行する場合は変更します。
$SNMP_SERVERS	ネットワーク上でSNMPサーバを定義し、SNMPサーバでの攻撃をスキャンするルールで使用されます。	SNMPサーバを実行する場合は変更します。
$SNORT_BPF	その後バージョン5.3.0以降にアップグレードされるバージョン5.3.0以前のFirepower Systemソフトウェア リリースのシステム上に存在する場合のみに表示されるレガシー拡張変数を特定します。	変更しません。この変数は表示または削除のみが可能です。削除後に、編集または復元することはできません。
$SQL_SERVERS	ネットワーク上のデータベース サーバを定義し、データベース対象エクスプロイトを指定するルールで使用されます。	はい。SQLサーバを実行する場合は変更します。
$SSH_PORTS	ネットワーク上のSSHサーバのポートを定義し、SSHサーバのエクスプロイト ルールに使用されます。	はい。デフォルト ポート以外の SSH サーバのポートを使用する場合（webインターフェイスでのデフォルト ポートを表示できます）。
$SSH_SERVERS	ネットワーク上のSSHサーバを定義し、SSH対象エクスプロイトを指定するルールで使用されます。	はい。SSHサーバを実行している場合は、$HOME_NET を適切に定義してから、$SSH_SERVERS の値として $HOME_NET を含める必要があります。
$TELNET_SERVERS	ネットワーク上の既知の Telnet サーバを定義し、Telnet サーバ対象エクスプロイトを指定するルールで使用されます。	Telnet サーバを実行する場合は変更します。
$USER_CONF		

変数名	説明	変更しますか
	Web インターフェイスを介して利用可能できる場合を除き、1 つ以上の特徴を設定できる一般的なツールを提供します。 `$USER_CONF` の設定が競合または重複していると、システムは停止します。	機能の説明で指示されている場合や、サポートによる指示があった場合を除き、変更しません。

ネットワーク変数

ネットワーク変数で表される IP アドレスを、侵入ポリシーで有効にした侵入ルール、侵入ポリシー ルール抑制、動的ルール状態、およびアダプティブ プロファイルで使用することができます。ネットワーク変数とネットワーク オブジェクトおよびネットワーク オブジェクト グループとの相違点として、ネットワーク変数は侵入ポリシーおよび侵入ルールに固有のものです。一方、ネットワーク オブジェクトおよびグループを使用すると、アクセス コントロール ポリシー、ネットワーク変数、侵入ルール、ネットワーク検出ルール、イベント検索、レポートなど、システムの Web インターフェイスのさまざまな場所で IP アドレスを表すことができます。

次の設定でネットワーク変数を使用して、ネットワーク上のホストの IP アドレスを指定できます。

- 侵入ルール：侵入ルールの [送信元 IP（Source IPs）] および [宛先 IP（Destination IPs）] 見出しフィールドを使用すると、パケット インスペクションを、特定の送信元または宛先 IP アドレスを持つパケットに制限することができます。
- 抑制：送信元または宛先の侵入ルール抑制の [ネットワーク（Network）] フィールドを使用すると、特定の 1 つの IP アドレスまたは IP アドレス範囲が侵入ルールやプリプロセッサをトリガーした場合の侵入イベント通知を抑制できます。
- 動的ルール状態：送信元または宛先の動的ルール状態の [ネットワーク（Network）] フィールドを使用すると、指定時間内に発生した侵入ルールやプリプロセッサ ルールの一致数が多すぎる場合に、それを検出できます。
- アダプティブ プロファイル：アダプティブ プロファイルの [ネットワーク（Networks）] フィールドに、パッシブ展開でパケット フラグメントおよび TCP ストリームのリアセンブルを改善する必要があるホストが示されます。

このセクションで示されるフィールドで変数を使用する場合、侵入ポリシーにリンクされた変数セットは、侵入ポリシーを使用するアクセス コントロール ポリシーで処理されるネットワーク トラフィックでの変数値を決定します。

次のネットワーク設定を任意に組み合わせて変数に追加できます。

- 使用可能なネットワーク リストから選択したネットワーク変数、ネットワーク オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせ
- [新規変数（New Variable）] または [変数の編集（Edit Variable）] ページから追加した個々のネットワーク オブジェクト（独自の変数や、他の既存の変数、さらに今後の変数にこれらを追加できます）

- リテラルの単一 IP アドレスまたはアドレス ブロック

  それぞれを個別に追加することにより、複数のリテラル IP アドレスとアドレス ブロックをリストできます。IPv4 および IPv6 アドレスとアドレス ブロックを単独で、または任意に組み合わせてリストできます。IPv6 アドレスを指定するときには、RFC 4291 で定義された任意のアドレス指定規則を使用できます。

追加する変数での包含ネットワークのデフォルト値は `any` で、これは任意の IPv4 または IPv6 アドレスを示します。除外ネットワークのデフォルト値は `none` です。これは「ネットワークなし」を意味します。また、リテラル値の中でアドレス `::` を指定すると、包含ネットワーク リストで任意の IPv6 アドレスを指定でき、除外リストでは IPv6 アドレスなしを指定できます。

除外リストにネットワークを追加すると、指定されたアドレスおよびアドレス ブロックが除外されます。つまり、除外された IP アドレスやアドレス ブロックを除き、任意の IP アドレスに一致させることができます。

たとえば、リテラル アドレス `192.168.1.1` を除外すると 192.168.1.1 以外の任意の IP アドレスが指定され、`2001:db8:ca2e::fa4c` を除外すると 2001:db8:ca2e::fa4c 以外の任意の IP アドレスが指定されます。

リテラル ネットワークまたは使用可能なネットワークを任意に組み合わせて、除外で使用できます。たとえば、リテラル値 `192.168.1.1` および `192.168.1.5` を除外すると、192.168.1.1 と 192.168.1.5 以外の任意の IP アドレスが含まれます。つまり、システムはこの構文を「192.168.1.1 **でなく、しかも** 192.168.1.5 **でない**」と解釈し、大カッコ内に列挙されたものを除くすべての IP アドレスに一致させます。

ネットワーク変数を追加または編集するときには、次の点に注意してください。

- 論理的に言って、値 `any` を除外することはできません。any を除外すると「アドレスなし」を意味することになります。たとえば、除外ネットワーク リストに、値 `any` を持つ変数を追加することはできません。
- ネットワーク変数は、指定された侵入ルールおよび侵入ポリシー機能に関するトラフィックを識別します。プリプロセッサ ルールは、侵入ルールで使われているネットワーク変数で定義されたホストとは無関係に、イベントをトリガーできることに注意してください。
- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、アドレス ブロック 192.168.5.0/24 を包含し、192.168.6.0/24 を除外することはできません。

ポート変数

ポート変数は、侵入ポリシーで有効になった侵入ルールの [送信元ポート（Source Port）] および [宛先ポート（Destination Port）] ヘッダー フィールドで使用できる TCP ポートと UDP ポートを表します。ポート変数とポート オブジェクトおよびポート オブジェクト グループとの相違点は、ポート変数が侵入ルール固有のものであることです。TCP や UDP 以外のプロトコル用にポート オブジェクトを作成して、ポート変数、アクセス コントロール ポリシー、ネットワーク検出ルール、イベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。

侵入ルールの [送信元ポート（Source Port）] および [宛先ポート（Destination Port）] ヘッダー フィールドでポート変数を使用すると、パケット インスペクションを特定の送信元または宛先 TCP/UDP ポートを持つパケットに制限することができます。

これらのフィールドで変数を使用した場合、アクセス コントロール ルールまたはポリシーに関連付けられた侵入ポリシーにリンクされる変数セットは、アクセス コントロール ポリシーが展開されるネットワーク トラフィックでのこれらの変数の値を決定します。

次のポート設定を任意に組み合わせて変数に追加できます。

- 使用可能なポート リストから選択したポート変数およびポート オブジェクトの任意の組み合わせ

  使用可能なポート リストには、ポート オブジェクト グループが表示されず、したがってこれらを変数に追加できないことに注意してください。

- [新規変数（New Variable）] または [変数の編集（Edit Variable）] ページから追加した個々のポート オブジェクト（独自の変数や、他の既存の変数、さらに今後の変数にこれらを追加できます）

  有効な変数値は TCP および UDP ポートのみです（どちらのタイプでも値 `any` を含む）。新しい変数のページまたは変数の編集ページを使用して、有効な変数値ではない有効なポート オブジェクトを追加した場合、オブジェクトはシステムに追加されますが、使用可能なオブジェクト リストには表示されません。オブジェクト マネージャを使用して、変数で使われるポート オブジェクトを編集する場合、有効な変数値にのみ値を変更できます。

- 単一のリテラル ポート値とポート範囲

  ポート範囲はダッシュ（-）を使って区切る必要があります。下位互換性のために、コロンで指定されるポート範囲もサポートされていますが、作成するポート変数ではコロンを使用できません。

  複数のリテラル ポートの値および範囲をリストするには、それぞれを個別に追加して任意に組み合わせることができます。

ポート変数を追加または編集するときには、次の点に注意してください。

- 追加する変数での包含ポートのデフォルト値は `any` で、これは任意のポートまたはポート範囲を示します。除外ポートのデフォルト値は `none` で、これは「ポートなし」を示します。

  ヒント 値 `any` を持つ変数を作成するには、特定の値を追加せずに変数に名前を付けて保存します。

- 論理的に言って、値 `any` を除外することはできません。any を除外すると「ポートなし」を意味することになります。たとえば、値 `any` を持つ変数を除外ポート リストに追加した場合、変数セットを保存することはできません。

- 除外リストにポートを追加すると、指定されたポートおよびポート範囲が除外されます。つまり、除外されたポートまたはポート範囲を除き、任意のポートに一致させることができます。

- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、ポート範囲 10 から 50 を包含し、ポート 60 を除外することはできません。

拡張変数

拡張変数を使用すると、他の方法では Web インターフェイスで設定できない機能を設定することができます。現在、Firepower システムで使用可能な拡張変数は 2 つのみで、そのうち USER_CONF 拡張変数のみ編集可能です。

USER_CONF

USER_CONF は、Web インターフェイスで通常設定できない 1 つ以上の機能を設定するための汎用ツールです。

注意 機能の説明またはサポート担当の指示に従う場合を除き、拡張変数 USER_CONF を使用して侵入ポリシー機能を設定**しないで**ください。競合または重複する設定が存在すると、システムが停止します。

USER_CONF を編集するときには、1 行に合計 4096 文字まで入力できます。行は自動的に折り返します。変数の最大長 8192 文字、またはディスク スペースなどの物理制限に達するまで、任意の数の有効な指示または行数を含めることができます。コマンド ディレクティブでは、完全な引数の後にバックスラッシュ（\）行連結文字を使用します。

USER_CONF をリセットすると、空になります。

SNORT_BPF

SNORT_BPF はレガシー拡張変数です。バージョン 5.3.0 以降にアップグレードされる前の旧バージョンの Firepower システム ソフトウェア リリースのときにシステムでこの変数が設定された場合にのみ、これが表示されます。この変数は表示または削除のみが可能です。削除後に、編集または復元することはできません。

この変数を使用すると、Berkeley Packet Filter（BPF）を適用して、システムに到達する前のトラフィックをフィルタできました。SNORT_BPF に備わっていたフィルタリング機能を今後も適用するには、この変数の代わりにアクセス コントロール ルールを使用してください。この変数は、システム アップグレード前に存在していた設定でのみ表示されます。

変数のリセット

変数セットの新しい変数ページまたは変数の編集ページで、変数をデフォルト値にリセットできます。次の表に、変数をリセットするときの基本原則を要約します。

表 *44*：変数のリセット値

リセットする変数のタイプ	それが含まれるセットタイプ	リセット後の値
デフォルト	デフォルト	ルール更新値
ユーザ定義	デフォルト	任意
デフォルトまたはユーザ定義	カスタム	現在のデフォルト セット値（変更/未変更にかかわらず）

カスタムセットの変数をリセットすると、単にデフォルトセット内のその変数の現在値にリセットされます。

逆に、デフォルトセットの変数の値をリセットまたは変更すると、すべてのカスタムセット内のその変数のデフォルト値が常に更新されます。リセット アイコンがグレー表示され、その変数をリセットできないことを示している場合、そのセットでは変数のカスタマイズ値が存在しないことを意味します。カスタム セット内の変数の値をすでにカスタマイズした場合を除き、デフォルト セットの変数を変更すると、変数セットがリンクされた侵入ポリシーで使われている値が更新されます。

（注） デフォルトセット内の変数を変更するときには、その変更により、リンクされたカスタムセットの変数を使用する侵入ポリシーがどのような影響を受けるか評価するのが適切です（特に、カスタム セット内の変数値をカスタマイズしていない場合）。

変数セット内のリセットアイコン（）の上にポインタを置くと、リセット値を確認できます。カスタマイズされた値とリセット値が同じである場合は、次のいずれかを示しています。

- カスタム セットまたはデフォルト セットの中で、値 any を持つ変数を追加した
- カスタムセットの中で、明示的な値を持つ変数を追加し、設定した値をデフォルト値として使用することを選択した

セットに変数を追加する

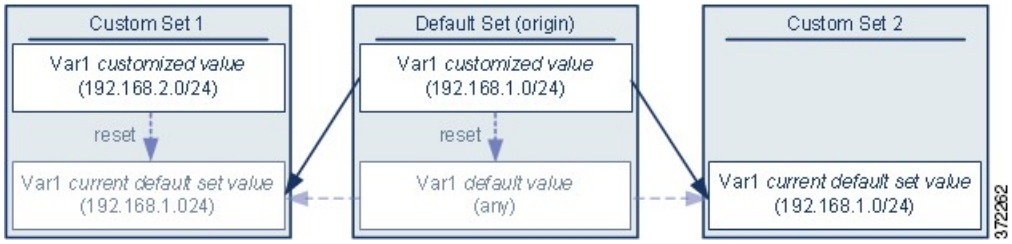
変数セットに変数を追加すると、他のすべてのセットにもその変数が追加されます。カスタム セットから変数を追加する場合は、設定値をデフォルト セットのカスタマイズ値として使用するかどうかを選択する必要があります。

- 設定値（たとえば、192.168.0.0/16）を**使用する**場合、変数は、デフォルト値 any を持つカスタマイズ値として設定値を使用するデフォルト セットに追加されます。デフォルト セットの現在の値によって他のセットのデフォルト値が決まるため、他のカスタムセットの初期のデフォルト値は設定値（この例では 192.168.0.0/16）になります。

- 設定値を**使用しない**場合、変数はデフォルト値 `any` のみを使用してデフォルト セットに追加され、こうして、他のカスタム セットの初期のデフォルト値は `any` になります。

例：デフォルト セットへのユーザ定義変数の追加

次の図は、値が `192.168.1.0/24` のデフォルト セットにユーザ定義の変数 `Var1` を追加した場合のセットのインタラクションを示しています。



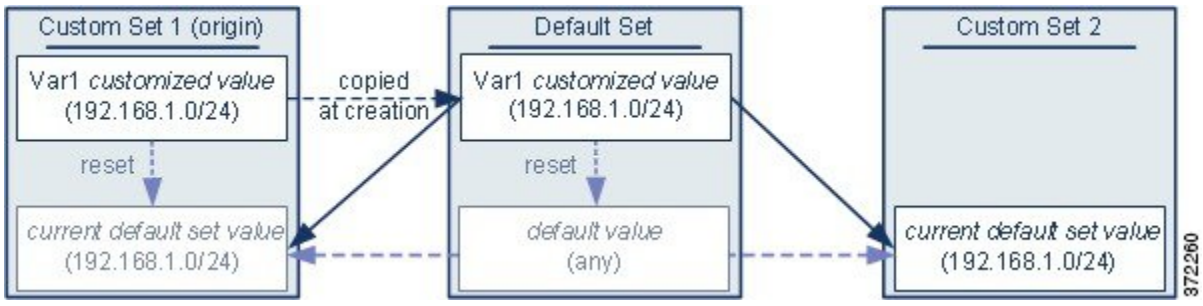
任意のセットで `Var1` の値をカスタマイズできます。`Var1` がカスタマイズされていない Custom Set 2 では、この値は `192.168.1.0/24` です。Custom Set 1 では、`Var1` のカスタマイズ値 `192.168.2.0/24` はデフォルト値をオーバーライドします。デフォルト セットのユーザ定義変数をリセットすると、すべてのセットのそのデフォルト値が `any` にリセットされます。

この例では、Custom Set 2 で `Var1` を更新しなかった場合、デフォルト セットで `Var1` をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 `Var1` が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

この例では示されていませんが、セット間のインタラクションは、デフォルト セットのデフォルト変数をリセットすると現在のルール更新で Cisco によって設定された値に、そのデフォルト変数がリセットされること以外は、ユーザ定義変数およびデフォルト変数で同じであることに注意してください。

例：カスタム セットへのユーザ定義変数の追加

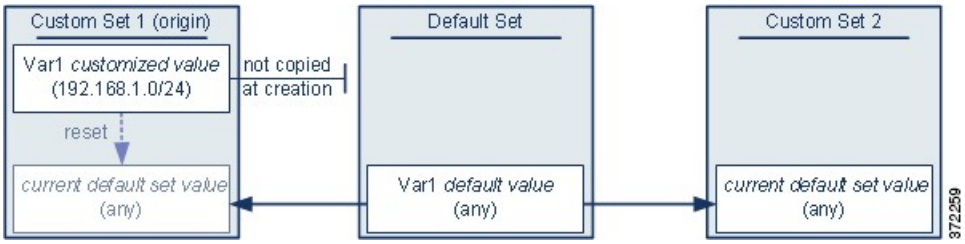
次の 2 つの例は、カスタム セットにユーザ定義変数を追加した場合の変数セットのインタラクションについて示しています。新しい変数を保存すると、設定値を他のセットのデフォルト値として使用するかどうかを尋ねるプロンプトが出されます。次の例では、設定値を**使用する**という選択がなされています。



Custom Set 1 からの `Var1` の発信元を除き、この例は `Var1` をデフォルト セットに追加した上述の例と同じであることに注意してください。`Var1` のカスタマイズ値 `192.168.1.0/24` を Custom Set 1

に追加すると、値はデフォルト値 any を持つカスタマイズ値としてデフォルト セットにコピーされます。その後、Var1 の値とインタラクションは、Var1 をデフォルトセットに追加した場合と同じになります。前述の例と同様、デフォルト セットで Var1 をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 Var1 が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

次の例では、前述の例にあるように値が 192.168.1.0/24 の Var1 を Custom Set 1 に追加しますが、Var1 の設定値を他のセットのデフォルト値として**使用しない**ことを選択します。



このアプローチでは、Var1 をデフォルト値 any を持つすべてのセットに追加します。Var1 を追加したら、任意のセットでその値をカスタマイズできます。このアプローチの利点は、デフォルトセットでVar1 を最初にカスタマイズしないことによって、デフォルトセットの値をカスタマイズし、Var1 をカスタマイズしていない Custom Set 2 などのセット内の現在の値を意図せずに変更してしまうリスクが軽減されます。

変数のネスト

循環したネストにならない限り、変数をネストすることができます。否定形の変数をネストすることはできません。

有効なネストされた変数

以下の例では、SMTP_SERVERS、HTTP_SERVERS、OTHER_SERVERS がネストしても有効な変数です。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
SMTP_SERVERS	カスタマイズされたデフォルト	10.1.1.1	—
HTTP_SERVERS	カスタマイズされたデフォルト	10.1.1.2	—
OTHER_SERVERS	ユーザ定義	10.2.2.0/24	—
HOME_NET	カスタマイズされたデフォルト	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

無効なネストされた変数

以下の例では、HOME_NET はネストすると無効な変数です。HOME_NET をネストすると、変数の循環になるためです。つまり、OTHER_SERVERS の定義には HOME_NET が含まれるため、HOME_NET はそれ自体でネストすることになります。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
SMTP_SERVERS	カスタマイズされたデフォルト	10.1.1.1	—
HTTP_SERVERS	カスタマイズされたデフォルト	10.1.1.2	—
OTHER_SERVERS	ユーザ定義	10.2.2.0/24 HOME_NET	—
HOME_NET	カスタマイズされたデフォルト	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

ネストでサポートされない否定形の変数

否定形の変数のネストはサポートされないため、以下の例に示されているように、保護ネットワークの外部にある IP アドレスを表す変数 NONCORE_NET を使用することはできません。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
HOME_NET	カスタマイズされたデフォルト	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
EXTERNAL_NET	カスタマイズされたデフォルト	—	HOME_NET
DMZ_NET	ユーザ定義	10.4.0.0/16	—
NOT_DMZ_NET	ユーザ定義	—	DMZ_NET
NONCORE_NET	ユーザ定義	EXTERNAL_NET NOT_DMZ_NET	—

ネストでサポートされない否定形の変数の代替手段

上記の例の代替手段として、以下に示す変数NONCORE_NETを作成することで、保護ネットワークの外部にあるIPアドレスを表すことができます。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
HOME_NET	カスタマイズされたデフォルト	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
DMZ_NET	ユーザ定義	10.4.0.0/16	—
NONCORE_NET	ユーザ定義	—	HOME_NET DMZ_NET

変数セットの管理

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ2 オブジェクトタイプのリストから [変数セット（Variable Set）] を選択します。

ステップ3 変数セットを管理します。

- 追加：カスタムの変数セットを追加するには、[変数セットの追加（Add Variable Set）] をクリックします。変数セットの作成, （413 ページ）を参照してください。
- 削除：カスタムの変数セットを削除するには、変数セットの横にある削除アイコン（  ）をクリックして、[はい（Yes）]をクリックします。デフォルトの変数セットまたは先祖ドメインに属している変数セットは削除できません。

（注） 削除する変数セットで作成された変数は、別のセットで削除されたり他の方法で影響を受けることはありません。

- 編集：変数セットを編集するには、変更する変数セットの横にある編集アイコン（  ）をクリックします。オブジェクトの編集, （380 ページ）を参照してください。
- フィルタ処理：変数セットを名前でフィルタリングするには、名前の入力を開始します。入力中にページが更新され、一致する名前が表示されます。名前のフィルタリングをクリアするには、フィルタ フィールドにあるクリア アイコン（  ）をクリックします。
- 変数の管理：変数セットに含まれる変数を管理するには、変数の管理, （414 ページ）を参照してください。

変数セットの作成

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 オブジェクト タイプのリストから [変数セット（Variable Set）] を選択します。

ステップ 3 [変数セットの追加（Add Variable Set）] をクリックします。

ステップ 4 名前を入力します。
マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 必要に応じて、[説明（Description）] を入力します。

ステップ 6 セット内の変数を管理します（変数の管理, （414 ページ）を参照）。

ステップ 7 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入, （320 ページ） を参照）。

変数の管理

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 オブジェクト タイプのリストから [変数セット（Variable Set）] を選択します。

ステップ 3 編集する変数セットの横にある編集アイコン（）をクリックします。
代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 変数を管理します。

- 表示：変数の完全な値を表示するには、変数の横の [値（Value）] 列内の値にポインタを重ねます。
- 追加：変数を追加するには、[追加（Add）] をクリックします。変数の追加, （415 ページ）を参照してください。
- 削除：変数の横にある削除アイコン（）をクリックします。変数の追加後に変数セットを保存した場合は、[はい（Yes）] をクリックして、変数の削除を確認します。
  次の変数は削除できません。
  - デフォルトの変数
  - 侵入ルールや別の変数で使用されているユーザ定義変数
  - 先祖ドメインに属している変数
- 編集：編集する変数の横にある編集アイコン（）をクリックします。変数の編集, （416 ページ）を参照してください。

- リセット：変更した変数をデフォルト値にリセットするには、変更した変数の横にあるリセット アイコン（）をクリックします。リセット アイコンがグレー表示の場合は、次のいずれかが当てはまります。
  - 現在の値がすでにデフォルト値になっている。
  - 設定が先祖ドメインに属している。

ヒント アクティブなリセット アイコンの上にポインタを移動して、デフォルト値を表示します。

ステップ 5 [保存（Save）]をクリックして、変数セットを保存します。その変数セットがアクセス コントロール ポリシーで使用されている場合は、[はい（Yes）] をクリックして変更を保存することを確認します。
デフォルト セットの現在の値によって他のすべてのセットのデフォルト値が決まるため、デフォルト セットの変数を変更またはリセットすると、デフォルト値がカスタマイズされていない他のセットの現在の値が変更されます。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入，（320 ページ） を参照）。

変数の追加

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

手順

ステップ 1 変数セット エディタで、[追加（Add）] をクリックします。
ステップ 2 [名前（Name）] に一意の変数名を入力します。
ステップ 3 [タイプ（Type）] ドロップダウン リストから、[ネットワーク（Network）] または [ポート（Port）] を選択します。
ステップ 4 変数の値を指定します。

- 使用可能ネットワークまたはポートのリストの項目を包含リストまたは除外リストに移動する場合は、1つまたは複数の項目を選択してドラッグアンドドロップするか、[包含（Include）] または [除外（Exclude）] をクリックします。

  ヒント ネットワーク変数またはポート変数の包含リストと除外リストにあるアドレスやポートが重複している場合、除外されているアドレスまたはポートが優先されます。

- 1つのリテラル値を入力し、[追加（Add）] をクリックします。ネットワーク変数の場合、単一の IP アドレスまたはアドレス ブロックを入力できます。ポート変数の場合、単一ポートまたはポート範囲を追加できます。ポート範囲は上限値と下限値をハイフン（-）で区切ります。複数のリテラル値を入力する場合は、必要に応じてこの手順を繰り返します。

- 包含リストまたは除外リストから項目を削除するには、項目の横にある削除アイコン（）をクリックします。

（注） ネットワーク変数の場合、包含または除外する項目のリストは、リテラル文字列や既存の変数、オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせで構成できます。

ステップ 5 [保存（Save）] をクリックして変数を保存します。カスタム セットから新しい変数を追加する場合、次のオプションがあります。

- [はい（Yes）] をクリックすると、設定値を使用する変数がデフォルト セットのカスタマイズ値として追加され、結果として他のカスタム セットのデフォルト値として追加されます。
- [いいえ（No）] をクリックすると、変数はデフォルト セットのデフォルト値 `any` として追加され、結果として他のカスタム セットのデフォルト値として追加されます。

ステップ 6 [保存（Save）] をクリックして変数セットを保存します。変更内容が保存され、変数セットにリンクされているアクセス コントロール ポリシーに失効ステータスが表示されます。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入，（320 ページ） を参照）。

変数の編集

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

カスタム変数とデフォルト変数の両方を編集できます。

既存の変数の [名前（Name）] と [タイプ（Type）] の値は変更できません。

手順

ステップ 1 変数セット エディタで変更する変数の横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 2 変数を変更します。

- 利用可能なネットワークまたはポートのリストから、含める項目のリストまたは除外する項目のリストに項目を移動するには、1 つ以上の項目を選択してからドラッグ アンド ドロップするか、または [含める（Include）] か [除外（Exclude）] をクリックします。

  ヒント ネットワーク変数またはポート変数の包含リストと除外リストにあるアドレスやポートが重複している場合、除外されているアドレスまたはポートが優先されます。

- 1 つのリテラル値を入力し、[追加（Add）] をクリックします。ネットワーク変数の場合、単一の IP アドレスまたはアドレス ブロックを入力できます。ポート変数の場合、単一ポートまたはポート範囲を追加できます。ポート範囲は上限値と下限値をハイフン（-）で区切ります。複数のリテラル値を入力する場合は、必要に応じてこの手順を繰り返します。

- 含めるリストまたは除外リストから項目を削除するには、項目の横にある削除アイコン（  ）をクリックします。

（注） ネットワーク変数の場合、包含または除外する項目のリストは、リテラル文字列や既存の変数、オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせで構成できます。

ステップ 3 [保存（Save）] をクリックして変数を保存します。

ステップ 4 [保存（Save）] をクリックして変数セットを保存します。変数セットがアクセス コントロール ポリシーで使用されている場合、[はい（Yes）] をクリックして変更の保存を確認します。変更内容が保存され、変数セットにリンクされているアクセス コントロール ポリシーに失効ステータスが表示されます。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入，（320 ページ） を参照）。

セキュリティ インテリジェンスのリストとフィード

セキュリティ インテリジェンスのリストとフィードは、以下を収集することでトラフィックをすばやくフィルタリングするのに役立ちます。

- IP アドレスとアドレス ブロック：アクセス コントロール ポリシーでセキュリティ インテリジェンスの一部としてブラックリスト化およびホワイトリスト化するのに使用します。
- ドメイン名：DNS ポリシーでセキュリティ インテリジェンスの一部としてブラックリスト化およびホワイトリスト化するのに使用します。
- URL：アクセス コントロール ポリシーでセキュリティ インテリジェンスの一部としてブラックリスト化およびホワイトリスト化するのに使用します。また、セキュリティ インテリジェンス後に分析およびトラフィック処理フェーズが実行されるアクセス コントロール ルール ルールで、URL リストを使用することもできます。

一覧

リストは、手動で管理される静的コレクションです。

デフォルトで、アクセス コントロール ポリシーと DNS ポリシーは、セキュリティ インテリジェンスの一部としてグローバルブラックリストおよびホワイトリストを使用します。[今すぐホワイトリストに登録（Whitelist Now）] および [今すぐブラックリストに登録（Blacklist Now）] アクションを使用することで、再展開することなくセキュリティインテリジェンスリストを作成して実装できます。[今すぐブラックリストに登録（Blacklist Now）]、[今すぐホワイトリストに登録（Whitelist Now）]、およびグローバル リスト，（420 ページ）を参照してください。

カスタム リストは、フィードやグローバル リストを増補および微調整できます。ただし、カスタム リストを実装するには再展開する必要があります。

フィード

フィードは、HTTP または HTTPS で一定期間更新する動的コレクションです。

定期的に更新される Cisco Intelligence Feed を使用すると、Talos からの最新の脅威インテリジェンスに基づいてネットワーク トラフィックをフィルタリングできます。また、サード パーティのフィードを使用することもできます。あるいは、カスタム内部フィードを使用すると、複数の Firepower Management Center からなる大規模な導入で企業全体のブラックリストを簡単に保守できます。

システムがフィードを更新する際は、変更が伝搬されるまで数分かかりますが、再展開の必要はありません。システムがフィードをインターネットから更新するタイミングを厳密に制御したい場合は、そのフィードの自動更新を無効にすることができます。ただし、自動更新を行えば、最新の関連するデータであることが確実になります。

（注） システムはカスタム フィードのダウンロード時にピア SSL 証明書の検証を実行**しません**。また、システムは、証明書のバンドルまたは自己署名証明書を使用したリモート ピアの検証もサポートしていません。

リストとフィードの書式設定

各リストまたはフィードは、500MB未満の単純なテキストファイルでなければなりません。リストファイルの拡張子は.txtでなければなりません。1行につきエントリまたはコメントを1つ（IPアドレス1つ、URL 1つ、ドメイン名1つ）含めます。

ヒント 含めることができるエントリの数は、ファイルの最大サイズによって制限されます。たとえば、コメントがなくURLの長さの平均が100文字（PunycodeまたはUnicode表現と改行のパーセントを含む）のURLリストには、524万を超えるエントリを含めることができます。

DNSリストエントリ内では、ドメイン ラベルとしてアスタリスク（*）ワイルドカード文字を指定できます。その場合、すべてのラベルがワイルドカードと一致します。たとえば、`www.example.*` のエントリは `www.example.com` と `www.example.co` の両方に一致します。

ソースファイル内にコメント行を含める場合は、シャープ（#）文字で開始する必要があります。コメントが含まれるソース ファイルをアップロードすると、システムによってアップロード中にコメントが削除されます。ダウンロードするソース ファイルには、コメントを除くすべてのエントリが含まれます。

システムが破損したフィードまたは認識不能なエントリがあるフィードをダウンロードした場合、システムは古いフィードデータを引き続き使用します（これが初回のダウンロードである場合を除く）。ただし、システムがフィード内のエントリを1つでも認識できる場合、システムは認識できるエントリを使用します。

セキュリティ インテリジェンス オブジェクトのクイック リファレンス

オブジェクト タイプ（Object Type）	機能の編集	編集後に再度展開しますか?
デフォルト（カスタム入力）ホワイトリストとブラックリスト：グローバル、子孫、ドメイン固有	コンテキスト メニューを使用してエントリを追加。 オブジェクト マネージャを使用してエントリを削除。	エントリを追加後、いいえ。 エントリを削除後、はい。
カスタム ホワイトリストとブラックリスト	オブジェクト マネージャを使用して新しいリストと交換リストをアップロード。	○

オブジェクト タイプ（Object Type）	機能の編集	編集後に再度展開しますか?
システム提供インテリジェンス フィード	オブジェクト マネージャを使用して更新頻度を無効または変更。	なし
カスタム フィード	オブジェクト マネージャを使用して完全に変更。	なし
シンクホール	オブジェクト マネージャを使用して完全に変更。	○

[今すぐブラックリストに登録（Blacklist Now）]、[今すぐホワイトリストに登録（Whitelist Now）]、およびグローバル リスト

Firepower Management Center のコンテキスト メニュー（コンテキスト メニュー, （31 ページ） を参照）では、セキュリティ インテリジェンスを使って、すばやくブラックリストやホワイトリストに登録することができます。たとえば、エクスプロイトの試行に関連した侵入イベントでルーティング可能な IP アドレスのセットに気付いた場合、それらの IP アドレスを即座にブラックリストに入れることができます。変更内容が伝達されるまでに数分かかる場合がありますが、再度展開する必要はありません。

[今すぐブラックリストに登録（Blacklist Now）] と [今すぐホワイトリストに登録（Whitelist Now）] のコンテキスト メニュー オプションは、IP アドレス、URL、DNS 要求ホットスポットに使用可能です。コンテキスト メニューでブラックリストまたはホワイトリストに登録すると、選択した項目が該当するデフォルト グローバル リストに追加されます。デフォルトでは、アクセス コントロール ポリシーと DNS ポリシーがすべてのセキュリティ ゾーンに適用されるグローバル リストを使用します。ポリシーごとに、これらのリストを使用しないように選択することができます。

（注） これらのオプションは、セキュリティ インテリジェンスにのみ適用されます。セキュリティ インテリジェンスは、すでにファースト パスされたトラフィックをブラックリストに登録することはできません。同様に、セキュリティ インテリジェンスでホワイトリストに登録しても、それに一致するトラフィックが自動的に信頼されることもファースト パスされることもありません。詳細については、セキュリティ インテリジェンスについて, （831 ページ）を参照してください。

コンテキスト メニュー オプション	対象項目	対象グローバル リスト
[今すぐブラックリストに追加（Blacklist Now）] [今すぐホワイトリストに追加（Whitelist Now）]	IP アドレス	[グローバル ブラックリスト（Global Blacklist）] [グローバル ホワイトリスト（Global Whitelist）]

コンテキスト メニュー オプション	対象項目	対象グローバル リスト
[今すぐ URL に HTTP/S 接続をブラックリストする（Blacklist HTTP/S Connections to URL Now）] [今すぐ URL に HTTP/S 接続をホワイトリストする（Whitelist HTTP/S Connections to URL Now）]	URL	[URL グローバル ブラックリスト（Global Blacklist for URL）] [URL グローバル ホワイトリスト（Global Whitelist for URL）]
[今すぐドメインに HTTP/S 接続をブラックリストする（Blacklist HTTP/S Connections to Domain Now）] [今すぐドメインに HTTP/S 接続をホワイトリストする（Whitelist HTTP/S Connections to Domain Now）]	ドメイン全体	[URL グローバル ブラックリスト（Global Blacklist for URL）] [URL グローバル ホワイトリスト（Global Whitelist for URL）]
[今すぐドメインに DNS 要求をブラックリストする（Blacklist DNS Requests to Domain Now）] [今すぐドメインに DNS 要求をホワイトリストする（Whitelist DNS Requests to Domain Now）]	ドメイン全体の DNS 要求	[DNS グローバル ブラックリスト（Global Blacklist for DNS）] [DNS グローバル ホワイトリスト（Global Whitelist for DNS）]

マルチドメイン展開では、グローバル リストだけでなくドメイン リストにも項目を登録することで、ブラックリストやホワイトリストを適用する Firepower システム ドメインを選択することができます。セキュリティ インテリジェンス リストとマルチテナンシー, （421 ページ）を参照してください。

セキュリティ インテリジェンス リストにエントリを追加すると、アクセス制御に影響が出るため、次のうちいずれか 1 つが必須です。

- 管理者（Administrator）アクセス
- デフォルト ロールの組み合わせ：ネットワーク管理者（Network Admin）またはアクセス管理者（Access Admin）に加えてセキュリティ アナリスト（Security Analyst）およびセキュリティ承認者（Security Approver）
- アクセス コントロール ポリシーの変更（Modify Access Control Policy）と設定をデバイスに展開（Deploy Configuration to Devices）の両方のアクセス許可を持つカスタム ロール。

セキュリティ インテリジェンス リストとマルチテナンシー

マルチドメイン展開では、グローバル ドメインは、グローバルなブラックリストとホワイトリストを所有しています。グローバル リストに対して項目を追加または削除できるのは、グローバル

管理者のみです。サブドメイン ユーザがネットワーク、ドメイン名、および URL をホワイトリストとブラックリストに追加できるように、マルチテナンシーでは次のものが追加されます。

- ドメイン リスト：コンテンツが特定のサブドメインにのみ適用されるホワイトリストまたはブラックリスト。グローバル リストは、グローバル ドメインのドメイン リストです。
- 子孫ドメイン リスト：現在のドメインの子孫のドメイン リストを集約するホワイトリストまたはブラックリスト。

ドメイン リスト

グローバル リストに（編集ではなく）アクセスできることに加えて、各サブドメインには独自の名前付きリストがあり、そのコンテンツはそのサブドメインにのみ適用されます。たとえば、Company A という名前のサブドメインは、次のリストを所有するとします。

- ドメイン ブラックリスト - Company A およびドメイン ホワイトリスト - Company A
- DNS のドメイン ブラックリスト - Company A、および DNS のドメイン ホワイトリスト - Company A
- URL のドメイン ブラックリスト - Company A、および URL のドメイン ホワイトリスト - Company A

現在のドメインより上位の管理者は、これらのリストに入力できます。コンテキスト メニューを使用して、現在のドメインとすべての子孫ドメインの項目をブラックリストまたはホワイトリストに追加できます。ただし、ドメイン リストから項目を削除できるのは、関連付けられたドメインの管理者のみです。

たとえば、グローバル管理者はグローバル ドメインと Company A のドメインの同じ IP アドレスをブラックリストに追加できますが、それを Company B のドメインのブラックリストには追加できません。このアクションにより、同じ IP アドレスが次のリストに追加されます。

- （グローバル管理者のみが削除できる）グローバル ブラックリスト
- （Company A の管理者のみが削除できる）ドメインブラックリスト- Company A

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

子孫ドメイン リスト

子孫ドメインリストは、現在のドメインの子孫のドメインリストを集約するホワイトリストまたはブラックリストです。リーフ ドメインには、子孫ドメイン リストはありません。

子孫ドメインリストが便利なのは、上位レベルのドメインの管理者が一般的なセキュリティインテリジェンス設定を適用できる一方で、サブドメイン ユーザは独自の展開で項目をブラックリストやホワイトリストに追加できるためです。

たとえば、グローバル ドメインには、次の子孫ドメイン リストがあります。

- 子孫ブラックリスト - グローバルおよび子孫のホワイトリスト - グローバル

- URL の子孫ブラックリスト - グローバル、および子孫の URL のホワイトリスト - グローバル
- URL の子孫ブラックリスト - グローバル、および子孫の URL のホワイトリスト - グローバル

（注） 子孫ドメイン リストは、手動で入力されたリストではなく象徴的な集約であるため、オブジェクト マネージャには表示されません。それを使用できる場所、つまり、アクセス コントロール ポリシーと DNS ポリシーに表示されます。

セキュリティ インテリジェンス フィードの更新頻度の変更

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

システムが提供するフィードは削除できませんが、更新頻度を変更（または無効に設定）できます。デフォルトで、フィードは 2 時間ごとに更新されます。

マルチドメイン展開では、システムが提供するフィードはグローバルドメインに属し、このドメインの管理者のみが変更できます。ユーザは、各自が使用するドメインに属するカスタムフィードの更新頻度を更新できます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、更新頻度を変更するフィードのタイプを選択します。

ステップ 3 更新するフィードの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [更新頻度（Update Frequency）] を編集します。

ステップ 5 [保存（Save）] をクリックします。

カスタム セキュリティ インテリジェンス フィード

カスタムまたはサードパーティのセキュリティ インテリジェンス フィードを使用すると、インターネット上で定期的に更新される他の信頼できるホワイトリストおよびブラックリストによっ

て、システムが提供するインテリジェンス フィードを拡張することができます。内部フィードをセットアップすることもできます。これは、1 つのソース リストを使用して導入環境で複数の Firepower Management Center を更新する場合に役立ちます。

（注） セキュリティ インテリジェンス フィードでは、/0 ネットマスクを使ってアドレス ブロックをホワイトリスト登録またはブラックリスト登録することはできません。ポリシーですべてのトラフィックをモニタまたはブロックする場合は、[モニタ（Monitor）]または[ブロック（Block）] ルール アクションを含むアクセス コントロール ルールを使用し、デフォルト値 any を [送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] それぞれに設定します。

フィードを設定する場合は、URL を使用して場所を指定します。この URL は Punycode によりエンコードできません。デフォルトで、システムは設定した間隔でフィード ソース全体をダウンロードし、管理対象デバイスを自動更新します。

md5 チェックサムを使用して、更新フィードをダウンロードするかどうか判断するようにシステムを設定することもできます。システムが最後にフィードをダウンロードした後にチェックサムが変更されていない場合、再ダウンロードする必要はありません。特に内部フィードが大きい場合には、md5 チェックサムを使用することができます。md5 チェックサムは、チェックサムのみを含む単純なテキスト ファイルに保存する必要があります。コメントはサポートされていません。

手動でセキュリティ インテリジェンス フィードを更新すると、インテリジェンス フィードを含め、すべてのフィードが更新されます。

セキュリティ インテリジェンス フィードの作成

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、追加するフィード タイプを選択します。

ステップ 3 上記で選択したフィード タイプに適したオプションをクリックします。

- [ネットワーク リストとフィードの追加（Add Network Lists and Feeds）]
- [DNS リストとフィードの追加（Add DNS Lists and Feeds）]

- [URL リストとフィードの追加（Add URL Lists and Feeds）]

ステップ 4 フィードの名前を [名前（Name）] に入力します。
マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [タイプ（Type）] ドロップダウンリストから [フィード（Feed）] を選択します。

ステップ 6 [フィード URL（Feed URL）] を入力します。

ステップ 7 オプションで、[MD5 URL] を入力します。

ステップ 8 [更新頻度（Update Frequency）] を選択します。

ステップ 9 [保存（Save）] をクリックします。
フィードの更新を無効にした場合を除き、システムはフィードをダウンロードして検証しようとします。

手動によるセキュリティ インテリジェンス フィードの更新

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（セキュリティ インテリジェンス）	保護（セキュリティ インテリジェンス）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、フィード タイプを選択します。

ステップ 3 [フィードの更新（Update Feeds）] をクリックして、確認します。

ステップ 4 [OK] をクリックします。

フィードの更新をダウンロードして検証した後、Firepower Management Center はすべての変更内容を管理対象デバイスに通知します。導入環境では、更新されたフィードを使用してトラフィックのフィルタリングが開始されます。

カスタム セキュリティ インテリジェンス リスト

セキュリティ インテリジェンス リストは、IP アドレス、アドレス ブロック、URL、またはドメイン名の単純なスタティック リストで、ユーザがシステムに手動でアップロードします。カスタム リストは、単一の Firepower Management Center の管理対象デバイスで、フィードやグローバル リストの 1 つを増やしたり、微調整したりする場合に役立ちます。

たとえば、信頼できるフィードが重要なリソースへのアクセスを誤ってブロックしているものの、このフィードが全体的に部門にとって有用である場合、IPアドレスフィードオブジェクトをアクセス コントロール ポリシーのブラックリストから削除する代わりに、誤って分類された IP アドレスだけが含まれるカスタム ホワイトリストを作成できます。

（注） セキュリティ インテリジェンス リストでは、/0 ネットマスクを使ってアドレス ブロックをホワイトリスト登録またはブラックリスト登録することはできません。ポリシーですべてのトラフィックをモニタまたはブロックする場合は、[モニタ（Monitor）] または [ブロック（Block）] ルール アクションを含むアクセス コントロール ルールを使用し、デフォルト値 any を [送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] それぞれに設定します。

リスト エントリのフォーマットについて、次の点に注意してください。

- アドレス ブロックのネットマスクは、IPv4 および IPv6 の場合、それぞれ 0 から 32、または 0 から 128 までの整数になります。
- ドメイン名に含まれる Unicode は Punycode 形式でエンコードされる必要があります。大文字と小文字は区別されません。
- ドメイン名の文字の大文字と小文字は区別されません。
- URL に含まれる Unicode はパーセントエンコーディング形式でエンコードする必要があります。
- URL サブディレクトリの文字の大文字と小文字は区別されます。
- シャープ記号（#）で始まるリスト エントリは、コメントと見なされます。

リスト エントリの照合について、次の点に注意してください。

- URL または DNS リストにより高位レベルのドメインが存在する場合、システムはそれより低いレベルのドメインを一致とします。たとえば、DNS リストに example.com を追加すると、システムは www.example.com と test.example.com の両方を一致とします。
- システムは DNS または URL リスト エントリに対して DNS ルックアップを（フォワード ルックアップ、リバース ルックアップともに）行いません。たとえば、URL リストに http://192.168.0.2 を追加し、これがルックアップすれば http://www.example.com であったとします。この場合、システムは http://192.168.0.2 のみ一致とし、http://www.example.com は一致となりません。

- URL リストに末尾がスラッシュ（/）記号で終わる URL を追加した場合、そのエントリに一致するのは完全に一致する URL のみとなります。
- URL または DNS リストに末尾にスラッシュ記号のない URL を追加した場合、そのエントリと同じプレフィックスを持つ URL は一致となります。たとえば、URL リストに `www.example.com` を追加すると、システムは `www.example.com` と `www.example.com/example` の両方を一致とします。

新しいセキュリティ インテリジェンス リストの Firepower Management Center へのアップロード

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

セキュリティ インテリジェンス リストを変更するには、ソース ファイルを変更して、新しいコピーをアップロードする必要があります。Web インターフェイスを使用してファイルの内容を変更することはできません。ソース ファイルへのアクセス権がない場合は、システムからコピーをダウンロードします。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、リストのタイプを選択します。

ステップ 3 上記の手順で選択したリストに該当するオプションをクリックします。

- [ネットワーク リストとフィードの追加（Add Network Lists and Feeds）]
- [DNS リストとフィードの追加（Add DNS Lists and Feeds）]
- [URL リストとフィードの追加（Add URL Lists and Feeds）]

ステップ 4 名前を入力します。
マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [タイプ（Type）] ドロップダウン リストから、[リスト（List）] を選択します。

ステップ 6 [参照（Browse）]をクリックしてリストの `.txt` ファイルを位置指定し、[アップロード（Upload）] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入，（320 ページ） を参照）。

セキュリティ インテリジェンス リストの更新

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、リストのタイプを選択します。

ステップ 3 更新するリストの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 編集するリストのコピーが必要な場合、[ダウンロード（Download）] をクリックし、ブラウザのプロンプトに従ってリストをテキスト ファイルとして保存します。

ステップ 5 必要に応じてリストを変更します。

ステップ 6 [セキュリティ インテリジェンス（Security Intelligence）] ポップアップ ウィンドウで、[参照（Browse）]をクリックして、変更されたリストを参照し、[アップロード（Upload）]をクリックします。

ステップ 7 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入，（320 ページ） を参照）。

シンクホール オブジェクト

シンクホール オブジェクトとは、シンクホール内のすべてのドメイン名のルーティング不可アドレスか、またはサーバに解決されないIPアドレスのいずれかを付与するDNSサーバを表します。DNS ポリシー ルール内のシンクホール オブジェクトを参照して、一致するトラフィックをシンクホールにリダイレクトすることができます。オブジェクトには、IPv4アドレスとIPv6アドレスの両方を割り当てる必要があります。

シンクホール オブジェクトの作成

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 オブジェクト タイプのリストから [シンクホール（Sinkhole）] を選択します。

ステップ 3 [シンクホールの追加（Add Sinkhole）] をクリックします。

ステップ 4 名前を入力します。
マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 シンクホールの [IPv4 アドレス（IPv4 Address）] と [IPv6 アドレス（IPv6 Address）] を入力します。

ステップ 6 次の選択肢があります。

- シンクホール サーバへのトラフィックをリダイレクトする場合は、[シンクホールへの接続のログ（Log Connections to Sinkhole）] を選択します。
- 非解決 IP アドレスにトラフィックをリダイレクトする場合は、[シンクホールへの接続をブロックしてログ（Block and Log Connections to Sinkhole）] を選択します。

ステップ 7 侵入の痕跡（IoC）のタイプをシンクホールに割り当てるには、[タイプ（Type）] ドロップダウンからいずれかのタイプを選択します。

ステップ 8 [保存（Save）] をクリックします。

ファイル リスト

AMP for Firepowerを使用しており、AMPクラウドがファイルの性質を誤って特定した場合は、このファイルをファイル リストに追加して、今後さらに検出できます。このファイルは、SHA-256ハッシュ値を使用して指定されます。各ファイル リストには、一意のSHA-256値を最大10000個まで含めることができます。

ファイル リストには2種類の事前定義済みカテゴリがあります。

クリーン リスト

このリストにファイルを追加すると、システムはAMPクラウドがクリーンな性質を割り当てた場合と同様にファイルを扱います。

カスタム検出リスト

このリストにファイルを追加すると、システムはAMPクラウドがマルウェアの性質を割り当てた場合と同様にファイルを扱います。

マルチドメイン展開では、各ドメインにクリーン リストとカスタム検出リストが存在します。下位レベルのドメインでは、先祖のリストを表示できますが、変更できません。

これらのリストに含まれているファイルに手動でブロッキング動作を指定するため、システムはこれらのファイルの性質についてAMPクラウドに照会しません。ファイルのSHA値を計算するには、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）] アクションと [マルウェア ブロック（Block Malware）] アクションのどちらか、および一致するファイル タイプを使用して、ファイル ポリシー内のルールを設定する必要があります。

注意 クリーン リストにマルウェアを**含めない**でください。クリーン リストによって、AMPクラウドおよびカスタム検出リストの両方がオーバーライドされます。

ファイル リストのソース ファイル

SHA-256値のリストと説明を含むコンマ区切り値（CSV）ソース ファイルをアップロードすることによって、複数のSHA-256値をファイル リストに追加できます。Firepower Management Centerはその内容を検証し、有効なSHA-256値をファイル リストに入れます。

ソース ファイルは、ファイル名拡張子.csvの単純なテキスト ファイルである必要があります。見出しはポンド記号（#）で始まる必要があります。これはコメントとして処理され、アップロードされません。各エントリには、1つのSHA-256値の後に説明が含まれる必要があり、LFまたはCR+LF改行文字で終わる必要があります。システムはエントリ内のこれ以外の情報をすべて無視します。

次の点に注意してください。

- ファイル リストからソース ファイルを削除すると、それに関連付けられているすべてのSHA-256ハッシュもファイル リストから削除されます。

- ソース ファイルのアップロードに成功した結果、10000 個を超える個別の SHA-256 値がファイル リストに含まれる場合は、複数のファイルをファイル リストにアップロードすることはできません。
- システムは、アップロード時に 256 文字を超える説明を最初の 256 文字で切り捨てます。説明にコンマを含める場合は、エスケープ文字（\）を使用する必要があります。説明が含まれていない場合、代わりにソース ファイル名が使用されます。
- 重複しないすべての SHA-256 値がこのファイル リストに追加されます。すでにファイル リストに存在する SHA-256 値を含むソース ファイルをアップロードした場合、新しくアップロードされた値によって既存の SHA--256 値が変更されることはありません。SHA-256 値に関連するキャプチャ済みファイル、ファイル イベント、またはマルウェア イベントを表示するとき、個々の SHA-256 値から脅威名または説明が得られます。
- システムはソース ファイル内の無効な SHA-256 値をアップロードしません。
- アップロードされた複数のソース ファイル内に同じ SHA--256 値に関するエントリが含まれる場合、システムは最も新しい値を使用します。
- 1 つのソース ファイル内に同じ SHA-256 値のエントリが複数含まれる場合、システムは最後のものを使用します。
- オブジェクト マネージャ内でソース ファイルを直接編集することはできません。変更を行うには、最初にソース ファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。
- ソース ファイルに関連付けられたエントリ数とは、個別の SHA-256 値の数です。ファイル リストからソース ファイルを削除すると、ファイル リストに含まれる SHA-256 エントリの合計数は、ソース ファイル内の有効なエントリ数だけ減少します。

ファイル リスト別の SHA-256 値の追加

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

ファイルの SHA-256 値を送信して、それをファイル リストに追加できます。重複する SHA-256 値は追加できません。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

はじめる前に

- イベント ビューからファイルまたはマルウェア イベントを右クリックし、コンテキスト メニューで [フル テキストの表示（Show Full Text）] を選択し、ファイルの SHA-256 値全体をコピーし、ファイルリストに貼り付けます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 オブジェクト タイプのリストから [ファイル リスト（File List）] を選択します。

ステップ 3 ファイルの追加場所となるクリーン リストまたはカスタム検出リストの横の編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [追加元（Add by）] ドロップダウンリストから [SHA 値の入力（Enter SHA Value）] を選択します。

ステップ 5 [説明（Description）] フィールドにソース ファイルの説明を入力します。

ステップ 6 [SHA-256] フィールドにファイル全体の値を入力し、または貼り付けます。システムでは値の部分的な一致はサポートされません。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入，（320 ページ） を参照）。

（注） 設定の変更が展開されたら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。

ファイル リストへの個々のファイルのアップロード

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

ファイル リストに追加するファイルのコピーがある場合、分析用にファイルを Firepower Management Center にアップロードできます。システムはファイルの SHA-256 値を計算し、ファイルをリストに追加します。SHA-256 を計算するとき、システムはファイル サイズを制限しません。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 オブジェクト タイプのリストから [ファイル リスト（File List）] を選択します。

ステップ 3 ファイルの追加場所となるクリーン リストまたはカスタム検出リストの横の編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [追加（Add by）] ドロップダウン リストから、[SHA の計算（Calculate SHA）] を選択します。

ステップ 5 オプションで、[説明（Description）] フィールドにファイルの説明を入力します。説明を入力しない場合、アップロード時にファイル名が説明として使用されます。

ステップ 6 [参照（Browse）] をクリックし、アップロードするファイルを選択します。

ステップ 7 [SHA の計算と追加（Calculate and Add SHA）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入, （320 ページ） を参照）。

（注） 設定の変更を導入すると、その後システムはそのリストのファイルを AMP クラウドでクエリしなくなります。

ファイル リストへのソース ファイルのアップロード

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [ファイル リスト（File List）] をクリックします。

ステップ 3 ソース ファイルからの値の追加先となるファイル リストの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [追加方法（Add by）] ドロップダウン リストで [SHA のリスト（List of SHAs）] を選選択します。

ステップ 5 オプションで、[説明（Description）] フィールドにソース ファイルの説明を入力します。説明を入力しない場合、システムはファイル名を使用します。

ステップ 6 [参照（Browse）]をクリックしてソース ファイルを参照してから、[リストのアップロードと追加（Upload and Add List）] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入，（320 ページ） を参照）。

（注） ポリシーを展開したら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。

ファイル リストの SHA-256 値の編集

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

ファイル リストの個々の SHA-256 値を編集または削除することができます。オブジェクト マネージャ内でソース ファイルを直接編集できないことに注意してください。変更を行うには、最初にソース ファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [ファイル リスト（File List）] をクリックします。

ステップ 3 ファイルの変更対象となるクリーン リストまたはカスタム検出リストの横の編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 次の操作を実行できます。

- 変更する SHA-256 値の横にある編集アイコン（  ）をクリックし、必要に応じて [SHA-256] または [説明（Description）] の値を変更します。
- 削除する SHA-256 値の横にある削除アイコン（  ）をクリックします。

ステップ 5 [保存（Save）] をクリックし、リストのファイル エントリを更新します。

ステップ 6 [保存（Save）] をクリックして、ファイル リストを保存します。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入, （320 ページ） を参照）。

（注） 設定の変更が展開されたら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。

ファイル リストからのソース ファイルのダウンロード

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 オブジェクト タイプのリストから [ファイル リスト（File List）] を選択します。

ステップ 3 ソースファイルのダウンロード対象となるクリーンリストまたはカスタム検出リストの横の編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 ダウンロードするソース ファイルの横にある表示アイコン（）をクリックします。

ステップ 5 [SHA リストのダウンロード（Download SHA List）] をクリックし、プロンプトに従ってソースファイルを保存します。

ステップ 6 [閉じる（Close）] をクリックします。

暗号スイート リスト

暗号スイート リストは複数の暗号スイートからなるオブジェクトです。定義済み暗号スイートの値は、SSL または TLS 暗号化セッションのネゴシエートに使われる暗号スイートを表しています。暗号スイートおよび暗号スイート リストを SSL ルールで使用すると、クライアントとサーバが暗号スイートを使って SSL セッションをネゴシエートしたかどうかに基づいて暗号化トラフィッ

クを制御できます。SSL ルールに暗号スイート リストを追加すると、リスト内のいずれかの暗号スイートでネゴシエートされた SSL セッションがルールに一致します。

（注） Webインターフェイスでは暗号スイートリストと同じ場所で暗号スイートを使用できますが、暗号スイートを追加、変更、削除することはできません。

暗号スイート リストの作成

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 オブジェクト タイプのリストから [暗号スイート リスト（Cipher Suite List）] を選択します。

ステップ 3 [暗号スイートの追加（Add Cipher Suites）] をクリックします。

ステップ 4 名前を入力します。
マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [使用可能な暗号（Available Ciphers）] リストから、1 つ以上の暗号スイートを選択します。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 オプションで、[選択された暗号（Selected Ciphers）] リストで、削除する暗号スイートの隣にある削除アイコン（）をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入, （320 ページ） を参照）。

識別名オブジェクト

それぞれの識別名オブジェクトは、公開鍵証明書のサブジェクトまたは発行元にリストされた識別名を表します。SSL ルールで識別名オブジェクトとグループを使用すると、サブジェクトまたは発行元として識別名を含むサーバ証明書を使ってクライアントとサーバが SSL セッションをネゴシエートしたかどうかに基づき、暗号化トラフィックを制御できます。

識別名オブジェクトには、共通名属性（CN）を含めることができます。「CN=」なしで共通名を追加すると、システムはオブジェクトを保存する前に「CN=」を追加します。

さらに、次の表に示す属性を含む識別名を追加することもできます。属性はカンマで区切って使用します。

表 *45*：識別名の属性

属性（**Attribute**）	説明	使用可能な値
C	国コード（Country Code）	2 つの英字
CN	Common Name	最大 64 文字の英数字、バックスラッシュ（/）、ハイフン（-）、引用符（"）、アスタリスク（*）、スペース文字
O	Organization	最大 64 文字の英数字、バックスラッシュ（/）、ハイフン（-）、引用符（"）、アスタリスク（*）、スペース文字
OU	組織	最大 64 文字の英数字、バックスラッシュ（/）、ハイフン（-）、引用符（"）、アスタリスク（*）、スペース文字

ワイルドカードとして1つ以上のアスタリスク（*）を属性に定義できます。共通名属性では、ドメイン名ラベルごとに 1 つ以上のアスタリスクを定義できます。ワイルド カードはそのラベル内でのみ照合されますが、ワイルド カードを使用して複数のラベルを定義できます。例については、以下の表を参照してください。

表 *46*：共通名属性のワイルドカードの例

属性（**Attribute**）	一致	一致しない
CN=”*ample.com”	example.com	mail.example.com example.text.com ampleexam.com

属性（**Attribute**）	一致	一致しない
CN=”exam*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*xamp*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*.example.com”	mail.example.com	example.com example.text.com ampleexam.com
CN=”*.com”	example.com ampleexam.com	mail.example.com example.text.com
CN=”*.*.com”	mail.example.com example.text.com	example.com ampleexam.com

識別名オブジェクトの作成

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [識別名（Distinguished Name）] ノードを展開し、[個別オブジェクト（Individual Objects）] を選択します。

ステップ 3 [識別名の追加（Add Distinguished Name）] をクリックします。

ステップ 4 名前を入力します。
マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [DN] フィールドに、識別名または共通名の値を入力します。次の選択肢があります。

- 識別名を追加する場合は、識別名オブジェクト，（438 ページ）に示されている属性をカンマで区切って含めることができます。
- 共通名を追加する場合は、複数のラベルとワイルドカードを含めることができます。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入，（320 ページ） を参照）。

PKI オブジェクト

SSL アプリケーションの PKI オブジェクト

PKI オブジェクトは、導入をサポートするために必要な公開鍵証明書、およびペアになった秘密鍵を表します。内部 CA オブジェクトおよび信頼できる CA オブジェクトは、認証局（CA）証明書で構成されます。また、内部 CA オブジェクトには、証明書とペアになった秘密鍵も含まれます。内部証明書オブジェクトおよび外部証明書オブジェクトは、サーバ証明書で構成されます。また、内部証明書オブジェクトには、証明書とペアになった秘密鍵も含まれます。

信頼できる認証局オブジェクトと内部証明書オブジェクトを使用して ISE への接続を設定する場合、ISE をアイデンティティ ソースとして使用できます。

内部証明書オブジェクトを使用してキャプティブ ポータルを設定する場合、システムはキャプティブ ポータルデバイスがユーザの Web ブラウザに接続する際に、デバイスのアイデンティティを検証できます。

信頼できる認証局オブジェクトを使用してレルムを設定する場合、LDAP または AD サーバへのセキュア接続を設定できます。

SSL ルールで PKI オブジェクトを使用する場合、以下のものを使用して暗号化されたトラフィックを照合することができます。

- 外部証明書オブジェクト内の証明書
- 信頼できる CA オブジェクトの CA によって署名された証明書、または信頼できる CA チェーン内で署名された証明書

SSL ルールで PKI オブジェクトを使用する場合、以下のものを復号できます。

- 発信トラフィック：内部 CA オブジェクトを使ってサーバ証明書を再署名することによって復号します
- 受信トラフィック：内部証明書オブジェクトにある既知の秘密鍵を使用して復号します

証明書とキーの情報を手動で入力し、その情報を含むファイルをアップロードします。場合によっては、新しい CA 証明書や秘密キーを生成することができます。

オブジェクト マネージャで PKI オブジェクトのリストを表示すると、システムは証明書のサブジェクト識別名をオブジェクト値として表示します。証明書の完全なサブジェクト識別名を表示するには、値の上にポインタを移動してください。証明書に関する他の詳細を表示するには、PKI オブジェクトを編集します。

（注） Firepower Management Center および管理対象デバイスは、内部 CA オブジェクトと内部証明書オブジェクトに保存されるすべての秘密キーを、保存前にランダムに生成されたキーを使って暗号化します。パスワード保護されている秘密キーをアップロードすると、アプライアンスはユーザ提供のパスワードを使って秘密キーを復号し、ランダムに生成されたキーを使ってそれを再暗号化してから保存します。

内部認証局オブジェクト

設定されたそれぞれの内部認証局（CA）オブジェクトは、組織で制御される CA の CA 公開鍵証明書を表します。このオブジェクトは、オブジェクト名、CA 証明書、およびペアになった秘密鍵からなります。SSL ルールで内部 CA オブジェクトとグループを使用すると、内部 CA によってサーバ証明書に再署名することにより、発信する暗号化トラフィックを復号できます。

（注） [復号 - 再署名（Decrypt - Resign）] SSL ルールで内部 CA オブジェクトを参照する場合、ルールが暗号化セッションに一致すると、SSL ハンドシェイクのネゴシエート中は証明書を信頼できないという警告がユーザのブラウザに表示されることがあります。これを回避するには、信頼できるルート証明書のクライアントまたはドメイン リストに内部 CA オブジェクト証明書を追加します。

次の方法で内部 CA オブジェクトを作成できます。

- RSA ベースまたは楕円曲線ベースの既存の CA 証明書と秘密キーをインポートする
- 新しい RSA ベースの自己署名 CA 証明書と秘密キーを生成する
- RSA ベースの未署名の CA 証明書と秘密キーを生成する内部 CA オブジェクトを使用する前に、証明書に署名するために証明書署名要求（CSR）を別の CA に送信する必要があります。

署名付き証明書を含む内部 CA オブジェクトを作成した後で、CA 証明書と秘密鍵をダウンロードできるようになります。システムは、ダウンロードされた証明書と秘密キーをユーザ提供のパスワードで暗号化します。

システムで生成された場合でも、ユーザによって作成された場合でも、内部 CA オブジェクトの名前は変更できますが、他のオブジェクト プロパティは変更できません。

使用中の内部 CA オブジェクトは削除できません。さらに、SSL ポリシーで使用される内部 CA オブジェクトを編集すると、関連するアクセスコントロールポリシーが失効します。変更を反映させるには、アクセス コントロール ポリシーを再度展開する必要があります。

CA 証明書と秘密キーのインポート

X.509 v3 CA 証明書と秘密キーをインポートすることによって、内部 CA オブジェクトを設定できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

秘密キー ファイルがパスワード保護されている場合は、復号パスワードを提供できます。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書またはキーの情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

（注） ルールに [復号 - 再署名（Decrypt - Resign）] アクションを設定すると、そのルールでは、設定されているルール条件に加えて、参照される内部 CA 証明書の暗号化アルゴリズムのタイプに基づいてトラフィックが照合されます。たとえば、楕円曲線ベースのアルゴリズムで暗号化された発信トラフィックを復号するには、楕円曲線ベースの CA 証明書をアップロードする必要があります。

CA 証明書と秘密キーのインポート

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [PKI] ノードを展開して、[内部 CA（Internal CAs）] を選択します。

ステップ 3 [CA のインポート（Import CA）] をクリックします。

ステップ 4 名前を入力します。
マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6 [キー（Key）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

ステップ 7 アップロード ファイルがパスワード保護されている場合は、[暗号化および次のパスワード:（Encrypted, and the password is:）] チェックボックスをオンにして、パスワードを入力します。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入, （320 ページ） を参照）。

CA 証明書および秘密キーの生成

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

識別情報を提供することで、RSA ベースの自己署名 CA 証明書と秘密キーを生成するように内部 CA オブジェクトを設定できます。

生成される CA 証明書の有効期間は 10 年です。[有効期間の開始（Valid From）] の日付は、生成の一週間前です。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 [CA の生成（Generate CA）] をクリックします。

ステップ 4 名前を入力します。
マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 ID 属性を入力します。

ステップ 6 [自己署名 CA の生成（Generate self-signed CA）] をクリックします。

新しい署名付き証明書

署名付き証明書を CA から取得することによって、内部 CA オブジェクトを設定できます。これは、次の 2 段階からなります。

- 内部 CA オブジェクトを設定するための識別情報を指定します。これにより、未署名の証明書およびペアになった秘密鍵が生成され、指定した CA に対する証明書署名要求（CSR）が作成されます。
- CA により署名付き証明書が発行されたら、それを内部 CA オブジェクトにアップロードして、未署名の証明書と置き換えます。

署名付き証明書が含まれている場合にのみ、SSL ルールで内部 CA オブジェクトを参照できます。

未署名の CA 証明書と CSR の作成

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 [CA の生成（Generate CA）] をクリックします。

ステップ 4 名前を入力します。
マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 ID 属性を入力します。

ステップ 6 [CSR の作成（Generate CSR）] をクリックします。

ステップ 7 CA に送信するために CSR をコピーします。

ステップ 8 [OK] をクリックします。

次の作業

- CA によって発行される署名済み証明書をアップロードする必要があります。次のページを参照してください。 CSR への応答として発行された署名付き証明書のアップロード, （445 ページ）

CSR への応答として発行された署名付き証明書のアップロード

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

一度アップロードすると、署名付き証明書は SSL ルールで参照できます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 CSR を待機している未署名の証明書を含む CA オブジェクトの横の編集アイコン（  ）をクリックします。

ステップ 4 [証明書のインストール（Install Certificate）] をクリックします。

ステップ 5 [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6 アップロードファイルがパスワード保護されている場合は、[暗号化済み、パスワード：（Encrypted, and the password is:）] チェック ボックスをオンにして、パスワードを入力します。

ステップ 7 [保存（Save）] をクリックして、CA オブジェクトに署名付き証明書をアップロードします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入，（320 ページ） を参照）。

CA 証明書および秘密キーのダウンロード

証明書および鍵の情報を含むファイルを内部CAオブジェクトからダウンロードすることにより、CA 証明書およびペアになった秘密鍵をバックアップまたは転送できます。

注意 ダウンロードされた鍵情報は必ず安全な場所に保存してください。

システムは、内部 CA オブジェクトに保存されている秘密鍵をディスクに保存する前に、ランダムに生成された鍵を使って暗号化します。証明書および秘密鍵を内部 CA オブジェクトからダウンロードすると、システムはまず情報を復号してから、証明書および秘密鍵の情報を含むファイルを作成します。その後、ダウンロード ファイルを暗号化するためにシステムで使われるパスワードを提供する必要があります。

注意 システム バックアップの一部としてダウンロードされる秘密鍵は、復号されてから、非暗号化バックアップ ファイルに保存されます。

CA 証明書と秘密キーのダウンロード

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

現在のドメインおよび先祖ドメインの両方の CA 証明書をダウンロードできます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 証明書および秘密キーをダウンロードする対象となる内部 CA オブジェクトの横の編集アイコン（  ）をクリックします。

マルチドメイン導入では、表示アイコン（  ）をクリックして、先祖ドメインのオブジェクトの証明書および秘密キーをダウンロードします。

ステップ 4 [ダウンロード（Download）] をクリックします。

ステップ 5 [パスワード（Password）] および [パスワードの確認（Confirm Password）] フィールドに、暗号化パスワードを入力します。

ステップ 6 [OK] をクリックします。

信頼できる認証局オブジェクト

設定した信頼できる認証局（CA）オブジェクトは、それぞれ信頼できる CA に属する CA 公開鍵証明書を表します。このオブジェクトは、オブジェクト名と CA 公開鍵証明書からなります。次のものに設定された外部 CA オブジェクトとグループを使用できます。

- 信頼できる CA、または信頼チェーン内のいずれかの CA によって署名された証明書で暗号化されたトラフィックを制御するための SSL ポリシー。
- LDAP または AD サーバへのセキュアな接続を確立するためのレルムの設定。
- ISE 接続。[pxGrid サーバ CA（pxGrid Server CA）] フィールドと [MNT サーバ CA（MNT Server CA）] フィールドで信頼できる認証局オブジェクトを選択します。

信頼できるCAオブジェクトを作成した後で、その名前を変更したり、証明書失効リスト（CRL）を追加したりすることはできますが、他のオブジェクト プロパティを変更することはできません。オブジェクトに追加できるCRLの数には制限がありません。オブジェクトにアップロード済みの CRL を変更するには、オブジェクトをいったん削除して再作成する必要があります。

（注） オブジェクトにCRLを追加しても、ISEの統合設定でオブジェクト使用する際に影響はありません。

使用中の信頼できる CA オブジェクトを削除することはできません。また、使用中の信頼できる CA オブジェクトを編集すると、関連付けられているアクセス コントロール ポリシーが最新ではなくなります。変更を反映させるには、アクセスコントロールポリシーを再度展開する必要があります。

信頼できる CA オブジェクト

外部 CA オブジェクトは、X.509 v3 CA 証明書をアップロードすることによって設定できます。次のサポートされている形式のいずれかでエンコードしたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

ファイルがパスワードで保護されている場合は、復号パスワードを提供する必要があります。証明書がPEM形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

ファイルに適切な証明書情報が含まれる場合にのみ、CA証明書をアップロードできます。システムはオブジェクトを保存する前に証明書を検証します。

信頼できる CA オブジェクトの追加

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [PKI] ノードを展開し、[信頼できる CA（Trusted CAs）] を選択します。

ステップ 3 [信頼できる CA の追加（Add Trusted CAs）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6 ファイルがパスワード保護されている場合は、[暗号化、パスワード：（Encrypted, and the password is:）] チェックボックスをオンにして、パスワードを入力します。

ステップ 7 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入, （320 ページ） を参照）。

信頼できる CA オブジェクトの証明書失効リスト

信頼できる CA オブジェクトに CRL をアップロードできます。信頼できる CA オブジェクトを SSL ポリシーの中で参照すると、セッションの暗号化証明書を発行した CA がその後で証明書を取り消したかどうかに基づいて、暗号化されたトラフィックを制御できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

CRL を追加した後、失効した証明書のリストを表示することができます。オブジェクトにアップロード済みの CRL を変更するには、オブジェクトをいったん削除して再作成する必要があります。

適切な CRL を含んでいるファイルのみをアップロードできます。信頼できる CA オブジェクトに追加できる CRL の数には制限がありません。ただし、CRL をアップロードした場合、別の CRL を追加する前に、オブジェクトをその都度保存する必要があります。

（注） オブジェクトに CRL を追加しても、ISE の統合設定でオブジェクト使用する際に影響はありません。

信頼できる CA オブジェクトへの証明書失効リストの追加

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

（注） オブジェクトに CRL を追加しても、ISE の統合設定でオブジェクト使用する際に影響はありません。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [PKI] ノードを展開し、[信頼できる CA（Trusted CAs）] を選択します。

ステップ 3 信頼できる CA オブジェクトの横にある編集アイコン（）をクリックします。
代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [CRL の追加（Add CRL）] をクリックして、DER または PEM でエンコードされた CRL ファイルをアップロードします。

ステップ 5 [OK] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入，（320 ページ） を参照）。

外部証明書オブジェクト

設定済みのそれぞれの外部証明書オブジェクトは、組織に属さないサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名と証明書からなります。SSL ルールで外部証明書オブジェクトとグループを使用すると、サーバ証明書で暗号化されたトラフィックを制御できます。

たとえば、信頼できる自己署名サーバ証明書をアップロードできますが、信頼できる CA 証明書を使って検証することはできません。

X.509 v3 サーバ証明書をアップロードすることによって、外部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

適切なサーバ証明書情報を含んでいるファイルだけをアップロードできます。システムはオブジェクトを保存する前にファイルを検証します。証明書が PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

外部証明書オブジェクトの追加

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [PKI] ノードを展開し、[外部証明書（External Certs）] を選択します。

ステップ 3 [外部証明書の追加（Add External Cert）] をクリックします。

ステップ 4 名前を入力します。
マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバ証明書ファイルをアップロードします。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入, （320 ページ） を参照）。

内部証明書オブジェクト

設定済みのそれぞれの内部証明書オブジェクトは、組織に属するサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名、公開鍵証明書、およびペアになった秘密鍵からなります。内部証明書オブジェクトとグループは、以下で使用することができます。

- SSL ルール。既知の秘密キーを使用する組織のサーバの 1 つに着信するトラフィックを復号します。
- ISE 接続。[MC サーバ証明書（MC Server Certificate）] フィールド用の内部証明書オブジェクトを選択します。
- キャプティブ ポータル設定。ユーザの Web ブラウザに接続する際にキャプティブ ポータル デバイスのアイデンティティを認証するように設定します。[サーバ証明書（Server Certificate）] フィールド用の内部証明書オブジェクトを選択します。

X.509 v3 RSA ベースまたは楕円曲線ベースのサーバ証明書およびペアの秘密キーをアップロードすることにより、内部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

ファイルがパスワード保護されている場合は、復号パスワードを提供する必要があります。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書またはキーの情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

内部証明書オブジェクトを作成した後、その名前を変更することはできますが、他のオブジェクト プロパティを変更することはできません。

使用中の内部証明書オブジェクトは削除できません。さらに、使用中の内部証明書オブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を反映させるには、アクセス コントロール ポリシーを再度展開する必要があります。

内部証明書オブジェクトの追加

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

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）]を選択します。

ステップ 2 [PKI] ノードを展開し、[内部証明書（Internal Certs）] を選択します。

ステップ 3 [内部証明書の追加（Add Internal Cert）] をクリックします。

ステップ 4 名前を入力します。
マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバ証明書ファイルをアップロードします。

ステップ 6 [キー（Key）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

ステップ 7 アップロードする秘密キー ファイルがパスワード保護されている場合は、[暗号化済み、パスワード：（Encrypted, and the password is:）] チェックボックスをオンにして、パスワードを入力します。

ステップ 8 [保存（Save）] をクリックします。

第 V 部

アプライアンス管理の基本

第 18 章

Firepower Management Center の基礎

以下のトピックでは、Firepower Management Center の基礎について説明します。

Firepower Management Center

Firepower Management Center を使用して、Firepower システムを構成するすべてのデバイスを管理できます。デバイスを管理するには、Firepower Management Center とデバイスの間に、双方向の SSL 暗号化通信チャネルをセットアップします。Firepower Management Center はこのチャネルを使用して、そのデバイスへのネットワーク トラフィックの分析および管理の方法に関する情報をそのデバイスに送信します。そのデバイスはトラフィックを評価すると、イベントを生成し、同じチャネルを使用してそれらのイベントを Firepower Management Center に送信します。

デバイス管理

Firepower Management Center は、Firepower システムのキー コンポーネントです。Firepower システムを構成するあらゆるデバイスを管理したり、ネットワーク上で検出された脅威を集約し、分析して対処するために、Firepower Management Center を使用できます。

Firepower Management Center を使用してデバイスを管理すると、以下の利点があります。

- すべてのデバイスのポリシーを単一の場所から設定できるため、設定の変更が容易になります。
- さまざまなタイプのソフトウェア アップデートをデバイスにインストールできます。
- 正常性ポリシーを管理対象デバイスに適用して、Firepower Management Center からデバイスのヘルス ステータスをモニタできます。

Firepower Management Center は、侵入イベント、ネットワーク検出情報、およびデバイスのパフォーマンス データを集約して相互に関連付けます。そのため、ユーザはデバイスが相互の関連でレポートする情報をモニタして、ネットワーク上で行われている全体的なアクティビティを評価することができます。

Firepower Management Center を使用することで、デバイス動作のほぼすべての側面を管理できます。

（注） Firepower Management Center は、http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html で使用可能な互換性マトリックスで指定されている特定の以前のリリースを実行しているデバイスを管理できますが、これらの以前のリリースのデバイスでは新しい機能は利用できません。

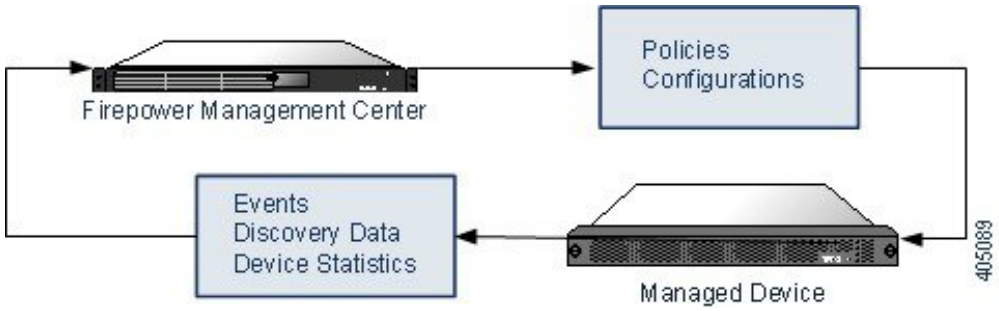
Firepower Management Center で管理できるデバイス

Firepower Management Center を Firepower システムの展開環境における中央の管理ポイントとして使用して、次の各デバイスを管理することができます。

- 7000 および 8000 シリーズ デバイス
- ASA FirePOWER モジュール
- NGIPSv デバイス

デバイスを管理する際の情報は、SSL で暗号化されたセキュアな TCP トンネルを介して、Firepower Management Center とデバイスの間で送信されます。

次の図に、Firepower Management Center と管理対象デバイスの間で送信される情報をリストします。アプライアンス間で送信されるイベントとポリシーのタイプは、デバイス タイプに基づくことに注意してください。



ポリシーとイベント以外の機能

Firepower Management Center では、ポリシーをデバイスに展開したり、デバイスからイベントを受信するだけでなく、以下のデバイス関連のタスクも実行できます。

デバイスのバックアップ

NGIPSv デバイスや ASA FirePOWER モジュールのバックアップ ファイルを作成、復元することは**できません**。

物理的な管理対象デバイス自体からそのバックアップを実行する場合は、デバイス設定**のみ**をバックアップできます。設定データと統合ファイル（任意）をバックアップするには、管理 Firepower Management Center を使用してデバイスのバックアップを実行します。

イベント データをバックアップするには、管理 Firepower Management Center のバックアップを実行します。

デバイスの更新

シスコは適宜、Firepower システムの更新プログラムをリリースしています。これらのアップデートには以下が含まれます。

- 侵入ルールの更新（新しいルールや更新された侵入ルールが含まれる場合があります）
- 脆弱性データベースの更新
- 地理位置情報の更新
- ソフトウェア パッチおよびアップデート

Firepower Management Center を使用して、管理対象デバイスに更新プログラムをインストールできます。

関連トピック

バックアップ ファイル, （175 ページ）

NAT 環境

ネットワーク アドレス変換（NAT）とは、ルータを介したネットワーク トラフィックの送受信方式であり、送信元または宛先 IP アドレスの再割り当てが行われます。NAT の最も一般的な用途は、プライベート ネットワークがインターネットと通信できるようにすることです。スタティック NAT は 1:1 変換を実行し、デバイスとの Firepower Management Center 通信に支障はありませんが、ポート アドレス変換（PAT）がより一般的です。PAT では、単一のパブリック IP アドレスと一意のポートを使用してパブリック ネットワークにアクセスできます。これらのポートは必要に応じて動的に割り当てられるため、PAT ルータの背後にあるデバイスへの接続は開始できません。

通常は、ルーティングと認証の両方の目的で両方の IP アドレス（登録キー付き）が必要です。Firepower Management Center がデバイスの IP アドレスを指定し、デバイスが Firepower Management Center の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。Firepower Management Center およびデバイスでは、初期登録の認証と承認を行うために、登録キーおよびNAT ID（IP アドレスではなく）を使用します。

たとえば、デバイスを Firepower Management Center に追加したときにデバイスの IP アドレスがわからない場合（たとえばデバイスが PAT ルータの背後にある場合）は、NAT ID と登録キーのみを指定します。デバイス上で、Firepower Management Center の IP アドレス、同じ NAT ID、および同じ登録キーを指定します。デバイスが Firepower Management Center の IP アドレスに登録されます。この時点で、Firepower Management Center は IP アドレスの代わりに NAT ID を使用してデバイスを認証します。

NAT 環境では NAT ID を使用するのが最も一般的ですが、NAT ID を使用することで、多数のデバイスを簡単に Firepower Management Center に追加することができます。Firepower Management Center で、追加するデバイスごとに一意の NAT ID を指定し、次に各デバイスで、Firepower Management Center の IP アドレスと NAT ID の両方を指定します。注：NAT ID はデバイスごとに一意でなければなりません。

第 19 章

デバイスの管理の基本

次のトピックでは、Firepower システムでデバイスを管理する方法について説明します。

[デバイス管理（Device Management）] ページ

[デバイス管理（Device Management）] ページには、登録されたデバイス、7000 および 8000 シリーズ デバイスのハイ アベイラビリティ ペア、およびデバイス グループを管理するために使用できる、一連の情報とオプションが表示されます。このページには、現在 Firepower Management Center に登録されているすべてのデバイスの一覧が表示されます。

[ソート基準（sort-by）] ドロップダウン リストを使用すると、グループ、ライセンス、モデル、またはアクセス コントロール ポリシーのいずれかのカテゴリでデバイス一覧をソートできます。マルチドメイン導入では、ドメイン（その導入のデフォルトの表示カテゴリ）を基準にソートすることもできます。デバイスはリーフ ドメインに属している必要があります。

デバイス カテゴリに属するデバイスの一覧は、展開または縮小表示できます。デフォルトでは、デバイス一覧が展開されます。

デバイス一覧の詳細については、以下の表を参照してください。

表 47 : *[デバイス一覧（Device List）]* のフィールド

フィールド	説明
[名前（Name）]	Firepower Management Center でデバイスに使用されている表示名。名前の左側にあるステータス アイコンは、その名前の現在のヘルス ステータスを示します。
グループ	管理対象デバイスを割り当てたグループ。
モデル	管理対象デバイスのモデル。
ライセンスのタイプ（License Type）	管理対象デバイスで有効なライセンス。
アクセス コントロール ポリシー（Access Control Policy）	現在導入されているアクセス コントロール ポリシーへのリンク。システムがアクセス コントロール ポリシーを古いものとして識別すると、そのリンクの横に警告アイコン（）が表示されます。

関連トピック

Firepower の機能ライセンスについて, （127 ページ）
ヘルス モニタリングについて, （251 ページ）
アクセス コントロール ポリシーの管理, （786 ページ）

管理対象デバイスのフィルタリング

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

Firepower Management Center が大量のデバイスを管理する場合、[デバイス管理（Device Management）] ページの結果を絞り込むことで特定のデバイスを見つけやすくなります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 デバイスのリストを絞り込むには、[デバイス名（Device Name）][デバイス/ホスト名（Device/Host Name）] フィールドにデバイス名の全体または一部を入力します。

ステップ 3 フィルタをクリアするには：

- [デバイス名（Device Name）][デバイス/ホスト名（Device/ Host Name）] フィールドをクリアします。
- [一部のデバイスがリストされていません。（Not all devices are listed.）すべてのデバイスを一覧表示するには、ここをクリックしてください。（Click here to list all devices）] リンクを選択してください。

リモート管理の設定

Firepower System デバイスを管理できるようにするには、デバイスと Firepower Management Center との間に双方向の SSL 暗号化通信チャネルをセットアップする必要があります。このチャネルを使用して、両方のアプライアンスが設定とイベント情報を共有します。ハイアベイラビリティピアも、このチャネルを使用します。このチャネルは、デフォルトではポート 8305/tcp に位置します。

（注） この章では、FMC にデバイスを登録する前にローカル Web インターフェイスを使用して、7000 または 8000 シリーズデバイスのリモート管理の設定方法について説明します。他のモデルのリモート管理の設定の詳細については、適切なクイックスタートガイドを参照してください。

2 つのアプライアンス間の通信を可能にするためには、アプライアンスが互いを認識する手段を提供しなければなりません。Firepower System では 3 つの基準を使用して、通信を許可します。

- 通信を確立する対象のアプライアンスのホスト名または IP アドレス。

  NAT 環境では、ルーティング可能なアドレスがもう一方のアプライアンスにないとしても、リモート管理を設定する際、または管理対象アプライアンスを追加する際には、ホスト名または IP アドレスのいずれかを指定する必要があります。

- 接続を識別するために自己生成される、最大 37 文字の英数字による登録キー。
- Firepower System が NAT 環境で通信を確立するために利用できるオプションの一意の英数字による NAT ID。

  NAT ID は、管理対象アプライアンスを登録するために使用されているすべての NAT ID の間で**一意でなければなりません**。

関連トピック

NAT 環境, （459 ページ）

Firepower Management Center へのデバイスの追加

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

Firepower Management Center に 1 つのデバイスを追加するには、ここに示す手順を実行します。冗長性やパフォーマンスのためにデバイスをリンクする場合、次の点を念頭に置いて、この手順を実行する必要があります。

- 8000 シリーズ スタック：この手順を使用して各デバイスを Firepower Management Center に追加した後、スタックを確立します（デバイス スタックの確立, （538 ページ）を参照）。
- 7000 および 8000 シリーズ ハイ アベイラビリティ：この手順を使用して各デバイスを Firepower Management Center に追加した後、高可用性を確立します（デバイスのハイ アベイラビリティの確立, （520 ページ）を参照）。ハイ アベイラビリティ スタックの場合、デバイスをスタックしてから、スタック間のハイ アベイラビリティを確立します。

はじめる前に

- デバイスを Firepower Management Center の管理対象として設定します。7000 および 8000 シリーズデバイスについては、管理対象デバイス上のリモート管理の設定, （486 ページ）を参照してください。他のモデルのリモート管理設定の詳細については、該当するクイックスタートガイドを参照してください。
- IPv4 を使用して登録した Firepower Management Center とデバイスを IPv6 に変換する場合は、デバイスをいったん削除してから再登録する必要があります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 [追加（Add）] ドロップダウン メニューから、[デバイスの追加（Add Device）] を選択します。

ステップ 3 [ホスト（Host）] フィールドに、追加するデバイスの IP アドレスまたはホスト名を入力します。デバイスのホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

NAT 環境では、Firepower Management Center の管理対象としてデバイスを設定するときに Firepower Management Center の IP アドレスまたはホスト名をすでに指定した場合、デバイスの IP アドレスまたはホスト名を指定する必要がない場合があります。詳細については、NAT 環境, （459 ページ）を参照してください。

ステップ 4 [表示名（Display Name）] フィールドに、Firepower Management Center でのデバイスの表示名を入力します。

ステップ 5 [登録キー（Registration Key）] フィールドに、Firepower Management Center の管理対象としてデバイスを設定したときに使用したのと同じ登録キーを入力します。登録キーは、1 回限り使用可能な共有シークレットです。

ステップ 6 マルチドメイン展開では、現在のドメインに関係なく、デバイスをリーフ ドメインに割り当てます。
現在のドメインがリーフ ドメインである場合、デバイスは自動的に現在のドメインに追加されます。現在のドメインがリーフ ドメインでない場合、登録後、デバイスを設定するために、リーフ ドメインに切り替える必要があります。

ステップ 7 必要に応じて、デバイスをデバイス グループに追加します。

ステップ 8 登録後すぐに、デバイスに展開する最初の [アクセス コントロール ポリシー（Access Control Policy）] を選択するか、新しいポリシーを作成します。
デバイスが選択したポリシーに適合しない場合、展開は失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。この障害の原因を解決した後、デバイスに手作業で設定を行います。

ステップ 9 デバイスに適用するライセンスを選択します。
従来型のデバイスでは、次の点に注意してください。

- コントロール、マルウェア、URL フィルタリング ライセンスには、保護ライセンスが必要です。
- VPN ライセンスでは、7000 または 8000 シリーズ デバイスを必要とします。
- コントロール ライセンスは、NGIPSv と ASA FirePOWER デバイスでサポートされていますが、8000 シリーズ Fastpath ルール、スイッチング、ルーティング、スタック、デバイスのハイ アベイラビリティを設定することはできません。

ステップ 10 デバイスの設定時に、NAT ID を使用した場合、[詳細（Advanced）] セクションを展開し、[一意の NAT ID（Unique NAT ID）] フィールドに同じ NAT ID を入力します。

ステップ 11 [パケットの転送（Transfer Packets）] チェックボックスをオンにし、デバイスで Firepower Management Center にパケットを転送することを許可します。
このオプションは、デフォルトで有効です。無効にすると、Firepower Management Center へのパケット転送が完全に禁止されます。

ステップ 12 [登録（Register）] をクリックします。
Firepower Management Center がデバイスのハートビートを確認して通信を確立するまでに、最大 2 分かかる場合があります。

関連トピック

基本的なアクセス コントロール ポリシーの作成, （787 ページ）

Firepower Management Center からのデバイスの削除

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

デバイスを管理する必要がなくなった場合、Firepower Management Center からそのデバイスを削除できます。デバイスを削除すると、以下のようになります。

- Firepower Management Center とそのデバイスとの間のすべての通信が切断されます。
- [デバイス管理（Device Management）] ページからデバイスが削除されます。
- プラットフォーム設定ポリシーで、NTP を介して Firepower Management Center から時間を受信するようにデバイスが設定されている場合は、デバイスがローカル時間管理に戻されます。

デバイスを後者で管理するには、デバイスを Firepower Management Center に再度追加します。

（注） デバイスを削除し、再び追加すると、Firepower Management Center Web インターフェイスによって、アクセス コントロール ポリシーを再適用するよう求められます。ただし、登録時に NAT と VPN ポリシーを再適用するオプションはありません。以前に適用された NAT または VPN 設定はすべて登録時に削除されるため、登録が完了した後に再適用する必要があります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 削除するデバイスの横にある削除アイコン（）をクリックします。

ステップ 3 デバイスを削除することを確認します。

デバイス コンフィギュレーションの設定

アプライアンス エディタの [デバイス（Device）] ページには、詳細なデバイス設定および情報が表示されます。また、デバイス設定の一部（ライセンスの有効化と無効化、デバイスのシャットダウンと再起動、管理の変更、詳細オプションの設定など）を変更することもできます。

一般的なデバイスの設定

[デバイス（Device）] タブの [全般（General）] セクションには、以下の表に記載された設定を表示します。

表 *48* : *[全般（General）]* セクション テーブルのフィールド

フィールド	説明
[名前（Name）]	Firepower Management Center でのデバイスの表示名。
パケット転送（Transfer Packets）	管理対象デバイスがイベントを含むパケット データを Firepower Management Center に送信するかどうか。
展開を強制（Force Deploy）	デバイスのすべてのポリシーおよびデバイス設定の更新を強制的に展開します。

デバイス ライセンスの設定

[デバイス（Device）] タブの [ライセンス（License）] セクションでは、そのデバイスに対して有効になっているライセンスが表示されます。

関連トピック

Firepower の機能ライセンスについて, （127 ページ）

デバイス システムの設定

[デバイス（Device）] タブの [システム（System）] セクションには、次の表に示すように、システム情報の読み取り専用テーブルが表示されます。

表 *49* : *[システム（System）]* セクション テーブルのフィールド

フィールド	説明
モデル	管理対象デバイスのモデル名と番号。
シリアル（Serial）	管理対象デバイスのシャーシのシリアル番号。
時刻（Time）	デバイスの現在のシステム時刻。

フィールド	説明
バージョン（Version）	管理対象デバイスに現在インストールされているソフトウェアのバージョン。
ポリシー	管理対象デバイスに現在展開されているプラットフォーム設定ポリシーへのリンク。

デバイスをシャットダウンまたは再起動することもできます。

デバイス ヘルスの設定

[デバイス（Device）]タブの[ヘルス（Health）]セクションには、以下の表に記載された情報を表示します。

表 *50*：*[ヘルス（Health）]セクション* テーブルのフィールド

フィールド	説明
Status	デバイスの現在のヘルス ステータスを表すアイコン。アイコンをクリックすると、アプライアンスのヘルス モニタが表示されます。
ポリシー	現在デバイスで展開されている、読み取り専用バージョンの正常性ポリシーへのリンク。
ブラックリスト	[ヘルス ブラックリスト（Health Blacklist）]ページへのリンク。このページでは、ヘルス ブラックリスト モジュールを有効または無効に設定できます。

関連トピック

アプライアンス ヘルス モニタの表示, （272 ページ）
正常性ポリシーの編集, （263 ページ）
正常性ポリシー モジュールのブラックリスト登録, （266 ページ）

デバイス管理設定

[デバイス（Device）]タブの[管理（Management）]セクションには、以下の表に記載されたフィールドを表示します。

表 *51* : *[*管理（*Management*）*]* セクション テーブルのフィールド

フィールド	説明
ホスト	デバイスの IP アドレスまたはホスト名。ホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前（つまり、ホスト名）です。
ステータス	Firepower Management Center と管理対象デバイス間の通信チャネルのステータスを示すアイコン。ステータスアイコンにポインタを置くと、Firepower Management Center が最後にデバイスにアクセスした時間を表示することができます。

デバイスの詳細設定

[デバイス（Device）] タブの [詳細設定（Advanced）] セクションには、以下で説明する詳細設定のテーブルが表示されます。上記の設定は、いずれも [詳細設定（Advanced）] セクションを使用して編集できます。

表 *52* : *[*詳細設定（*Advanced*）*]* セクションのテーブルのフィールド

フィールド	説明	サポートされるデバイス
アプリケーションバイパス（Application Bypass）	デバイスでの自動アプリケーション バイパスの状態。	7000 & 8000 シリーズ、NGIPSv、ASA FirePOWER
バイパスしきい値（Bypass Threshold）	自動アプリケーションバイパスのしきい値（ミリ秒）。	7000 & 8000 シリーズ、NGIPSv、ASA FirePOWER
ローカルルータトラフィックを検査する（Inspect Local Router Traffic）	デバイスで、ルーテッド インターフェイスで受信した自己を宛先とするトラフィック（ICMP、DHCP、および OSPF トラフィックなど）を検査するかどうかを示します。	7000 & 8000 シリーズ
高速パス ルール（Fast-Path Rules）	デバイスで作成されている 8000 シリーズ高速パス ルールの数。	8000 シリーズ

デバイス情報の表示

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

マルチドメイン展開では、先祖ドメインは、子孫ドメイン内のすべてのデバイスに関する情報を表示できます。デバイスを編集するリーフ ドメインに位置している必要があります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 表示するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、先祖ドメインに位置している場合、表示アイコン（  ）をクリックすると、読み取り専用モードで子孫ドメインのデバイスを表示できます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 次の情報が表示されます。

- [全般（General）]：デバイスの一般設定を表示します（一般的なデバイスの設定, （467 ページ）を参照）。
- [ライセンス（License）]：デバイスのライセンス情報を表示します（デバイス ライセンスの設定, （467 ページ）を参照）。
- [システム（System）]：デバイスのシステム情報を表示します（デバイス システムの設定, （467 ページ）を参照）。
- [ヘルス（Health）]：デバイスの現在のヘルス ステータスに関する情報を表示します（デバイス ヘルスの設定, （468 ページ）を参照）。
- [管理（Management）]：Firepower Management Center とデバイスの間の通信チャネルに関する情報を表示します（デバイス管理設定, （468 ページ）を参照）。
- [詳細（Advanced）]：高度な機能設定に関する情報を表示します（デバイスの詳細設定, （469 ページ）を参照）。

デバイス管理設定の編集

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

（注） 場合によっては、（デバイスの LCD パネルまたは CLI などを使用して）別の方法でデバイスのホスト名や IP アドレスを編集する場合は、次の手順を実行して、管理用の Firepower Management Center でホスト名や IP アドレスを手動で更新する必要があります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 管理オプションを変更するデバイスの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブをクリックします。
ヒント スタック構成のデバイスの場合、アプライアンス エディタの[デバイス（Devices）]ページで、個々のデバイスの管理オプションを変更します。

ステップ 4 次の操作を実行できます。

- リモート管理の無効化：[管理（Management）]セクションのスライダをクリックして、デバイスの管理を有効または無効にします。管理を無効化すると、Firepower Management Center とデバイス間の接続がブロックされますが、Firepower Management Center からデバイスは削除**されません**。デバイスを管理する必要がなくなった場合は、Firepower Management Center からのデバイスの削除, （466 ページ）を参照してください。
- 管理ホストの編集：[管理（Management）]セクションの編集アイコン（）をクリックし、[ホスト（Host）] フィールドで名前または IP アドレスを変更し、[保存（Save）] をクリックします。この設定を使用して、管理ホスト名を指定したり、仮想 IP アドレスを再生成することができます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

一般的なデバイス設定の編集

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

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 [一般（General）] セクションで、編集アイコン（  ）をクリックします。

ステップ 5 [名前（Name）] に、管理対象デバイスの名前を入力します。

ヒント スタック構成のデバイスの場合、アプライアンス エディタの [スタック（Stack）] ページで、スタックでデバイスに割り当てられている名前を編集します。アプライアンス エディタの [デバイス（Devices）] ページでは、個々のデバイスに割り当てられているデバイス名を編集できます。

ステップ 6 [パケットの転送（Transfer Packets）] 設定を変更します。

- パケット データをイベントと一緒に Firepower Management Center に保存できるようにするには、[パケットの転送（Transfer Packets）] チェックボックスをオンにします。
- 管理対象デバイスがイベントと一緒にパケット データを送信できないようにするには、このチェックボックスをオフにします。

ステップ 7 [強制展開（Force Deploy）] をクリックし、デバイスに現在のポリシーとデバイス設定の展開を強制します。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

デバイス ライセンスの有効化と無効化

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

Firepower Management Center で使用可能なライセンスがある場合、デバイスでそのライセンスを有効にすることができます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 ライセンスを有効または無効にするデバイスの横にある編集アイコン（  ）をクリックします。マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ヒント スタック構成のデバイスの場合、アプライアンス エディタの [スタック（Stack）] ページで、スタックに対してラインセンスを有効または無効にします。

ステップ 4 [ライセンス（License）] セクションで、編集アイコン（  ）をクリックします。

ステップ 5 管理対象デバイスに対して有効または無効にするライセンスの横にあるチェックボックスをオンまたはオフにします。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

関連トピック

Firepower の機能ライセンスについて，（127 ページ）

詳細なデバイス設定の編集

アプリケーション バイパス、ローカル ルータ トラフィックのインスペクション、および高速パスのルールを設定できます。

自動アプリケーション バイパスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	7000 & 8000 シリーズ、NGIPSv、ASA FirePOWER	リーフのみ	Admin Network Admin

自動アプリケーション バイパス（AAB）機能は、インターフェイスでのパケット処理時間に制限を設け、この時間を超過した場合、パケットに検出のバイパスを許可します。この機能は任意の展開で使用できますが、インライン展開ではとりわけ価値があります。

パケット処理の遅延は、ネットワークで許容できるパケット レイテンシとバランスを取って調整します。Snort 内での不具合やデバイスの誤った設定が原因で、トラフィックの処理時間が指定のしきい値を超えると、AAB により、その障害発生から 10 分以内に Snort が再起動され、トラブルシューティング データが生成されます。このデータを分析することで、過剰な処理時間の原因を調査できます。

一般に、遅延しきい値を超えた後は、高速パス パケットに対して侵入ポリシーの [ルール遅延しきい値（Rule Latency Thresholding）] を使用します。[ルール遅延しきい値（Rule Latency Thresholding）] により、エンジンがシャットダウンされたり、しきい値データが生成されることはありません。

検出がバイパスされると、デバイスがヘルス モニタリング アラートを生成します。

注意 単一パケットに過剰な処理時間がかかっている場合、AAB がアクティブになります。AAB のアクティブ化は、いくつかのパケットのインスペクションを一時的に中断する Snort プロセスを部分的に再起動します。インスペクションが中断されている間に、パケットがドロップされるかインスペクションを行わずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 高度なデバイス設定を編集するデバイスの横にある編集アイコン（  ）をクリックします。マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブ（またはスタック構成のデバイスの場合は [スタック（Stack）] タブ）をクリックし、[詳細（Advanced）] セクションの編集アイコン（）をクリックします。

ステップ 4 [自動アプリケーション バイパス（Automatic Application Bypass）] をオンにします。

ステップ 5 [バイパスしきい値（Bypass Threshold）] に 250 ～ 60,000 ミリ秒を入力します。デフォルト設定は 3000 ミリ秒（ms）です。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ローカル ルータ トラフィックの検査

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

ローカル内トラフィックがレイヤ 3 展開のモニタ ルールと一致する場合、そのトラフィックは検査をバイパスすることがあります。トラフィックの検査を確認するには、[ローカル ルータ トラフィックの検査（Inspect Local Router Traffic）] を有効にします。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 高度なデバイス設定を編集するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Devices）] タブ（スタック構成のデバイスの場合は [スタック（Stack）] タブ）をクリックして、[詳細（Advanced）] セクションの編集アイコン（）をクリックします。

ステップ 4 7000 または 8000 シリーズ デバイスがルータとして展開されている場合は、[ローカル ルータ トラフィックの検査] をオンにして、例外トラフィックを検査します。

ステップ 5 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

高速パス ルールの設定（8000 シリーズ）

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

トラフィック処理の初期形式として、8000シリーズ高速パスルールでは、それ以上のインスペクションやロギングを行わずに8000シリーズデバイスを介してトラフィックを直接送信できます。（パッシブ展開では、8000 シリーズ高速パス ルールは単に分析を停止します）。各 8000 シリーズ高速パス ルールは、特定のセキュリティ ゾーンまたはインライン インターフェイス セットに適用されます。8000 シリーズ高速パス ルールはハードウェア レベルで機能するため、高速パス トラフィックには、次の単純な外部ヘッダーの基準のみを使用できます。

- 発信側および応答側の IP アドレスまたはアドレス ブロック
- プロトコル、および TCP と UDP の場合は、発信側および応答側のポート
- VLAN ID（Admin. VLAN ID）

デフォルトでは、8000シリーズ高速パスルールは指定した発信側から指定した応答側への接続に影響します。ルールの基準を満たすすべての接続を高速パス処理するには、どちらのホストが発信側か応答側かに関係なく、ルールを双方向にすることができます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 ルールを設定する 8000 シリーズ デバイスの横にある編集アイコン（  ）をクリックします。マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブ（またはスタック構成のデバイスの場合は [スタック（Stack）] タブ）をクリックし、[詳細（Advanced）] セクションの編集アイコン（）をクリックします。

ステップ 4 [新しい IPv4 ルール（New IPv4 Rule）] または [新しい IPv6 ルール（New IPv6 Rule）] をクリックします。

ステップ 5 [ドメイン（Domain）] ドロップダウン リストから、インライン セットまたはパッシブ セキュリティ ゾーンを選択します。

ステップ 6 高速パス処理するトラフィックを設定します。トラフィックは高速パス処理のためのすべての条件を満たしている必要があります。

- [発信側（Initiator）] および [応答側（Responder）]（必須）：発信側および応答側の IP アドレスまたはアドレス ブロックを入力します。
- [プロトコル（Protocol）]：プロトコルを選択するか、[すべて（All）] を選択します。

- [発信側ポート（Initiator Port）] および [応答側ポート（Responder Port）] : TCP および UDP トラフィックの場合は、発信側ポートと応答側ポートを入力します。フィールドを空白のままにするか、Any と入力して、すべての TCP または UDP トラフィックに一致するようにします。ポートのカンマ区切りリストを入力できますが、ポート範囲を入力することはできません。
- [VLAN] : VLAN ID を入力します。フィールドを空白のままにするか、Any と入力して、VLAN タグに関係なくすべてのトラフィックに一致するようにします。

ステップ 7 （任意）ルールを [双方向（Bidirectional）] にします。

ステップ 8 [保存（Save）] をクリックしてから、もう一度 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

システム シャットダウンの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	すべて（ASA FirePOWER を除く）	リーフのみ	Admin/Network Admin

（注） Firepower システムのユーザ インターフェイスでは、ASA FirePOWER のシャットダウンまたは再起動はできません。それぞれのデバイスをシャット ダウンする方法の詳細については、ASA の資料を参照してください。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 再起動するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ヒント スタックに含まれるデバイスの場合、アプライアンス エディタの [デバイス（Devices）] ページで、個々のデバイスをシャット ダウンまたは再起動します。

ステップ 4 デバイスをシャットダウンするには、[システム（System）] セクションでデバイスのシャットダウン アイコン（  ）をクリックします。

ステップ 5 プロンプトが表示されたら、デバイスのシャットダウンを確認します。

ステップ 6 デバイスを再起動するには、デバイスの再起動アイコン（  ）をクリックします。

ステップ 7 プロンプトが表示されたら、デバイスを再起動することを確認します。

インターフェイス テーブル ビュー

ハードウェア ビューの下にあるインターフェイス テーブル ビューには、デバイスで使用可能なすべてのインターフェイスが一覧表示されます。テーブル内のナビゲーション ツリーを展開すると、設定されているすべてのインターフェイスを表示できます。インターフェイスの横にある矢印アイコンをクリックして、インターフェイスを縮小または展開することで、サブコンポーネントの非表示/表示を切り替えることができます。このインターフェイス テーブル ビューには、各インターフェイスに関する以下の要約情報が表示されます。

従来のデバイスのインターフェイス

[MAC アドレス（MAC Address）] 列と [IP アドレス（IP Address）] 列が表示されるのは、8000 シリーズ デバイスのみです。詳細については、次の表を参照してください。

表 *53*：従来のデバイスのインターフェイス テーブル ビューのフィールド

フィールド	説明
[名前（Name）]	各インターフェイス タイプは、タイプとリンク ステート（該当する場合）を示す固有のアイコンによって表されます。名前またはアイコンの上にマウス ポインタを移動すると、インターフェイス タイプ、速度、デュプレックス モード（該当する場合）がツールチップに表示されます。インターフェイス アイコンについては、インターフェイスアイコン，（489ページ）を参照してください。 アイコンでは、インターフェイスの現在のリンク状態を示す表示方法が使用されています。次の 3 つの状態のいずれかが表示されます。 • エラー（  ） • 障害（  ） • 使用不可（  ） 論理インターフェイスのリンク状態は、親物理インターフェイスのリンク状態と同じです。ASA FirePOWER モジュールには、リンク状態は表示されません。無効化されたインターフェイスは、半透明のアイコンで表されます。 アイコンの右側に表示されるインターフェイス名は自動生成されます。ただし、ハイブリッド インターフェイスと ASA FirePOWER インターフェイスの名前はユーザが定義します。ASA FirePOWER インターフェイスについては、名前が付けられており、リンクを持つ有効なインターフェイスのみが表示されることに注意してください。 物理インターフェイスでは、物理インターフェイスの名前が表示されます。論理インターフェイスでは、物理インターフェイスの名前と、割り当てられている VLAN タグが表示されます。 ASA FirePOWER インターフェイスでは、複数のセキュリティ コンテキストがある場合は、セキュリティ コンテキストの名前とインターフェイスの名前が表示されます。セキュリティ コンテキストが 1 つしかない場合は、インターフェイスの名前のみが表示されます。
セキュリティ ゾーン（Security Zone）	インターフェイスが割り当てられているセキュリティ ゾーン。セキュリティ ゾーンを追加または編集するには、編集アイコン（  ）をクリックします。
使用者（Used by）	インターフェイスが割り当てられているインライン セット、仮想スイッチ、または仮想ルータ。ASA FirePOWER モジュールでは、[使用者（Used by）] 列は表示されません。

フィールド	説明
MAC アドレス（MAC Address）	スイッチド機能およびルーテッド機能で有効にされているインターフェイスに対して表示される MAC アドレス。 NGIPSv デバイスの場合、表示された MAC アドレスにより、デバイス上に設定されたネットワーク アダプタと、[インターフェイス（Interfaces）] ページに表示されるインターフェイスを対応させることができます。ASA FirePOWER モジュールでは、MAC アドレスは表示されません。
IP アドレス	インターフェイスに割り当てられた IP アドレス。マウスのポインタを IP アドレスの上に重ねると、その IP アドレスがアクティブであるか非アクティブであるかを確認できます。非アクティブな IP アドレスはグレー表示されます。ASA FirePOWER モジュールでは、IP アドレスは表示されません。

デバイス グループ管理

Firepower Management Center でデバイスをグループ化すると、複数のデバイスへのポリシーの展開やアップデートのインストールを簡単に行えます。グループに属するデバイスのリストは、展開または縮小表示できます。デフォルトでは、このリストは縮小表示されます。

マルチドメイン展開では、リーフ ドメイン内でのみデバイス グループを作成できます。Firepower Management Center をマルチテナンシー向けに設定すると既存のデバイス グループは削除されます。デバイス グループはリーフ ドメイン レベルで再度追加できます。

デバイス グループの追加

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

デバイス グループにより、複数デバイスへのポリシーの割り当てとインストール更新が簡単にできます。

スタック内または高可用性ペア内のプライマリ デバイスをグループに追加すると、両方のデバイスがグループに追加されます。デバイスのスタック構成を解除または高可用性ペアを分解しても、これらのデバイスは両方ともグループに属したままになります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 [追加（Add）] ドロップダウン メニューから、[グループの追加（Add Group）] を選択します。

ステップ 3 名前を入力します。

ステップ 4 [使用可能なデバイス（Available Devices）] から、デバイス グループに追加するデバイスを 1 つ以上選択します。複数のデバイスを選択する場合は、Ctrl または Shift キーを押しながらクリックします。

ステップ 5 [追加（Add）] をクリックして、選択したデバイスをデバイス グループに追加します。

ステップ 6 [OK] をクリックして、デバイス グループを追加します。

デバイス グループの編集

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

任意のデバイス グループに含まれる一連のデバイスを変更できます。アプライアンスは、現行のグループから削除してからでないと、新しいグループに追加できません。

アプライアンスを新しいグループに移動しても、そのアプライアンスのポリシーが、新しいグループにすでに割り当てられているポリシーに変更される訳ではありません。グループのポリシーを新しいデバイスに割り当てる必要があります。

スタック内またはデバイスのハイ アベイラビリティ ペア内のプライマリ デバイスをグループに追加すると、両方のデバイスがグループに追加されます。デバイスのスタック構成を解除または高可用性ペアを分解しても、これらのデバイスは両方ともグループに属したままになります。

マルチドメイン展開では、デバイス グループは、それらが作成されたドメイン内でのみ編集できます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 編集するデバイス グループの横にある編集アイコン（  ）をクリックします。

ステップ 3 必要に応じて、[名前（Name）] フィールドに、グループの新しい名前を入力します。

ステップ 4 [使用可能なデバイス（Available Devices）] から、デバイス グループに追加するデバイスを 1 つ以上選択します。複数のデバイスを選択する場合は、Ctrl または Shift キーを押しながらクリックします。

ステップ 5 [追加（Add）] をクリックして、選択したデバイスをデバイス グループに追加します。

ステップ 6 必要に応じて、デバイス グループからデバイスを削除するには、削除するデバイスの横にある削除アイコン（  ）をクリックします。

ステップ 7 [OK] をクリックして、デバイス グループに加えた変更を保存します。

第 VI 部

設定の基本

第 20 章

従来型デバイスの管理の基本

次のトピックでは、Firepower システムで従来型デバイス（7000 および 8000 シリーズデバイス、ASA with FirePOWER サービス、NGIPSv）を管理する方法について説明します。

リモート管理の設定

Firepower System デバイスを管理できるようにするには、デバイスと Firepower Management Center との間に双方向の SSL 暗号化通信チャネルをセットアップする必要があります。このチャネルを使用して、両方のアプライアンスが設定とイベント情報を共有します。ハイアベイラビリティピアも、このチャネルを使用します。このチャネルは、デフォルトではポート 8305/tcp に位置します。

（注） この章では、FMC にデバイスを登録する前にローカル Web インターフェイスを使用して、7000 または 8000 シリーズデバイスのリモート管理の設定方法について説明します。他のモデルのリモート管理の設定の詳細については、適切なクイックスタートガイドを参照してください。

2 つのアプライアンス間の通信を可能にするためには、アプライアンスが互いを認識する手段を提供しなければなりません。Firepower System では 3 つの基準を使用して、通信を許可します。

- 通信を確立する対象のアプライアンスのホスト名または IP アドレス。

  NAT 環境では、ルーティング可能なアドレスがもう一方のアプライアンスにないとしても、リモート管理を設定する際、または管理対象アプライアンスを追加する際には、ホスト名または IP アドレスのいずれかを指定する必要があります。

- 接続を識別するために自己生成される、最大 37 文字の英数字による登録キー。

- Firepower System が NAT 環境で通信を確立するために利用できるオプションの一意の英数字による NAT ID。

  NAT ID は、管理対象アプライアンスを登録するために使用されているすべての NAT ID の間で**一意でなければなりません**。

管理対象デバイス上のリモート管理の設定

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

手順

ステップ 1 管理するデバイスの Web インターフェイスで、[設定（Configuration）] > [ASA FirePOWER の設定（ASA FirePOWER Configuration）] > [統合（Integration）] > [リモート管理（Remote Management）] を選択します。

ステップ 2 [リモート管理（Remote Management）] タブが表示されていない場合は、クリックします。

ステップ 3 [マネージャの追加（Add Manager）] をクリックします。

ステップ 4 [管理ホスト（Management Host）] フィールドに、このアプライアンスを管理するために使用する Firepower Management Center について、次のいずれかを入力します。

- IP アドレス
- 完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前（つまり、ホスト名）

注意 ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

NAT 環境では、管理対象アプライアンスを追加する際に IP アドレスまたはホスト名を指定する予定の場合、ここで IP アドレスまたはホスト名を指定する必要はありません。その場合、Firepower システムは後で指定される NAT ID を使用して、管理対象アプライアンスの Web インターフェイス上のリモート マネージャを識別します。

ステップ 5 [登録キー（Registration Key）] フィールドに、アプライアンス間の通信をセットアップするために使用する登録キーを入力します。

ステップ 6 NAT 環境の場合は、[固有 NAT ID（Unique NAT ID）] フィールドに、アプライアンス間の通信をセットアップするために使用する、英数字による一意の NAT ID を入力します。

ステップ 7 [保存（Save）] をクリックします。

次の作業

- アプライアンスが相互に通信できることを確認し、ステータスとして [登録保留（Pending Registration）] が表示されるまで待ちます。
- このデバイスを Firepower Management Center に追加します。Firepower Management Center へのデバイスの追加, （464 ページ）を参照してください。

管理対象デバイスでのリモート管理の編集

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

リモート マネージャを編集するには、次の点に注意してください。

- [ホスト（Host）] フィールドでは、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前（つまり、ホスト名）を指定します。
- [名前（Name）] フィールドには、Firepower システムのコンテキストでのみ使用される、管理アプライアンスの表示名を指定します。別の表示名を入力しても、管理デバイスのホスト名は変更されません。

手順

ステップ 1 デバイスの Web インターフェイスで、[システム（System）] > [統合（Integration）] を選択します。

ステップ 2 まだ表示されていない場合は、[リモート管理（Remote Management）] タブをクリックします。

ステップ 3 次の操作を実行できます。

- リモート管理の無効化：マネージャの横にあるスライダをクリックして、これを有効または無効にします。管理を無効化すると、Firepower Management Center とデバイス間の接続がブロックされますが、Firepower Management Center からデバイスは削除**されません**。デバイスを管理する必要がなくなった場合は、Firepower Management Center からのデバイスの削除, （466 ページ）を参照してください。
- マネージャ情報の編集：変更するマネージャの横にある編集アイコン（  ）をクリックして、[名前（Name）] および [ホスト（Host）] フィールドをクリックし、[保存（Save）] をクリックします。

管理ポートの変更

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

アプライアンスは、双方向の SSL 暗号化通信チャネルを使用して通信します。このチャネルは、デフォルトではポート 8305 に位置します。

設定をデフォルトのままにすることを**強く**奨励します。管理ポートがネットワークでの他の通信と競合する場合には、他のポートを選択できます。通常、管理ポートの変更は、Firepower System のインストール時に行います。

注意 管理ポートを変更する場合は、導入内の相互に通信する必要があるすべてのアプライアンスの管理ポートを変更する必要があります。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [管理インターフェイス（Management Interfaces）] をクリックします。

ステップ 3 [共有設定（Shared Settings）] セクションで、[リモート管理ポート（Remote Management Port）] フィールドに使用するポート番号を入力します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- このアプライアンスと通信する必要がある、展開環境内のすべてのアプライアンスについて、この手順を繰り返します。

インターフェイス構成時の設定

アプライアンス エディタの [インターフェイス（Interfaces）] ページには、詳細なインターフェイス設定情報が表示されます。このページは、物理ハードウェア ビューとインターフェイステーブル ビューで構成されており、構成の詳細情報にドリルダウンできます。このページからインターフェイスを追加したり編集したりできます。

物理的なハードウェア ビュー

[インターフェイス（Interfaces）] ページの一番上には、7000 または 8000 シリーズ デバイスの物理的なハードウェア ビューがグラフィカル表示されます。

物理的なハードウェア ビューは、次の目的で使用します。

- ネットワーク モジュールのタイプ、部品番号、およびシリアル番号を確認する
- インターフェイス テーブル ビューでインターフェイスを選択する
- インターフェイス エディタを開く
- インターフェイスの名前、タイプ、リンクの有無、速度設定、およびインターフェイスがバイパス モードになっているかを確認する
- エラーまたは警告の詳細を参照する

インターフェイス アイコン

表 *54*：インターフェイス アイコンのタイプと説明

アイコン	インターフェイス タイプ	詳細
	物理的：未設定の物理インターフェイス。	物理スイッチドインターフェイスの設定，（681 ページ）または 物理ルーテッド インターフェイスの設定，（693 ページ）
	パッシブ：パッシブ展開でトラフィックを分析するように設定されているセンシング インターフェイス。	パッシブ インターフェイスの設定，（500 ページ）
	インライン：インライン展開でトラフィックを処理するように設定されているセンシング インターフェイス。	インライン インターフェイスの設定，（504 ページ）
	スイッチド：レイヤ 2 展開でトラフィックを切り替えるように設定されているインターフェイス。	スイッチド インターフェイスの設定，（680 ページ）
	ルーテッド：レイヤ 3 展開でトラフィックをルーティングするように設定されているインターフェイス。	ルーテッド インターフェイス，（692 ページ）

アイコン	インターフェイス タイプ	詳細
	集約：1つの論理リンクとして設定されている複数の物理インターフェイス。	集約インターフェイスについて，（731 ページ）
	集約スイッチド：レイヤ 2 展開で 1 つの論理リンクとして設定されている複数の物理インターフェイス。	集約スイッチドインターフェイスの追加，（738 ページ）
	集約ルーテッド：レイヤ 3 展開で 1 つの論理リンクとして設定されている複数の物理インターフェイス。	集約ルーテッドインターフェイスの追加，（741 ページ）
	ハイブリッド：仮想ルータと仮想スイッチ間でトラフィックをブリッジするように設定されている論理インターフェイス。	論理ハイブリッド インターフェイス，（749 ページ）
	ASA FirePOWER：ASA FirePOWER モジュールがインストールされた ASA デバイスに設定されているインターフェイス。	Cisco ASA FirePOWER インターフェイスの管理，（494 ページ）

物理ハードウェア ビューの使用

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

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 管理するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 グラフィカル インターフェイスを使用して、以下を実行できます。

- 選択：インターフェイスを選択する場合、インターフェイスアイコンをクリックします。システムは、インターフェイス テーブルの関連項目を強調表示します。

- 編集：インターフェイス エディタを開く場合、インターフェイス アイコンをダブルクリックします。
- エラーまたは警告情報の表示：エラーまたは警告に関する詳細を表示するには、ネットワーク モジュール上の影響を受けるポートの上にカーソルを置きます。
- インターフェイス情報の表示：インターフェイスの名前、インターフェイスのタイプ、インターフェイスにリンク画が存在するかどうか、インターフェイスの速度設定、インターフェイスが現在バイパス モードであるかどうかについて表示するには、インターフェイス上にカーソルを置きます。
- ネットワーク モジュール情報の表示：ネットワーク モジュールのタイプ、製品番号、シリアル番号を表示するには、ネットワーク モジュールの左下隅にある黒い円の上にカーソルを置きます。

センシング インターフェイスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	従来型（Classic）	リーフのみ	Admin/Network Admin

アプライアンス エディタの [インターフェイス（Interfaces）] ページで、Firepower システムの展開に応じて、管理対象デバイスのセンシング インターフェイスを設定できます。管理対象デバイスには、合計 1024 個のインターフェイスを設定できることに注意してください。

（注） Firepower Management Center では、ASA FirePOWER が SPAN ポート モードで展開されている場合、ASA インターフェイスを表示しません。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 インターフェイスを設定するデバイスの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 設定するインターフェイスの横にある編集アイコン（）をクリックします。

ステップ 4 インターフェイス エディタを使用して、センシング インターフェイスを設定します。

- [HA リンク（HA Link）]：デバイスのハイアベイラビリティ ペアの各メンバーに設定されたインターフェイスを、（ハイアベイラビリティ リンク インターフェイスとも呼ばれる）デバイス間の冗長通信チャネルとして機能させるには、[HA リンク（HA Link）] をクリックし、HA リンク インターフェイスの設定，（492 ページ）の説明に従って続行します。
- [インライン（Inline）]：設定されたインターフェイスでインライン展開のトラフィックを処理するように設定するには、[インライン（Inline）] をクリックし、インラインインターフェイスの設定，（504 ページ）の説明に従って続行します。
- [パッシブ（Passive）]：設定されたインターフェイスでパッシブ展開のトラフィックを分析するように設定するには、[パッシブ（Passive）] をクリックし、パッシブインターフェイスの設定，（500 ページ）の説明に従って続行します。
- [ルーテッド（Routed）]：設定されたインターフェイスでレイヤ 3 展開のトラフィックをルーティングするように設定するには、[ルーテッド（Routed）] をクリックし、ルーテッドインターフェイス，（692 ページ）の説明に従って続行します。
- [スイッチド（Switched）]：設定されたインターフェイスでレイヤ 2 展開のトラフィックをスイッチングするように設定するには、[スイッチド（Switched）] をクリックし、スイッチドインターフェイスの設定，（680 ページ）の説明に従って続行します。

ステップ 5 [保存（Save）] をクリックして構成を完了します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

HA リンク インターフェイスの設定

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

7000 または 8000 シリーズ デバイスの高可用性ペアを確立した後、物理インターフェイスをハイアベイラビリティ（HA）リンク インターフェイスとして設定できます。このリンクは、ペアリングされたデバイス間でヘルス情報を共有するために使用する、冗長通信チャネルとして機能します。1 つのデバイスに HA リンク インターフェイスを設定すると、自動的に 2 番目のデバイスにインターフェイスが設定されます。同じブロードキャスト ドメインに、両方の HA リンクを設定する必要があります。

ダイナミック NAT は、他の IP アドレスとポートにマップする IP アドレスとポートの動的割り当てに依存します。HA リンクがなければ、これらのマッピングはフェールオーバーで失われます。

その場合、変換されたすべての接続は高可用性ペアで新しくアクティブになったデバイスを介してルーティングされることになるため、それらの接続は失敗します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 HA リンク インターフェイスを設定するピアの横にある編集アイコン（  ）をクリックします。マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 HA リンク インターフェイスとして設定するインターフェイスの横にある編集アイコン（  ）をクリックします。

ステップ 4 [HA リンク（HA Link）] をクリックします。

ステップ 5 [有効（Enabled）] チェックボックスをオンにします。

（注） チェックボックスをオフにした場合、システムはインターフェイスを管理上停止し、無効にします。

ステップ 6 [モード（Mode）] ドロップダウン リストからリンク モードを指定するオプションを選択するか、[自動ネゴシエーション（Autonegotiation）] を選択して、速度とデュプレックスの設定を自動ネゴシエートするようにインターフェイスを設定します。

ステップ 7 [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または自動 MDIX のいずれかを指定するオプションを選択します。

（注） 通常、[MDI/MDIX] は [自動 MDIX（Auto-MDIX）] に設定します。これにより、MDI と MDIX の間の切り替えが自動的に処理され、リンクが確立されます。

ステップ 8 [MTU] フィールドに最大伝送ユニット（MTU）を入力します。
MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。詳細については、7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）を参照してください。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

ステップ 9 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

Snort® の再起動シナリオ，（324 ページ）
7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲，（495 ページ）

インターフェイスの無効化

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

インターフェイス タイプを[なし（None）]に設定することで、インターフェイスを無効にすることができます。無効にされたインターフェイスは、インターフェイス リストでグレー表示されます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 インターフェイスを無効にするデバイスの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 無効にするインターフェイスの横にある編集アイコン（）をクリックします。

ステップ 4 [なし（None）] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

Cisco ASA FirePOWER インターフェイスの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	ASA FirePOWER	リーフのみ	Admin/Network Admin

ASA FirePOWER インターフェイスを編集する際に、Firepower Management Center から設定できるのは、インターフェイスのセキュリティ ゾーンのみです。

ASA FirePOWER インターフェイスを完全に設定するには、ASA 専用ソフトウェアおよび CLI を使用します。ASA FirePOWER およびスイッチを編集して、マルチ コンテキスト モードからシングル コンテキスト モード（またはその逆）に切り替えると、ASA FirePOWER はそのインターフェイスの名前をすべて変更します。ASA FirePOWER の更新されたインターフェイス名を使用するように、すべての Firepower System セキュリティ ゾーン、相関ルール、関連する設定を再設定する必要があります。ASA FirePOWER インターフェイスの設定の詳細については、ASA のマニュアルを参照してください。

（注） ASA FirePOWER インターフェイスのタイプは変更できません。また、Firepower Management Center からインターフェイスを無効にすることもできません。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 インターフェイスを編集するデバイスの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インターフェイス（Interfaces）] タブが表示されていない場合は、そのタブをクリックします。

ステップ 4 編集するインターフェイスの横にある編集アイコン（）をクリックします。

ステップ 5 [セキュリティ ゾーン（Security Zone）] ドロップダウンリストから既存のセキュリティ ゾーンを選択するか、[新規（New）] を選択して新しいセキュリティ ゾーンを追加します。

ステップ 6 [保存（Save）] をクリックして、セキュリティ ゾーンを設定します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

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

デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

（注） システムは、設定された MTU 値から 18 バイトを切り捨てます。594 より小さい IPv4 MTU または 1298 より小さい IPv6 MTU を設定しないでください。

従来のデバイス モデル	MTU 範囲
7000 & 8000 シリーズ	576 ～ 9234（管理インターフェイス） 576 ～ 10172（インラインセット、パッシブインターフェイス） 576 ～ 9922（その他）
NGIPSv	576 ～ 9018（すべてのインターフェイス、インラインセット）

関連トピック

MTU について

セキュリティ ゾーン オブジェクトのリビジョンの同期

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

セキュリティゾーンオブジェクトを更新すると、システムはそのオブジェクトの新しいリビジョンを保存します。その結果、同じセキュリティ ゾーン内の管理対象デバイスに、インターフェイスで設定されたセキュリティ オブジェクトの異なるリビジョンがある場合、接続が重複しているようなログが記録される可能性があります。

接続の重複が報告されていることに気づいた場合、同じリビジョンのオブジェクトを使用するよう、すべての管理対象デバイスを更新できます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 セキュリティ ゾーンの選択を更新するデバイスの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 重複する接続のイベントを記録しているインターフェイスのそれぞれについて、[セキュリティゾーン（Security Zone）] を別のゾーンに変更して [保存（Save）] をクリックした後、目的のゾーンに再び設定し、もう一度 [保存（Save）] をクリックします。

ステップ 4 重複イベントを記録しているデバイスごとに、ステップ 2 から 3 を繰り返します。続行する前に、すべてのデバイスを編集する必要があります。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

注意 同期させるすべてのデバイスでインターフェイスのゾーン設定を編集するまでは、デバイスに設定変更を展開しないでください。すべての管理対象デバイスに同時に展開する必要があります。

第 21 章

IPS デバイスの展開と設定

以下のトピックでは、IPS 展開でデバイスを設定する方法について説明します。

IPS デバイスの展開と設定の概要

パッシブまたはインラインのいずれかの IPS 展開でデバイスを設定できます。パッシブ展開では、ネットワーク トラフィックのフローからアウトオブバンドでシステムを展開します。インライン展開では、2 つのポートを一緒にバインドすることで、ネットワーク セグメント上でシステムを透過的に設定します。

パッシブ IPS 展開

パッシブ（受動）IPS 展開では、Firepower システムはスイッチ SPAN またはミラー ポートを使用してネットワークを流れるトラフィックをモニタします。SPAN またはミラー ポートでは、スイッチ上の他のポートからトラフィックをコピーできます。これにより、ネットワーク トラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション（トラフィックのブロッキングやシェーピングなど）を実行することができません。パッシブ インターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。

（注） アウトバウンド トラフィックにはフロー制御パケットが含まれています。そのため、アプライアンスのパッシブ インターフェイスにアウトバウンド トラフィックが表示されることがあり、設定によっては、イベントが生成されることもあります。これは正常な動作です。

Firepower システムのパッシブ インターフェイス

管理対象デバイス上の 1 つ以上の物理ポートをパッシブ インターフェイスとして設定できます。

パッシブ インターフェイスがトラフィックをモニタすることを可能にする場合、銅線インターフェイスでのみ使用可能なモードおよび MDI/MDIX 設定を指定します。8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

パッシブ インターフェイスを無効にする場合、ユーザはセキュリティのためにアクセスできなくなります。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

パッシブ インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 パッシブ インターフェイスを設定するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 パッシブインターフェイスとして設定するインターフェイスの横にある編集アイコン（  ）をクリックします。

ステップ 4 [パッシブ（Passive）] をクリックします。

ステップ 5 セキュリティ ゾーンにパッシブ インターフェイスを関連付けるには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して、新しいセキュリティ ゾーンを追加します。セキュリティ ゾーン オブジェクトの作成, （392 ページ）を参照してください。

ステップ 6 [有効（Enabled）] チェックボックスをオンにします。
このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 7 7000 & 8000 シリーズのみ：[モード（Mode）] ドロップダウン リストからリンク モードを指定するか、または [自動ネゴシエーション（Auto Negotiation）] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようにインターフェイスを設定します。
モード設定は銅線インターフェイスにのみ使用できます。

8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

ステップ 8 7000 & 8000 シリーズのみ：[MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または自動 MDIX のいずれかを指定します。
[MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。

デフォルトでは、[MDI/MDIX] は [自動 MDIX（Auto-MDIX）] に設定され、MDI と MDIX の間の切り替えを自動的に処理してリンクを確立します。

ステップ 9 [MTU] フィールドに最大伝送ユニット（MTU）を入力します。
MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

ステップ 10 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

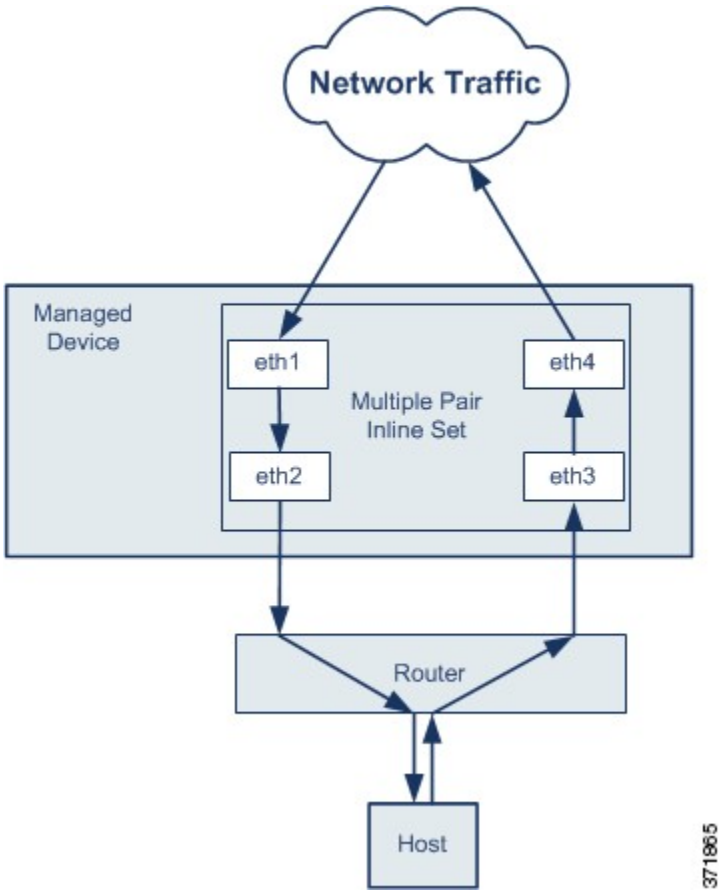
インライン IPS 展開

インライン IPS 展開では、2 つのポートを一緒にバインドすることで、ネットワーク セグメント上で Firepower システムを透過的に設定します。これによって、隣接するネットワーク デバイスの設定がなくても、任意のネットワーク環境にシステムをインストールすることができます。インライン インターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インライン セットの外部に再送信されます。

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

デバイス トラフィックがインバウンドであるかアウトバウンドであるかに応じて、異なるインライン インターフェイス ペアを介してネットワーク上のホストと外部ホスト間のトラフィックをルーティングするように、管理対象デバイスのインターフェイスを設定できます。これは非同期ルーティング設定です。非同期ルーティングを展開し、インライン セットに 1 つのインターフェイス ペアしか含めないと、デバイスがトラフィックの半分しか認識しないため、ネットワーク トラフィックが適切に分析されない可能性があります。同じインライン インターフェイス セットに複数のインライン インターフェイス ペアを追加すると、システムがインバウンド トラフィックとアウトバウンド トラフィックを同じトラフィック フローの一部として識別できるようになります。これは、同じセキュリティ ゾーンにインターフェイス ペアを含めることによっても実現できます。

非同期ルーティング構成を通過するトラフィックから接続イベントが生成された場合、そのイベントは同じインライン インターフェイス ペアの入力インターフェイスと出力インターフェイスを識別できます。たとえば、次の図の構成では、eth3 を入力インターフェイス、eth2 を出力インターフェイスとして識別する接続イベントが生成されます。これは、この構成の予期される動作です。



（注） 単一のインライン インターフェイス セットに複数のインターフェイス ペアを割り当てたときに、重複トラフィックの問題が発生した場合は、システムがパケットを一意に識別できるように再設定します。たとえば、別のインライン セットにインターフェイス ペアを再度割り当てるか、セキュリティ ゾーンを変更することができます。

インライン セットを使用するデバイスでは、デバイス再起動後にパケットを転送するようソフトウェア ブリッジが自動的にセットアップされます。デバイスが再起動しているときには、実行中のソフトウェア ブリッジがありません。インライン セットでパイパス モードを有効にすると、デバイスの再起動中にハードウェア バイパスになります。その場合、システムが停止して再起動する際に、デバイスとのリンクの再ネゴシエーションが原因で数秒間のパケットが失われる可能性があります。ただし、Snort の再起動中にシステムはトラフィックを通過させます。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

Firepower システムのインライン インターフェイス

管理対象デバイス上の 1 つ以上の物理ポートをインライン インターフェイスとして設定できます。インライン インターフェイスがインライン展開環境のトラフィックを処理するには、その前に、インライン インターフェイスのペアをインライン セットに割り当てる必要があります。

（注）

- インラインペアのインターフェイスをそれぞれ異なる速度に設定した場合、またはインターフェイスが異なる速度にネゴシエートされる場合は、システムによって警告が出されます。
- インターフェイスをインラインインターフェイスとして設定すると、そのインターフェイスの NetMod 上の隣接ポートも自動的にインライン インターフェイスとなり、インライン インターフェイスのペアが完成します。
- NGIPSv デバイスでインライン インターフェイスを設定するには、隣接するインターフェイスを使用してインライン ペアを作成する必要があります。

インライン インターフェイスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 インターフェイスを設定するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 設定するインターフェイスの横にある編集アイコン（  ）をクリックします。

ステップ 4 [インライン（Inline）] をクリックします。

ステップ 5 インラインインターフェイスをセキュリティゾーンと関連付ける場合は、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。

- [新規（New）] を選択して、新しいセキュリティ ゾーンを追加します。セキュリティ ゾーン オブジェクトの作成, （392 ページ）を参照してください。

ステップ 6 [インライン セット（Inline Set）] ドロップダウン リストから既存のインライン セットを選択するか、[新規（New）] を選択して新しいインライン セットを追加します。

（注） 新しいインライン セットを追加する場合は、インライン インターフェイスを設定した後、設定する必要があります。インライン セットの追加, （507 ページ）を参照してください。

ステップ 7 [有効（Enabled）] チェックボックスをオンにします。
このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8 7000 & 8000 シリーズのみ：[モード（Mode）] ドロップダウン リストからリンク モードを指定するか、または [自動ネゴシエーション（Auto Negotiation）] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようにインターフェイスを設定します。
モード設定は銅線インターフェイスにのみ使用できます。

8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

ステップ 9 7000 & 8000 シリーズのみ：[MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または自動 MDIX のいずれかを指定します。
[MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。

デフォルトでは、[MDI/MDIX] は [自動 MDIX（Auto-MDIX）] に設定され、MDI と MDIX の間の切り替えを自動的に処理してリンクを確立します。

ステップ 10 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

Firepower システムのインライン セット

インライン展開でインラインインターフェイスを使用するには、事前に、インラインセットを設定してインラインインターフェイス ペアをそれらに割り当てる必要があります。インラインセットは、デバイス上の 1 つ以上のインライン インターフェイス ペアからなるグループです。インライン インターフェイス ペアは、一度に 1 つのインライン セットにのみ属することができます。

[デバイス管理（Device Management）] ページの [インライン セット（Inline Sets）] タブには、デバイスに設定されているすべてのインライン セットのリストが表示されます。

[デバイスの管理（Device Management）] ページの [インライン セット（Inline Sets）] タブからインラインセットを追加できます。または、インラインインターフェイスを設定するときにインライン セットを追加できます。

インライン セットにはインライン インターフェイス ペア**のみ**を割り当てることができます。管理対象デバイスでインラインインターフェイスを設定する前にインラインセットを作成する必要がある場合は、空のインライン セットを作成し、後からそれにインターフェイスを追加できます。インライン セットの名前を入力する場合は、英数字とスペースを使用できます。

[名前（Name）]

インライン セットの名前。

インターフェイス

インライン セットに割り当てられているすべてのインライン ペアのリスト。[インターフェイス（Interfaces）] タブでペアのいずれかのインターフェイスを無効にした場合、そのペアは含まれません。

MTU

インライン セットの最大伝送ユニット。MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

フェールセーフ（Failsafe）

トラフィックに検出のバイパスと、デバイス経由の続行を許可します。管理対象デバイスは、内部トラフィック バッファをモニタし、それらのバッファが満杯である場合は検出をバイパスします。

バイパス モード（Bypass Mode）

Firepower 7000 または 8000 シリーズ のみ：インライン セットの設定済みバイパス モード。この設定により、インターフェイスに障害が発生した場合のインライン インターフェイスのリレーの応答方法が決まります。バイパスモードは、トラフィックがインターフェイスを通過し続けることを許可します。非バイパス モードは、トラフィックをブロックします。

注意 バイパス モードでは、アプライアンスの再起動時に少数のパケットが失われることがあります。高可用性ペアの 7000 または 8000 シリーズ デバイスのインライン セット、NGIPSv デバイスのインライン セット、8000 シリーズ デバイスの非バイパス NetMod、Firepower 7115 または 7125 デバイスの SFP モジュールには、バイパス モードを設定できません。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

インライン セットの表示

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

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 インライン セットを表示するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インライン セット（Inline Sets）] タブをクリックします。

インライン セットの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 インライン セットを追加するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インライン セット（Inline Sets）] タブをクリックします。

ステップ 4 [インライン セットの追加（Add Inline Set）] をクリックします。

ステップ 5 名前を入力します。

ステップ 6 [インターフェイス（Interfaces）] の横で、1 つ以上のインライン インターフェイス ペアを選択し、選択項目の追加アイコン（  ）をクリックします。すべてのインターフェイス ペアをインライン セットに追加するには、「すべてを追加」アイコン（  ）をクリックします。

ヒント インライン セットからインライン インターフェイスを削除するには、1 つ以上のインライン インターフェイス ペアを選択して、選択項目の削除アイコン（  ）をクリックします。インライン セットからすべてのインターフェイス ペアを削除するには、「すべてを削除」アイコン（  ）をクリックします。また、[インターフェイス（Interfaces）] タブでペアのいずれかのインターフェイスを無効にすると、ペアが削除されます。

ステップ 7 [MTU] フィールドに最大伝送ユニット（MTU）を入力します。
MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

ステップ 8 に検出をバイパスさせ、デバイス にトラフィックを通すには、[フェールセーフ（Failsafe）] を選択します。
管理対象デバイスは、内部トラフィック バッファをモニタし、それらのバッファが満杯である場合は検出をバイパスします。

ステップ 9 7000 および 8000 シリーズ の場合のみ、バイパス モードを指定します:

- トラフィックがインターフェイスを通過し続けることを許可するには、[バイパス（Bypass）] をクリックします。
- トラフィックをブロックするには、[バイパスしない（Non-Bypass）] をクリックします。

（注） 高可用性ペアの 7000 または 8000 シリーズ デバイスのインライン セット、NGIPSv デバイスのインライン セット、8000 シリーズ デバイスの非バイパス ネットワーク モジュール、Firepower 7115 または 7125 デバイスの SFP モジュールには、バイパス モードを設定できません。

ステップ 10 必要に応じて、詳細な設定を行います。インライン セットの詳細オプション, （509 ページ） を参照してください。

ステップ 11 [OK] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

インライン セットの詳細オプション

インライン セットを設定する際に考慮できる詳細オプションがいくつかあります。

タップ モード

7000 および 8000 シリーズ デバイスでは、インライン（またはフェール オープン可能なインライン）インターフェイス セットを作成するときにタップ モードを使用できます。

タップ モードの場合、デバイスはインラインで展開されますが、パケットがデバイスを通過する代わりに各パケットのコピーがデバイスに送信され、ネットワーク トラフィック フローは影響を受けません。パケット自体ではなくパケットのコピーを処理するので、パケットをドロップするように設定したルールおよび置換キーワードを使用するルールはパケット ストリームに影響を及ぼしません。ただし、これらのタイプのルールでは、トリガーされた侵入イベントが生成され、侵入イベントのテーブル ビューには、トリガーの原因となったパケットがインライン展開でドロップされたことが示されます。

インライン展開されたデバイスでタップ モードを使用することには、利点があります。たとえば、デバイスがインラインであるかのようにデバイスとネットワークの間の配線をセットアップし、デバイスが生成するタイプの侵入イベントを分析することができます。その結果に基づいて、効率性に影響を与えることなく最適なネットワーク保護を提供するように、侵入ポリシーを変更して廃棄ルールを追加できます。デバイスをインラインで展開する準備ができたら、タップ モードを無効にして、デバイスとネットワーク間の配線を再びセットアップせずに、不審なトラフィックのドロップを開始することができます。

ただし、同じインラインセットに対してこのオプションと厳格な TCP 強制を有効にすることはできません。

リンク ステートの伝達（Propagate Link State）

リンク ステートの伝達は、インラインセットのペアの両方で状態を追跡できるようにするためにバイパス モードで設定されるインライン セットの機能です。リンク ステートの伝達は、銅線と光ファイバの両方の設定可能なバイパス インターフェイスで使用できます。

リンク ステートの伝達によって、インライン セットのインターフェイスの 1 つが停止した場合、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、2番目のインターフェイスも自動的に起動します。つまり、1 つのインターフェイスのリンク ステートが変化すると、アプライアンスはその変化を検知し、それに合わせて他のインターフェイスのリンク ステートを更新します。ただし、アプライアンスがリンク ステートの変更を伝達するのに最大 4 秒かかります。

リンク ステートの伝達は、ルータが障害状態のネットワークデバイスを避け、トラフィックを自動的に再ルーティングするよう設定された、復元力の高いネットワーク環境では特に有効です。

リンク ステートの伝達は 7000 および 8000 シリーズ デバイスのみでサポートされていることに注意してください。

高可用性ペアの 7000 および 8000 シリーズ デバイスで設定されたインライン セットのリンク ステートの伝達を無効にすることはできません。

トランスペアレント インライン モード（Transparent Inline Mode）

[トランスペアレント インライン モード（Transparent Inline Mode）] オプションを使用すると、デバイスを「Bump In The Wire」として機能させることができます。つまり、デバイスは、送信元と宛先に関係なく、認識するすべてのネットワーク トラフィックを転送するということです。7000 および 8000 シリーズのデバイスではこのオプションを無効にできないことに注意してください。

厳格な TCP 強制（Strict TCP Enforcement）

最大限の TCP セキュリティを実現するため、厳格な強制を有効にすることができます。この機能は、3 ウェイ ハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
- 応答側が SYN-ACK を送信する前に TCP 接続の発信側から送信された非 SYN/RST パケット
- SYN の後、セッションの確立前に TCP 接続のレスポンダから送信された非 SYN-ACK/RST パケット
- 発信側または応答側のどちらかから送信された、確立された TCP 接続の SYN パケット

なお、このオプションは、7000 および 8000 シリーズ デバイスでのみ使用できます。また、同じインライン セットに対してこのオプションとタップ モードを有効にすることはできません。

高度なインライン セット オプションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 インライン セットを編集するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インライン セット（Inline Sets）] タブをクリックします。

ステップ 4 編集するインライン セットの横にある編集アイコン（  ）をクリックします。

ステップ 5 [Advanced] タブをクリックします。

ステップ 6 インライン セットの詳細オプション，（509 ページ）の説明に従ってオプションを設定します。

ステップ 7 [OK] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

インライン セットの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	リーフのみ	Admin/Network Admin

インラインセットを削除すると、そのセットに割り当てられたインラインインターフェイスを別のセットに含めることができるようになります。それらのインターフェイスは削除されません。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 インライン セットを削除するデバイスの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インライン セット（Inline Sets）] タブをクリックします。

ステップ 4 削除するインライン セットの横にある削除アイコン（  ）をクリックします。

ステップ 5 プロンプトが表示されたら、インライン セットを削除することを確認します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

第 VII 部

のハイ アベイラビリティと拡張性

第 22 章

7000 および 8000 シリーズ デバイスのハイ アベイラビリティ

次の各トピックでは、Firepower システムにおける Firepower 7000 シリーズおよび 8000 シリーズ デバイスのハイ アベイラビリティの設定方法について説明します。

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

7000 および 8000 シリーズ デバイス ハイ アベイラビリティを利用することで、2 つのピア デバイス間または 2 つのピア デバイス スタック間のネットワーキング機能と設定データの冗長性を確保できます。

2 つのピア デバイスまたは 2 つのピア デバイス スタックを、ポリシーの展開、システムの更新、登録を行う単一の論理システムとして機能するハイ アベイラビリティ ペアとして構成することにより、構成の冗長性を実現できます。その他の設定データは、システムによって自動的に同期されます。

（注） スタティック ルート、非 SFRP IP アドレス、およびルーティングの優先順位は、ピア デバイスまたはピア デバイス スタック間で同期されません。各ピア デバイスまたはピア デバイス スタックは、独自のルーティング インテリジェンスを維持します。

関連トピック

SFRP, （700 ページ）
仮想スイッチの詳細設定, （687 ページ）

デバイスのハイ アベイラビリティ要件

7000 および 8000 シリーズ デバイスのハイ アベイラビリティ ペアを構成するには、以下に従う必要があります。

- 単一デバイスと単一デバイスのペア、またはデバイス スタックとデバイス スタックのペアのみを構成できます。
- 両方のデバイスまたはデバイス スタックが正常なヘルス ステータスであり、同じソフトウェアを実行し、同じライセンスが有効になっている必要があります。詳細については、ヘルス モニタの使用, （271 ページ）を参照してください。特に、デバイスでのハードウェア障害は許容されません。ハードウェア障害が発生すると、デバイスがメンテナンス モードに入り、フェールオーバーがトリガーされます。

  （注） デバイスのペアを構成した後は、ペアを構成する個々のデバイスのライセンス オプションを変更することはできませんが、ハイ アベイラビリティ ペア全体のライセンスは変更できます。

- 各デバイスまたはスタック内の各プライマリ デバイスにインターフェイスを設定する必要があります。
- 両方のデバイスまたはデバイス スタックのプライマリ メンバーが同じモデルである必要があり、銅ケーブルまたは光ファイバの同じインターフェイスが必要です。
- デバイス スタックのハードウェア構成は同一でなければなりませんが、インストール済みのマルウェア ストレージ パックについてはその限りではありません。たとえば、Firepower 8290 と別の 8290 のペアを構成することができます。どちらかのスタック内でマルウェア ストレージ パックが、どのデバイスに存在しなくても、1 つのデバイスにのみ、またはすべてのデバイスに存在しても構いません。

注意 シスコから供給されたハード ドライブ以外はデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、シスコから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パックのサポートが必要な場合は、サポートにお問い合わせください。詳細については、*Firepower System Malware Storage Pack Guide*を参照してください。

- デバイスが NAT ポリシーのターゲットとなっている場合、両方のピアに同じ NAT ポリシーを適用する必要があります。
- マルチドメイン展開では、7000 または 8000 シリーズ デバイスのハイ アベイラビリティまたはリーフ ドメイン内のデバイス スタックのみを確立できます。

デバイス ハイ アベイラビリティ フェールオーバーとメンテナンス モード

7000 および 8000 シリーズ デバイス ハイ アベイラビリティのフェールオーバーは、手動または自動で行われます。手動でフェールオーバーをトリガーするには、ペアを構成するデバイスまたはスタックのいずれかでメンテナンス モードを開始します。

自動フェールオーバーは、アクティブ デバイスまたはアクティブ スタックの正常性が損なわれた場合、システム更新時、または管理者権限によりデバイスがシャットダウンされた場合に発生します。また、自動フェールオーバーは、アクティブ デバイスまたはデバイス スタックで NMSB 障害、NFE 障害、ハードウェア障害、ファームウェア障害、重大なプロセス障害、ディスク フル エラー、または2つのスタック構成のデバイス間のリンク障害が起きた場合にも発生します。バックアップ のデバイスまたはスタックの正常性がアクティブ デバイス同様に損なわれている場合は、フェールオーバーは行われず、クラスタは縮退状態になります。また、いずれかのデバイスまたはデバイス スタックがメンテナンス モードになっている場合も、フェールオーバーは行われません。アクティブ スタックからスタック ケーブルを切断すると、そのスタックはメンテナンス モードに入ることに注意してください。アクティブ スタックのセカンダリ デバイスをシャットダウンした場合も、スタックはメンテナンス モードに入ります。

（注） ハイ アベイラビリティ ペアのアクティブなメンバーがメンテナンス モードになり、アクティブ ロールが他のペア メンバーにフェールオーバーされた場合、元のアクティブ ペアのメンバーは、通常動作に復帰したときに自動的にアクティブ ロールを再要求しません。

デバイスの高可用性ペアでのポリシーの導入と更新

ポリシーを導入する際は、個々のデバイスやデバイス スタックではなく、デバイスの高可用性ペアにポリシーを導入します。ポリシーの導入が失敗すると、システムはいずれのデバイスまたはスタックにもポリシーを導入しません。ポリシーは最初にアクティブ デバイスまたはスタックに

導入されてから、バックアップに導入されます。したがって、高可用性ペアでは常に、ピアのいずれかがネットワーク トラフィックを処理します。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。このインスペクション中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。 Firepower 7010、7020、および 7030 の管理対象デバイスでは、設定変更の展開に最大 5 分かかる場合があります。利用できない時間を最小限にするために、導入は変更時間帯に実行します。Snort® の再起動シナリオ, （324 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定, （327 ページ）を参照してください。

個々のデバイスまたはスタックが更新を受信するのではなく、高可用性ペアを構成するデバイスが単一のエンティティとして更新を受信します。更新が開始されると、システムは最初にバックアップ デバイスまたはスタックに更新を導入します。それによって、そのデバイスまたはスタックはメンテナンス モードに入ります。この状態は、必要なプロセスが再開してデバイスがトラフィックの処理を再び開始するまで維持されます。その後、システムはアクティブ デバイスまたはスタックに更新を導入して、同じプロセスを行います。

展開タイプとデバイス ハイ アベイラビリティ

7000 または 8000 シリーズ デバイスのハイ アベイラビリティ構成は、Firepower システム展開（パッシブ、インライン、ルーテッド、またはスイッチド）に応じて決定します。同時に複数のロールを持たせてシステムを展開することもできます。4 つの展開タイプのうち、ハイ アベイラビリティを用いた冗長性をもたらすためにデバイスまたはスタックの構成が必要になるのは、パッシブ展開のみです。他の展開タイプでは、デバイス ハイ アベイラビリティを使用しても使用しなくてもネットワークの冗長性を確立できます。各展開タイプにおけるハイ アベイラビリティの概要については、以降の各項を参照してください。

（注） レイヤ 3 の冗長性については、デバイス ハイ アベイラビリティを使わずに、Cisco Redundancy Protocol（SFRP）により実現できます。SFRP では、指定した IP アドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。ネットワークの冗長性では、2 つのデバイスまたは 2 つのスタックが同一のネットワーク接続を提供するように設定することで、ネットワーク上の他のホストに対する接続を維持できます。

パッシブ展開での冗長性

一般に、パッシブ インターフェイスは中央スイッチのタップ ポートに接続されます。この場合、スイッチを通過するトラフィックのすべてを、パッシブ インターフェイスで分析することが可能になります。複数のデバイスが同じタップ フィードに接続されている場合、システムはそれぞれのデバイスからイベントを生成します。ハイ アベイラビリティ ペアとして構成されているデバイ

スは、アクティブまたはバックアップ のいずれかとして機能するため、システムはシステム障害が発生したとしてもトラフィックを分析できると同時に、重複するイベントを防止できます。

インライン展開での冗長性

インライン セットは、自身を通過するパケットのルーティングを制御できないため、展開環境で常にアクティブになっていなければなりません。したがって、冗長性を確立できるかどうかは、外部システムがトラフィックを適切にルーティングするかどうかに依存します。冗長インライン セットは、7000 または 8000 シリーズ デバイスのハイ アベイラビリティを使用しても使用しなくても設定できます。

冗長インライン セットを展開するには、循環ルーティングを防止する一方で、トラフィックがインラインセットのいずれか 1 つだけを通過できるようにネットワーク トポロジーを設定します。インライン セットのいずれかで障害が発生すると、周辺ネットワークインフラストラクチャがゲートウェイ アドレスへの接続が切断されたことを検出し、ルートを調整して冗長セット経由でトラフィックを送信します。

ルーテッド展開での冗長性

IP ネットワーク内のホストは、既知のゲートウェイ アドレスを使用してトラフィックをさまざまなネットワークに送信する必要があります。ルーテッド展開で冗長性を確立するには、ルーテッドインターフェイスがゲートウェイ アドレスを共有し、そのアドレスに対するトラフィックを常に 1 つのインターフェイスだけが処理するようにしなければなりません。そのためには、仮想ルータで同じ数の IP アドレスを維持する必要があります。1 つのインターフェイスがアドレスをアドバタイズします。そのインターフェイスがダウンすると、バックアップ インターフェイスがアドレスのアドバタイズを開始します。

ハイ アベイラビリティ ペアのメンバーではないデバイスでは、複数のルーティングされたインターフェイス間で共有するゲートウェイ IP アドレスの設定し、SFRP によって冗長性を確保します。SFRP は、7000 または 8000 シリーズ デバイスのハイ アベイラビリティを使用しても使用しなくても設定できます。また、OSPF や RIP などのダイナミック ルーティングを使用して冗長性を確保することもできます。

スイッチド展開での冗長性

スイッチド展開では、高度な仮想スイッチ設定の 1 つであるスパニング ツリープロトコル（STP）を使用して冗長性を確保します。STP はブリッジ型ネットワーク トポロジを管理するプロトコルです。このプロトコルは、バックアップ リンクを設定することなく、冗長リンクでスイッチド インターフェイスの自動バックアップ を行えるように設計されています。スイッチド展開でのデバイスは、STP に依存して、冗長インターフェイス間のトラフィックを管理します。同じブロードキャスト ネットワークに接続されている 2 つのデバイスは、STP によって計算されたトポロジに基づいてトラフィックを受信します。

（注） 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアに展開する予定の仮想スイッチを設定する際には、STP を有効にするよう強く推奨します。

デバイスのハイ アベイラビリティ設定

7000 または 8000 シリーズ デバイスのハイ アベイラビリティを確立する際には、デバイスまたはスタックのうちの一方をアクティブとして指定し、もう一方をバックアップとして指定します。システムは、マージした設定を、ペアを構成するデバイスに適用します。競合が存在する場合、システムはアクティブとして指定されたデバイスまたはスタックの設定を適用します。

デバイスのペアを構成した後は、ペアを構成する個々のデバイスのライセンス オプションを変更することはできませんが、ハイ アベイラビリティ ペア全体のライセンスは変更できます。スイッチド インターフェイスまたはルーテッド インターフェイスで設定しなければならないインターフェイス属性がある場合、システムはハイ アベイラビリティ ペアを確立しますが、そのステータスを保留中に設定します。ユーザが必要な属性を設定した後、システムはハイ アベイラビリティ ペアを完成させて、正常なステータスに設定します。

ハイ アベイラビリティ ペアを確立した後、[デバイス管理（Device Management）] ページでは、ピア デバイスまたはスタックが単一のデバイスとして扱われます。デバイスのハイ アベイラビリティ ペアは、アプライアンス リストではハイ アイコン アイコン（  ）が表示されます。ユーザが行った設定変更は、いずれもペアを構成するデバイスの間で同期されます。[デバイス管理（Device Management）] ページには、ハイ アベイラビリティ ペアのどのデバイスまたはスタックがアクティブであるかが表示されます。アクティブなデバイスまたはスタックは、手動または自動フェールオーバーが発生すると変更されます。

デバイスのハイ アベイラビリティ ペアの登録を Firepower Management Center から削除すると、その登録は両方のデバイスまたはスタックから削除されます。デバイスのハイ アベイラビリティ ペアを Firepower Management Center から削除する方法は、個々の管理対象デバイスを削除する場合の方法と同じです。

登録が削除されたハイ アベイラビリティ ペアは、別の Firepower Management Center に登録できます。ハイ アベイラビリティ ペアを構成する一方のデバイスを登録するには、ペアのうちアクティブ デバイスにリモート管理を追加してから、そのデバイスを Firepower Management Center に追加します。これにより、ペア全体が追加されます。ハイ アベイラビリティ ペアのうちスタック構成のデバイスを登録するには、どちらか一方のスタックのプライマリ デバイスにリモート管理を追加してから、そのデバイスを Firepower Management Center に追加します。これにより、ペア全体が追加されます。

デバイスのハイ アベイラビリティ ペアを確立すると、ハイ アベイラビリティ リンク インターフェイスを設定できます。

デバイスのハイ アベイラビリティの確立

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

7000 & 8000 シリーズ デバイスのハイ アベイラビリティ ペアを確立する際には、デバイスまたはスタックのうちの一方をアクティブとして指定し、もう一方をバックアップとして指定します。システムは、マージした設定を、ペア内のデバイスに適用します。競合が存在する場合、システムはアクティブとして指定されたデバイスまたはスタックの設定を適用します。

マルチドメイン展開では、ハイ アベイラビリティ ペアのデバイスは同じドメインに属している必要があります。

はじめる前に

- すべての要件が満たされていることを確認します。デバイスのハイ アベイラビリティ要件, （516 ページ）を参照してください。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 [追加（Add）] ドロップダウン メニューから、[ハイ アベイラビリティの追加（Add High Availability）] を選択します。

ステップ 3 名前を入力します。

ステップ 4 デバイスまたはスタックにロールを割り当てます。

a) [アクティブ（Active）][アクティブ ピア（Active Peer）] のデバイスまたはスタックをハイ アベイラビリティ ペア用に選択します。

b) [バックアップ（Backup）][スタンバイ ピア（Standby Peer）] のデバイスまたはスタックをハイ アベイラビリティ ペア用に選択します。

ステップ 5 [追加（Add）]をクリックします。このプロセスではデータの同期が行われるため、プロセスが完了するまでに数分かかります。

デバイスのハイ アベイラビリティの編集

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

7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアを確立した後は、デバイス設定を変更すると、通常はハイ アベイラビリティ ペア全体の設定も変更されます。

[一般（General）]セクションのステータス アイコンにマウスのポインタを合わせると、ハイ アベイラビリティ ペアのステータスが表示されます。また、ペア内のデバイスまたはスタックのどれがアクティブ ピアで、どれがバックアップ ピアであるかも確認できます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 設定を編集するデバイスのハイ アベイラビリティ ペアの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [ハイ アベイラビリティ（High Availability）] ページのセクションを使用して、単一のデバイス設定を変更する場合と同じように、ハイ アベイラビリティ ペアの設定を変更します。

高可用性ペアの個々のデバイスの設定

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

7000 または 8000 シリーズ デバイスの高可用性ペアを確立した後でも、ペア内の個々のデバイスに対して設定できる属性がいくつかあります。ペアリングされたデバイスに変更を加える方法は、単一のデバイスに変更を加える場合の方法と同じです。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 設定を編集するデバイスの高可用性ペアの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス] タブをクリックします。

ステップ 4 [選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するデバイスを選択します。

ステップ 5 [デバイス（Devices）] ページのセクションを使用して、単一のデバイスに対して変更を加える場合と同じように、ペアリングされた個々のデバイスに変更を加えます。

高可用性ペアの個々のデバイス スタックの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	Control	Firepower 8140、Firepower 8200 ファミリ、Firepower 8300 ファミリ	リーフのみ	Admin/Network Admin

高可用性ペアにスタック構成の 8000 シリーズ デバイスを設定すると、編集可能なスタック属性が制限されます。ペアリングされたスタックの名前は編集できます。また、高可用性ペアのデバイスでのインターフェイスの設定, （524 ページ）で説明している手順に従って、スタックのネットワーク設定を編集できます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 設定を編集するデバイスの高可用性ペアの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [スタック（Stacks）] タブをクリックします。

ステップ 4 [選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するスタックを選択します。

ステップ 5 [一般（General）] セクションの横にある編集アイコン（  ）をクリックします。

ステップ 6 名前を入力します。

ステップ 7 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

高可用性ペアのデバイスでのインターフェイスの設定

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

7000 または 8000 シリーズ デバイスの高可用性ペアの個々のデバイスに、インターフェイスを設定できます。ただし、その場合には、ペアのピア デバイスにも同等のインターフェイスを設定する必要があります。ペアリングされたスタックの場合は、スタックのプライマリ デバイスのそれぞれに、同じインターフェイスを設定する必要があります。仮想ルータを設定するときに、その仮想ルータを設定するスタックを選択します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 インターフェイスを設定するデバイスの高可用性ペアの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インターフェイス（Interfaces）] タブをクリックします。

ステップ 4 [選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するデバイスを選択します。

ステップ 5 個々のデバイスに設定する場合と同じようにインターフェイスを設定します。

関連トピック

仮想ルータ設定, （702 ページ）

デバイスのハイ アベイラビリティ ペアにおけるアクティブ ピアの切り替え

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

7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアを確立した後、アクティブなピア デバイスまたはスタックをバックアップに手動で切り替えることができます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 アクティブ ピアを変更するデバイスのハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン（  ）をクリックします。

ステップ 3 次の操作を実行できます。

- ハイ アベイラビリティ ペアでバックアップ ピアをアクティブ ピアにすぐに切り替える場合は、[はい（Yes）] をクリックします。
- キャンセルして[デバイス管理（Device Management）]ページに戻る場合は、[いいえ（No）] をクリックします。

高可用性ピアのメンテナンス モードへの切り替え

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

7000 または 8000 シリーズ デバイス高可用性ペアを設定した後で、デバイスのメンテナンスを実行するために、いずれかのピアをメンテナンス モードに切り替えることで、手動でフェールオーバーをトリガーできます。メンテナンス モードでは、システムが管理目的で管理インターフェイスを除くすべてのインターフェイスをダウンさせます。メンテナンスの完了後、ピアを再度有効にして、通常の動作を再開できます。

（注） 高可用性ペアの両方のピアを同時にメンテナンス モードにしないでください。これを行うと、そのペアではトラフィックを検査できなくなります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 メンテナンスモードを開始するピアの横にあるメンテナンスモード切り替えアイコン（）をクリックします。

ステップ 3 [はい（Yes）] をクリックして、メンテナンス モードを確定します。

次の作業

- メンテナンスが完了したら、メンテナンスモード切り替えアイコン（）を再度クリックして、ピアのメンテナンス モードを終了します。

高可用性ペアのスタック内のデバイスの交換

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	Control	Firepower 8140、8200 ファミリ、8300 ファミリ	任意（Any）	Admin/Network Admin

高可用性ペアのメンバーになっているスタックをメンテナンス モードに切り替えた後で、スタック内のセカンダリ デバイスを別のデバイスと交換できます。選択できるデバイスは、現在スタックのメンバーにも、ペアにもなっていないデバイスのみです。新しいデバイスは、デバイス スタックを確立する場合と同じガイドラインに従っている必要があります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 メンテナンス モードを開始するスタック メンバーの横にあるメンテナンス モード切り替えアイコン（）をクリックします。

ステップ 3 [はい（Yes）] をクリックして、メンテナンス モードを確定します。

ステップ 4 デバイス交換アイコン（）をクリックします。

ステップ 5 ドロップダウンリストから [交換デバイス（Replacement Device）] を選択します。

ステップ 6 [交換（Replace）] をクリックして、デバイスを交換します。

ステップ 7 メンテナンス モード切り替えアイコン（）を再度クリックすると、スタックのメンテナンス モードが即時に終了します。

（注） デバイス設定を再展開する必要はありません。

デバイスのハイ アベイラビリティ状態共有

デバイスのハイ アベイラビリティ状態共有を使用すると、ハイ アベイラビリティ ペアのデバイスまたはスタックで、可能な限り状態を同期できます。したがって、いずれか一方のデバイスまたはスタックで障害が発生しても、もう一方のピアがトラフィック フローを中断せずに引き継ぐことができます。状態共有を使用しない場合、以下の機能が適切にフェールオーバーしない可能性があります。

- 厳格な TCP 強制
- 単方向アクセス コントロール ルール
- ブロッキングの永続性

ただし、状態共有を有効にすると、システム パフォーマンスが低下することに注意してください。

ハイ アベイラビリティ状態共有を設定するには、あらかじめハイ アベイラビリティ ペアの両方のデバイスまたはスタック構成のプライマリ デバイスで HA リンク インターフェイスを設定し、有効にする必要があります。Firepower 82xx ファミリおよび 83xx ファミリには 10 G の HA リンクが必要ですが、他のモデルのデバイスには 1 G の HA リンクで十分です。

HA リンク インターフェイスを変更する前に、状態共有を無効にする必要があります。

（注） ペアを構成するデバイスでフェールオーバーが発生した場合は、アクティブ デバイス上の既存の SSL 暗号化セッションがすべて終了されます。ハイ アベイラビリティ状態共有を設定しているとしても、これらのセッションをバックアップ デバイスで再ネゴシエートする必要があります。SSL セッションを確立しているサーバがセッションの再利用をサポートしている場合でも、バックアップ デバイスに SSL セッション ID がないと、セッションを再ネゴシエートできません。

厳格な TCP 強制

ドメインに対して厳密な TCP 適用を有効にすると、システムは TCP セッションで正常ではないパケットをすべてドロップします。たとえば、未確立の接続で受信した SYN 以外のパケットはドロップされます。状態共有が有効な場合、厳密な TCP 適用が有効にされているとしても、ハイ アベイラビリティ ペアのデバイスは、フェールオーバー後に接続を再び確立することなく TCP セッションを続行できます。厳密な TCP 適用は、インライン セット、仮想ルータ、および仮想スイッチで有効にすることができます。

単方向アクセス コントロール ルール

単方向アクセス コントロール ルールを設定している場合、システムがフェールオーバーの後に接続ミッドストリームを再評価する際に、ネットワーク トラフィックが意図されたものとは異なるアクセス コントロール ルールに一致する可能性があります。たとえば、ポリシーに以下の 2 つのアクセス コントロール ルールが含まれているとします。

```
Rule 1: Allow from 192.168.1.0/24 to 192.168.2.0/24
Rule 2: Block all
```

状態共有が有効でない場合、フェールオーバーの後に 192.168.1.1 ～ 192.168.2.1 からの許可される接続がまだアクティブになっているために、次のパケットが応答パケットとしてみなされると、システムは接続を拒否します。状態共有が有効であれば、ミッドストリーム ピックアップが既存の接続に一致することになり、接続が引き続き許可されます。

ブロッキングの永続性

アクセス コントロール ルールやその他の要素に基づいて、最初のパケットで多数の接続がブロックされるとしても、システムが接続のブロッキングを決定する前に、いくつかのパケットを許可する場合があります。状態共有が有効な場合、システムはピア デバイスまたはスタックでも即時に接続をブロックします。

ハイ アベイラビリティ ペアの状態共有を確立するときに、次のオプションを設定できます。

[有効（Enabled）]

状態共有を有効にするには、このチェックボックスをクリックします。チェックボックスをクリアすると、状態共有が無効になります。

最短フロー寿命（Minimum Flow Lifetime）

最小セッション時間（ミリ秒）を指定します。この時間を経過すると、システムがセッションの同期メッセージを送信します。0 ～ 65535 の整数を使用できます。この最小フロー有効期間に達しないセッションは、いずれも同期されず、接続のパケットを受信した時点でのみ、同期が行われます。

最短同期間隔インターバル（Interval

セッションの更新メッセージ最短間隔（ミリ秒）を指定します。0 ～ 65535 の整数を使用できます。最短同期間隔を設定することで、特定の接続が最短有効期間に達した後、その接続に対して、設定された値より頻繁に同期メッセージが送信されないようにします。

HTTP URL の最大文字数（Maximum HTTP URL Length）

ペアを構成するデバイス間で同期する、URL の最大文字数を指定します。0 ～ 225 の整数を使用できます。

関連トピック

HA リンク インターフェイスの設定, （492 ページ）

デバイスのハイ アベイラビリティ状態共有の確立

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

デバイスのハイ アベイラビリティ状態共有を使用すると、ハイ アベイラビリティ ペア内の 7000 または 8000 シリーズ デバイスまたはスタック間で、可能な限り状態を同期できます。したがって、いずれか一方のデバイスまたはスタックで障害が発生しても、もう一方のピアがトラフィック フローを中断せずに引き継ぐことができます。

注意 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ状態共有オプションを変更すると、プライマリ デバイスとセカンダリ デバイスの Snort プロセスが再起動され、両方のデバイスのトラフィック インスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

手順

ステップ 1 デバイスのハイ アベイラビリティ ペアのデバイスごとに HA リンク インターフェイスを設定します。HA リンク インターフェイスの設定, （492 ページ）を参照してください。

ステップ 2 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 3 編集するデバイス ハイ アベイラビリティ ペアの横にある編集アイコン（  ）をクリックします。マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 4 [状態共有（State Sharing）] セクションの横にある編集アイコン（  ）をクリックします。

ステップ 5 状態共有の値を下げてペア内のピアの準備状況を改善するか、値を上げてパフォーマンスを向上できるようにします。

（注） シスコでは、展開で値を変更する正当な理由がない限り、デフォルト値を使用することを推奨しています。

ステップ 6 [OK] をクリックして変更を保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

HA リンク インターフェイスの設定, （492 ページ）
Snort® の再起動シナリオ , （324 ページ）

トラブルシューティングのためのデバイスのハイアベイラビリティの状態共有統計情報

以下の項では、デバイスごとに表示可能な統計情報と、7000 および 8000 シリーズ デバイスのハイ アベイラビリティ ペアの状態共有設定をトラブルシューティングするためにどのように利用できるかを説明します。

受信メッセージ（ユニキャスト）（Messages Received (Unicast)）

ペアを構成するピアから受信した、ハイ アベイラビリティ同期メッセージの数です。

値は、ピアが送信したメッセージ数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。トラフィックが停止すると、値は安定し、受信したメッセージ数が送信されたメッセージ数と一致します。

トラブルシューティングを行う場合は、受信したメッセージ数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同等であることを確認します。各ピアでの送信数の値は、対応するピアでの受信数の値とほぼ同じ率で増えていなければなりません。

受信したメッセージの数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

受信パケット数（Packets received）

システムはオーバーヘッドを低減させるために、複数のメッセージを単一のパケットにまとめます。[受信パケット数（Packets Received）] カウンタは、デバイスが受信したこれらのデータ パケットとその他の制御パケットの数を表示します。

値は、ピア デバイスが送信したパケット数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。受信メッセージの数は、ピアが送信したメッセージ数と同等で、同じ率で増加していなければなりません。したがって、受信したパケットの数も同じ動作となるはずです。

トラブルシューティングを行う場合は、受信したパケットと送信されたメッセージの両方を確認して増加率を比較し、値が同じ率で増加していることを確認します。ペアを構成するピアでの送信の値が増えている場合、デバイスでの受信の値も同じ率で増えているはずです。

受信したパケットの数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

合計受信バイト数（Total Bytes Received）

ピアで受信されたパケットの合計バイト数です。

値は、もう一方のピアが送信したバイト数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信した合計バイト数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同じ率で増えていることを確認します。ペアを構成するピアでの送信の値が増えている場合、デバイスでの受信の値も同じ率で増えているはずです。

受信バイト数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

受信プロトコル バイト数（Protocol Bytes Received）

受信したプロトコル オーバーヘッドのバイト数です。この数には、セッション状態同期メッセージのペイロードを除くすべてが含まれます。

値は、ピアが送信したバイト数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信した合計バイト数を確認してプロトコル データと比較し、実際の状態データがどれだけ共有されているのかを調べます。プロトコル データが送信されるデータの大部分を占めている場合は、最小同期間隔を調整できます。

受信したプロトコル バイト数が、受信した合計バイト数と同等の割合で増えている場合は、サポートに連絡してください。受信したプロトコル バイト数が受信した合計バイト数に占める割合は、最小限でなければなりません。

送信メッセージ（Messages Sent）

ペアを構成するピアに送信した、ハイ アベイラビリティ同期メッセージの数です。

このデータは、受信メッセージ数との比較で役立ちます。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信したメッセージ数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同等であることを確認します。

送信したメッセージ数が、受信した合計バイト数と同等の割合で増えている場合は、サポートに連絡してください。

送信バイト数（Bytes Sent）

ピアに送信したハイ アベイラビリティ同期メッセージの合計送信バイト数です。

このデータは、受信メッセージ数との比較で役立ちます。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。ピアで受信されたバイト数は、この値と同等であり、それより大きい値にはなっていないはずです。

受信した合計バイト数が、送信されたバイト数と同じような比率で増えていない場合は、サポートに連絡してください。

Tx Errors

システムがペアを構成するピアに送信するメッセージ用にスペースを割り当てるときに、メモリ割り当てに失敗した回数です。

この値は両方のピアで常にゼロでなければなりません。この数がゼロでない場合、あるいは着実に増加している場合（これは、システムにメモリ割り当てが不可能なエラーが発生していることを示します）は、サポートに連絡してください。

Tx オーバーラン（Tx Overruns）

システムがメッセージをトランジット キューに入れようとして失敗した回数です。

この値は両方のピアで常にゼロでなければなりません。値がゼロでない場合、あるいは着実に増加している場合、これは、システムが HA リンクの間で過剰なデータを共有していて、データの送信に時間がかかりすぎていることを示します。

HA リンク MTU がデフォルト値（9918 または 9922）未満に設定されている場合は、値を増やす必要があります。最小フロー有効期間と最小同期間隔の設定を変更することで、HA リンク間で共有されるデータ量を減らし、この数の増加を防ぐことができます。

この値がゼロにならない場合、または増加し続けている場合は、サポートに連絡してください。

最近のログ（Recent Logs）

システム ログには、最新のハイ アベイラビリティ同期メッセージが表示されます。ログには、ERROR または WARN メッセージが示されていてはなりません。ログの内容は、常にピア間で同等でなければなりません（接続ソケットの数が同じであるなど）。

ただし、場合によっては、対照的なデータが表示されることもあります。たとえば、一方のピアがもう一方のピアから接続を受信したことをレポートしている場合、それぞれのログで参照される IP アドレスは異なります。このログから、ハイ アベイラビリティ状態共有接続を包括的に理解し、接続で発生したすべてのエラーを確認できます。

ログに、ERROR または WARN メッセージ、あるいは単なる通知目的ではないようなメッセージが示されている場合は、サポートに連絡してください。

デバイス ハイ アベイラビリティの状態共有統計情報の表示

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

状態共有を確立した後は、[ハイ アベイラビリティ（High Availability）] ページの [状態共有（State Sharing）] セクションで、設定に関する以下の情報を確認できます。

- 使用されている HA リンク インターフェイスおよび現在のリンク状態
- 問題のトラブルシューティングに使用できる、同期に関する詳細な統計情報

状態共有の統計情報は、主に、送受信されたハイ アベイラビリティ同期トラフィックのさまざまな側面に関するカウンタで、その他のエラーカウンタも含まれます。さらに、ハイアベイラビリティ ペアのデバイスごとの最新システム ログも表示できます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 編集するデバイス ハイ アベイラビリティ ペアの横にある編集アイコン（  ）をクリックします。マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [状態共有（State Sharing）] セクションで、統計情報表示アイコン（  ）をクリックします。

ステップ 4 ハイ アベイラビリティ ペアがデバイス スタックで構成されている場合、表示する [デバイス（Device）] を選択します。

ステップ 5 次の操作を実行できます。

- [更新（Refresh）] をクリックして統計情報を更新します。
- [表示（View）] をクリックして、ハイ アベイラビリティ ペアのデバイスごとの最新システム ログを表示します。

デバイス高可用性ペアの分離

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

7000 または 8000 シリーズ デバイス高可用性ペアを分離（分断）すると、次のようになります。

- アクティブなピア（デバイスまたはスタック）は、完全な展開機能を維持します
- バックアップ ピア（デバイスまたはスタック）はインターフェイス設定を失って、アクティブ ピアにフェールオーバーします。ただし、インターフェイス設定をアクティブのままにすることを選択すると、バックアップ ピアは通常の動作を再開します。
- バックアップ ピアは、常にパッシブ インターフェイスの設定を失います。
- メンテナンス モードのピアは、通常の動作を再開します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 分断する高可用性ペアの横にある HA の分断アイコン（  ）をクリックします。

ステップ 3 必要に応じて、バックアップ ピアのインターフェイス設定を削除するためのチェックボックスをオンにします。
この手順により、管理インターフェイス以外のすべてのインターフェイスを管理のためにダウンさせます。

ステップ 4 [Yes] をクリックします。

第 23 章

8000 シリーズ デバイスのスタック構成

次のトピックでは、Firepower システムにおける Firepower 8000 シリーズ デバイス スタックの使用方法について説明します。

デバイス スタックについて

スタック構成に含まれるデバイスを使用して、ネットワーク セグメントで検査されるトラフィックの量を増やすことができます。それぞれのスタック構成では、スタックに含まれるすべてのデバイスが同じハードウェアを使用していなければなりません。ただし、マルウェア ストレージ パックが一部またはすべてのデバイスにインストールされていたり、どのデバイスにもインストールされていなかったりする場合があります。また、以下のスタック構成に従って、同じデバイス ファミリのデバイスを使用する必要があります。

スタック構成は Firepower 8140、Firepower 8200 ファミリ、Firepower 8300 ファミリのデバイスでサポートされます。

81xx ファミリの場合：

- 2 台の Firepower 8140

82xx ファミリの場合：

- 最大 4 台の Firepower 8250
- 1 台の Firepower 8260（プライマリ デバイスおよびセカンダリ デバイス）
- 1 台の Firepower 8270（容量 40 G のプライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 台の Firepower 8290（容量 40 G のプライマリ デバイスと 3 つのセカンダリ デバイス）

83xx ファミリの場合：

- 最大 4 台の Firepower 8350
- 最大 4 つの AMP8350
- 1 台の Firepower 8360（容量 40 G のプライマリ デバイスと 1 つのセカンダリ デバイス）
- 1 つの AMP8360（容量 40 G のプライマリ デバイスとセカンダリ デバイス）
- 1 台の Firepower 8370（容量 40 G のプライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの AMP8370（容量 40 G のプライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 台の Firepower 8390（容量 40 G のプライマリ デバイスと 3 つのセカンダリ デバイス）
- 1 つの AMP8390（容量 40 G のプライマリ デバイスと 3 つのセカンダリ デバイス）

スタック構成の詳細については、*Cisco Firepower 8000 Series Getting Started Guide*を参照してください。マルウェア ストレージ パックの詳細については、*Firepower System Malware Storage Pack Guide*を参照してください。*Firepower System Malware Storage Pack Guide*

注意 シスコから供給されたハード ドライブ以外はデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、シスコから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パックのサポートが必要な場合は、サポートにお問い合わせください。詳細については、*Firepower System Malware Storage Pack Guide*を参照してください。

スタック構成を確立するときに、各スタック構成デバイスのリソースを 1 つの共有構成に統合します。

1つのデバイスをプライマリ デバイスとして指定し、そのデバイスにスタック全体のインターフェイスを設定します。その他のデバイスはセカンダリ デバイスとして指定します。セカンダリ デバイスは、現在トラフィックを検知していないデバイスで、かつインターフェイス上にリンクがないデバイスでなければなりません。

単一のデバイスを設定する場合と同じように、プライマリデバイスを分析対象のネットワークセグメントに接続します。*Cisco Firepower 8000 Series Getting Started Guide*で説明されているスタック構成のデバイスの配線手順に従って、セカンダリ デバイスをプライマリ デバイスに接続します。

スタック構成に含まれるすべてのデバイスは、同じハードウェアを使用し、同じソフトウェアバージョンを実行し、同じライセンスが適用されている必要があります。デバイスが NAT ポリシーのターゲットとなっている場合は、プライマリデバイスとセカンダリデバイスの両方に同じ NAT ポリシーを適用する必要があります。更新は、Firepower Management Center からスタック全体に対して展開する必要があります。スタック構成の1つ以上のデバイスで更新に失敗した場合、スタックはバージョンが混在した状態になります。バージョンが混在するスタックには、ポリシーを展開することも、更新を展開することもできません。この状態を修正するには、スタックを解除するか、バージョンが異なる個々のデバイスを削除し、それらのデバイスを個別に更新してからスタック構成を再確立します。デバイスをスタックに入れた後は、ライセンスの変更は、スタック全体に対してのみ行うことができます。

スタック構成を確立した後は、スタック構成に含まれるすべてのデバイスが単一の共有構成のように機能します。プライマリデバイスで障害が発生した場合、トラフィックはセカンダリデバイスに渡されません。この場合、セカンダリデバイスでスタック ハートビートが失敗したことを通知する、ヘルス アラートが生成されます。

スタック内のセカンダリ デバイスで障害が発生すると、設定可能なバイパスが有効になっているインライン セットがプライマリ デバイス上でバイパス モードになります。それ以外のすべての設定では、システムは、失敗したセカンダリデバイスへ継続してトラフィックをロードバランスします。いずれの場合も、リンクが失われたことを示すためのヘルス アラートが生成されます。

デバイス スタックは展開内で単一のデバイスと同じように使用できますが、いくつかの例外があります。ハイ アベイラビリティ ペアに 7000 または 8000 シリーズ デバイスがある場合は、デバイスのハイ アベイラビリティ ペアまたはハイ アベイラビリティ ペアのデバイスをスタックできません。また、デバイス スタックに NAT を設定することもできません。

（注） スタック構成のデバイスからのイベント データを、eStreamer を使用して外部クライアント アプリケーションに配信する場合は、各デバイスからデータを収集して、各デバイスが同じように設定されていることを確認します。eStreamer 設定は、スタック構成のデバイス間で自動的に同期されません。

マルチドメイン展開では、同じドメインに属しているデバイスのみをスタックできます。

関連トピック

ヘルス モニタリングについて，（251 ページ）

デバイス スタック設定

2 台の Firepower 8140 デバイス、最大 4 台の Firepower 8250、1 台の Firepower 8260、1 台の Firepower 8270、1 台の Firepower 8290、最大 4 台の Firepower 8350、1 台の Firepower 8360、1 台の Firepower 8370、または 1 台の Firepower 8390 をスタック構成し、それらを組み合わせたリソースを単一の

共有設定で使用することによって、ネットワーク セグメントで検査されるトラフィック量を増やすことができます。ハイ アベイラビリティ ペアに 7000 または 8000 シリーズ デバイスがある場合、デバイスのハイ アベイラビリティ ペア、またはハイ アベイラビリティ ペアの一方のデバイスのスタックは構成できません。ただし、2 つのデバイス スタックのハイ アベイラビリティ ペアを構成できます。

デバイス スタックを確立すると、これらのデバイスは、[デバイス管理（Device Management）] ページで単一のデバイスとして扱われます。デバイス スタックには、アプライアンスのリストでスタック アイコン（）が表示されます。

デバイス スタックの登録を Firepower Management Center から削除すると、その登録は両方のデバイスから削除されます。スタックに含まれるデバイスを Firepower Management Center から削除する方法は、単一の管理対象デバイスを削除する場合と同じです。削除したスタックは、別の Firepower Management Center に登録できます。新しい Firepower Management Center に、スタックに含まれるデバイスのいずれか 1 つを登録するだけで、スタック全体が表示されるようになります。

デバイス スタックを確立した後は、スタックを解除して再確立しない限り、デバイスのプライマリまたはセカンダリとしての役割を変更することはできません。ただし、次の作業を実行できます。

- 最大 4 台の Firepower 8250 を 1 つのスタックの限度として、2 台または 3 台の Firepower 8250、1 台の Firepower 8260、または 1 台の Firepower 8270 からなる既存のスタックにセカンダリ デバイスを追加できます。
- 最大 4 台の Firepower 8350 を 1 つのスタックの限度として、2 台または 3 台の Firepower 8350、1 台の Firepower 8360、または 1 台の Firepower 8370 からなる既存のスタックにセカンダリ デバイスを追加できます。

デバイスを追加する場合、スタックのプライマリ デバイスに、追加のデバイスを配線するために必要なスタック NetMods がなければなりません。たとえば、プライマリに単一のスタック NetMod しかない Firepower 8260 を使用している場合、このスタックに別のセカンダリ デバイスを追加することはできません。セカンダリ デバイスを既存のスタックに追加する方法は、最初にスタックに含まれるデバイスの設定を確立したときの方法と同じです。

デバイス スタックの確立

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
該当なし	任意（Any）	Firepower 8140、8200 ファミリ、8300 ファミリ	任意（Any）	Admin/Network Admin

スタック内のすべてのデバイスが同じハードウェア モデル（たとえば、Firepower 8140 と別の 8140）である必要があります。8200 ファミリおよび 8300 ファミリでは、合計 4 つのデバイス（1 つのプライマリ デバイスと最大 3 つのセカンダリ デバイス）でスタックを構成できます。

マルチドメイン展開では、スタック内のすべてのデバイスが同じドメインに属している必要があります。

はじめる前に

- プライマリ デバイスとして指定するユニットを決定します。
- プライマリとセカンダリの関係を指定する前に、ユニット間の配線が適切に行われていることを確認します。ケーブルについては、*Cisco Firepower 8000 Series Getting Started Guide*を参照してください。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 [追加（Add）] ドロップダウン メニューから、[スタックの追加（Add Stack）] を選択します。

ステップ 3 [プライマリ（Primary）] ドロップダウン リストから、プライマリ デバイスとして運用するために配線したデバイスを選択します。

（注） プライマリ デバイスとして配線されていないデバイスを選択すると、以降の手順を実行できなくなります。

ステップ 4 名前を入力します。

ステップ 5 [追加（Add）] をクリックし、スタックに含めるデバイスを選択します。

ステップ 6 [プライマリ デバイスのスロット（Slot on Primary Device）] ドロップダウン リストから、プライマリ デバイスをセカンダリ デバイスに接続するスタック構成ネットワーク モジュールを選択します。

ステップ 7 [セカンダリ デバイス（Secondary Device）] ドロップダウン リストから、セカンダリ デバイスとして運用するために配線したデバイスを選択します。

ステップ 8 [セカンダリ デバイスのスロット（Slot on Secondary Device）] ドロップダウン リストから、セカンダリ デバイスをプライマリ デバイスに接続するスタック構成ネットワーク モジュールを選択します。

ステップ 9 [追加（Add）] をクリックします。

ステップ 10 複数の Firepower 8250、1 つの Firepower 8260、1 つの Firepower 8270 の既存のスタック、複数の Firepower 8350、1 つの Firepower 8360 または 1 つの Firepower 8370 の既存のスタックにセカンダリ デバイスを追加する場合は、手順 5 ～ 9 を繰り返します。

ステップ 11 [スタック（Stack）]をクリックし、デバイス スタックを確立するか、セカンダリ デバイスを追加します。このプロセスではシステム データの同期が行われるため、プロセスが完了するまでに数分かかることに注意してください。

関連トピック

7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて, （515 ページ）
Firepower Management Center からのデバイスの削除, （466 ページ）
Firepower Management Center へのデバイスの追加, （464 ページ）

デバイス スタックの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
該当なし	任意（Any）	Firepower 8140、Firepower 8200 ファミリ、Firepower 8300 ファミリ	リーフのみ	Admin/Network Admin

デバイス スタックを確立した後は、デバイス設定を変更すると、通常はスタック全体の設定も変更されます。単一のデバイスの [デバイス（Device）] ページで設定を変更する場合と同じように、アプライアンス エディタの [スタック（Stack）] ページで、スタック設定に変更を加えることができます。

スタックの表示名を変更したり、ライセンスを有効または無効にしたり、システム ポリシーや正常性ポリシーを表示したり、詳細設定を構成したりすることができます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2 設定を編集する、スタックに含まれるデバイスの横にある編集アイコン（  ）をクリックします。マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [スタック（Stack）] ページのセクションを使用して、単一のデバイス設定を変更する場合と同じように、スタック構成の設定を変更します。

スタック内のデバイスの交換

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	任意（Any）	FirePOWER 8140、8200 ファミリ、8300 ファミリ	任意（Any）	Admin/Network Admin

Firepower Management Center がデバイスと通信できない場合に、スタックを分離してデバイスの登録を解除するには、デバイスに接続して CLI コマンドを使用する必要があります。詳細については、関連する章「コンフィギュレーション コマンド, （2226 ページ）」の **stacking disable** CLI コマンドおよび **delete** CLI コマンドを参照してください。

スタック内のデバイスを交換するには、以下を行います。

手順

ステップ 1 デバイスを含むスタックを選択し、そのスタックを交換して解除します。詳細については、スタック構成のデバイスの分離, （544 ページ）を参照してください。

ステップ 2 Firepower Management Center からデバイスを登録解除します。詳細については、Firepower Management Center からのデバイスの削除, （466 ページ）を参照してください。

ステップ 3 交換デバイスを Firepower Management Center に登録します。詳細については、Firepower Management Center へのデバイスの追加, （464 ページ）を参照してください。

ステップ 4 交換デバイスを含むデバイス スタックを作成します。詳細については、デバイス スタックの確立, （538 ページ）を参照してください。

高可用性ペアのスタック内のデバイスの交換

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	Control	Firepower 8140、8200 ファミリ、8300 ファミリ	任意（Any）	Admin/Network Admin

高可用性ペアのメンバーになっているスタックをメンテナンス モードに切り替えた後で、スタック内のセカンダリ デバイスを別のデバイスと交換できます。選択できるデバイスは、現在スタッ

クのメンバーにも、ペアにもなっていないデバイスのみです。新しいデバイスは、デバイス スタックを確立する場合と同じガイドラインに従っている必要があります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 メンテナンス モードを開始するスタック メンバーの横にあるメンテナンス モード切り替えアイコン（  ）をクリックします。

ステップ 3 [はい（Yes）] をクリックして、メンテナンス モードを確定します。

ステップ 4 デバイス交換アイコン（）をクリックします。

ステップ 5 ドロップダウンリストから [交換デバイス（Replacement Device）] を選択します。

ステップ 6 [交換（Replace）] をクリックして、デバイスを交換します。

ステップ 7 メンテナンス モード切り替えアイコン（  ）を再度クリックすると、スタックのメンテナンス モードが即時に終了します。

（注） デバイス設定を再展開する必要はありません。

スタックに含まれる個々のデバイスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	任意（Any）	Firepower 8140、Firepower 8200 ファミリ、Firepower 8300 ファミリ	リーフのみ	Admin/Network Admin

デバイス スタックを確立した後でも、スタック内の個々のデバイスに対して設定できる属性がいくつかあります。スタックに設定されたデバイスに変更を加える方法は、単一のデバイスに変更を加える場合の方法と同じです。このページでは、デバイスの表示名の変更、システム設定の表示、デバイスのシャットダウンまたは再起動、ヘルス情報の表示、およびデバイス管理設定の編集を行うことができます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 設定を編集する、スタックに含まれるデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するデバイスを選択します。

ステップ 5 [デバイス（Devices）] ページのセクションを使用して、単一のデバイスに対して変更を加える場合と同じように、スタックに含まれる個々のデバイスに変更を加えます。

スタック構成のデバイスでのインターフェイスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
該当なし	任意（Any）	Firepower 8140、Firepower 8200 ファミリ、Firepower 8300 ファミリ	リーフのみ	Admin/Network Admin

管理インターフェイスを除き、スタック構成のデバイスにインターフェイスを設定するには、スタックのプライマリ デバイスの [インターフェイス（Interfaces）] ページを使用します。管理インターフェイスを設定する場合は、スタックに含まれる任意のデバイスを選択できます。

Firepower スタック構成デバイスの [インターフェイス（Interfaces）] ページに、個々のデバイスのハードウェアおよびインターフェイスのビューがあります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 プライマリ スタック構成デバイスの横で、編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インターフェイス（Interfaces）] タブをクリックします。

ステップ 4 [選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するデバイスを選択します。

ステップ 5 個々のデバイスに設定する場合と同じようにインターフェイスを設定します。センシング インターフェイスの設定，（491 ページ）を参照してください。

関連トピック

管理インターフェイス，（564 ページ）

スタック構成のデバイスの分離

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
該当なし	任意（Any）	FirePOWER 8140、8200 ファミリ、8300 ファミリ	任意（Any）	Admin/Network Admin

デバイスのスタック構成を使用する必要がなくなった場合、スタックを解除してデバイスを分離できます。

（注） スタック構成のデバイスに障害が発生した場合や、スタックのメンバー デバイス間の通信に障害が発生した場合は、Firepower Management Center Web インターフェイスを使用してスタック構成のデバイスを分離することはできません。この場合は、補助 CLI コマンド `configure stacking disable` を使用して、それぞれのデバイスから個別にスタック設定を削除します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 分断するデバイス スタックの横にあるスタックの分断アイコン（）をクリックします。

ヒント スタックを分断することなく、3 台以上の Firepower 8250 デバイスのスタックからセカンダリ デバイスを削除するには、スタックからの削除アイコン（）をクリックします。セカンダリ デバイスを削除すると、システムがそのデバイス抜きで動作するスタックを再設定する間、トラフィック検査、トラフィック フロー、またはリンク状態が短時間中断されます。

ステップ 3 [はい（Yes）] をクリックして、デバイス スタックを分離します。

スタック内のデバイスの交換

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
該当なし	任意（Any）	FirePOWER 8140、8200 ファミリ、8300 ファミリ	任意（Any）	Admin/Network Admin

Firepower Management Center がデバイスと通信できない場合に、スタックを分離してデバイスの登録を解除するには、デバイスに接続して CLI コマンドを使用する必要があります。詳細については、関連する章「コンフィギュレーション コマンド, （2226 ページ）」の **stacking disable** CLI コマンドおよび **delete** CLI コマンドを参照してください。

スタック内のデバイスを交換するには、以下を行います。

手順

ステップ 1 デバイスを含むスタックを選択し、そのスタックを交換して解除します。詳細については、スタック構成のデバイスの分離, （544 ページ）を参照してください。

ステップ 2 Firepower Management Center からデバイスを登録解除します。詳細については、Firepower Management Center からのデバイスの削除, （466 ページ）を参照してください。

ステップ 3 交換デバイスを Firepower Management Center に登録します。詳細については、Firepower Management Center へのデバイスの追加, （464 ページ）を参照してください。

ステップ 4 交換デバイスを含むデバイス スタックを作成します。詳細については、デバイス スタックの確立, （538 ページ）を参照してください。

第 VIII 部

アプライアンス プラットフォームの設定

第 24 章

システム設定（System Configuration）

以下のトピックでは、Firepower Management Center および管理対象デバイスでシステム設定を行う方法について説明します。

システム設定の概要

システム設定の設定値は、Firepower Management Center またはクラシック管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、NGIPSv）のいずれかに適用されます。

- Firepower Management Center では、これらの構成設定は「ローカル」のシステム設定の一部です。Firepower Management Center 上のシステム設定は単一システムに固有のものであり、Management Center のシステム設定への変更はそのシステムのみに影響する点に注意してください。
- クラシック管理対象デバイスでは、プラットフォーム設定ポリシーの一部として Firepower Management Center から設定を適用します。共有ポリシーを作成して、展開全体で同様の設定になっている可能性の高い、管理対象デバイスに最適なシステム設定の設定値のサブセットを設定します。

ヒント 7000 および 8000 シリーズ デバイスでは、ローカル Web インターフェイスからコンソール設定やリモート管理などのシステム設定の制限付きタスクを実行できます。これらは、プラットフォーム設定ポリシーを使用して 7000 または 8000 シリーズ デバイスに適用される設定とは異なります。

Firepower Management Center システム設定のナビゲーション

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

システム設定により、Firepower Management Center の基本設定を特定します。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 ナビゲーション ウィンドウを使用して、変更する設定を選択します。詳細については、表 55：システム設定，（551 ページ）を参照してください。

システム設定

次の表に Firepower Management Center のシステム設定の説明を示します。この表では、7000 および 8000 シリーズ デバイスについて、デバイスのローカル Web インターフェイスから構成する設定、および Firepower Management Center から展開したプラットフォーム設定ポリシーを使用して構成する設定も示します。

表 *55*：システム設定

設定	説明	他の設定元	
		プラットフォーム設定	7000 & 8000 シリーズ
情報	アプライアンスに関する最新情報を表示し、表示名を編集します。アプライアンス情報, （553 ページ）を参照してください。	No	Yes
HTTPS Certificate	必要に応じて、信頼できる認証局の HTTPS サーバ証明書を要求し、システムに証明書をアップロードします。カスタム HTTPS 証明書, （555 ページ）を参照してください。	No	Yes
外部データベース アクセス	データベースへの外部読み取り専用アクセスを有効にし、ダウンロードするクライアント ドライバを提供します。外部データベース アクセスの設定, （560 ページ）を参照してください。	No	No
データベース	Firepower Management Center が保存できる各イベントのタイプの最大数を指定します。データベース イベント数の制限, （562 ページ）を参照してください。	No	No
管理インターフェイス	アプライアンスの IP アドレス、ホスト名、プロキシ設定などのオプションを変更します。管理インターフェイス, （564 ページ）を参照してください。	No	Yes
プロセス	Firepower システム関連のプロセスをシャットダウン、リブート、または再起動します。システムのシャットダウンと再起動, （579 ページ）を参照してください。	No	Yes
リモート ストレージ デバイス	バックアップとレポート用のリモート ストレージ デバイスを設定します。リモート ストレージ管理, （582 ページ）を参照してください。	No	No
リコンサイルの変更	過去 24 時間にわたるシステムへの変更の詳細なレポートを送信するようにシステムを設定します。変更調整, （587 ページ）を参照してください。	No	Yes

設定	説明	他の設定元	
		プラットフォーム設定	7000 & 8000 シリーズ
アクセス コントロールの設定	ユーザがアクセス コントロール ポリシーを追加または変更する際にユーザにコメントを要求するようにシステムを設定します。ポリシー変更のコメント, （588 ページ）を参照してください。	No	No
アクセス リスト	どのコンピュータが特定のポートでシステムにアクセスできるかを制御します。アクセス リスト, （590 ページ）を参照してください。	Yes	No
監査ログ	外部ホストに監査ログを送信するようにシステムを設定します。監査ログ, （591 ページ）を参照してください。	Yes	No
ダッシュボード	ダッシュボードのカスタム分析ウィジェットを有効にします。ダッシュボード設定, （594 ページ）を参照してください。	No	No
DNS キャッシュ	イベント表示ページで IP アドレスを自動的に解決するようにシステムを設定します。DNS キャッシュ, （595 ページ）を参照してください。	No	No
電子メール通知	メール ホストを設定し、暗号化方式を選択して、電子メールベースの通知とレポートに認証クレデンシャルを提供します。電子メールの通知, （596 ページ）を参照してください。	No	No
外部認証	アカウントが外部認証されるユーザのデフォルトのユーザ ロールを設定します。次を参照してください。 外部認証の設定, （631 ページ）	Yes	No
侵入ポリシーの設定	ユーザが侵入ポリシーを変更する際にユーザにコメントを要求するようにシステムを設定します。ポリシー変更のコメント, （588 ページ）を参照してください。	No	No
[言語（Language）]	Web インターフェイスに異なる言語を指定します。言語の選択, （597 ページ）を参照してください。	Yes	No
ログイン バナー	ユーザがログインすると表示されるカスタム ログイン バナーを作成します。ログイン バナー, （599 ページ）を参照してください。	Yes	No
ネットワーク分析ポリシーの設定	ユーザがネットワーク分析ポリシーを変更する際にユーザにコメントを要求するようにシステムを設定します。ポリシー変更のコメント, （588 ページ）を参照してください。	No	No
SNMP	Simple Network Management Protocol （SNMP）のポーリングを有効にします。SNMP ポーリング, （600 ページ）を参照してください。	Yes	No

設定	説明	他の設定元	
		プラットフォーム設定	7000 & 8000 シリーズ
STIG コンプライアンス	米国国防総省によって設定される特定の要件の順守を有効にします。STIG コンプライアンス, （602 ページ）を参照してください。	Yes	No
時刻（Time）	現在の時刻設定を確認し、現在のシステム設定の時刻同期の設定が[ローカル設定で手動（Manually in Local Configuration）]に設定されている場合は、時間を変更します。時刻および時刻の同期, （604 ページ）を参照してください。	No	Yes
時刻の同期	システムの時刻の同期を管理します。時刻および時刻の同期, （604 ページ）を参照してください。	Yes	No
シェル タイムアウト	ユーザのログイン セッションが非アクティブによりタイムアウトするまでのアイドル時間の長さを分単位で設定します。セッション タイムアウト, （609 ページ）を参照してください。	Yes	No
脆弱性マッピング	ホスト IP アドレスから送受信されるアプリケーション プロトコル トラフィックの脆弱性をそのホスト IP アドレスにマップします。脆弱性マッピング, （611 ページ）を参照してください。	No	No
コンソール設定	VGA またはシリアル ポート経由、または Lights-Out Management（LOM）経由のコンソール アクセスを設定します。リモート コンソールのアクセス管理, （612 ページ）を参照してください。	No	制限付き
VMware ツール	VMware ツールを有効にして Firepower Management Center Virtual で使用します。VMware Tools と仮想システム, （620 ページ）を参照してください。	適用対象外	適用対象外

関連トピック

Firepower プラットフォーム設定の概要, （625 ページ）

アプライアンス情報

Web インターフェイスの[情報（Information）]ページには、次の表に示す情報が含まれています。別途記載のない限り、フィールドはすべて読み取り専用です。

フィールド	説明
[名前（Name）]	アプライアンスに割り当てられた名前。この名前は Firepower システムのコンテキスト内でのみ使用されることに注意してください。ホスト名をアプライアンスの名前として使用できますが、このフィールドに別の名前を入力しても、ホスト名が変更されることはありません。
製品モデル（Product Model）	アプライアンスのモデル名。
シリアル番号（Serial Number）	アプライアンスのシリアル番号。
ソフトウェア バージョン（Software Version）	アプライアンスに現在インストールされているソフトウェアのバージョン。
Firepower Management Center へのパケット転送を禁止(Prohibit Packet Transfer to the Defense Center)	管理対象デバイスがイベントに合わせてパケット データを送信し、Firepower Management Center 上にデータを保存するかを指定します。この設定は、7000 および 8000 シリーズ デバイスのローカル Web インターフェイスで使用できます。
オペレーティング システム（Operating System）	アプライアンス上で現在実行されているオペレーティング システム。
オペレーティング システム バージョン（Operating System Version）	アプライアンス上で現在実行されているオペレーティング システムのバージョン。
IPv4 アドレス（IPv4 Address）	デフォルト管理インターフェイス（`eth0`）の IPv4 アドレス。IPv4 の管理が無効になっている場合は、このフィールドにそのことが示されます。
IPv6 アドレス（IPv6 Address）	デフォルト管理インターフェイス（`eth0`）の IPv6 アドレス。IPv6 の管理が無効になっている場合は、このフィールドに表示されます。
現在のポリシー（Current Policies）	現在展開されているシステム レベルのポリシー。ポリシーが最後に適用された後で更新されていると、ポリシー名がイタリック体で表示されます。
モデル番号（Model Number）	内部フラッシュ ドライブに保存されているアプライアンス固有のモデル番号。この番号は、トラブルシューティングで重要になる場合があります。

システム情報の表示および変更

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

Firepower Management Center の Web インターフェイスまたは 7000 および 8000 シリーズ ローカル Web インターフェイスの情報ページでは、製品名やモデル番号など、読み取り専用の情報を含むシステムについての情報を提供します。このページでは、システムの表示名の変更を変更することもできます。また、7000 および 8000 シリーズ デバイスの場合、パケット転送を禁止する機能もあります。

（注） パケット転送を禁止することは、侵入ポリシー違反をトリガーしたパケットの具体的な内容について気にする必要がない低帯域幅の展開で、効果を発揮する可能性があります。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 オプションで、以下のシステム情報の設定を変更します。

- 名前：表示名を変更するには、[名前（Name）] フィールドに名前を入力します。
- パケット転送の禁止：Firepower Management Center にパケット データを送信しないようにするには、[管理センターへのパケット転送を禁止する（Prohibit Packet Transfer to the Management Center）] チェックボックスをオンにします。このオプションは、7000 または 8000 シリーズ デバイスのローカル Web インターフェイスでのみ使用できます。

ステップ 3 [保存（Save）] をクリックします。

カスタム HTTPS 証明書

Firepower Management Center および 7000 および 8000 シリーズ デバイスは、セキュア ソケット レイヤ（SSL）証明書によりシステムと Web ブラウザ間に暗号化チャネルを確立することができます。すべての Firepower デバイスにデフォルト証明書が含まれていますが、これはグローバル レベルで既知の CA から信頼された認証局（CA）によって生成された証明書ではありません。したがって、デフォルト証明書ではなく、グローバル レベルで既知の CA または内部で信頼された CA 署名付きのカスタム証明書の使用を検討してください。

システム情報と指定したID情報に基づいて、証明書要求を生成できます。ブラウザによって信頼されている内部認証局（CA）がインストールされている場合は、生成された要求に対して証明書に自己署名することができます。生成された要求を認証局に送信して、サーバ証明書を要求することもできます。認証局（CA）から署名付き証明書を取得すると、その証明書をインポートできます。

クライアント ブラウザの証明書チェック機能を使用して、Firepower システムの Web サーバへのアクセスを制限できます。ユーザ証明書を有効にすると、Web サーバはユーザのブラウザ クライアントで有効なユーザ証明書が選択されていることを確認します。そのユーザ証明書は、サーバ証明書で使用されているのと同じ信頼できる認証局によって生成されている必要があります。以下の状況ではいずれの場合もブラウザは Web インターフェイスをロードできません。

- ユーザがブラウザに無効な証明書を選択する。
- ユーザがブラウザにサーバ証明書に署名した認証局が生成していない証明書を選択する。
- ユーザがブラウザにデバイスの証明書チェーンの認証局が生成していない証明書を選択する。

サーバに証明書失効リスト（CRL）をロードすることもできます。CRL には認証局によって無効とされた証明書が記載されているため、Web サーバはクライアント ブラウザ証明書の有効性を確認することができます。ユーザが CRL にある失効した証明書の一覧に含まれる証明書を選択した場合、ブラウザは Web インターフェイスをロードできません。

現在のサーバ証明書の表示

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

ログインしているアプライアンスのサーバ証明書のみを表示できます。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

証明書署名要求の生成と送信

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	任意（Any）	従来型（Classic）	グローバルのみ	Admin

ローカル構成の [HTTPS 証明書（HTTPS Certificate）] ページから、この手順を使用して証明書要求を生成する場合は、1 つのシステムに対して 1 つの証明書しか生成できません。同様に、広く知られている CA または内部的に信頼できる CA によって署名されていない証明書をインストールすると、システムへの接続時にセキュリティ警告が表示されます。

証明書要求用に生成されるキーは、ベース 64 エンコードの PEM 形式です。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [新規 CSR の生成（Generate New CSR）] をクリックします。

ステップ 4 [国名（2 文字のコード）（Country Name (two-letter code)）] フィールドに国番号を入力します。

ステップ 5 [都道府県（State or Province）] フィールドに、都道府県名を入力します。

ステップ 6 [市区町村（Locality or City）] を入力します。

ステップ 7 [組織（Organization）] の名前を入力します。

ステップ 8 [部門（Organizational Unit (Department)）] の名前を入力します。

ステップ 9 [共通名（Common Name）] フィールドに、証明書を要求するサーバの完全修飾ドメイン名を入力します。

（注） 証明書に表示されるとおりに正確に、サーバの完全修飾ドメイン名を [共通名（Common Name）] フィールドに入力する必要があります。一般名と DNS ホスト名が一致しない場合は、アプライアンスに接続するときに警告が表示されます。

ステップ 10 [生成（Generate）] をクリックします。

ステップ 11 テキスト エディタを開きます。

ステップ 12 証明書要求のテキスト ブロック全体（`BEGIN CERTIFICATE REQUEST` 行と `END CERTIFICATE REQUEST` 行を含む）をコピーして、空のテキスト ファイルに貼り付けます。

ステップ 13 このファイルを *servername*`.csr` として保存します。*servername* は証明書を使用するサーバの名前です。

ステップ 14 [保存（Save）] をクリックします。

次の作業

- 署名されたサーバ証明書をアップロードします。サーバ証明書のアップロード, （558 ページ）を参照してください。

サーバ証明書のアップロード

証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、証明書チェーン（証明書パスとも呼ばれる）も提供する必要があります。ユーザ証明書が必要な場合は、証明書チェーンに中間認証局が含まれる認証局によってユーザ証明書が生成されている必要があります。

サーバ証明書のアップロード

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

証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、証明書チェーン（証明書パスとも呼ばれる）も提供する必要があります。ユーザ証明書が必要な場合は、証明書チェーンに中間認証局が含まれる認証局によってユーザ証明書が生成されている必要があります。

はじめる前に

- 証明書署名要求を生成します。証明書署名要求の生成と送信, （557 ページ）を参照してください。
- この CSR ファイルを証明書の要求先となる認証局にアップロードするか、この CSR を使用して自己署名証明書を作成します。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [Import HTTPS Certificate] をクリックします。

ステップ 4 テキスト エディタでサーバ証明書を開き、テキスト ブロック全体（`BEGIN CERTIFICATE` 行と `END CERTIFICATE` 行を含む）をコピーして、[サーバ証明書（Server Certificate）] フィールドに貼り付けます。

ステップ 5 秘密キーをアップロードする場合、秘密キー ファイルを開き、テキストブロック全体（`BEGIN RSA PRIVATE KEY` 行と `END RSA PRIVATE KEY` 行を含む）をコピーして、[秘密キー（Private Key）] フィールドに貼り付けます。

ステップ 6 提供する必要がある中間証明書を開き、各証明書のテキストブロック全体をコピーして、[Certificate Chain] フィールドに貼り付けます。

ステップ 7 [保存（Save）] をクリックします。

有効なユーザ証明書の強制

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

システムは識別符号化規則（DER）形式による CRL のアップロードをサポートしています。1 つのサーバにロードできる CRL は 1 つだけです。

失効した証明書のリストを最新の状態に保つため、CRL を更新するスケジュール タスクを作成できます。直近に更新された CRL がインターフェイスに表示されます。

（注） ユーザ証明書を有効にし、その後で Web インターフェイスにアクセスするには、ブラウザに有効なユーザ証明書が存在する（またはリーダーに CAC が挿入されている）**必要があります**。

はじめる前に

- ユーザ証明書を生成するためにサーバ証明書に使用したものと同じ認証局を使用します。
- 証明書の中間証明書をアップロードします。サーバ証明書のアップロード, （558 ページ）を参照してください。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [ユーザ証明書の有効化（Enable User Certificates）] を選択します。プロンプトが表示されたら、ドロップダウンリストから該当する証明書を選択します。

ステップ 4 CRL を取得するには、[CRL のフェッチの有効化（Enable Fetching of CRL）] を選択します。

ステップ 5 既存の CRL ファイルへの有効な URL を入力して、[CRL の更新（Refresh CRL）] をクリックします。指定した URL にある現行の CRL がサーバにロードされます。

（注） CRL のフェッチを有効にすると、CRL を定期的に更新するスケジュール タスクが作成されます。このタスクを編集して、更新の頻度を設定します。

ステップ 6 サーバ証明書を作成したのと同じ認証局によって生成された有効なユーザ証明書があることを確認します。

注意 ユーザ証明書を有効にして設定を保存した場合、ブラウザの証明書ストアに有効なユーザ証明書が存在していないと、アプライアンスへのすべての Web サーバ アクセスが無効になります。設定を保存する前に、有効な証明書がインストールされていることを確認してください。

ステップ 7 [保存（Save）] をクリックします。

外部データベース アクセスの設定

サードパーティ製クライアントによるデータベースへの読み取り専用アクセスを許可するように、Firepower Management Center を設定できます。これによって、次のいずれかを使用して SQL でデータベースを照会できるようになります。

- 業界標準のレポート作成ツール（Actuate BIRT、JasperSoft iReport、Crystal Reports など）
- JDBC SSL 接続をサポートするその他のレポート作成アプリケーション（カスタム アプリケーションを含む）
- シスコが提供する RunQuery と呼ばれるコマンドライン型 Java アプリケーション（インタラクティブに実行することも、1 つのクエリの結果をカンマ区切り形式で取得することもできる）

Firepower Management Center のシステム設定を使用して、データベース アクセスを有効にして、選択したホストにデータベースの照会を許可するアクセス リストを作成します。このアクセス リストは、アプライアンスのアクセスは制御しません。

次のツールを含むパッケージをダウンロードすることもできます。

- RunQuery（シスコが提供するデータベース クエリ ツール）

- InstallCert（アクセスしたい Firepower Management Center から SSL 証明書を取得して受け入れるために使用できるツール）
- データベースへの接続時に使用する必要がある JDBC ドライバ

データベース アクセスを構成するためにダウンロードしたパッケージ内のツールの使用方法については、『*Firepower System Database Access Guide*』を参照してください。

データベースへの外部アクセスの有効化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [外部データベース アクセス（External Database Access）] をクリックします。

ステップ 3 [外部データベース アクセスの許可（Allow External Database Access）] チェックボックスをオンにします。

ステップ 4 [サーバ ホスト名（Server Hostname）] フィールドに、適切な値を入力します。サードパーティ アプリケーションの要件に応じて、この値は、Firepower Management Center の完全修飾ドメイン名（FQDN）、IPv4 アドレス、または IPv6 アドレスにできます。

ステップ 5 [クライアント JDBC ドライバ（Client JDBC Driver）] の横にある [ダウンロード（Download）] をクリックし、ブラウザのプロンプトに従って `client.zip` パッケージをダウンロードします。

ステップ 6 1 つ以上の IP アドレスからのデータベース アクセスを追加するには、[ホストの追加（Add Hosts）] をクリックします。[アクセス リスト（Access List）] フィールドに [IP アドレス（IP Address）] フィールドが表示されます。

ステップ 7 [IP アドレス（IP Address）] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、`any` を入力します。

ステップ 8 [追加（Add）] をクリックします。

ステップ 9 [保存（Save）] をクリックします。

ヒント 最後に保存されたデータベース設定に戻すには、[更新（Refresh）] をクリックします。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）

データベース イベント数の制限

Firepower Management Center が保存できる各イベント タイプの最大数を指定できます。パフォーマンスを向上させるには、定期的に処理するイベント数に合わせてイベント数の制限を調整する必要があります。一部のイベント タイプでは、ストレージを無効にすることができます。

システムは侵入イベント、ディスカバリ イベント、監査レコード、セキュリティ インテリジェンス データ、URL フィルタリング データをアプライアンスのデータベースから自動的にプルーニングします。イベントが自動的にプルーニングされると自動で電子メール通知を生成するようにシステムを設定できます。また、手動でディスカバリ データベースやユーザ データベースをプルーニングし、Firepower Management Center データベースからディスカバリ データや接続データを消去することもできます。

データベース イベント数の制限の設定

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

はじめる前に

- Firepower Management Center のデータベースからイベントがプルーニングされた場合に電子メール通知を受信するには、電子メール サーバを設定する必要があります。メール リレーホストおよび通知アドレスの設定, （596 ページ）を参照してください。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [データベース（Database）] を選択します。

ステップ 3 各データベースについて、保存するレコードの数を入力します。
各データベースが保持できるレコード数の詳細については、データベース イベント数の制限, （563 ページ）を参照してください。

ステップ 4 必要に応じて、[データ プルーニング通知のアドレス（Data Pruning Notification Address）] フィールドに、プルーニング通知を受信する電子メール アドレスを入力します。

ステップ 5 [保存（Save）] をクリックします。

データベース イベント数の制限

次の表に、Firepower Management Center に保存可能な各イベント タイプのレコードの最小数と最大数を示します。

表 *56*：データベース イベント数の制限

イベント タイプ（**Event Type**）	上限	下限
侵入イベント	1,000 万（Management Center Virtual） 2,000 万（MC750） 3,000 万（ MC1500） 6,000 万（MC2000） 1 億 5,000 万（MC3500） 3 億（MC4000）	10,000
検出イベント	1,000 万 2,000 万（MC2000 および MC4000）	0（ストレージを無効化）
接続イベント セキュリティ インテリジェンス イベント	5,000 万（Management Center 仮想） 5,000 万（MC750） 1 億（ MC1500） 3 億（MC2000） 5 億（MC3500） 10 億（MC4000） 制限は接続イベントとセキュリティ インテリジェンス イベントの間で共有されます。設定済みの最大数の合計がこの制限を超えることはできません。	0（ストレージを無効化）
接続の要約（集約された接続イベント）	5,000 万（Management Center 仮想） 5,000 万（MC750） 1 億（ MC1500） 3 億（MC2000） 5 億（MC3500） 10 億（MC4000）	0（ストレージを無効化）

イベント タイプ（Event Type）	上限	下限
相関イベントおよびコンプライアンスのホワイト リスト イベント	100 万 200 万（MC2000 および MC4000）	1 つ
マルウェア イベント	1,000 万 2,000 万（MC2000 および MC4000）	10,000
ファイル イベント	1,000 万 2,000 万（MC2000 および MC4000）	0（ストレージを無効化）
ヘルス イベント	100 万	0（ストレージを無効化）
監査レコード	100,000	1 つ
修復ステータス イベント	1,000 万	1 つ
ホワイトリスト違反履歴	30 日間の違反履歴	1 日の履歴
ユーザ アクティビティ（ユーザ イベント）	1,000 万	1 つ
ユーザ ログイン（ユーザ履歴）	1,000 万	1 つ
侵入ルール更新のインポート ログ レコード	100 万	1 つ

管理インターフェイス

セットアップの完了後、管理ネットワーク設定を変更することができます。これには、Management Centerと管理対象デバイスの両方での管理インターフェイス、ホスト名、検索ドメイン、DNSサーバ、HTTP プロキシの追加が含まれます。

管理インターフェイスについて

デフォルトでは、Firepower Management Center はすべてのデバイスを 1 つの管理インターフェイス上で制御します。各デバイスにはManagement Center と通信するための管理インターフェイスが 1 つ含まれています。

また、初期設定（Management Centerおよび管理対象デバイスの両方）や、管理者としてManagement Center にログインする際にも管理インターフェイスで行います。

管理インターフェイスは、スマート ライセンス サーバとの通信、更新プログラムのダウンロード、その他の管理機能の実行にも使用します。

Firepower Management Center 上の管理インターフェイス

Firepower Management Center では、初期セットアップ、管理者の HTTP アクセス、デバイスの管理、ならびにその他の管理機能（ライセンス管理や更新など）に、eth0 インターフェイスが使用されます。

同じネットワーク上、あるいは別のネットワーク上に、追加の管理インターフェイスを設定することもできます。Management Center が管理するデバイスの数が多い場合、管理インターフェイスをさらに追加することで、スループットとパフォーマンスの向上につながります。これらの管理インターフェイスをその他すべての管理機能に使用することもできます。管理インターフェイスごとに、対応する機能を限定することをお勧めします。たとえば、ある特定の管理インターフェイスを HTTP 管理者アクセス用に使用し、別の管理インターフェイスをデバイスの管理に使用するなどです。

デバイス管理用に、管理インターフェイスには 2 つの別個のトラフィック チャネルがあります。管理トラフィック チャネルはすべての内部トラフィック（デバイス管理に固有のデバイス間トラフィックなど）を伝送し、イベント トラフィック チャネルはすべてイベント トラフィック（Web イベントなど）を伝送します。オプションで、Management Center 上にイベントを処理するためのイベント専用インターフェイスを別個に設定することもできます。設定できるイベント専用インターフェイスは 1 つだけです。イベント トラフィックは大量の帯域幅を使用する可能性があるので、管理トラフィックからイベント トラフィックを分離することで、Management Center のパフォーマンスを向上させることができます。たとえば、10 GigabitEthernet インターフェイスをイベント インターフェイスとして割り当て、可能なら、1 GigabitEthernet インターフェイスを管理用に使用します。たとえば、イベント専用インターフェイスは完全にセキュアなプライベート ネットワーク上に設定し、通常の管理インターフェイスはインターネットにアクセスできるネットワーク上で使用することをお勧めします。目的がスループットの向上だけである場合は、管理インターフェイスとイベント インターフェイスを同じネットワーク上で使用することもできます。

以下の機能は、デフォルトの管理インターフェイス（eth0）でのみサポートされます。

- DHCP IP アドレッシング。他の管理インターフェイスでは静的 IP アドレスを使用する必要があります。
- 新しいデバイスを登録する際の NAT ID の使用。
- Lights-Out Management

管理対象デバイス上の管理インターフェイス

一部のモデルでは、イベント トラフィック専用として設定できる追加管理インターフェイスがあり、Management Center との通信中に管理トラフィックとイベント トラフィックを分離できます。

デバイスをセットアップするときに、接続先とする Management Center の IP アドレスを指定します。初期登録時は、管理トラフィックとイベント トラフィックの両方がこのアドレスに送信されます。注：場合によっては、Management Center が別の管理インターフェイスで初期接続を確立す

ることがあります。その場合、以降の接続では指定したIPアドレスの管理インターフェイスを使用する必要があります。

デバイスと Management Center の両方に別個のイベント インターフェイスが設定されている場合は、デバイスと Management Center が互いのイベント インターフェイスを管理通信中に学習した後、ネットワークで許可されていれば、後続のイベント トラフィックがそれらのインターフェイス間で送られます。イベントネットワークがダウンすると、イベントトラフィックは、通常の管理インターフェイスに戻ります。デバイスは、可能な場合に別個のイベント インターフェイスを使用しますが、管理インターフェイスは常にバックアップです。管理対象デバイス上で 1 つの管理インターフェイスだけを使用している場合、管理トラフィックを Management Center 管理インターフェイスに送信できませんし、イベント トラフィックを別個の Management Center イベント インターフェイスに送信することもできません。Management Center と管理対象デバイスの両方で別個のイベント インターフェイスを使用する必要があります。

管理インターフェイスのサポート

管理インターフェイスの場所については、ご使用のモデルのハードウェア インストレーションガイドを参照してください。

（注）

（注）

Firepower Management Center および管理対象デバイスの各モデルでサポートされる管理インターフェイスについては、以下の表を参照してください。

表 *57*：*Firepower Management Center* でサポートされる管理インターフェイス

モデル	管理インターフェイス
MC750、MC1500、MC3500	eth0（デフォルト） eth1
MC2000、MC4000	eth0（デフォルト） eth1 eth2 eth3
Firepower Management Center Virtual	eth0（デフォルト）

表 *58*：管理対象デバイスでサポートされる管理インターフェイス

モデル	管理インターフェイス	オプションのイベントインターフェイス
7000 シリーズ	eth0	サポートなし
8000 シリーズ	eth0	eth1
NGIPSv	eth0	サポートなし
ASA 5585-X 上の ASA FirePOWER サービス モジュール	eth0 （注） eth0 は、管理 1/0 インターフェイスの内部名です。	eth1 （注） eth1 は、管理 1/1 インターフェイスの内部名です。
ASA 5506-X、5508-X、5516-X 上の ASA FirePOWER サービス モジュール	eth0 （注） eth0 は、管理 1/1 インターフェイスの内部名です。	サポートなし
ASA 5512-X ～ 5555-X 上の ASA FirePOWER サービス モジュール	eth0 （注） eth0 は、管理 0/0 インターフェイスの内部名です。	サポートなし

管理インターフェイス上のネットワーク ルート

管理インターフェイスはスタティック ルートのみをサポートします。Management Center または管理対象デバイスをセットアップすると、セットアップ プロセスにより、指定したゲートウェイ IP アドレスへデフォルトの管理インターフェイスを介して到達するデフォルトのルートが作成します。このルートを削除することはできません。また、このルートで変更できるのはゲートウェイ アドレスのみです。

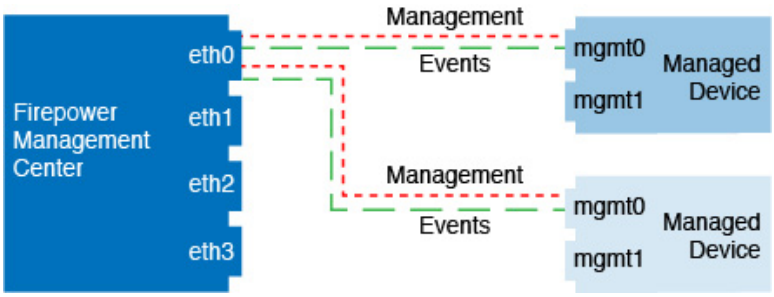
さらにスタティック ルートを追加できます。正しいインターフェイスとゲートウェイを指定して、任意のリモート ネットワークへのルートを追加します。

管理インターフェイスのルーティングは、データ インターフェイスに対して設定するルーティングとは完全に別のものです。

管理およびイベント トラフィック チャネルの例

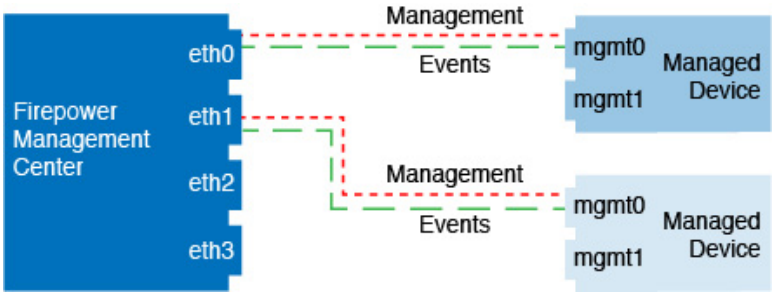
以下に、Firepower Management Center と管理対象デバイスでデフォルト管理インターフェイスのみを使用する例を示します。

図 *1*：*Firepower Management Center* 上で単一の管理インターフェイスを使用する場合



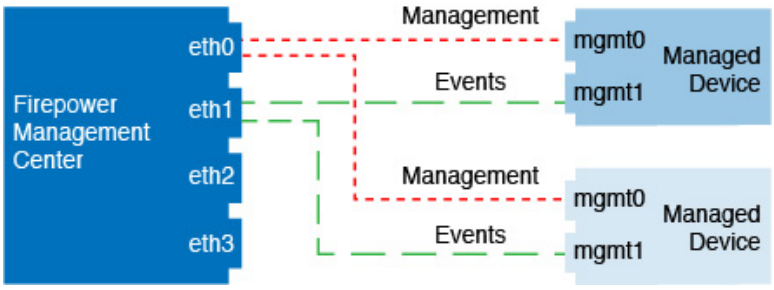
以下に、Firepower Management Center でデバイスごとに別個の管理インターフェイスを使用する例を示します。この場合、各管理対象デバイスが 1 つの管理インターフェイスを使用します。

図 *2*：*Firepower Management Center* 上の複数の管理インターフェイスを使用する場合



以下に、個別のイベント インターフェイスを使用する Firepower Management Center と管理対象デバイスの例を示します。

図 *3*：*Firepower Management Center* 上の個別のイベント インターフェイスと管理対象デバイスを使用する場合



以下に、Firepower Management Center 上で複数の管理インターフェイスと個別のイベント インターフェイスが混在し、個別のイベント インターフェイスを使用する管理対象デバイスと単一の管理インターフェイスを使用する管理対象デバイスが混在する例を示します。

図 4：管理インターフェイスとイベント インターフェイスを混在させて使用する場合

管理インターフェイスの設定

Firepower Management Center に対して、および各管理対象デバイスに対して管理インターフェイス設定を変更できます。

7000 & 8000 シリーズ デバイスでは、Management Center インターフェイスと同様の Web インターフェイスを使用して管理インターフェイス設定を構成できます。vNGIPS、および ASA FirePOWER モジュールでは、CLI を使用してこれらの設定を構成する必要があります。また、CLI は 7000 & 8000 シリーズ で必要に応じて使用できます。Management Center では CLI を使用することはできません。（Management Center は、Cisco TAC の監督下にある場合に限り、Linux シェル アクセスをサポートします。Firepower システムのユーザ インターフェイス を参照してください）。

関連トピック

通信ポートの要件, （2189 ページ）

Firepower Management Center 管理インターフェイスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

Firepower Management Center で管理インターフェイスの設定を変更します。オプションとして追加の管理インターフェイスを有効にしたり、イベントのみのインターフェイスを設定したりできます。

注意 接続されている管理インターフェイスを変更する場合は十分にご注意ください。設定エラーのために再接続できない場合は、Management Center コンソール ポートにアクセスして、Linux シェルでネットワーク設定を再設定する必要があります。この操作では、Cisco TAC に連絡する必要があります。

手順

ステップ 1 [システム（System）]>[設定（Configuration）] を選択し、次に [管理インターフェイス（Management Interfaces）] を選択します。

ステップ 2 [インターフェイス（Interfaces）] エリアで、設定するインターフェイスの横にある [編集（Edit）] をクリックします。
このセクションでは、利用可能なすべてのインターフェイスがリストされます。インターフェイスをさらに追加することはできません。

それぞれの管理インターフェイスに対して、以下のオプションを設定できます。

- [有効にする（Enabled）]：管理インターフェイスを有効にします。デフォルト eth0 管理インターフェイスを無効にしないでください。eth0 インターフェイスを必要とするプロセスもあります。
- [チャネル（Channels）]：イベントのみのインターフェイスを設定します。Management Center では 1 つのイベント インターフェイスしか設定できません。これを行うには、[管理トラフィック（Management Traffic）] チェックボックスをオフにし、[イベント トラフィック（Event Traffic）] チェックボックスをオンのままにします。その他の管理インターフェイスの場合は、両方のチェックボックスをオンにする必要があります。
- [モード（Mode）]：リンク モードを指定します。GigabitEthernet インターフェイスでは、自動ネゴシエーションの値を変更しても反映されないことに注意してください。
- [MTU]：最大伝送ユニット（MTU）を設定します。デフォルトは 1500 です。設定可能な MTU の範囲は、モデルとインターフェイスのタイプによって異なる場合があります。

  システムは、設定された MTU 値から自動的に 18 バイトを削減するため、IPv6 の場合、1298 未満の値は MTU の最小値である 1280 に準拠しません。IPv4 の場合は、594 未満の値は MTU の最小値 576 に準拠しません。たとえば、構成値 576 は自動的に 558 に削減されます。
- [MDI/MDIX]：[自動-MDIX（Auto-MDIX）] を設定します。
- [IPv4 設定（IPv4 Configuration）]：IPv4 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：IPv4 の管理 IP アドレスとネットマスクを手動で入力します。
  - [DHCP]：DHCP を使用するインターフェイスを設定します（eth0 のみ）。
  - [無効（Disabled）]：無効 IPv4。IPv4 と IPv6 の両方を無効にしないでください。

- [IPv6 設定（IPv6 Configuration）]：IPv6 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：IPv6 の管理 IP アドレスとプレフィックス長を手動で入力します。
  - [DHCP]：DHCPv6 を使用するインターフェイスを設定します（eth0 のみ）。
  - [ルータ割当て（Router Assigned）]：ステートレス自動設定を有効にします。
  - [無効（Disabled）]：IPv6 を無効にします。IPv4 と IPv6 の両方を無効にしないでください。

ステップ 3 [ルート（Routes）] エリアで、スタティック ルートを編集アイコン（  ）をクリックして編集するか、またはルートを追加アイコン（）をクリックして追加します。表示アイコン（  ）をクリックして、ルートの統計を表示します。

（注） デフォルト ルートでは、ゲートウェイ IP アドレスのみを変更できます。

次の設定をスタティック ルートに対して設定できます。

- [宛先（Destination）]：ルートを作成する宛先ネットワークのアドレスを設定します。
- [ネットマスク（Netmask）] または [プレフィックス長（Prefix Length）]：ネットワークのネットマスク（IPv4）またはプレフィックス長（IPv6）を設定します。
- [インターフェイス（Interface）]：出力管理インターフェイスを設定します。
- [ゲートウェイ（Gateway）]：ゲートウェイ IP アドレスを設定します。

ステップ 4 [共有設定（Shared Settings）] エリアで、すべてのインターフェイスで共有されているネットワーク パラメータを設定します。

（注） eth0 インターフェイスで [DHCP] を選択すると、DHCP サーバから取得する共有設定の一部を手動で指定することができなくなります。

次の共有設定を行うことができます。

- [ホスト名（Hostname）]：Management Center ホスト名を設定します。ホスト名を変更する場合、syslog メッセージに反映される新しいホスト名を使用するには、Management Center を再起動します。再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。
- [ドメイン（Domains）]：カンマで区切られた、Management Center の検索ドメインを設定します。これらのドメインは、**ping system**など、コマンドで完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。
- [プライマリ DNS サーバ（Primary DNS Serve）]、[セカンダリ DNS サーバ（Secondary DNS Server）]、[ターシャリ DNS サーバ（Tertiary DNS Server）]：優先度順に使用される DNS サーバを設定します。

- [リモート管理ポート（Remote Management Port）]：管理対象デバイスとの通信用のリモート管理ポートを設定します。Management Center および管理対象デバイスは、双方向の SSL 暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。

  （注） Cisco は、リモート管理ポートをデフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、展開内の相互に通信する必要がある**すべての**デバイスの管理ポートを変更する必要があります。

ステップ 5 [プロキシ（Proxy）] 領域で、HTTP プロキシを設定します。
Management Center は、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように構成されています。HTTP ダイジェスト経由で認証できるプロキシ サーバを使用できます。

（注） NT LAN Manager（NTLM）認証を使用するプロキシはサポートされません。

a) [有効（Enabled）] チェックボックスをオンにします。
b) [HTTP プロキシ（HTTP Proxy）] フィールドに、プロキシ サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
c) [ポート（Port）] フィールドに、ポート番号を入力します。
d) [プロキシ認証の使用（Use Proxy Authentication）] を選択してから [ユーザ名（User Name）] と [パスワード（Password）] を入力して、認証資格情報を設定します。

ステップ 6 [保存（Save）] をクリックします。

従来型デバイス Web インターフェイスでのデバイス管理インターフェイスの設定

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

Web インターフェイスを使用して、管理対象デバイスの管理インターフェイスの設定を変更します。モデルでサポートされている場合に、オプションでイベント インターフェイスを有効にすることができます。

注意 慎重に管理インターフェイスに変更を加えてください。構成エラーで再接続できなくなると、デバイスのコンソール ポートへのアクセスおよび CLI での再設定が必要になります。

手順

ステップ 1 [システム（System）]>[設定（Configuration）]を選択して、[管理インターフェイス（Management Interfaces）]を選択します。

ステップ 2 [インターフェイス（Interfaces）]エリアで、設定するインターフェイスの横にある[編集（Edit）]をクリックします。
このセクションでは、利用可能なすべてのインターフェイスがリストされます。インターフェイスをさらに追加することはできません。

それぞれの管理インターフェイスに対して、以下のオプションを設定できます。

- [有効にする（Enabled）]：管理インターフェイスを有効にします。デフォルトeth0管理インターフェイスを無効に**しないでください**。eth0インターフェイスを必要とするプロセスもあります。
- [チャネル（Channels）]：（8000シリーズのみ）イベント オンリーのインターフェイスを設定します。8000シリーズのデバイスでeth1管理インターフェイスを有効にして、イベントインターフェイスとして機能させることができます。これを設定するには、[管理トラフィック（Management Traffic）]チェックボックスをオフにして、[イベント トラフィック（Event Traffic）]チェックボックスをオンのままにしておきます。eth0管理インターフェイスを入力するには、両方のチェックボックスをオンのままにしておきます。

  管理チャネルとイベントチャネルの両方にデフォルト管理インターフェイスを使用することをお勧めします。その後、別個のイベント専用インターフェイスを有効にします。Firepower Management Centerイベント専用インターフェイスは管理チャネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャネルを単に無効にしてください。
- [モード（Mode）]：リンク モードを指定します。GigabitEthernetインターフェイスでは、自動ネゴシエーションの値を変更しても反映されないことに注意してください。
- [MTU]：最大伝送ユニット（MTU）を設定します。デフォルトは1500です。設定可能なMTUの範囲は、モデルとインターフェイスのタイプによって異なる場合があります。

  システムは、設定されたMTU値から自動的に18バイトを削減するため、IPv6の場合、1298未満の値はMTUの最小値である1280に準拠しません。IPv4の場合は、594未満の値はMTUの最小値576に準拠しません。たとえば、構成値576は自動的に558に削減されます。
- [MDI/MDIX]：[自動-MDIX（Auto-MDIX）]を設定します。
- [IPv4設定（IPv4 Configuration）]：IPv4 IPアドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：IPv4の管理IPアドレスとネットマスクを手動で入力します。
  - [DHCP]：DHCPを使用するインターフェイスを設定します（eth0のみ）。
  - [無効（Disabled）]：無効IPv4。IPv4とIPv6の両方を無効に**しないでください**。

- [IPv6 設定（IPv6 Configuration）]：IPv6 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：IPv6 の管理 IP アドレスとプレフィックス長を手動で入力します。
  - [DHCP]：DHCPv6 を使用するインターフェイスを設定します（eth0 のみ）。
  - [ルータ割当て（Router Assigned）]：ステートレス自動設定を有効にします。
  - [無効（Disabled）]：IPv6 を無効にします。IPv4 と IPv6 の両方を無効にしないでください。

ステップ 3 [ルート（Routes）] エリアで、スタティック ルートを編集アイコン（  ）をクリックして編集するか、またはルートを追加アイコン（  ）をクリックして追加します。表示アイコン（  ）をクリックして、ルートの統計を表示します。

（注） デフォルト ルートでは、ゲートウェイ IP アドレスのみを変更できます。

次の設定をスタティック ルートに対して設定できます。

- [宛先（Destination）]：ルートを作成する宛先ネットワークのアドレスを設定します。
- [ネットマスク（Netmask）] または [プレフィックス長（Prefix Length）]：ネットワークのネットマスク（IPv4）またはプレフィックス長（IPv6）を設定します。
- [インターフェイス（Interface）]：出力管理インターフェイスを設定します。
- [ゲートウェイ（Gateway）]：ゲートウェイ IP アドレスを設定します。

ステップ 4 [共有設定（Shared Settings）] エリアで、すべてのインターフェイスで共有されているネットワーク パラメータを設定します。

（注） eth0 インターフェイスで [DHCP] を選択すると、DHCP サーバから取得する共有設定の一部を手動で指定することができなくなります。

以下の共有設定を行うことができます。

- [ホスト名（Hostname）]：デバイスのホスト名を設定します。ホスト名を変更する場合、Syslog メッセージに新しいホスト名を反映させるには、デバイスをリブートします。再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。
- [ドメイン（Domains）]：カンマで区切ったデバイスの検索ドメインを設定します。これらのドメインは、コマンドで完全修飾ドメイン名を指定しないときに、ホスト名に ping system などとして加えられます。**ping system** ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。
- [プライマリ DNS サーバ（Primary DNS Server）]、[セカンダリ DNS サーバ（Secondary DNS Server）]、[テリタリ DNS サーバ（Tertiary DNS Server）]：DNS サーバが優先順で使用されるよう設定します。

- [リモート管理ポート（Remote Management Port）]：Management Center で通信のリモート管理ポートを設定します。Management Center および管理対象デバイスは、双方向の SSL 暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。

  （注） Cisco は、リモート管理ポートをデフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要がある**すべての**デバイスの管理ポートを変更する必要があります。

ステップ 5 [LCD パネル（LCD Panel）] エリアで、[ネットワーク設定の再設定を許可（Allow reconfiguration of network settings）] チェックボックスをオンにして、デバイスの LCD パネルを使用したネットワーク設定の変更を有効にします。
LCDパネルを使用して、デバイスのIPアドレスを編集できます。変更が管理Firepower Management Centerに反映されていることを確認します。状況によっては、Firepower Management Center でデータを手動で更新することが必要になります。

注意 LCD パネルを使用した再構成を許可すると、セキュリティ リスクが発生する可能性があります。LCD パネルを使用してネットワーク設定を構成する場合は、物理アクセスだけが必要で、認証は必要ありません。このオプションを有効にするとセキュリティ上の問題が発生する可能性があることを示す警告が Web インターフェイスに表示されます。

ステップ 6 [プロキシ（Proxy）] エリアで、HTTP プロキシ設定をします。
デバイスは、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように設定されています。HTTP ダイジェスト経由で認証できるプロキシ サーバを使用できます。

（注） NT LAN Manager（NTLM）認証を使用するプロキシはサポートされません。

a) [有効（Enabled）] チェックボックスをオンにします。
b) [HTTP プロキシ（HTTP Proxy）] フィールドに、プロキシ サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
c) [ポート（Port）] フィールドに、ポート番号を入力します。
d) [プロキシ認証の使用（Use Proxy Authentication）] を選択してから [ユーザ名（User Name）] と [パスワード（Password）] を入力して、認証資格情報を設定します。

ステップ 7 [保存（Save）] をクリックします。

CLI でのデバイス管理インターフェイスの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	従来型（Classic）	グローバルのみ	Admin

CLI を使用して、管理対象デバイスの管理インターフェイスの設定を変更します。これらの設定の多くは、初期セットアップ時に設定されたものです。この手順に従うことで、それらの設定を変更でき、さらに設定を追加できます（例：モデルでサポートされる場合にイベント インターフェイスを有効化する、スタティック ルートを追加する）。クラシック デバイス CLI については、このガイドのコマンド ライン リファレンス, （2193 ページ）を参照してください。

注意 SSH を使用する際は、慎重に管理インターフェイスに変更を加えてください。構成エラーで再接続できなくなると、デバイスのコンソール ポートへのアクセスが必要になります。

はじめる前に

- [configure user add] コマンドを使用して、CLI にログインできるユーザ アカウントを作成できます。**configure user add**
- 7000 & 8000 シリーズ デバイスで、ユーザ アカウントの作成, （78 ページ）の説明に従って、Web インターフェイスでユーザ アカウントも作成できます。

手順

ステップ 1 コンソール ポートから、または SSH を使用して、デバイス CLI に接続します。コマンドライン インターフェイスへのログイン, （29 ページ）を参照してください。

ステップ 2 管理者のユーザ名とパスワードでログインします。

ステップ 3 イベント オンリーのインターフェイスを有効にします（サポート モデルについては、管理インターフェイスのサポート, （566 ページ）参照）。

configure network management-interface enable *management_interface*

configure network management-interface disable-management-channel *management_interface*

例：

これは Firepower 4100 または 9300 デバイスの例です。有効なインターフェイス名はデバイス タイプによって異なります。

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Preserve existing configuration- currently no IP addresses on eth1 to update (bootproto
IPv4:,bootproto IPv6:
at /usr/local/sf/lib/perl/5.10.1/SF/NetworkConf/NetworkSettings.pm line 821.
Configuration updated successfully

>
```

管理チャネルとイベント チャネルの両方にデフォルト管理インターフェイスを使用することをお勧めします。その後、別個のイベント専用インターフェイスを有効にします。Firepower Management Center イベント専用インターフェイスは管理チャネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャネルを単に無効にしてください。

ステップ 4 管理インターフェイスまたはイベント インターフェイスのネットワーク設定をします。*management_interface* 引数を指定しない場合は、デフォルト管理インターフェイスのネットワーク設定を変更します。イベント インターフェイスを設定する際には、必ず *management_interface* 引数を指定してください。イベント インターフェイスは、管理インターフェイスの個別のネットワーク、または同じネットワークに配置できます。自分で設定するインターフェイスに接続すると、切断されます。新しい IP アドレスに再接続できます。

a) IPv4 アドレスを設定します。

- 手動設定

  configure network ipv4 manual *ip_address netmask gateway_ip* [*management_interface*]

  例：

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.

>
```

- DHCP（デフォルト管理インターフェイスのみでサポート）。

  configure network ipv4 dhcp

b) IPv6 アドレスを設定します。

- ステートレス自動設定

  configure network ipv6 router [*management_interface*]

  例：

```
> configure network ipv6 router management1
Setting IPv6 network configuration.
Network settings changed.

>
```

- 手動設定

  configure network ipv6 manual *ip6_address ip6_prefix_length* [*ip6_gateway_ip*] [*management_interface*]

  例：

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 2001:0DB8:BA98::3211
management1
Setting IPv6 network configuration.
Network settings changed.

>
```

- DHCPv6（デフォルト管理インターフェイスのみでサポート）。

  configure network ipv6 dhcp

ステップ 5 スタティック ルートを追加します。
configure network static-routes {**ipv4** | **ipv6**} **add** *management_interface destination_ip netmask_or_prefix gateway_ip*

例：

```
> configure network static-routes ipv4 add management0 10.89.89.0 255.255.255.0 10.10.1.1
Configuration updated successfully

> configure network static-routes ipv4 add management1 10.89.89192.168.6.0 255.255.255.0
10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

スタティック ルートを表示するには、**show network-static-routes** と入力します（デフォルト ルートは表示されません）。

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : management0
Destination               : 10.89.89.0
Gateway                   : 10.10.1.1
Netmask                   : 255.255.255.0
[…]
```

ステップ 6 ホスト名の設定
configure network hostname 名前

例：

```
> configure network hostname farscape1
```

再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。

ステップ 7 検索ドメインを設定します。
configure network dns searchdomains *domain_list*

例：

```
> configure network dns searchdomains example.com,cisco.com
```

カンマで区切ったデバイスの検索ドメインを設定します。これらのドメインは、コマンドで完全修飾ドメイン名を指定しないときに、ホスト名に ping system などとして加えられます。**ping system**

ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。

ステップ 8 カンマで区切った 3 つの DNS サーバを設定します。
configure network dns servers *dns_ip_list*

例：

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

ステップ 9 Management Center で通信のリモート管理ポートを設定します。
configure network management-interface tcpport *number*

例：

```
> configure network management-interface tcpport 8555
```

Management Center および管理対象デバイスは、双方向の SSL 暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。

（注） Cisco は、リモート管理ポートをデフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要がある**すべての**デバイスの管理ポートを変更する必要があります。

ステップ 10 HTTP プロキシを設定します。デバイスは、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように設定されています。HTTP ダイジェスト経由で認証できるプロキシ サーバを使用できます。コマンド発行後に、HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかをユーザは尋ねられます。認証が必要な場合はプロキシのユーザ名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。
configure network http-proxy

例：

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

システムのシャットダウンと再起動

アプライアンス上のプロセスのシャットダウンおよび再起動を制御するには、Firepower システムの Web インターフェイスを使用します。アプライアンスのシャットダウンは、設定データを失うことなく、安全にシステムの電源を切って再起動する準備をします。

Firepower Management Center 上のプロセスを制御できる、以下のオプションがあります。

- システムのシャットダウン：Firepower システムのグレースフル シャットダウンを開始します。
- システムの再起動：システムを通常の方法でシャット ダウンして再起動します。
- コンソールの再起動：通信、データベース、HTTP サーバのプロセスを再起動します。これは通常、トラブルシューティングの際に使用されます。

以上のオプションは、7000および8000シリーズ管理対象デバイスすべてで共通に使用できます。これらのデバイス上で Snort プロセスを再起動することもできます。

注意 電源ボタンを使用してアプライアンスを停止**しないでください**。データが失われる可能性があります。Webインターフェイスを使用して完全にアプライアンスをシャットダウンする必要があります。

注意 Snort プロセスを再起動すると、一時的にトラフィック インスペクションが中断されます。この中断中にトラフィックがドロップされるか、インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

Firepower 仮想管理対象デバイスの場合、VMware などの仮想インフラストラクチャーには一般的に、仮想マシンのシャットダウン方法、再起動方法、中断方法を定義する設定可能な電源オプションが用意されています。これらのオプションをどのように設定するかについては、使用している仮想プラットフォームのドキュメンテーションを参照してください。

（注） VMware 上で稼働する Firepower 仮想管理対象デバイスの場合、VMware ツールにカスタム電源オプションが含まれています。したがって、グレースフルシャットダウンを設定するには、仮想マシンに VMware ツールがインストールされている必要があります。

システムのシャット ダウンと再起動

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

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [プロセス（Process）] を選択します。

ステップ 3 アプライアンスをシャットダウンするには、以下を実行します。

- Management Center：[管理センターのシャットダウン（Shutdown Management Center）] の横にある [コマンドの実行（Run Command）] をクリックします。
- 管理対象デバイス：[アプライアンスのシャットダウン（Shutdown Appliance）] の横にある [コマンドの実行（Run Command）] をクリックします。

ステップ 4 アプライアンスを再起動するには、以下を実行します。

- Management Center：[管理センターの再起動（Reboot Management Center）] の横にある [コマンドの実行（Run Command）] をクリックします。
- 管理対象デバイス：[アプライアンスの再起動（Reboot Appliance）] の横にある [コマンドの実行（Run Command）] をクリックします。

（注） Firepower Management Center または管理対象デバイスを再起動すると、アプライアンスからログアウトされます。システムはデータベース チェックを実行しますが、これは完了するのに 1 時間かかります。

ステップ 5 アプライアンスを再起動するには、以下を実行します。

- Management Center：[管理センターの再起動（Restart Management Center）] の横にある [コマンドの実行（Run Command）] をクリックします。
- 管理対象デバイス：[アプライアンス コンソールの再起動（Restart Appliance Console）] の横にある [コマンドの実行（Run Command）] をクリックします。

（注） Firepower Management Center を再起動すると、ネットワーク マップ内に削除されたホストが再表示されることがあります。

ステップ 6 管理対象デバイスで Snort プロセスを再起動するには、[Snort の再起動（Restart Snort）] の横にある [コマンドの実行（Run Command）] をクリックします。

（注） このコマンドは、7000 および 8000 シリーズ デバイスのローカル Web インターフェイスでのみ使用できます。

注意 Snort プロセスを再開すると、一時的にトラフィック検査が中断されます。この中断中にトラフィックがドロップするか、検査なしで通過するかどうかは、デバイスの設定方法によって異なります。詳細については、Snort® の再起動によるトラフィックの動作，（326 ページ）を参照してください。

関連トピック

Snort® の再起動シナリオ，（324 ページ）

リモート ストレージ管理

Firepower Management Center では、バックアップおよびレポートのローカル ストレージまたはリモート ストレージとして、以下を使用することができます。

- ネットワーク ファイル システム（NFS）
- サーバ メッセージ ブロック（SMB）/Common Internet File System（CIFS）
- セキュア シェル（SSH）

（注） システムがサポートするバックアップおよびリモート ストレージのサーバ メッセージ ブロック プロトコルはバージョン 1 のみです。

1 つのリモート システムにバックアップを送信し、別のリモート システムにレポートを送信することはできませんが、どちらかをリモート システムに送信し、もう一方を Firepower Management Center に格納することは可能です。

ヒント リモート ストレージを構成して選択した後は、接続データベースの制限を**増やさなかった**場合に**のみ**、ローカル ストレージに戻すことができます。

ローカル ストレージの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] を選択します。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [ローカル（リモート ストレージなし）（Local (No Remote Storage)）] を選択します。

ステップ 4 [保存（Save）] をクリックします。

リモート ストレージの NFS の設定

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

はじめる前に

- 外部リモート ストレージ システムが機能しており、Management Center からアクセスできることを確認します。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [NFS] を選択します。

ステップ 4 接続情報を追加します。

- [ホスト（Host）] フィールドに、ストレージ システムの IPv4 アドレスまたはホスト名を入力します。
- [ディレクトリ（Directory）] フィールドに、ストレージ領域へのパスを入力します。

ステップ 5 必要に応じて、[詳細オプションの使用（Use Advanced Options）] チェックボックスをオンにして、必要なコマンド ライン オプションを入力します。リモート ストレージの管理詳細設定オプション, （586 ページ）を参照してください。

ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。
- リモート ストレージへのバックアップに関する [ディスク容量のしきい値（Disk Space Threshold）] を入力します。デフォルトは 90% です。

ステップ 7 設定をテストするには、[テスト（Test）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

リモート ストレージの SMB の設定

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

はじめる前に

- 外部リモート ストレージ システムが機能しており、Management Center からアクセスできることを確認します。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [SMB] を選択します。

ステップ 4 接続情報を追加します。

- [ホスト（Host）] フィールドに、ストレージ システムの IPv4 アドレスまたはホスト名を入力します。
- [共有（Share）] フィールドに、ストレージ領域の共有を入力します。システムに認識されるのは、ファイルのフルパスではなく、最上位の共有だけであることに注意してください。指定した共有ディレクトリをリモート バックアップ先として使用するには、それを Windows システムで共有する必要があります。
- 必要に応じて、[ドメイン（Domain）] フィールドにリモート ストレージ システムのドメイン名を入力します。
- [ユーザ名（Username）] フィールドにストレージ システムのユーザ名を入力し、[パスワード（Password）] フィールドにそのユーザのパスワードを入力します。

ステップ 5 必要に応じて、[詳細オプションの使用（Use Advanced Options）] チェックボックスをオンにして、必要なコマンド ライン オプションを入力します。リモート ストレージの管理詳細設定オプション，（586 ページ）を参照してください。

ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。

- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。

ステップ 7 設定をテストするには、[テスト（Test）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

リモート ストレージの SSH の設定

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

注意 アプライアンスの STIG 準拠を有効にすると、そのアプライアンスのリモート ストレージでは SSH を使用できません。

はじめる前に

- 外部リモート ストレージ システムが機能しており、Firepower Management Center からアクセスできることを確認します。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [SSH] を選択します。

ステップ 4 接続情報を追加します。

- [ホスト（Host）] フィールドに、ストレージ システムの IP アドレスまたはホスト名を入力します。
- [ディレクトリ（Directory）] フィールドに、ストレージ領域へのパスを入力します。
- [ユーザ名（Username）] フィールドにストレージ システムのユーザ名を入力し、[パスワード（Password）] フィールドにそのユーザのパスワードを入力します。接続ユーザ名の一部としてネットワーク ドメインを指定するには、ユーザ名の前にドメインを入力し、スラッシュ（/）で区切ります。
- SSH キーを使用するには、[SSH 公開キー（SSH Public Key）] フィールドの内容をコピーして authorized_keys ファイルに貼り付けます。

ステップ 5 必要に応じて、[詳細オプションの使用（Use Advanced Options）] チェックボックスをオンにして、必要なコマンド ライン オプションを入力します。リモート ストレージの管理詳細設定オプション，（586 ページ）を参照してください。

ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。

ステップ 7 設定をテストする場合は、[テスト（Test）] をクリックする必要があります。

ステップ 8 [保存（Save）] をクリックします。

リモート ストレージの管理詳細設定オプション

セキュア コピー（SCP）を使用してレポートとバックアップを保存するためにネットワーク ファイル システム（NFS）プロトコル、サーバ メッセージ ブロック（SMB）プロトコル、または SSH を選択すると、NFS、SMB、SSH マウントのマニュアル ページに記載されているいずれかのマウント バイナリ オプションを使用するために、[詳細設定オプションの使用] チェックボックスを選択できます。

SMB を選択すると、次の形式で [コマンド ライン オプション（Command Line Options）] フィールドにセキュリティ モードを入力します。

`sec=`*`mode`*
`mode` は、リモート ストレージで使用するセキュリティ モードです。

表 *59*：*SMB* セキュリティ モードの設定

[モード（Mode）]	説明
なし	NULL ユーザ（名前なし）として接続します。
`krb5`	Kerberos バージョン 5 認証を使用します。
`krb5i`	Kerberos 認証とパケット署名を使用します。
`ntlm`	NTLM パスワード ハッシュを使用します。（デフォルト）
`ntlmi`	署名付きの NTLM パスワード ハッシュを使用します（`/proc/fs/cifs/PacketSigningEnabled` がオンになっている場合またはサーバが署名を要求する場合はデフォルト）。
`ntlmv2`	NTLMv2 パスワード ハッシュを使用します。

[モード（Mode）]	説明
ntlmv2i	パケット署名付きの NTLMv2 パスワード ハッシュを使用します。

変更調整

ユーザが行う変更をモニタし、変更が部門の推奨する標準に従っていることを確認するため、過去24時間に行われたシステム変更の詳細なレポートを電子メールで送信するようにシステムを構成できます。ユーザが変更をシステム構成に保存するたびに、変更のスナップショットが取得されます。変更調整レポートは、これらのスナップショットを組み合わせて、最近のシステム変更の概要を提供します。

次の図は、変更調整レポートの [ユーザ（User）] セクションの例を示しています。ここには、各構成の変更前の値と変更後の値の両方が一覧表示されています。ユーザが同じ構成に対して複数の変更を行った場合は、個々の変更の概要が最新のものから順に時系列でレポートに一覧表示されます。

過去 24 時間に行われた変更を参照できます。

変更調整の設定

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

はじめる前に

- 24 時間にシステムに行われた変更のメール送信されるレポートを受信する電子メール サーバを設定します。詳細については、メール リレー ホストおよび通知アドレスの設定, （596 ページ）を参照してください。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [変更調整（Change Reconciliation）] をクリックします。

ステップ 3 [有効（Enable）] チェックボックスをオンにします。

ステップ 4 [実行する時間（Time to Run）] ドロップダウン リストから、システムが変更調整レポートを送信する時刻を選択します。

ステップ 5 [メール宛先（Email to）] フィールドにメール アドレスを入力します。

ヒント 電子メール アドレスを追加したら、いつでも [最新のレポートの再送信（Resend Last Report）] をクリックして、最新の変更調整レポートのコピーを受信者に再送信できます。

ステップ 6 ポリシーの変更を追加する場合は、[ポリシー設定を含める（Include Policy Configuration）] チェックボックスをオンにします。

ステップ 7 過去 24 時間のすべての変更を含める場合は、[全変更履歴を表示（Show Full Change History）] チェックボックスをオンにします。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

監査ログを使って変更を調査する，（2177 ページ）

変更調整オプション

[ポリシー設定を含める（Include Policy Configuration）] オプションは、ポリシーの変更のレコードを変更調整レポートに含めるかどうかを制御します。これには、アクセス制御、侵入、システム、ヘルス、およびネットワーク検出の各ポリシーの変更が含まれます。このオプションを選択しなかった場合は、ポリシーの変更はどれもレポートに表示されません。このオプションは Firepower Management Center のみで使用できます。

[すべての変更履歴を表示する（Show Full Change History）] オプションは、過去 24 時間のすべての変更のレコードを変更調整レポートに含めるかどうかを制御します。このオプションを選択しなかった場合は、変更がカテゴリごとに統合された形でレポートに表示されます。

ポリシー変更のコメント

ユーザがアクセス コントロール ポリシー、侵入ポリシー、またはネットワーク分析ポリシーを変更した場合、それらのポリシー関連の変更をコメント機能を使用してトラッキングするように Firepower システムを設定することができます。

ポリシー変更のコメントが有効にされていると、管理者はコメントにアクセスして、導入で重要なポリシーが変更された理由を素早く評価できます。オプションで、侵入ポリシーおよびネットワーク分析ポリシーに対する変更を監査ログに書き込むこともできます。

ポリシーの変更を追跡するコメントの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

ユーザがアクセスコントロールポリシー、侵入ポリシー、またはネットワーク分析ポリシーを変更する場合に、コメントの入力を要求するようにFirepowerシステムを設定できます。コメントを使用して、ユーザのポリシーの変更の理由を追跡できます。ポリシーの変更に関するコメントを有効にした場合、コメントをオプションまたは必須に設定できます。システムは、ポリシーに対する新しい変更が保存されるたびに、ユーザにコメントを入力するようプロンプトを出します。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。
システム設定オプションは、左側のナビゲーション パネルに表示されます。

ステップ 2 次のいずれかのポリシー コメントの設定を行います□

- アクセス コントロール ポリシーのコメント設定には、[アクセス コントロールの設定（Access Control Preferences）] をクリックします。
- 侵入ポリシーのコメント設定には、[侵入ポリシー設定（Intrusion Policy Preferences）] をクリックします。
- ネットワーク分析ポリシーのコメント設定には、[ネットワーク分析ポリシー設定（Network Analysis Policy Preferences）] をクリックします。

ステップ 3 各ポリシー タイプに次の選択肢があります。

- [無効化（Disabled）] : 変更のコメントを無効にします。
- [オプション（Optional）] : コメントの変更について記述するオプションをユーザに提供します。
- [必須（Required）] : 保存する前にコメントで変更について説明するようにユーザに要求します。

ステップ 4 侵入ポリシーまたはネットワーク分析ポリシーのコメントには、次のオプションがあります。

- 侵入ポリシーのすべての変更を監査ログに書き込むには、[侵入ポリシーの変更を監査ログに書き込む（Write changes in Intrusion Policy to audit log）] をオンにします。

- ネットワーク分析ポリシーのすべての変更を監査ログに書き込むには、[ネットワーク分析ポリシーの変更を監査ログに書き込む（Write changes in Network Analysis Policy to audit log）] をオンにします。

ステップ 5 [保存（Save）] をクリックします。

アクセス リスト

Firepower Management Center およびクラシック管理対象デバイスでは、アクセス リストを使用して、IP アドレスとポートを基準にシステムへのアクセスを制限できます。デフォルトでは、任意の IP アドレスに対して以下のポートが有効化されています。

- 443（HTTPS）：Web インターフェイス アクセスに使用されます。
- 22（SSH）：コマンド ライン アクセスに使用されます。

さらに、ポート 161 で SNMP 情報をポーリングするためのアクセスも追加できます。

注意 デフォルトでは、アクセスは制限されていません。よりセキュアな環境で運用するために、特定の IP アドレスに対するアクセスを追加してから、デフォルトの any オプションを削除することを検討してください。

システムのアクセス リストの設定

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

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

このアクセス リストは、外部データベース アクセスを制御しないので注意してください。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。
- 管理対象デバイス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [アクセス リスト（Access List）] をクリックします。

ステップ 3 現在の設定の 1 つを削除するために、削除アイコン（）をクリックすることもできます。

注意 アプライアンスのインターフェイスへの接続に現在使用されている IP アドレスへのアクセスを削除し、`IP=any port=443` のエントリが存在しない場合、ポリシーを展開した時点でシステムへのアクセスは失われます。

ステップ 4 1 つ以上の IP アドレスへのアクセスを追加するには、[ルールの追加（Add Rules）] をクリックします。

ステップ 5 [IP アドレス（IP Address）] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、`any` を入力します。

ステップ 6 [SSH]、[HTTPS]、[SNMP]、またはこれらのオプションの組み合わせを選択して、これらの IP アドレスで有効にするポートを指定します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）

監査ログ

Firepower Management Center および従来型管理対象デバイスは、ユーザ アクティビティに関する読み取り専用の監査情報をログに記録します。Management Center および 7000 および 8000 シリーズ の Web インターフェイスでは、監査ログ イベントは標準イベント ビューに表示されます。標準イベント ビューでは、監査ビューの任意の項目に基づいて監査ログ メッセージの表示、並べ替え、フィルタ処理ができます。監査情報を簡単に削除したり、それに関するレポートを作成したりすることができ、ユーザが行った変更に関する詳細なレポートを表示することもできます。

監査ログ メッセージを syslog に送信するよう、Firepower Management Center および従来型管理対象デバイスを設定することもできます。設定するには、syslog サーバ、およびメッセージに関連

付ける重大度、ファシリティ、オプション タグを指定します。タグは、syslog の監査ログ メッセージと一緒に表示されます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。syslog メッセージにはファシリティおよび重大度は含まれません。これらの値は syslog メッセージを受信するシステムにメッセージの分類方法を示す値です。

また、監査ログ メッセージを HTTP サーバにストリーミングするよう、Firepower Management Center および従来型管理対象デバイスで設定することもできます。

監査ログ ストリーミング設定は、アプライアンスのタイプによって異なる設定の一部となっています。

- Firepower Management Center では、監査ログのストリーミングはシステム設定の一部です。
- クラシック管理対象デバイスでは、監査ログ ストリーミングは Firepower Management Center プラットフォーム設定ポリシーの一部です。

いずれの場合も、システム設定の変更を保存するか、共有プラットフォーム設定ポリシーを展開するまでは設定は有効になりません。

外部ストリーミングの監査ログの設定

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

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

次に、出力構造の例を示します。

```
Date Time Host [Tag] Sender: [User_Name]@[User_IP], [Subsystem], [Action]
```

現地の日付、時刻、およびホスト名の後に、角括弧で囲まれたオプション タグが続き、送信側デバイス名の後に監査ログ メッセージが続きます。

次に例を示します。

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3500: admin@10.1.1.2, Operations > Monitoring, Page
View
```

はじめる前に

- 外部ホストが機能していることと、監査ログを送信するシステムからアクセスできることを確認します。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。
- 管理対象デバイス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択して、Firepower ポリシーを作成または編集します。

ステップ 2 [監査ログ（Audit Log）] をクリックします。

ステップ 3 [監査ログを Syslog に送信（Send Audit Log to Syslog）] ドロップダウン メニューから、[有効化（Enabled）] を選択します。

ステップ 4 [ホスト（Host）] フィールドにあるホストの IP アドレスまたは完全修飾名を使用して、監査情報の宛先ホストを指定します。デフォルト ポート（514）が使用されます。

注意 監査ログを受け入れるように設定しているコンピュータが、リモート メッセージを受け入れるようにセットアップされていない場合、ホストは監査ログを受け入れません。

ステップ 5 [syslog ファシリティ（syslog Facility）] を選択します。

ステップ 6 重大度を選択します。

ステップ 7 必要に応じて、[タグ（オプション）（Tag (optional)）] フィールドで参照タグを挿入します。

ステップ 8 定期的な監査ログの更新を外部 HTTP サーバに送信するには、[監査ログを HTTP サーバに送信（Send Audit Log to HTTP Server）] ドロップダウン リストから [有効化（Enabled）] を選択します。

ステップ 9 [監査情報を送信する URL（URL to Post Audit）] フィールドに、監査情報の送信先 URL を指定します。次にリストされている HTTP POST 変数を要求するリスナー プログラムに対応する URL を入力する必要があります。

- `subsystem`
- `actor`
- `event_type`
- `message`
- `action_source_ip`
- `action_destination_ip`
- 結果
- 時刻

- `tag`（上記のように定義されている場合）

注意 暗号化されたポストを許可するには、HTTPS URL を使用する必要があります。外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があるので注意してください。

ステップ 10 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

ダッシュボード設定

ダッシュボードでは、ウィジェットを使用することにより、現在のシステム ステータスが一目でわかります。ウィジェットは小さな自己完結型コンポーネントであり、Firepower システムのさまざまな側面に関するインサイトを提供します。Firepower システムには、事前定義された複数のダッシュボード ウィジェットが付属しています。

[カスタム分析（Custom Analysis）] ウィジェットがダッシュボードで有効になるように、Firepower Management Center を設定できます。

関連トピック

ダッシュボードについて，（223 ページ）

ダッシュボードのカスタム分析ウィジェットの有効化

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

[カスタム分析（Custom Analysis）] ダッシュボード ウィジェットを使用して、柔軟でユーザによる構成が可能なクエリに基づいてイベントのビジュアル表現を作成します。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [ダッシュボード（Dashboard）] をクリックします。

ステップ 3 ユーザが [カスタム分析（Custom Analysis）] ウィジェットをダッシュボードに追加できるようにするには、[カスタム分析ウィジェットの有効化（Enable Custom Analysis Widgets）] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

DNS キャッシュ

イベント表示ページで、IP アドレスを自動的に解決するようにシステムを設定できます。また、アプライアンスによって実行される DNS キャッシュの基本的なプロパティを設定できます。DNS キャッシングを設定すると、追加のルックアップを実行せずに、以前に解決した IP アドレスを識別できます。これにより、IP アドレスの解決が有効になっている場合に、ネットワーク上のトラフィックの量を減らし、イベント ページの表示速度を速めることができます。

DNS キャッシュ プロパティの設定

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

DNS 解決のキャッシングは、以前に解決された DNS ルックアップのキャッシングを許可するシステム全体の設定です。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [DNS キャッシュ（DNS Cache）] を選択します。

ステップ 3 [DNS 解決のキャッシング（DNS Resolution Caching）] ドロップダウン リストから、次のいずれかを選択します。

- [有効化（Enabled）]：キャッシングを有効にします。

- [無効化（Disabled）]：キャッシングを無効にします。

ステップ 4 [DNS キャッシュ タイムアウト（分）（DNS Cache Timeout（in minutes））] フィールドで、非アクティブのために削除されるまでDNSエントリがメモリ内にキャッシュされる時間（分単位）を入力します。
デフォルトは 300 分（5 時間）です。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

イベント ビュー設定の設定，（38 ページ）
管理インターフェイス，（564 ページ）

電子メールの通知

次の処理を行う場合は、メール ホストを設定します。

- イベントベースのレポートの電子メール送信
- スケジュールされたタスクのステータス レポートの電子メール送信
- 変更調整レポートの電子メール送信
- データプルーニング通知の電子メール送信
- 検出イベント、インパクト フラグ、相関イベント アラート、侵入イベント アラート、およびヘルス イベント アラートでの電子メールの使用

電子メール通知を設定する場合、システムとメール リレーホスト間の通信に使用する暗号化方式を選択し、必要に応じて、メール サーバの認証クレデンシャルを指定できます。設定した後、接続をテストできます。

メール リレー ホストおよび通知アドレスの設定

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

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [Email Notification] をクリックします。

ステップ 3 [メール リレー ホスト（Mail Relay Host）] フィールドで、使用するメール サーバのホスト名またはIPアドレスを入力します。入力したメールホストはアプライアンスからのアクセスを許可している必要があります。

ステップ 4 [ポート番号（Port Number）] フィールドに、電子メール サーバで使用するポート番号を入力します。
一般的なポートには次のものがあります。

- 25。暗号化を使用しない場合
- 465。SSLv3 を使用する場合
- 587。TLS を使用する場合

ステップ 5 [暗号化方式（Encryption Method）] を選択します。

- [TLS]：Transport Layer Security を使用して通信を暗号化します。
- [SSLv3]：セキュア ソケット レイヤを使用して通信を暗号化します。
- [なし（None）]：暗号化されていない通信を許可します。

（注） アプライアンスとメール サーバとの間の暗号化された通信では、証明書の検証は不要です。

ステップ 6 [送信元アドレス（From Address）] フィールドに、アプライアンスから送信されるメッセージの送信元電子メール アドレスとして使用する有効な電子メール アドレスを入力します。

ステップ 7 必要に応じて、メールサーバに接続する際にユーザ名とパスワードを指定するには、[認証を使用（Use Authentication）] を選択します。[ユーザ名（Username）] フィールドにユーザ名を入力します。パスワードを [パスワード（Password）] フィールドに入力します。

ステップ 8 設定したメール サーバを使用してテスト メールを送信するには、[テスト メールのサーバ設定（Test Mail Server Settings）] をクリックします。
テストの成功または失敗を示すメッセージがボタンの横に表示されます。

ステップ 9 [保存（Save）] をクリックします。

言語の選択

[言語（Language）] ページを使用して、Web インターフェイス用に異なる言語を指定できます。

別の言語の指定

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

この設定は、Firepower Management Center または 7000 および 8000 シリーズ 管理対象デバイスに適用されます。

- Firepower Management Center では、この設定はシステム設定の一部になります。
- 7000 および 8000 シリーズ 管理対象デバイスでは、この設定をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

注意 ここで指定した言語は、アプライアンスにログインしたすべてのユーザの Web インターフェイスに使用されます。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。
- 管理対象デバイス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [言語（Language）] をクリックします。

ステップ 3 使用する言語を選択します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ログイン バナー

[ログイン バナー（Login Banner）] ページを使用して、セキュリティ アプライアンスまたは共有ポリシーのセッション バナー、ログイン バナー、カスタム メッセージ バナーを指定できます。

バナーのテキストにはスペースを使用できますが、タブは使用できません。バナーには複数行のテキストを指定できます。テキストに空の行が含まれている場合、バナーでは、その行が改行（CR）として表示されます。使用できるのは、改行（Enter キーを押す）を含む ASCII 文字だけです。改行は 2 文字としてカウントされます。

Telnet または SSH を介してセキュリティ アプライアンスにアクセスしたときに、バナー メッセージを処理するのに十分なシステム メモリがなかった場合や、バナー メッセージの表示を試行して TCP 書き込みエラーが発生した場合には、セッションが閉じます。

カスタム ログイン バナーの追加

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

SSH または Web インターフェイスからログインするユーザに向けて表示するカスタム ログイン バナーを作成できます。

この設定は、Firepower Management Center または従来型の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

手順

ステップ 1 Firepower Management Center または Classic 管理対象デバイスのいずれを設定しているかに応じて、以下を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。

- 管理対象デバイスの場合：[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）] を選択するか、ファイアウォール ポリシーを作成、または編集します。

ステップ 2 [ログイン バナー（Login Banner）] を選択します。

ステップ 3 [カスタム ログイン バナー（Custom Login Banner）] フィールドに、使用するログイン バナー テキストを入力します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

SNMP ポーリング

Firepower Management Center およびクラシック管理対象デバイスには、Simple Network Management Protocol（SNMP）ポーリングを有効にすることができます。SNMP 機能は、SNMP プロトコルのバージョン 1、2、3 をサポートします。

この機能を使用して、次の要素にアクセスできます。

- 標準 Management Information Base（MIB）。これには、連絡先、管理、場所、サービス情報、IP アドレッシングやルーティングの情報、トランスミッション プロトコルの使用状況の統計などのシステムの詳細が含まれます。
- 7000 および 8000 シリーズ 管理対象デバイスの追加の MIB。これには、物理インターフェイス、論理インターフェイス、仮想インターフェイス、ARP、NDP、仮想ブリッジ、仮想ルータを通して渡されるトラフィックの統計が含まれます。

（注） SNMP プロトコルの SNMP バージョンを選択する際は、SNMPv2 では読み取り専用コミュニティのみをサポートし、SNMPv3 では読み取り専用ユーザのみをサポートすることに注意してください。SNMPv3 は AES128 による暗号化もサポートします。

SNMP 機能を有効にすると、システムで SNMP トラップを送信できなくなり、MIB の情報はネットワーク管理システムによるポーリングでのみ使用可能になることに注意してください。

SNMP ポーリングの設定

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

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

（注） システムをポーリングするには、使用する任意のコンピュータで SNMP アクセスを追加する必要があります。SNMP MIB には展開の攻撃に使用される可能性がある情報も含まれているので注意してください。SNMP アクセスのアクセス リストを MIB のポーリングに使用される特定のホストに制限することをお勧めします。SNMPv3 を使用し、ネットワーク管理アクセスには強力なパスワードを使用することもお勧めします。

SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

はじめる前に

- システムのアクセス リストの設定, （590 ページ）の説明に従って、使用するコンピュータごとに SNMP アクセスを追加し、システムをポーリングします。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。
- 管理対象デバイス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [SNMP] をクリックします。

ステップ 3 [SNMP バージョン（SNMP Version）] ドロップダウン リストから、使用する SNMP バージョンを選択します。

ステップ 4 次の選択肢があります。

- [バージョン 1（Version 1）] または [バージョン 2（Version 2）] を選択した場合は、[コミュニティ ストリング（Community String）] フィールドに SNMP コミュニティ名を入力します。手順 13 に進みます。

  （注） SNMPv2 は、読み取り専用コミュニティのみをサポートしています。

- [バージョン 3（Version 3）] を選択した場合、[ユーザを追加（Add User）] をクリックするとユーザ定義ページが表示されます。

  （注） SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

ステップ 5 ユーザ名を入力します。

ステップ 6 [認証プロトコル（Authentication Protocol）] ドロップダウン リストから、認証に使用するプロトコルを選択します。

ステップ 7 [認証パスワード（Authentication Password）] フィールドに SNMP サーバの認証に必要なパスワードを入力します。

ステップ 8 [パスワードの確認（Verify Password）] フィールドに、認証パスワードを再度入力します。

ステップ 9 使用するプライバシー プロトコルを [プライバシー プロトコル（Privacy Protocol）] リストから選択するか、プライバシー プロトコルを使用しない場合は [なし（None）] を選択します。

ステップ 10 [プライバシー パスワード（Privacy Password）] フィールドに SNMP サーバで必要な SNMP プライバシー キーを入力します。

ステップ 11 [パスワードの確認（Verify Password）] フィールドに、プライバシー パスワードを再度入力します。

ステップ 12 [追加（Add）] をクリックします。

ステップ 13 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

STIG コンプライアンス

米国連邦政府内の組織は、Security Technical Implementation Guides（STIG）に示されている一連のセキュリティ チェックリストに準拠しなければならない場合があります。Firepower システムは、米国国防総省で規定している STIG 要件のコンプライアンスをサポートしています。

展開内の任意のアプライアンスで STIG コンプライアンスを有効にする場合は、それをすべてのアプライアンスで有効にする必要があります。非準拠の管理対象デバイスを STIG 準拠の Firepower Management Center に登録したり、STIG 準拠デバイスを非準拠の Firepower Management Center に登録したりすることはできません。

STIG コンプライアンスを有効にした場合、適用可能なすべての STIG に厳格なコンプライアンスが保証されるわけではありません。。

STIG コンプライアンスを有効にすると、ローカル シェル アクセス アカウントのパスワードの複雑さや維持に関するルールが変わります。さらに、STIG コンプライアンス モードでは、SSH のリモート ストレージを使用できません。

注意 サポートからの支援なしでこの設定を無効にすることはできません。また、この設定はシステムのパフォーマンスに大きく影響する可能性があります。シスコでは、米国国防総省（DoD）のセキュリティ要件に準拠する以外の目的で、STIG コンプライアンスを有効にすることを推奨しません。

STIG コンプライアンスの有効化

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

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

注意 展開内の任意のアプライアンスで STIG コンプライアンスを有効にする場合は、それをすべてのアプライアンスで有効にする必要があります。サポートからの支援なしでこの設定を無効にすることはできません。また、この設定はシステムのパフォーマンスに大きく影響する可能性があります。シスコでは、米国国防総省（DoD）のセキュリティ要件に準拠する以外の目的で、STIG コンプライアンスを有効にすることを推奨しません。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。
- 管理対象デバイス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [STIG Compliance] をクリックします。

（注） STIG コンプライアンスを有効にすると、アプライアンスがリブートします。Firepower Management Center は、システム設定を保存するとリブートし、管理対象デバイスは、設定の変更を展開するとリブートします。

ステップ 3 STIG コンプライアンスをアプライアンスで永続的に有効にする場合は、[STIG コンプライアンスを有効化（Enable STIG Compliance）] を選択します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。
- アプライアンスがバージョン 5.2.0 より前のバージョンから更新された場合は、STIG コンプライアンスを有効にすると、アプライアンス証明書が再生成されます。展開全体で STIG コンプライアンスを有効にした後、管理対象デバイスを Firepower Management Center に再登録します。

時刻および時刻の同期

[時刻（Time）] ページを使用して、Firepower Management Center、あるいは 7000 または 8000 シリーズデバイスのローカル Web インターフェイスから現在の時刻と時刻源を表示することができます。

時刻の設定は、アプライアンスの大半のページで、[タイム ゾーン（Time Zone）] ページで設定したタイム ゾーン（デフォルトでは [アメリカ/ニューヨーク（America/New York）]）を使用してローカル時間で表示されますが、アプライアンス自体には UTC 時間を使用して保存されます。また、現在の時刻は [時刻の同期（Time Synchronization）] ページの上部に UTC で表示されます（ローカル時間は [手動（Manual）] の時計設定オプションで表示されます（有効になっている場合））。

時刻の同期は、[時刻の同期（Time Synchronization）] ページを使用して管理できます。時刻を同期する場合、以下の方法を選択できます。

- 手動で
- 1 つ以上の NTP サーバを使用（推奨）

ハードウェアの Firepower Management Center を NTP サーバとして使用できますが、仮想 Firepower Management Center は NTP サーバとして使用しないでください。

リモートの NTP サーバを指定する場合、アプライアンスにそのサーバに対するネットワーク アクセス権限が必要です。信頼できない NTP サーバを指定しないでください。NTP サーバへの接続では、構成されたプロキシ設定は使用されません。

（注） 時刻の同期後に、Firepower Management Center と管理対象デバイスの時刻が一致するようにしてください。時刻が一致していない場合、管理対象デバイスが Firepower Management Center と通信する際に意図しない結果が生じるおそれがあります。

手動での時間指定

Firepower Management Center の時刻同期が [ローカル設定で手動（Manually in Local Configuration）] に設定されている場合、システムの時刻を手動で設定できます。

- Firepower Management Center が NTP を使用して時間を提供するようにするには、NTP を使用して時間を提供するように Firepower Management Center を設定する**前**に、時間を手動で変更する必要があります。
- Firepower Management Center を NTP サーバとして設定してから時刻を変更する必要がある場合、NTP オプションを無効にして、時間を手動で変更してから NTP オプションを再度有効にする必要があります。

システムの時間が NTP に基づいて同期されている場合、Firepower Management Center の Web インターフェイスおよび 7000 および 8000 シリーズ デバイスのローカル Web インターフェイスで以下の情報を含む NTP ステータスを表示できます。

表 *60*：*NTP* ステータス

カラム（**Column**）	説明
NTP サーバ	構成済みの NTP サーバの IP アドレスと名前。
ステータス	NTP サーバの時間同期のステータス。 • [使用中（Being Used）] は、アプライアンスが NTP サーバと同期していることを示します。 • [利用可能（Available）] は、NTP サーバが使用可能であるものの、時間がまだ同期していないことを示します。 • [使用不可（Not Available）] は、NTP サーバが構成に含まれているものの、NTP デーモンがその NTP サーバを使用できないことを示します。 • [待機中（Pending）] は、NTP サーバが新しいか、または NTP デーモンが最近再起動されたことを示します。この値は、時間の経過とともに [使用中（Being Used）]、[利用可能（Available）]、または [使用不可（Not Available）] に変わるはずです。 • [不明（Unknown）] は、NTP サーバのステータスが不明であることを示します。

カラム（Column）	説明
オフセット	アプライアンスと構成済みのNTPサーバ間の時間の差（ミリ秒）。負の値はアプライアンスの時間がNTPサーバより遅れていることを示し、正の値は進んでいることを示します。
最終更新	NTPサーバと最後に時間を同期してから経過した時間（秒数）。NTPデーモンは、いくつかの条件に基づいて自動的に同期時間を調整します。たとえば、更新時間が大きい（300 秒など）場合、それは時間が比較的安定しており、NTPデーモンが小さい更新増分値を使用する必要がないと判断したことを示します。

時刻の手動設定

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

Firepower Management Center または 7000 および 8000 シリーズ デバイスのローカル Web インターフェイスで [時間（Time）] ページを使用して、現在の時刻と時刻源を表示できます。

（注） NTP を使用して Firepower Management Center に時間を提供させる場合、時間を手動で変更してから Management Center が NTP を使用して時間を提供するように設定します。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [時間同期（Time Synchronization）] をクリックします。

ステップ 3 [NTP を使用して時間を提供（Serve Time via NTP）] が [有効（Enabled）] の場合、[無効（Disable）] を選択します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [ローカル設定で手動（Manually in Local Configuration）] を選択します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [時間（Time）] をクリックします。

ステップ 8 [時間の設定（Set Time）] ドロップダウン リストを使用して時間を設定します。

ステップ 9 [適用（Apply）] をクリックします。

次の作業

- NTP を使用して Firepower Management Center に時間を提供させるには、次の説明に従って続行します。 Firepower Management Center からの時間の提供, （607 ページ）

Firepower Management Center からの時間の提供

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

（注） NTP を使用して時刻を提供するように Management Center を設定してから、後でそれを無効にした場合、管理対象デバイスの NTP サービスは引き続き Management Center と時刻を同期しようとします。新しい時刻ソースを確立するには、すべての該当するプラットフォーム設定ポリシーを更新および再展開する必要があります。

はじめる前に

- 手動で時間を変更します。時刻の手動設定, （606 ページ）を参照してください。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [時刻同期（Time Synchronization）] をクリックします。

ステップ 3 [NTP 経由で時刻を提供（Serve Time via NTP）] ドロップダウンリストから、[有効（Enabled）] を選択します。

ステップ 4 管理対象デバイスの [自分のクロックの設定（Set My Clock）] オプションについては、時刻の同期方法を指定するための次のオプションを選択できます。

- [ローカル設定で手動（Manually in Local Configuration）] を選択して、Firepower Management Center から NTP 経由で時刻を受信します。詳細については、時刻の手動設定, （606 ページ）を参照してください。
- [NTP 経由（Via NTP from）] を選択して、さまざまなサーバから NTP 経由で時刻を受信します。テキスト ボックスで、NTP サーバの IP アドレスのカンマ区切りリストを入力するか、DNS が有効になっている場合は、完全修飾ホスト名およびドメイン名を入力します。

注意 アプライアンスがリブートされ、ここで指定したものとは異なる NTP サーバ レコードを DHCP サーバが設定した場合、DHCP 提供の NTP サーバが代わりに使用されます。この状況を回避するには、同じ NTP サーバを設定するように DHCP サーバを設定します。

ステップ 5 [保存（Save）] をクリックします。

（注） Management Center を管理対象デバイスと同期するには、数分かかる場合があります。

時間の同期

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

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

手順

ステップ 1 Firepower Management Center または Classic 管理対象デバイスのいずれを設定しているかに応じて、以下を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。
- 管理対象デバイス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [時間同期（Time Synchronization）] をクリックします。

ステップ 3 管理対象デバイスで時刻を同期する方法を指定する次のオプションがあります。

- NTP を介して Management Center から時刻を受信するには、[NTP 経由で管理センターから（Via NTP from Management Center）] を選択します。詳細については、Firepower Management Center からの時間の提供, （607 ページ）を参照してください。

- [NTP 経由（Via NTP from）] を選択して、さまざまなサーバから NTP 経由で時刻を受信します。テキスト ボックスで、NTP サーバの IP アドレスのカンマ区切りリストを入力するか、DNS が有効になっている場合は、完全修飾ホスト名およびドメイン名を入力します。

ステップ 4 [保存（Save）] をクリックします。

（注） 設定された NTP サーバと管理対象デバイスを同期するには、数分かかる場合があります。さらに、管理対象デバイスを NTP サーバとして設定されている Management Center と同期する場合、Management Center 自体が NTP サーバを使用するように設定されていると、時刻を同期するのにいくらか時間がかかることがあります。これは、管理対象デバイスに時刻を提供するために、Management Center は設定された NTP サーバとまず同期する必要があるためです。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。
- Management Center と管理対象デバイスの時刻が一致していることを確認します。

セッション タイムアウト

Firepower システムの Web インターフェイスまたは補助コマンドライン インターフェイスの無人ログイン セッションは、セキュリティ上のリスクを生じさせる場合があります。ユーザのログイン セッションが非アクティブなったためにタイムアウトするまでのアイドル時間を分単位で設定できます。シェル（コマンドライン）セッションでも同様のタイムアウトを設定できます。

長期にわたり Web インターフェイスをパッシブかつセキュアにモニタする予定のユーザが、導入内に存在する可能性があります。ユーザ設定オプションで Web インターフェイスのセッション タイムアウトからユーザを除外することができます。メニュー オプションへの完全なアクセス権がある管理者ロールのユーザは、侵害が生じる場合、余分のリスクを生じさせますが、セッション タイムアウトから除外することはできません。

セッション タイムアウトの設定

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

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。

- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

システムへのシェル アクセスを制限する必要がある場合、追加オプションによって補助コマンドライン インターフェイスの `expert` コマンドを永続的に無効にすることができます。アプライアンスでエキスパート モードを無効にすると、構成シェル アクセスを持つユーザでも、シェルのエキスパート モードに入ることができなくなります。ユーザが補助コマンドライン インターフェイスのエキスパート モードに入ると、ユーザはシェルに応じた任意の Linux コマンドを実行できます。エキスパート モードに入っていない場合は、コマンドライン ユーザはコマンドライン インターフェイスが提供するコマンドだけを実行できます。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。
- 管理対象デバイス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [シェル タイムアウト（Shell Timeout）] をクリックします。

ステップ 3 次の選択肢があります。

- Web インターフェイスのセッション タイムアウトを設定するには、[ブラウザ セッション タイムアウト（分）（Browser Session Timeout (Minutes)）] フィールドに数値（分数）を入力します。デフォルト値は `60` で、最大値は `1440`（24 時間）です。このセッション タイムアウトからユーザを除外する方法については、ユーザ アカウント ログイン オプション，（81 ページ）を参照してください。
- コマンドライン インターフェイスのセッション タイムアウトを設定するには、[シェル タイムアウト（分）（Shell Timeout (Minutes)）] フィールドに数値（分数）を入力します。デフォルト値は `0` で、最大値は `1440`（24 時間）です。
- 補助コマンドライン インターフェイスで `expert` コマンドを永続的に無効にするには、[expert コマンドを永続的に無効化（Permanently Disable Expert Access）] チェックボックスを選択します。

注意 エキスパート モードが無効になった状態でポリシーをアプライアンスに展開した場合、Web インターフェイスまたは補助コマンドライン インターフェイスを介してエキスパート モードにアクセスする機能を復元することはできません。エキスパート モード機能を復元するには、サポートに問い合わせる必要があります。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

脆弱性マッピング

サーバのディスカバリイベントデータベースにアプリケーションIDが含まれており、トラフィックのパケットヘッダにベンダーおよびバージョンが含まれる場合、Firepowerシステムは、そのアドレスから送受信されるすべてのアプリケーションプロトコルトラフィックについて、脆弱性をホストIPアドレスに自動的にマップします。

パケットにベンダー情報もバージョン情報も含まれないサーバすべてに対して、システムでこれらのベンダーとバージョンレスのサーバのサーバトラフィックと脆弱性を関連付けるかどうかを設定できます。

たとえば、ホストがヘッダーにベンダーまたはバージョンが含まれていないSMTPトラフィックを提供しているとします。システム設定の[脆弱性マッピング（Vulnerability Mapping）]ページでSMTPサーバを有効にしてから、そのトラフィックを検出するデバイスを管理するFirepower Management Centerにその設定を保存した場合、SMTPサーバと関連付けられているすべての脆弱性がそのホストのホストプロファイルに追加されます。

ディテクタがサーバ情報を収集して、それをホストプロファイルに追加しますが、アプリケーションプロトコルディテクタは脆弱性のマッピングに使用されません。これは、カスタムアプリケーションプロトコルディテクタにベンダーまたはバージョンを指定できず、また脆弱性マッピング用のサーバを選択できないためです。

サーバの脆弱性のマッピング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Protection	Management Center	グローバルのみ	Admin

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [脆弱性マッピング（Vulnerability Mapping）] を選択します。

ステップ 3 次の選択肢があります。

- ベンダーまたはバージョンの情報が含まれていないアプリケーションプロトコルトラフィックを受信するホストに、サーバの脆弱性がマップされないようにするには、そのサーバのチェックボックスをオフにします。

- ベンダーまたはバージョンの情報が含まれていないアプリケーション プロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされるようにするには、そのサーバのチェックボックスをオフにします。

ヒント [有効（Enabled）]の横にあるチェックボックスを使用すると、すべてのチェックボックスを一度にオンまたはオフにできます。

ステップ 4 [保存（Save）] をクリックします。

リモート コンソールのアクセス管理

サポート対象システム上でリモートアクセスを行うため、VGA ポート（デフォルト）または物理アプライアンス上のシリアル ポートを介して Linux システムのコンソールを使用できます。組織の Cisco 導入の物理レイアウトに最も適したオプションを選択してください。

サポートされている物理ハードウェア ベースの Firepower システムでは、Serial Over LAN（SOL）接続のデフォルト管理インターフェイス（`eth0`）で Lights-Out 管理（LOM）を使用すると、システムの管理インターフェイスにログインすることなく、リモートでシステムをモニタまたは管理できます。アウトオブバンド管理接続のコマンドライン インターフェイスを使用すると、シャーシのシリアル番号の表示や状態（ファン速度や温度など）のモニタなどの、限定タスクを実行できます。

LOM は、システムとシステムを管理するユーザの両方で有効にする必要があります。システムとユーザを有効にした後、サードパーティ製の Intelligent Platform Management Interface（IPMI）ユーティリティを使用し、システムにアクセスして管理します。

システム上のリモート コンソール設定の構成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	Management Center および7000 & 8000 シリーズ	グローバルだけ	LOM アクセス権限のある Admin

はじめる前に

- デバイスの管理インターフェイスに接続されたサードパーティ スイッチング装置で、スパニング ツリー プロトコル（STP）を無効にします。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [コンソール構成（Console Configuration）] をクリックします。

ステップ 3 リモート コンソール アクセスのオプションを選択します。

- アプライアンスの VGA ポートを使用するには、[VGA] を選択します。
- アプライアンスのシリアル ポートを使用するか、Firepower Management Center、Firepower 7050、または 8000 シリーズ デバイス上で LOM/SOL を使用する場合には、[物理シリアル ポート（Physical Serial Port）] を選択します。
- 7000 シリーズ デバイス（Firepower 7050 以外）で LOM/SOL を使用する場合は、[Lights-Out Management] を選択します。これらのデバイスでは、SOL と通常のシリアル接続を同時に使用することはできません。

（注） リモート コンソールを [物理シリアル ポート（Physical Serial Port）] から [Lights-Out Management] に変更した場合や、70xx ファミリのデバイス（Firepower 7050 以外）で [Lights-Out Management] から [物理シリアル ポート（Physical Serial Port）] に変更した場合は、アプライアンスを 2 回リブートしないと、期待どおりのブート プロンプトが表示されないことがあります。

ステップ 4 SOL 経由で LOM を設定するには、必要な IPv4 設定を入力します。

- システムのアドレス構成（[DHCP] または [Manual（手動）]）を選択します。
- LOM に使用する IP アドレスを入力します。

  （注） LOM IP アドレスは、システムの管理インターフェイスの IP アドレスとは異なる必要があります。

- システムのネットマスクを入力します。
- システムのデフォルト ゲートウェイを入力します。

ステップ 5 [保存（Save）] をクリックします。

次の作業

- Lights-Out Management を設定した場合は、Lights-Out Management ユーザを有効にします。Lights-Out 管理のユーザ アクセス設定, （613 ページ）を参照してください。

Lights-Out 管理のユーザ アクセス設定

Lights-Out 管理機能を使用するユーザに対して、この機能の権限を明示的に付与する必要があります。LOM ユーザには、次のような制約もあります。

- ユーザに Administrator ロールを割り当てる必要があります。

- ユーザ名に使用できるのは最大 16 個の英数字です。LOM ユーザに対し、ハイフンやそれより長いユーザ名はサポートされていません。
- 71xx ファミリ デバイスへの設定を除き、パスワードには最大 20 文字の英数字を使用できます。Firepower 7110、7115、7120、または 7125 デバイスで LOM が有効になっている場合、パスワードには最大 16 文字の英数字を使用できます。20 または 16 文字よりも長いパスワードは、LOM ユーザに対してサポートされません。ユーザの LOM パスワードは、そのユーザのシステム パスワードと同じです。辞書に載っていない複雑な最大長のパスワードをアプライアンスに対して使用し、それを 3 か月ごとに変更することを推奨します。
- 物理 Firepower Management Center および 8000 シリーズ デバイスには、最大 13 人の LOM ユーザを設定できます。8000 シリーズ デバイスには、最大 8 人の LOM ユーザを設定できます。

あるロールを持つユーザのログイン中に LOM でそのロールを非アクティブ化してから再アクティブ化した場合や、ユーザのログインセッション中にそのユーザまたはユーザ ロールをバックアップから復元した場合、そのユーザは IPMItool コマンドへのアクセスを回復するために Web インターフェイスにログインし直す必要があります。

Lights-Out 管理ユーザ アクセスの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	Management Center および 7000 & 8000 シリーズ	グローバルだけ	LOM アクセス権限のある Admin

各システムのローカル Web インターフェイスを使用して、システムごとに LOM と LOM ユーザを設定します。つまり、Firepower Management Center を使用して管理対象デバイスで LOM を設定することはできません。同様に、ユーザはアプライアンスごとに個別に管理されるため、Firepower Management Center で LOM 対応ユーザを有効化または作成しても、管理対象デバイスのユーザにはその機能は転送されません。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [コンソール構成（Console Configuration）] をクリックします。

ステップ 3 [Lights Out 管理（Lights Out Management）] をクリックします。

ステップ 4 次の選択肢があります。

- 既存のユーザに LOM ユーザ アクセスを許可するには、リスト内のユーザ名の横にある編集アイコン（）をクリックします。

- 新しいユーザに LOM ユーザ アクセスを許可するには、[ユーザの作成（Create User）] をクリックします。

ステップ 5 [ユーザの設定（User Configuration）] で、Administrator ロールを有効にします。

ステップ 6 [Lights-Out 管理アクセスの許可（Allow Lights-Out Management Access）] チェックボックスをオンにします。

ステップ 7 [保存（Save）] をクリックします。

Serial over LAN 接続の設定

アプライアンスへの Serial over LAN 接続を作成するには、コンピュータ上でサードパーティ製の IPMI ユーティリティを使用します。Linux 系環境または Mac 環境を使用するコンピュータでは IPMItool を使用し、Windows 環境では IPMIutil を使用します。

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Linux

多くのディストリビューションで IPMItool が標準となっており、使用可能です。

Mac

Mac では、IPMItool をインストールする必要があります。最初に、Mac に Apple の XCode Apple Developer Tools がインストールされていることを確認します。これにより、コマンドライン開発用のオプション コンポーネント（新しいバージョンでは UNIX Development and System Tools、古いバージョンでは Command Line Support）がインストールされていることを確認できます。次に、MacPorts と IPMItool をインストールします。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

Windows

Windows では、IPMIutil をコンパイルする必要があります。コンパイラにアクセスできない場合は、IPMIutil 自体を使用してコンパイルできます。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

```
http://ipmiutil.sourceforge.net/
```

IPMI ユーティリティのコマンドについて

IPMIユーティリティで使用するコマンドは、次のIPMItoolの例に示したセグメントで構成されます。

```
ipmitool -I lanplus -H IP_address -U user_name command
```

引数の説明

- `ipmitool` はユーティリティを起動します
- `-I lanplus` はセッションの暗号化を有効にします
- `-H` IP_address はアクセスするアプライアンスの IP アドレスを示します
- `-U` user_name は権限を持つユーザの名前です
- - command は指定するコマンドの名前です

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Windows 用の同等のコマンドは次のとおりです。

```
ipmiutil command -V 4 -J 3 -N IP_address -Uuser_name
```

このコマンドは、アプライアンスのコマンドラインにユーザを接続します。これによって、ユーザは物理的にそのアプライアンスの近くにいるときと同じようにログインできます。場合によっては、パスワードの入力を求められます。

IPMItool を使用した Serial Over LAN の設定

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

手順

IPMItool を使用して、次のコマンドと、プロンプトが表示されたらパスワードを入力します:

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

IPMIutil を使用した Serial Over LAN の設定

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

手順

IPMIutil を使用して、次のコマンドと、プロンプトが表示されたらパスワードを入力します。

```
ipmiutil -J 3 -H IP_address -U username sol -a
```

Lights-Out 管理の概要

Lights-Out管理（LOM）では、システムにログインすることなく、デフォルトの管理インターフェイス（`eth0`）からSOL接続を介して一連の限定操作を実行できます。SOL接続を作成するコマンドに続いて、次のいずれかのLOMコマンドを使用します。コマンドが完了すると、接続は終了します。電源制御コマンドの中には、70xx Familyデバイスに対して有効でないものもあります。

（注） Firepower 71xx、Firepower 82xx、またはFirepower 83xxデバイスのベースボード管理コントローラ（BMC）は、ホストの電源がオンのときにのみ1 Gbpsのリンク速度でアクセスできます。デバイスの電源がオフの場合、BMCは10/100 Mbpsでのみイーサネット リンクを確立できます。したがって、デバイスにリモートから電源供給するためにLOMを使用している場合は、10/100 Mbpsのリンク速度だけを使用してデバイスをネットワークに接続してください。

注意 まれに、コンピュータがシステムの管理インターフェイスとは異なるサブネットにあり、そのシステムにDHCPが構成されている場合は、LOM機能にアクセスしようとすると失敗することがあります。この場合は、システムのLOMを無効にして再び有効にするか、または同じサブネット上のコンピュータをシステムとして使用して、その管理インターフェイスをpingすることができます。その後、LOMを使用できるようになるはずです。

注意 シスコでは、Intelligent Platform Management Interface（IPMI）標準（CVE-2013-4786）に内在する脆弱性を認識しています。システムのLights-Out管理（LOM）を有効にすると、この脆弱性にさらされます。この脆弱性を軽減するために、信頼済みユーザだけがアクセス可能なセキュアな管理ネットワークにシステムを展開し、辞書に載っていない複雑な最大長のパスワードをシステムに対して使用し、それを3か月ごとに変更してください。この脆弱性のリスクを回避するには、LOM を有効にしないでください。

システムへのアクセス試行がすべて失敗した場合は、LOMを使用してリモートでシステムを再起動できます。SOL接続がアクティブなときにシステムが再起動すると、LOMセッションが切断されるか、またはタイムアウトする可能性があります。

注意 システムが別の再起動の試行に応答している間は、システムを再起動**しないでください**。リモートでシステムを再起動すると、通常の方法でシステムがリブートしないため、データが失われる可能性があります。

表 *61*：*Lights-Out* 管理のコマンド

IPMItool	IPMIutil	説明
（適用なし）	`-V 4`	IPMIセッションの管理者権限を有効にします。
`-I lanplus`	`-J 3`	IPMI セッションの暗号化を有効にします。
`-H`	`-N`	リモート アプライアンスの IP アドレスを指定します。
`-U`	`-U`	認可された LOM アカウントのユーザ名を指定します。
`sol activate`	`sol -a`	SOL セッションを開始します。
`sol deactivate`	`sol -d`	SOL セッションを終了します。
`chassis power cycle`	`power -c`	アプライアンスを再起動します（70xx Familyデバイスでは無効）。
`chassis power on`	`power -u`	アプライアンスの電源を投入します。
`chassis power off`	`power -d`	アプライアンスの電源をオフにします（70xx Family デバイスでは無効）。
`sdr`	センサー	アプライアンスの情報（ファン速度や温度など）を表示します。

たとえば、アプライアンスの情報のリストを表示する IPMItool のコマンドは、次のとおりです。

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

IPMIutil ユーティリティの同等のコマンドは次のとおりです。

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

IPMItool による Lights-Out Management の設定

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

手順

プロンプトが表示されたら、IPMItool の次のコマンドとパスワードを入力します。

```
ipmitool -I lanplus -H IP_address -U user_name command
```

IPMIutil による Lights-Out Management の設定

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

手順

プロンプトが表示されたら、IPMIutil の次のコマンドとパスワードを入力します。

```
ipmiutil -J 3 -H IP_address -U username command
```

VMware Tools と仮想システム

VMware Tools は、仮想マシン向けのパフォーマンスを向上させるためのユーティリティ スイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をフルに活用できます。このシステムでは、VMware 上で実行される Firepower システムの仮想アプライアンスで次のプラグインがサポートされます。

- guestInfo
- powerOps
- timeSync
- vmbackup

サポートされるすべてのバージョンの ESXi で VMware Tools を有効にすることもできます。サポートされているバージョンの一覧については、『*Cisco Firepower NGIPSv for VMware* クイック スタート ガイド』を参照してください。VMware Tools のすべての機能については、VMware の Web サイト（http://www.vmware.com/）を参照してください。

VMware 向け Firepower Management Center での VMware ツールの有効化

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

NGIPSv には Web インターフェイスがないため、NGIPSv で VMware ツールを有効にするには、コマンドライン インターフェイスを使用する必要があります。*Cisco Firepower NGIPSv for VMware* クイック スタート ガイドを参照してください。

手順

ステップ 1 [システム（System）] > [設定（Configuration）]を選択します。

ステップ 2 [VMware ツール（VMware Tools）] をクリックします。

ステップ 3 [VMware ツールの有効化（Enable VMware Tools）] をクリックします。

ステップ 4 [保存（Save）] をクリックします。

第 25 章

管理対象デバイス用のプラットフォーム設定ポリシー

以下のトピックでは、プラットフォーム設定ポリシーについて、および管理対象デバイスにそれらを導入する方法について説明します。

プラットフォーム設定の概要

プラットフォーム設定ポリシーは、時刻の設定や外部認証など、展開内の他の管理対象デバイスと同様になる可能性の高い、管理対象デバイスの側面を定義する共有の機能またはパラメータのセットです。

共有ポリシーによって同時に複数の管理対象デバイスを設定することができ、これによって展開に一貫性をもたらし、管理の手間を合理化することができます。プラットフォーム設定ポリシーへの変更は、ポリシーを適用したすべての管理対象デバイスに影響します。デバイスごとに異なる設定を使用する場合でも、共有ポリシーを作成して目的のデバイスに適用する必要があります。

たとえば、組織のセキュリティ ポリシーではユーザのログイン時にアプライアンスに「無断使用禁止」のメッセージを表示する必要があるとします。プラットフォーム設定を使えば、プラットフォーム設定ポリシー内で一度ログイン バナーを設定するだけで完了します。

また、Firepower Management Center で複数のプラットフォーム設定ポリシーを活用することもできます。たとえば、さまざまな状況で別々のメールリレーホストを使用する場合や、さまざまなアクセス リストをテストする場合は、単一のポリシーを編集するのではなく、いくつかのプラットフォーム設定ポリシーを作成し、それらを切り替えることができます。

関連トピック

Firepower プラットフォームの設定, （626 ページ）
システム設定, （551 ページ）

プラットフォーム設定ポリシーの管理

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

[プラットフォームの設定（Platform Settings）] ページ（[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]）を使用して、プラットフォーム設定ポリシーを管理します。このページには、各ポリシーのデバイスのタイプが示されます。[ステータス（Status）] 列で、ポリシーのデバイス ターゲットが示されます。

手順

ステップ 1 [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]を選択します。

ステップ 2 プラットフォーム設定ポリシーを管理します。

- 作成：新しいプラットフォーム設定ポリシーを作成するには、[新規ポリシー（New Policy）] をクリックします。プラットフォーム設定ポリシーの作成, （623 ページ）を参照してください。
- コピー：プラットフォーム設定ポリシーをコピーするには、コピーアイコン（  ）をクリックします。
- 編集：既存のプラットフォーム設定ポリシーの設定を変更するには、編集アイコン（  ）をクリックします。
- 削除：使用されていないポリシーを削除するには、削除アイコン（  ）をクリックして、選択内容を確認します。

  注意 どのターゲット デバイスでも、最後に展開したポリシーは期限切れであっても削除しないでください。ポリシーを完全に削除する前に、それらのターゲットに別のポリシーを展開するようにしてください。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

プラットフォーム設定ポリシーの作成

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

手順

ステップ 1 [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックします。

ステップ 3 ドロップダウン リストから、デバイス タイプを選択します。

- クラシック管理対象デバイス用の共有ポリシーを作成する場合は、[Firepower設定（Firepower Settings）] を選択します。

ステップ 4 新しいポリシーの [名前（Name）]、および必要に応じて [説明（Description）] を入力します。

ステップ 5 必要に応じて、ポリシーを適用する [使用可能なデバイス（Available Devices）] を選択し、[ポリシーに追加（Add to Policy）] をクリック（またはドラッグ アンド ドロップ）して、選択したデバイスを追加します。[検索（Search）] フィールドに検索文字列を入力して、デバイスのリストを絞り込むことができます。

ステップ 6 [保存（Save）] をクリックします。
システムにより、ポリシーが作成され、編集のために開かれます。

ステップ 7 デバイス プラットフォーム タイプに基づいて、プラットフォーム設定を行います。

- Firepower 設定については、Firepower プラットフォーム設定の概要，（625 ページ）を参照してください。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

プラットフォーム設定ポリシーのターゲット デバイスの設定

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

新しいポリシーを作成すると同時にターゲット デバイスを追加したり、後で変更したりできます。

手順

ステップ 1 [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]を選択します。

ステップ 2 編集するプラットフォーム設定ポリシーの横にある編集アイコン（  ）をクリックします。

ステップ 3 [ポリシーの割り当て（Policy Assignment）] をクリックします。

ステップ 4 次のいずれかを実行します。

- デバイス、スタック、高可用性ペア、またはデバイス グループをポリシーに割り当てるには、[使用可能なデバイス（Available Devices）] リストで選択し、[ポリシーに追加（Add to Policy）] をクリックします。ドラッグ アンド ドロップを使用することもできます。
- デバイスの割り当てを削除するには、[選択されたデバイス（Selected Device）] リストのデバイス、スタック、高可用性ペア、またはデバイス グループの横にある削除アイコン（  ）をクリックします。

ステップ 5 [OK] をクリック

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 26 章

従来型デバイス用の Firepower プラットフォーム設定

次のトピックでは、Firepower プラットフォーム設定について、および従来型デバイスでそれを設定する方法について説明します。

Firepower プラットフォーム設定の概要

Firepower クラシック管理対象デバイス向けのプラットフォーム設定は無関係な機能の範囲を指定しますが、その値は複数のデバイス間で共有できます。この場合は、7000 および 8000 シリーズ、ASA FirePOWER モジュールや NGIPSv デバイスです。デバイスごとに異なる設定を使用する場合でも、共有ポリシーを作成して目的のデバイスに適用する必要があります。

関連トピック

管理対象デバイス用のプラットフォーム設定ポリシー，（621 ページ）

システム設定, （551 ページ）

Firepower プラットフォームの設定

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

プラットフォームを設定するには、既存のプラットフォーム設定ポリシーを編集するか、新しいポリシーを作成します。デバイスに現在展開されているプラットフォーム設定ポリシーを編集する場合、変更を保存した後にポリシーを再展開してください。

手順

ステップ 1 [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]を選択します。
既存のシステム ポリシーのリストを含む、[プラットフォーム設定（Platform Settings）] ページが表示されます。

ステップ 2 新しいポリシーを作成するか、既存のポリシーを編集します。

- 新しいポリシーを作成するには、プラットフォーム設定ポリシーの作成, （623 ページ）を参照してください。
- 既存のポリシーを編集するには、そのポリシーの横にある編集アイコン（）をクリックします。

[ポリシーの編集（Edit Policy）]ページが表示されます。ポリシー名とポリシーの説明を変更できます。プラットフォーム設定ポリシーのそれぞれの側面の設定については、次の項のいずれかを参照してください。

- システムのアクセス リストの設定, （590 ページ）
- 外部ストリーミングの監査ログの設定, （592 ページ）
- 外部認証の有効化, （632 ページ）
- 別の言語の指定, （598 ページ）
- カスタム ログイン バナーの追加, （599 ページ）
- セッション タイムアウトの設定, （609 ページ）
- SNMP ポーリングの設定, （600 ページ）
- STIG コンプライアンスの有効化, （603 ページ）

- Firepower Management Center からの時間の提供, （607 ページ）

ステップ 3 （オプション）[ポリシー割り当て（Policy Assignment）] をクリックして、ポリシーを展開する利用可能なデバイスを選択します。[ポリシーに追加（Add to Policy）] をクリックして（またはドラッグ アンド ドロップして）、選択したデバイスを追加します。
[検索（Search）] フィールドに検索文字列を入力して、デバイスのリストを絞り込むことができます。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

アクセス リスト

Firepower Management Center およびクラシック管理対象デバイスでは、アクセス リストを使用して、IP アドレスとポートを基準にシステムへのアクセスを制限できます。デフォルトでは、任意の IP アドレスに対して以下のポートが有効化されています。

- 443（HTTPS）：Web インターフェイス アクセスに使用されます。
- 22（SSH）：コマンド ライン アクセスに使用されます。

さらに、ポート 161 で SNMP 情報をポーリングするためのアクセスも追加できます。

注意 デフォルトでは、アクセスは制限されていません。よりセキュアな環境で運用するために、特定の IP アドレスに対するアクセスを追加してから、デフォルトの any オプションを削除することを検討してください。

システムのアクセス リストの設定

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

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。

- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

このアクセス リストは、外部データベース アクセスを制御しないので注意してください。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。
- 管理対象デバイス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [アクセス リスト（Access List）] をクリックします。

ステップ 3 現在の設定の 1 つを削除するために、削除アイコン（  ）をクリックすることもできます。

注意 アプライアンスのインターフェイスへの接続に現在使用されている IP アドレスへのアクセスを削除し、`IP=any port=443` のエントリが存在しない場合、ポリシーを展開した時点でシステムへのアクセスは失われます。

ステップ 4 1 つ以上の IP アドレスへのアクセスを追加するには、[ルールの追加（Add Rules）] をクリックします。

ステップ 5 [IP アドレス（IP Address）] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、`any` を入力します。

ステップ 6 [SSH]、[HTTPS]、[SNMP]、またはこれらのオプションの組み合わせを選択して、これらの IP アドレスで有効にするポートを指定します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

監査ログ

Firepower Management Center および従来型管理対象デバイスは、ユーザ アクティビティに関する読み取り専用の監査情報をログに記録します。Management Center および 7000 および 8000 シリーズ の Web インターフェイスでは、監査ログ イベントは標準イベント ビューに表示されます。標準イベント ビューでは、監査ビューの任意の項目に基づいて監査ログ メッセージの表示、並べ替

え、フィルタ処理ができます。監査情報を簡単に削除したり、それに関するレポートを作成したりすることができ、ユーザが行った変更に関する詳細なレポートを表示することもできます。

監査ログ メッセージを syslog に送信するよう、Firepower Management Center および従来型管理対象デバイスを設定することもできます。設定するには、syslog サーバ、およびメッセージに関連付ける重大度、ファシリティ、オプション タグを指定します。タグは、syslog の監査ログ メッセージと一緒に表示されます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。syslog メッセージにはファシリティおよび重大度は含まれません。これらの値は syslog メッセージを受信するシステムにメッセージの分類方法を示す値です。

また、監査ログ メッセージを HTTP サーバにストリーミングするよう、Firepower Management Center および従来型管理対象デバイスで設定することもできます。

監査ログ ストリーミング設定は、アプライアンスのタイプによって異なる設定の一部となっています。

- Firepower Management Center では、監査ログのストリーミングはシステム設定の一部です。
- クラシック管理対象デバイスでは、監査ログ ストリーミングは Firepower Management Center プラットフォーム設定ポリシーの一部です。

いずれの場合も、システム設定の変更を保存するか、共有プラットフォーム設定ポリシーを展開するまでは設定は有効になりません。

外部ストリーミングの監査ログの設定

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

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

次に、出力構造の例を示します。

```
Date Time Host [Tag] Sender: [User_Name]@[User_IP], [Subsystem], [Action]
```

現地の日付、時刻、およびホスト名の後に、角括弧で囲まれたオプション タグが続き、送信側デバイス名の後に監査ログ メッセージが続きます。

次に例を示します。

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3500: admin@10.1.1.2, Operations > Monitoring, Page
View
```

はじめる前に

- 外部ホストが機能していることと、監査ログを送信するシステムからアクセスできることを確認します。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。
- 管理対象デバイス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択して、Firepower ポリシーを作成または編集します。

ステップ 2 [監査ログ（Audit Log）] をクリックします。

ステップ 3 [監査ログを Syslog に送信（Send Audit Log to Syslog）] ドロップダウン メニューから、[有効化（Enabled）] を選択します。

ステップ 4 [ホスト（Host）] フィールドにあるホストの IP アドレスまたは完全修飾名を使用して、監査情報の宛先ホストを指定します。デフォルト ポート（514）が使用されます。

注意 監査ログを受け入れるように設定しているコンピュータが、リモート メッセージを受け入れるようにセットアップされていない場合、ホストは監査ログを受け入れません。

ステップ 5 [syslog ファシリティ（syslog Facility）] を選択します。

ステップ 6 重大度を選択します。

ステップ 7 必要に応じて、[タグ（オプション）（Tag (optional)）] フィールドで参照タグを挿入します。

ステップ 8 定期的な監査ログの更新を外部 HTTP サーバに送信するには、[監査ログを HTTP サーバに送信（Send Audit Log to HTTP Server）] ドロップダウン リストから [有効化（Enabled）] を選択します。

ステップ 9 [監査情報を送信する URL（URL to Post Audit）] フィールドに、監査情報の送信先 URL を指定します。次にリストされている HTTP POST 変数を要求するリスナー プログラムに対応する URL を入力する必要があります。

- `subsystem`
- `actor`
- `event_type`
- `message`
- `action_source_ip`
- `action_destination_ip`

- 結果
- 時刻
- tag（上記のように定義されている場合）

注意 暗号化されたポストを許可するには、HTTPS URL を使用する必要があります。外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があるので注意してください。

ステップ 10 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

外部認証の設定

外部認証サーバを参照する認証オブジェクトを作成する場合、外部認証を有効にすることにより、ローカル データベースを使用せずに、管理対象デバイスにログインしているユーザをそのサーバに認証させることができます。

外部認証を有効にすると、システムでは LDAP または RADIUS サーバのユーザのユーザ クレデンシャルが確認されます。さらに、ユーザがローカルの内部認証を有効にしており、ユーザ クレデンシャルが内部データベースにない場合、システムは一致するクレデンシャルのセットがないか外部サーバを検査します。ユーザが複数のシステムで同じユーザ名を持っている場合、すべてのサーバですべてのパスワードが動作します。ただし、使用可能な外部認証サーバで認証が失敗した場合、システムはローカル データベースの検査に戻らないので注意してください。

外部認証を有効にすると、アカウントが外部で認証されている任意のユーザのデフォルトのユーザ ロールを設定できます。これらのロールを組み合わせることができる場合は、複数のロールを選択できます。たとえば、自社の [ネットワーク セキュリティ（Network Security）] グループのユーザのみを取得する外部認証を有効にした場合、デフォルトのユーザ ロールを設定して [セキュリティ アナリスト（Security Analyst）] ロールを組み込み、ユーザが自分で追加のユーザ設定を行わなくても収集されたイベント データにアクセスできるようにすることが可能です。ただし、外部認証がセキュリティ グループに加えて他のユーザのレコードを取得する場合、デフォルトのロールを未選択のままにしておきたい場合もあります。

アクセス ロールが選択されていない場合、ユーザはログインできますが、どの機能にもアクセスできません。ユーザがログインを試行すると、アカウントがユーザ管理ページ（[システム（System）] > [ユーザ（Users）]）に表示されます。ここで、追加の権限を付与するアカウント設定を編集できます。

ヒント　1つのユーザロールを使用するようにシステムを設定してそのポリシーを適用し、後で設定を変更して別のデフォルトのユーザ ロールを使用する場合、アカウントを変更するか、削除して再作成するまで、変更前に作成されたユーザ アカウントはすべて、最初のユーザ ロールを保持します。

シェルアクセスまたはCAC認証および承認のためにLDAPサーバに対して認証できる一連のユーザを指定する場合は、それぞれに個別の認証オブジェクトを作成し、オブジェクトを個別に有効にする必要があります。

内部認証によってユーザがログインしようとすると、システムは最初にそのユーザがローカル ユーザ データベースに存在するかどうか検査します。ユーザが存在する場合、システムは次にユーザ名とパスワードをローカル データベースに対して検査します。一致が検出されると、ユーザは正常にログインします。ただし、ログインが失敗し、外部認証が有効になっている場合、システムはそれぞれの外部認証サーバに対して、ユーザを設定に表示される認証順序で検査します。ユーザ名およびパスワードが外部サーバからの結果と一致した場合、システムはユーザを、その認証オブジェクトに対してデフォルトの権限を持つ外部ユーザに変更します。

外部ユーザがログインしようとすると、システムは外部認証サーバに対してユーザ名およびパスワードを検査します。一致が検出されると、ユーザは正常にログインします。ログインが失敗した場合、ユーザのログイン試行は拒否されます。外部ユーザは、ローカル データベース内のユーザ リストに対して認証できません。ユーザが新しい外部ユーザの場合、外部認証オブジェクトのデフォルト権限を持つ外部ユーザ アカウントがローカル データベースに作成されます。

関連トピック

ユーザ アカウント，（77 ページ）

外部認証の有効化

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

はじめる前に

- 外部認証（External Authentication），（87 ページ）の説明に従って外部認証オブジェクトを設定します。

手順

ステップ 1 [デバイス（Devices）]>[プラットフォーム設定（Platform Settings）] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [外部認証（External Authentication）] をクリックします。

ステップ 3 [ステータス（Status）] ドロップダウン リストから [有効（Enabled）] を選択します。

ステップ 4 [デフォルト ユーザ ロール（Default User Role）] ドロップダウン リストから、ユーザ ロールを選択して、外部認証済みユーザに付与するデフォルト権限を定義します。

ステップ 5 外部サーバを使用して CLI またはシェル アクセス アカウントを認証する場合、[シェル認証（Shell Authentication）] ドロップダウン リストから [有効（Enabled）] を選択します。

ステップ 6 CAC 認証および認可を有効にする場合は、[CAC 認証（CAC Authentication）] ドロップダウン リストから使用可能な CAC 認証オブジェクトを選択します。CAC 認証および認可の設定の詳細については、CAC 認証, （90 ページ）を参照してください。

ステップ 7 事前設定された認証オブジェクトの使用を有効にするには、オブジェクトの横にあるチェックボックスをオンにします。外部認証を有効にするには、少なくとも 1 つの認証オブジェクトを指定する必要があります。
シェル認証を有効にした場合、CLI またはシェル アクセスを許可するよう設定された認証オブジェクトを選択する**必要があります**。

同じシステム設定で CLI またはシェル アクセスと、CAC 認証を制御するためには異なる認証オブジェクトを使用します。CAC 認証, （90 ページ）および LDAP シェル アクセスのフィールド, （108 ページ）を参照してください。

ステップ 8 必要に応じて、上矢印および下矢印を使用して、認証要求が行われたときに認証サーバがアクセスされる順序を変更できます。
CLI またはシェル アクセスのユーザは、認証オブジェクトがプロファイルの順序で最も高いサーバに対して**のみ**認証できることに注意してください。

ステップ 9 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

言語の選択

[言語（Language）] ページを使用して、Web インターフェイス用に異なる言語を指定できます。

別の言語の指定

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

この設定は、Firepower Management Center または 7000 および 8000 シリーズ 管理対象デバイスに適用されます。

- Firepower Management Center では、この設定はシステム設定の一部になります。
- 7000 および 8000 シリーズ 管理対象デバイスでは、この設定をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

注意 ここで指定した言語は、アプライアンスにログインしたすべてのユーザの Web インターフェイスに使用されます。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。
- 管理対象デバイス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [言語（Language）] をクリックします。

ステップ 3 使用する言語を選択します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ログイン バナー

[ログイン バナー（Login Banner）] ページを使用して、セキュリティ アプライアンスまたは共有ポリシーのセッション バナー、ログイン バナー、カスタム メッセージ バナーを指定できます。

バナーのテキストにはスペースを使用できますが、タブは使用できません。バナーには複数行のテキストを指定できます。テキストに空の行が含まれている場合、バナーでは、その行が改行（CR）として表示されます。使用できるのは、改行（Enter キーを押す）を含む ASCII 文字だけです。改行は 2 文字としてカウントされます。

Telnet または SSH を介してセキュリティ アプライアンスにアクセスしたときに、バナー メッセージを処理するのに十分なシステム メモリがなかった場合や、バナー メッセージの表示を試行して TCP 書き込みエラーが発生した場合には、セッションが閉じます。

カスタム ログイン バナーの追加

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

SSH または Web インターフェイスからログインするユーザに向けて表示するカスタム ログイン バナーを作成できます。

この設定は、Firepower Management Center または従来型の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

手順

ステップ 1 Firepower Management Center または Classic 管理対象デバイスのいずれを設定しているかに応じて、以下を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。

- 管理対象デバイスの場合：[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）] を選択するか、ファイアウォール ポリシーを作成、または編集します。

ステップ 2 [ログイン バナー（Login Banner）] を選択します。

ステップ 3 [カスタム ログイン バナー（Custom Login Banner）] フィールドに、使用するログイン バナー テキストを入力します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

セッション タイムアウト

Firepower システムの Web インターフェイスまたは補助コマンドライン インターフェイスの無人ログイン セッションは、セキュリティ上のリスクを生じさせる場合があります。ユーザのログイン セッションが非アクティブなったためにタイムアウトするまでのアイドル時間を分単位で設定できます。シェル（コマンドライン）セッションでも同様のタイムアウトを設定できます。

長期にわたり Web インターフェイスをパッシブかつセキュアにモニタする予定のユーザが、導入内に存在する可能性があります。ユーザ設定オプションで Web インターフェイスのセッション タイムアウトからユーザを除外することができます。メニュー オプションへの完全なアクセス権がある管理者ロールのユーザは、侵害が生じる場合、余分のリスクを生じさせますが、セッション タイムアウトから除外することはできません。

セッション タイムアウトの設定

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

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

システムへのシェル アクセスを制限する必要がある場合、追加オプションによって補助コマンドライン インターフェイスの `expert` コマンドを永続的に無効にすることができます。アプライアンスでエキスパート モードを無効にすると、構成シェル アクセスを持つユーザでも、シェルのエキスパート モードに入ることができなくなります。ユーザが補助コマンドライン インターフェイスのエキスパート モードに入ると、ユーザはシェルに応じた任意の Linux コマンドを実行できます。エキスパート モードに入っていない場合は、コマンドライン ユーザはコマンドライン インターフェイスが提供するコマンドだけを実行できます。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。
- 管理対象デバイス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [シェル タイムアウト（Shell Timeout）] をクリックします。

ステップ 3 次の選択肢があります。

- Web インターフェイスのセッション タイムアウトを設定するには、[ブラウザ セッション タイムアウト（分）（Browser Session Timeout (Minutes)）] フィールドに数値（分数）を入力します。デフォルト値は `60` で、最大値は `1440`（24 時間）です。このセッション タイムアウトからユーザを除外する方法については、ユーザ アカウント ログイン オプション，（81 ページ）を参照してください。
- コマンドライン インターフェイスのセッション タイムアウトを設定するには、[シェル タイムアウト（分）（Shell Timeout (Minutes)）] フィールドに数値（分数）を入力します。デフォルト値は `0` で、最大値は `1440`（24 時間）です。
- 補助コマンドライン インターフェイスで `expert` コマンドを永続的に無効にするには、[expert コマンドを永続的に無効化（Permanently Disable Expert Access）] チェックボックスを選択します。

注意 エキスパート モードが無効になった状態でポリシーをアプライアンスに展開した場合、Web インターフェイスまたは補助コマンドライン インターフェイスを介してエキスパート モードにアクセスする機能を復元することはできません。エキスパート モード機能を復元するには、サポートに問い合わせる必要があります。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

SNMP ポーリング

Firepower Management Center およびクラシック管理対象デバイスには、Simple Network Management Protocol（SNMP）ポーリングを有効にすることができます。SNMP 機能は、SNMP プロトコルのバージョン 1、2、3 をサポートします。

この機能を使用して、次の要素にアクセスできます。

- 標準 Management Information Base（MIB）。これには、連絡先、管理、場所、サービス情報、IP アドレッシングやルーティングの情報、トランスミッションプロトコルの使用状況の統計などのシステムの詳細が含まれます。
- 7000 および 8000 シリーズ 管理対象デバイスの追加の MIB。これには、物理インターフェイス、論理インターフェイス、仮想インターフェイス、ARP、NDP、仮想ブリッジ、仮想ルータを通して渡されるトラフィックの統計が含まれます。

（注） SNMP プロトコルの SNMP バージョンを選択する際は、SNMPv2 では読み取り専用コミュニティのみをサポートし、SNMPv3 では読み取り専用ユーザのみをサポートすることに注意してください。SNMPv3 は AES128 による暗号化もサポートします。

SNMP 機能を有効にすると、システムで SNMP トラップを送信できなくなり、MIB の情報はネットワーク管理システムによるポーリングでのみ使用可能になることに注意してください。

SNMP ポーリングの設定

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

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

（注） システムをポーリングするには、使用する任意のコンピュータで SNMP アクセスを追加する必要があります。SNMP MIB には展開の攻撃に使用される可能性がある情報も含まれているので注意してください。SNMP アクセスのアクセス リストを MIB のポーリングに使用される特定のホストに制限することをお勧めします。SNMPv3 を使用し、ネットワーク管理アクセスには強力なパスワードを使用することもお勧めします。

SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

はじめる前に

- システムのアクセス リストの設定, （590 ページ）の説明に従って、使用するコンピュータごとに SNMP アクセスを追加し、システムをポーリングします。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。
- 管理対象デバイス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [SNMP] をクリックします。

ステップ 3 [SNMP バージョン（SNMP Version）] ドロップダウン リストから、使用する SNMP バージョンを選択します。

ステップ 4 次の選択肢があります。

- [バージョン 1（Version 1）] または [バージョン 2（Version 2）] を選択した場合は、[コミュニティ ストリング（Community String）] フィールドに SNMP コミュニティ名を入力します。手順 13 に進みます。

  （注） SNMPv2 は、読み取り専用コミュニティのみをサポートしています。

- [バージョン 3（Version 3）] を選択した場合、[ユーザを追加（Add User）] をクリックするとユーザ定義ページが表示されます。

（注） SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

ステップ 5 ユーザ名を入力します。

ステップ 6 [認証プロトコル（Authentication Protocol）] ドロップダウン リストから、認証に使用するプロトコルを選択します。

ステップ 7 [認証パスワード（Authentication Password）] フィールドに SNMP サーバの認証に必要なパスワードを入力します。

ステップ 8 [パスワードの確認（Verify Password）] フィールドに、認証パスワードを再度入力します。

ステップ 9 使用するプライバシー プロトコルを [プライバシー プロトコル（Privacy Protocol）] リストから選択するか、プライバシー プロトコルを使用しない場合は [なし（None）] を選択します。

ステップ 10 [プライバシー パスワード（Privacy Password）] フィールドに SNMP サーバで必要な SNMP プライバシー キーを入力します。

ステップ 11 [パスワードの確認（Verify Password）] フィールドに、プライバシー パスワードを再度入力します。

ステップ 12 [追加（Add）] をクリックします。

ステップ 13 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

STIG コンプライアンス

米国連邦政府内の組織は、Security Technical Implementation Guides（STIG）に示されている一連のセキュリティ チェックリストに準拠しなければならない場合があります。Firepower システムは、米国国防総省で規定している STIG 要件のコンプライアンスをサポートしています。

展開内の任意のアプライアンスで STIG コンプライアンスを有効にする場合は、それをすべてのアプライアンスで有効にする必要があります。非準拠の管理対象デバイスを STIG 準拠の Firepower Management Center に登録したり、STIG 準拠デバイスを非準拠の Firepower Management Center に登録したりすることはできません。

STIG コンプライアンスを有効にした場合、適用可能なすべての STIG に厳格なコンプライアンスが保証されるわけではありません。。

STIG コンプライアンスを有効にすると、ローカル シェル アクセス アカウントのパスワードの複雑さや維持に関するルールが変わります。さらに、STIG コンプライアンス モードでは、SSH のリモート ストレージを使用できません。

注意 サポートからの支援なしでこの設定を無効にすることはできません。また、この設定はシステムのパフォーマンスに大きく影響する可能性があります。シスコでは、米国国防総省（DoD）のセキュリティ要件に準拠する以外の目的で、STIG コンプライアンスを有効にすることを推奨しません。

STIG コンプライアンスの有効化

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

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

注意 展開内の任意のアプライアンスで STIG コンプライアンスを有効にする場合は、それをすべてのアプライアンスで有効にする必要があります。サポートからの支援なしでこの設定を無効にすることはできません。また、この設定はシステムのパフォーマンスに大きく影響する可能性があります。シスコでは、米国国防総省（DoD）のセキュリティ要件に準拠する以外の目的で、STIG コンプライアンスを有効にすることを推奨しません。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。
- 管理対象デバイス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [STIG Compliance] をクリックします。

（注） STIG コンプライアンスを有効にすると、アプライアンスがリブートします。Firepower Management Center は、システム設定を保存するとリブートし、管理対象デバイスは、設定の変更を展開するとリブートします。

ステップ 3 STIG コンプライアンスをアプライアンスで永続的に有効にする場合は、[STIG コンプライアンスを有効化（Enable STIG Compliance）] を選択します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。
- アプライアンスがバージョン 5.2.0 より前のバージョンから更新された場合は、STIG コンプライアンスを有効にすると、アプライアンス証明書が再生成されます。展開全体で STIG コンプライアンスを有効にした後、管理対象デバイスを Firepower Management Center に再登録します。

時刻および時刻同期

[時刻（Time）] ページを使用して、Firepower Management Center、あるいは 7000 または 8000 シリーズデバイスのローカル Web インターフェイスから現在の時刻と時刻源を表示することができます。

時刻の設定は、アプライアンスの大半のページで、[タイム ゾーン（Time Zone）] ページで設定したタイム ゾーン（デフォルトでは [アメリカ/ニューヨーク（America/New York）]）を使用してローカル時間で表示されますが、アプライアンス自体には UTC 時間を使用して保存されます。また、現在の時刻は [時刻の同期（Time Synchronization）] ページの上部に UTC で表示されます（ローカル時間は [手動（Manual）] の時計設定オプションで表示されます（有効になっている場合））。

時刻の同期は、[時刻の同期（Time Synchronization）] ページを使用して管理できます。時刻を同期する場合、以下の方法を選択できます。

- 手動で
- 1 つ以上の NTP サーバを使用（推奨）

ハードウェアの Firepower Management Center を NTP サーバとして使用できますが、仮想 Firepower Management Center は NTP サーバとして使用しないでください。

リモートの NTP サーバを指定する場合、アプライアンスにそのサーバに対するネットワーク アクセス権限が必要です。信頼できない NTP サーバを指定しないでください。NTP サーバへの接続では、構成されたプロキシ設定は使用されません。

（注） 時刻の同期後に、Firepower Management Center と管理対象デバイスの時刻が一致するようにしてください。時刻が一致していない場合、管理対象デバイスが Firepower Management Center と通信する際に意図しない結果が生じるおそれがあります。

時刻の同期

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

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

手順

ステップ 1 Firepower Management Center または Classic 管理対象デバイスのいずれを設定しているかに応じて、以下を実行します。

- Management Center：[システム（System）] > [設定（Configuration）] を選択します。
- 管理対象デバイス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [時間同期（Time Synchronization）] をクリックします。

ステップ 3 管理対象デバイスで時刻を同期する方法を指定する次のオプションがあります。

- NTP を介して Management Center から時刻を受信するには、[NTP 経由で管理センターから（Via NTP from Management Center）] を選択します。詳細については、Firepower Management Center からの時間の提供, （607 ページ）を参照してください。

- [NTP 経由（Via NTP from）] を選択して、さまざまなサーバから NTP 経由で時刻を受信します。テキスト ボックスで、NTP サーバの IP アドレスのカンマ区切りリストを入力するか、DNS が有効になっている場合は、完全修飾ホスト名およびドメイン名を入力します。

ステップ 4 [保存（Save）] をクリックします。

（注） 設定された NTP サーバと管理対象デバイスを同期するには、数分かかる場合があります。さらに、管理対象デバイスを NTP サーバとして設定されている Management Center と同期する場合、Management Center 自体が NTP サーバを使用するように設定されていると、時刻を同期するのにいくらか時間がかかることがあります。これは、管理対象デバイスに時刻を提供するために、Management Center は設定された NTP サーバとまず同期する必要があるためです。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。
- Management Center と管理対象デバイスの時刻が一致していることを確認します。

第 IX 部

ネットワーク アドレス変換（NAT）

第 27 章

NAT ポリシー管理

以下のトピックでは、Firepower システム用の NAT ポリシーを管理する方法について説明します。

NAT ポリシーの管理

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

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカル ポリシーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

手順

ステップ 1 [デバイス（Devices）] > [NAT]を選択します。

ステップ 2 NAT ポリシーを管理します。

- コピー：コピーするポリシーの横にあるコピー アイコン（  ）をクリックします。NAT ポリシーのコピー, （652 ページ）を参照してください。
- 作成：[新規ポリシー（New Policy）] をクリックします。NAT ポリシーの作成, （648 ページ）を参照してください。
- 削除：削除するポリシーの横にある削除アイコン（  ）をクリックして、[OK] をクリックします。続行するかどうかを尋ねるプロンプトで、ポリシー内に別のユーザの未保存の変更が存在するかどうかも通知されます。

  注意 管理対象デバイスに NAT ポリシーを展開した後は、デバイスからそのポリシーを削除できません。その代わりに、ルールを持たない NAT ポリシーを展開して、すでに管理対象デバイスに存在する NAT ルールを削除する必要があります。また、どのターゲット デバイスでも、最後に展開したポリシーは期限切れであっても削除できません。ポリシーを完全に削除する前に、それらのターゲットに異なるポリシーを展開する必要があります。

- 展開：[展開（Deploy）] をクリックします（設定変更の導入, （320 ページ） を参照）。
- 編集：編集アイコン（  ）をクリックします。NAT ポリシーの設定, （649 ページ）を参照してください。
- [レポート（Report）]：レポート アイコン（  ）をクリックします（現在のポリシー レポートの生成, （333 ページ） を参照）。

NAT ポリシーの作成

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

新しいNATポリシーを作成する場合、少なくとも一意の名前を付ける必要があります。ポリシーの作成時にポリシー ターゲットを特定する必要はありませんが、ポリシーを展開する前に、この手順を実行する必要があります。ルールを持たないNATポリシーをデバイスに適用すると、そのデバイスからすべての NAT ルールが削除されます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカル ポリシーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

手順

ステップ 1 [デバイス（Devices）] > [NAT]を選択します。

ステップ 2 [新しいポリシー（New Policy）] ドロップダウン リストで、[Firepower NAT] を選択します。

ステップ 3 [名前（Name）] に一意の名前を入力します。
マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 ポリシーを展開するデバイスを選択します。

- [使用可能なデバイス（Available Devices）] リストでデバイスを選択し、[ポリシーに追加（Add to Policy）] をクリックします。
- [使用可能なデバイス（Available Devices）] リストから [選択されたデバイス（Selected Devices）] リストに、デバイスをクリックしてドラッグします。
- デバイスの横にある削除アイコン（）をクリックして、[選択されたデバイス（Selected Devices）] リストからデバイスを削除します。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

NAT ポリシーの設定

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

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカル ポリシーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

インターフェイスのタイプを、そのインターフェイスがあるデバイスを対象とするNATポリシーでの使用が無効なタイプに変更した場合、ポリシーはそのインターフェイスに削除済みのラベルを付けます。NAT ポリシーの [保存（Save）] をクリックすると、インターフェイスはポリシーから自動的に削除されます。

手順

ステップ 1 [デバイス（Devices）] > [NAT]を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 NAT ポリシーを設定します。

- ポリシー名や説明を変更するには、[名前（Name）] または [説明（Description）] フィールドをクリックし、必要に応じて文字を削除し、新しい名前または説明を入力します。マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。
- ポリシーの対象を管理するには、NAT ポリシーの対象の設定, （651 ページ）を参照してください。
- ポリシーの変更を保存するには、[保存（Save）] をクリックします。
- ポリシーにルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- 既存のルールを編集するには、ルールの横にある編集アイコン（）をクリックします。
- ルールを削除するには、ルールの横にある削除アイコン（）をクリックし、[OK] をクリックします。
- 既存のルールを有効または無効にするには、ルールを右クリックして [状態（State）] を選択し、[無効化（Disable）] または [有効化（Enable）] を選択します。
- 特定のルール属性の設定ページを表示するには、ルールの行にある条件の列で名前、値、またはアイコンをクリックします。たとえば、[送信元ネットワーク（Source Networks）] 列の

名前または値をクリックすると、選択したルールの [送信元ネットワーク（Source Networks）] ページが表示されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

NAT ポリシーの対象の設定

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

ポリシーを適用する管理対象デバイスは、ポリシーを作成または編集する際に特定できます。使用可能なデバイス、7000 または 8000 シリーズ スタック、および高可用性ペアのリストを検索して、選択したデバイスのリストに追加できます。

異なるバージョンの Firepower システムを実行中のスタック構成デバイスを対象にすることはできません（たとえば、デバイスのいずれかでアップグレードが失敗した場合）。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカル ポリシーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

手順

ステップ 1 [デバイス（Devices）] > [NAT]を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ポリシー割り当て（Policy Assignments）] をクリックします。

ステップ 4 次のいずれかを実行します。

- デバイス、スタック、高可用性ペア、またはデバイス グループをポリシーに割り当てるには、[使用可能なデバイス（Available Devices）] リストで選択し、[ポリシーに追加（Add to Policy）] をクリックします。ドラッグ アンド ドロップを使用することもできます。
- デバイスの割り当てを削除するには、[選択されたデバイス（Selected Device）] リストのデバイス、スタック、高可用性ペア、またはデバイス グループの横にある削除アイコン（）をクリックします。

ステップ 5 [OK] をクリック

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

NAT ポリシーのコピー

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

NAT ポリシーのコピーを作成できます。コピーには、ポリシーのすべてのルールと設定が含まれます。

マルチドメイン導入では、現在のドメインおよび先祖ドメインからポリシーをコピーできます。

手順

ステップ 1 [デバイス（Devices）] > [NAT] を選択します。

ステップ 2 コピーする NAT ポリシーの横にあるコピー アイコン（）をクリックします。

ステップ 3 [名前（Name）] に、ポリシーの一意の名前を入力します。
マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

ステップ 4 [OK] をクリックします。

第 28 章

7000 および 8000 シリーズ デバイス用の NAT

以下のトピックでは、7000および8000シリーズデバイス用にNATを設定する方法を示します。

NAT ポリシーの設定

特定のネットワーク ニーズを管理するためにさまざまな方法で NAT ポリシーを設定できます。次の操作を実行できます。

- 外部ネットワークに内部サーバを公開します。
  この設定では、外部IPアドレスから内部IPアドレスへのスタティック変換を定義するため、システムはネットワーク外部から内部サーバにアクセスできます。サーバに送信されるトラフィックは、外部 IP アドレスまたは IP アドレスとポートを対象とし、内部 IP アドレスまたは IP アドレスとポートに変換されます。サーバからのリターン トラフィックは、外部アドレスに再度変換されます。
- 内部ホスト/サーバが外部アプリケーションに接続できるようにします。
  この設定では、内部アドレスから外部アドレスへのスタティック変換を定義します。この定義により、内部ホストまたはサーバは、内部ホストまたはサーバが特定のIPアドレスおよびポートを持っていると予期する外部アプリケーションへの接続を開始できます。したがって、システムは内部ホストまたはサーバのアドレスを動的に割り当てることはできません。
- 外部ネットワークに対してプライベート ネットワーク アドレスを隠します。

  以下のいずれかの設定を使用して、内部ネットワーク アドレスをわかりにくくすることができます。

  - 内部ネットワークの必要に十分対応できるだけの数の外部 IP アドレスがある場合は、IPアドレスのブロックを使用できます。この設定では、すべての発信トラフィックの送

信元 IP アドレスを、外部に面する IP アドレスのうち未使用の IP アドレスに自動的に変換するダイナミック変換を作成します。

- 内部ネットワークの必要に対応できるだけの数の外部 IP アドレスがない場合は、限定した数の IP アドレスのブロックとポート変換を使用できます。この設定では、発信トラフィックの送信元 IP アドレスとポートを、外部に面する IP アドレスのうち未使用の IP アドレスとポートに自動的に変換するダイナミック変換を作成します。

注意 7000 または 8000 シリーズ デバイスの高可用性ペアでは、NAT 変換により影響を受けるすべてのネットワークがプライベートの場合、ペアを構成するデバイス上でのスタティック NAT ルールに対して個別のピア インターフェイスのみを選択します。パブリック ネットワークとプライベート ネットワーク間のトラフィックに影響するスタティック NAT ルールには、この設定を使用しないでください。

NAT ポリシーの設定ガイドライン

NAT ポリシーを設定するには、ポリシーに一意の名前を付け、ポリシーを展開するデバイスつまりターゲットを特定する必要があります。また、NAT ルールを追加、編集、削除、有効化、および無効化することができます。NAT ポリシーを作成または変更した後、ターゲット デバイスのすべてまたは一部にポリシーを展開できます。

スタンドアロン デバイスと同様に、NAT ポリシーをペアリングされたスタックを含む 7000 または 8000 シリーズ デバイス高可用性ペアに展開できます。ただし、個別のペアリングされたデバイスまたは高可用性ペア全体でインターフェイスのスタティック NAT ルールを定義し、送信元ゾーン内でインターフェイスを使用できます。ダイナミック ルールの場合、送信元ゾーンまたは宛先ゾーンで高可用性ペア全体のインターフェイスのみを使用できます。

注意 7000 または 8000 シリーズ デバイス高可用性ペアで、NAT 変換により影響を受けるすべてのネットワークがプライベートの場合、ペアリングされたデバイスのスタティック NAT ルールに対して、個別のピア インターフェイスのみを選択します。パブリック ネットワークとプライベート ネットワーク間のトラフィックに影響するスタティック NAT ルールに対してこの設定を使用**しない**でください。

HA リンク インターフェイスが確立されていないデバイス高可用性ペアでダイナミック NAT を設定した場合、両方のペアリングされたデバイスは別々にダイナミック NAT エントリを割り当て、システムはデバイス間でエントリを同期できません。

スタンドアロン デバイスと同様に、NAT ポリシーをデバイス スタックに展開できます。NAT ポリシーに含まれ、スタックのメンバーであるセカンダリ デバイスのインターフェイスに関連付けられているルールを持ったデバイスからデバイス スタックを確立した場合、セカンダリ デバイスのインターフェイスは NAT ポリシーに残ります。インターフェイスを持つポリシーを保存および展開できますが、ルールは変換を実現しません。

先祖ドメインの マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。 管理者は、NAT ポリシーのターゲットを子孫ドメインのデバイスに設定できます。こうすることで、子孫ドメインではカスタマイズされたローカル ポリシーを使用または置き換えることができます。

NAT ポリシー内のルール編成

NAT ポリシーの編集ページにはスタティックな NAT ルールとダイナミックな NAT ルールが別々に表示されます。このシステムでは、スタティック ルールは名前のアルファベット順に並べ替えられ、表示順序を変更できません。同一の照合値を持つスタティック ルールは作成できません。システムの照合では、ダイナミック変換を検査する前に、スタティック変換を検査します。

ダイナミック ルールは番号順に処理されます。各ダイナミック ルールの番号位置は、ページ左側のルールの横に表示されます。ダイナミック ルールは移動または挿入したり、ルールの順序を変更したりすることができます。たとえば、ダイナミック ルール 10 をダイナミック ルール 3 の下に移動した場合、ルール 10 がルール 4 になり、後に続くすべての番号が順次繰り上がります。

このシステムでは、ポリシーの編集ページ上のルールの番号順にパケットとダイナミック ルールを比較するので、ダイナミック ルールの位置は重要です。パケットがダイナミック ルールのすべての条件を満たすと、システムはパケットにそのルール条件を適用し、そのパケットに対する後続のルールはすべて無視します。

ダイナミック ルールを追加または編集する際、ダイナミック ルールの番号の位置を指定できます。新しいダイナミック ルールを追加する前にダイナミック ルールを強調表示して、強調表示したルールの下に新しいルールを挿入することもできます。

ルールの行内の空白部分をクリックすることにより、1 つ以上のダイナミック ルールを選択できます。選択したダイナミック ルールを新しい場所にドラッグ アンド ドロップできます。これにより、移動したルールと後続のすべてのルールの位置が変更されます。

選択したルールを既存のルールの上または下にカット アンド ペーストできます。スタティック ルールはスタティック変換リストにのみ、ダイナミック ルールはダイナミック変換リストにのみ貼り付けることができます。また、選択したルールを削除したり、既存のルール リスト内の任意の場所に新しいルールを挿入したりすることもできます。

先行ルールが優先して適用されるために決して一致することがないルールを示す、説明的な警告を表示することもできます。

展開にアクセス コントロール ポリシーが存在する場合、このシステムではアクセス制御を通過するまでトラフィックを変換することありません。

NAT ルールの編成

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

手順

ステップ 1 [デバイス（Devices）] > [NAT]を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 NAT ルールを編成します。

- ルールを選択するには、ルールの行の空白部分をクリックします。
- ルールの選択をクリアするには、ページの右下にあるリロードアイコン（）をクリックします。個別のルールをクリアするには、Ctrl キーを押しながら各ルールの行内の空白部分をクリックします。
- 選択したルールを切り取りまたはコピーするには、選択したルールの行の空白部分を右クリックして、[切り取り（Cut）] または [コピー（Copy）] を選択します。
- 切り取ったルールまたはコピーしたルールをルールリストに貼り付けるには、選択したルールを貼り付けるルールの行の空白部分を右クリックして、[上に貼り付け（Paste above）] または [下に貼り付け（Paste below）] を選択します。
- 選択したルールを移動するには、選択したルールを新しい位置の下にドラッグアンドドロップします。この移動先の位置は、ドラッグ時にポインタの上に表示される青い横線で示されます。
- ルールを削除するには、ルールの横にある削除アイコン（）をクリックして、[OK] をクリックします。
- 警告を表示するには、[警告の表示（Show Warnings）] をクリックします。

NAT ルールの警告とエラー

NAT ルールの条件が後続のルールによるトラフィックの照合をプリエンプション処理する場合があります。どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。

あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールは回避されます。いずれかの条件が異なっていた場合、後続のルールはプリエンプション処理されません。

NATポリシーの展開失敗の原因となるルールを作成した場合、ルールの横にエラーアイコン（  ）が表示されます。スタティック ルールに矛盾がある場合、または現時点で無効となるポリシーで使用されるネットワーク オブジェクトを編集した場合、エラーが発生します。たとえば、IPv6 アドレスのみを使用するようにネットワーク オブジェクトを変更した結果、少なくとも 1 つのネットワークが必要な状況で、そのオブジェクトを使用するルールに有効なネットワークがなくなると、エラーが発生します。エラーアイコンは自動的に表示されます。[警告を表示（Show Warnings）] をクリックする必要はありません。

NAT ルール警告の表示と非表示

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

手順

ステップ 1 [デバイス（Devices）] > [NAT]を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 警告を表示するには、[警告を表示（Show Warnings）] をクリックします。

ページが更新され、プリエンプション処理された各ルールの横に警告アイコン（  ）が表示されます。

ステップ 4 ルールの警告を表示するには、ルールの横にある警告アイコン（  ）の上にポインタを合わせます。

ルールをプリエンプション処理するルールを示すメッセージが表示されます。

ステップ 5 警告をクリアするには、[警告を非表示（Hide Warnings）] をクリックします。

ページが更新され、警告が消えます。

NAT ポリシー規則のオプション

NAT ルールは次の働きを持つ設定および条件のセットです。

- ネットワーク トラフィックを限定する
- 条件に一致するトラフィックの変換方法を指定する

既存の NAT ポリシーから NAT ルールを作成および編集します。各ルールは 1 つのポリシーにのみ属します。

ルールの追加と編集は同様の Web インターフェイスで行います。ページの上部でルールの名前、状態、タイプ、および位置（ダイナミックの場合）を指定します。ページの左側のタブを使用して、条件を構築します。条件タイプごとに独自のタブがあります。

次のリストは、NAT ルールの設定可能なコンポーネントを示しています。

[名前（Name）]

各ルールに一意の名前を付けます。スタティック NAT ルールでは、最大 22 文字を使用します。ダイナミック NAT ルールでは、最大 30 文字を使用します。印刷可能文字を使用できます。スペースや特殊文字を含めることができますが、コロン（:）は使用できません。

ルール状態（Rule State）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、変換用のネットワークトラフィックの評価に使用されません。NAT ポリシーのルール リストを表示すると、無効なルールはグレー表示されますが、変更は可能です。

タイプ（Type）

ルールのタイプによって、ルールの条件に一致するトラフィックの処理方法が決まります。NAT ルールを作成および編集する際、設定可能なコンポーネントはルール タイプによって異なります。

位置（Position）（ダイナミック ルールのみ）

NAT ポリシーのダイナミック ルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、NAT ルールを上から順にトラフィックと照合します。

ルールをポリシーに追加する際、参照ポイントとしてルール番号を使用し、特定のルールの上または下に配置することによって位置を指定します。既存のルールを編集するときには、同様の方法でルールを移動できます。

条件（Conditions）

ルール条件は変換する特定のトラフィックを識別します。条件はセキュリティ ゾーン、ネットワーク、および転送プロトコルのポートなど、複数の属性を任意に組み合わせてトラフィックと照合できます。

関連トピック

NAT ルールの作成および編集，（659 ページ）

NAT ルールの作成および編集

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

マルチドメイン導入では、現在のドメインで作成されたポリシーとルールが表示されます。これは編集できます。先祖ドメインで作成されたポリシーとルールも表示されますが、これは編集できません。下位のドメインで作成されたルールを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [デバイス（Devices）] > [NAT]を選択します。

ステップ 2 ルールを追加する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 新しいルールを追加するか、既存のルールを編集します。

- 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- 既存のルールを編集するには、そのルールの横にある編集アイコン（）をクリックします。

ステップ 4 [名前（Name）] に一意のルール名を入力します。

ステップ 5 次のルール コンポーネントを設定します。

- ルールを有効にするかどうかを指定します。
- [タイプ（Type）] で、ルール タイプを指定します。
- ルールの位置（ダイナミック ルールのみ）を指定します。
- ルールの条件を設定します。

（注） スタティック ルールは元の宛先ネットワークを含む必要があります。ダイナミック ルールは変換された送信元ネットワークを含む必要があります。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

NAT ルールのタイプ

すべての NAT ルールには次の働きを持つタイプが関連付けられています。

- ネットワーク トラフィックを限定する
- 条件に一致するトラフィックの変換方法を指定する

次に、NAT ルール タイプの概要を示します。

静的

スタティック ルールは宛先ネットワークと任意選択のポートおよびプロトコルで 1 対 1 の変換を提供します。スタティック変換を設定する場合、送信元ゾーン、宛先ネットワーク、および宛先ポートを設定できます。宛先ゾーンまたは送信元ネットワークを設定できません。

元の宛先ネットワークを指定する**必要**があります。宛先ネットワークでは、単一の IP アドレスを含むネットワーク オブジェクトおよびグループを選択するか、または単一の IP アドレスを表すリテラル IP アドレスを入力することのみが可能です。元の宛先ネットワークと変換後の宛先ネットワークはそれぞれ 1 つのみ指定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

元の宛先ポートと変換後の宛先ポートをそれぞれ 1 つ指定できます。元の宛先ポートを指定するには、その前に、元の宛先ネットワークを指定する必要があります。さらに、元の宛先ポートを指定しない場合は、変換後の宛先ポートを指定できません。また、変換後の値は、元の値のプロトコルと一致する必要があります。

注意 高可用性ペアとして構成されている 7000 または 8000 シリーズ デバイスのスタティック NAT ルールについては、NAT 変換で影響を受けるすべてのネットワークがプライベートの場合、個別のピア インターフェイスのみを選択します。パブリック ネットワークとプライベート ネットワーク間のトラフィックに影響するスタティック NAT ルールに対してこの設定を使用**しない**でください。

ダイナミック IP 専用

ダイナミック IP 専用ルールは多対多の送信元ネットワークを変換しますが、ポートおよびプロトコルを維持します。ダイナミック IP 専用変換を設定する場合、ゾーン、送信元ネットワーク、元の宛先ネットワーク、および元の宛先ポートを設定できます。変換後の宛先ネットワークまたは変換後の宛先ポートは設定できません。

変換後の送信元ネットワークを少なくとも 1 つ指定する**必要**があります。変換後の送信元ネットワーク値の数が元の送信元ネットワークの数よりも小さい場合、元のアドレスがすべて照合される前に変換後のアドレスが不足する可能性があるという警告がルールに表示されます。

同じパケットに一致する条件を持つルールが複数個ある場合、優先度の低いルールはデッド ルールとなり、トリガーされなくなります。デッド ルールにも警告が表示されます。ツールチップを表示して、デッド ルールに代わるルールを判別できます。

（注） デッド ルールを持つポリシーを保存し、展開することは可能ですが、ルールは変換を実現できません。

場合によっては、範囲の広いルールよりも優先される、範囲が限定されたルールを作成することをお勧めします。次に例を示します。

```
Rule 1: Match on address A and port A/Translate to address B
Rule 2: Match on address A/Translate to Address C
```

この例で、ルール 1 はルール 2 にも一致するいくつかのパケットに一致します。したがって、ルール 2 は完全に無効ではありません。

元の宛先ポートだけを指定した場合、変換後の宛先ポートを指定することはできません。

ダイナミック IP およびポート

ダイナミック IP およびポート ルールは多対 1 または多対多の送信元ネットワークとポートおよびプロトコルを変換します。ダイナミック IP およびポート変換を設定する場合、ゾーン、送信元ネットワーク、元の宛先ネットワーク、および元の宛先ポートを設定できます。変換後の宛先ネットワークまたは変換後の宛先ポートは設定できません。

変換後の送信元ネットワークを少なくとも 1 つ指定する**必要**があります。同じパケットに一致する条件を持つルールが複数個ある場合、優先度の低いルールはデッド ルールとなり、トリガーされなくなります。デッドルールにも警告が表示されます。ツールチップを表示して、デッドルールに代わるルールを判別できます。

（注） デッド ルールを持つポリシーを保存し、展開することは可能ですが、ルールは変換を実現できません。

元の宛先ポートだけを指定した場合、変換後の宛先ポートを指定することはできません。

（注） ダイナミック IP およびポート ルールを作成し、システムがポートを使用しないトラフィックを渡す場合、そのトラフィックに対して変換は発生しません。たとえば、送信元ネットワークに一致する IP アドレスからの ping（ICMP）は、ICMP がポートを使用しないため、マッピングされません。

NAT ルールの条件タイプ

次の表に、指定された NAT ルール タイプに基づいて設定可能な NAT ルールの条件タイプをまとめています。

表 *62*：*NAT* ルール タイプごとに使用可能な *NAT* ルールの条件タイプ

条件	静的	ダイナミック（IP 専用または IP およびポート）
送信元ゾーン（Source Zones）	オプション	オプション
宛先ゾーン（Destination Zones）	不可	オプション
元の送信元ネットワーク	不可	オプション
変換後の送信元ネットワーク	不可	**必須（Required）**
元の宛先ネットワーク	**必須（Required）**	オプション
変換後の宛先ネットワーク	任意。単一アドレスのみ	不可
元の宛先ポート	任意。単一ポートでのみ、元の宛先ネットワークを定義する場合のみ可能	オプション
変換後の宛先ポート	任意。単一ポートでのみ、元の宛先ポートを定義する場合のみ可能	不可

NAT ルールの条件と条件の仕組み

ルールに一致するトラフィックのタイプを識別するために NAT ルールに条件を追加できます。それぞれの条件タイプごとに、使用可能条件リストから、ルールに追加する条件を選択します。条件フィルタを適用できる場合は、条件フィルタを使って使用可能な条件を限定できます。使用可能な条件リスト、および選択した条件リストは、1 つの条件だけを含む場合も、数ページに及ぶ場合もあります。使用可能な条件は検索することができ、名前や値を入力するとそれに一致する条件だけが表示され、入力していくにつれてそのリストが更新されます。

条件のタイプに応じて、使用可能条件リストには、Ciscoから直接提供された条件と、他のFirepowerシステム機能を使って設定された条件が一緒に含まれることがあります。その中には、オブジェクトマネージャ（[オブジェクト（Objects）]>[オブジェクト管理（Object Management）]）を使って作成されたオブジェクト、個別の条件ページから直接作成されたオブジェクト、およびリテラル条件が含まれます。

NAT ルールの条件

次の表で説明されている条件のいずれかを満たすトラフィックを照合するためのNATルールを設定できます。

表 *63*：*NAT* ルールの条件タイプ

条件	説明
ゾーン	NAT ポリシーを展開できる 1 つ以上のルーテッド インターフェイスの設定。ゾーンは、送信元インターフェイスと宛先インターフェイスでトラフィックを分類するメカニズムであり、ルールに送信元のゾーン条件と宛先のゾーン条件を追加することができます。
ネットワーク	明示的に指定した、またはネットワーク オブジェクトとグループを使用した、個々のIPアドレス、CIDRブロック、およびプレフィックス長の組み合わせ。NAT ルールに送信元ネットワーク条件と宛先ネットワーク条件を追加できます。
宛先ポート	トランスポート プロトコルに基づいて作成される、個別のポート オブジェクトとグループ ポート オブジェクトを含むトランスポート プロトコル ポート。

NAT ルールへの条件の追加

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

NAT ルールへの条件の追加は基本的にどの条件のタイプでも同じです。左側の使用可能な条件のリストから選択して、右側で選択した条件の 1 つまたは 2 つのリストに、選択した条件を追加します。

すべての条件タイプで、使用可能な個々の条件を 1 つまたは複数クリックすると、それが強調表示され、選択状態になります。2 つのタイプのリスト間にあるボタンをクリックして選択した使

用可能な条件を選択した条件のリストに追加するか、または選択した使用可能な条件を選択した条件のリストにドラッグ アンド ドロップします。

選択済み条件リストには、タイプごとに最大50個までの条件を追加できます。たとえばアプライアンスの上限に達するまで、最大 50 個の送信元ゾーン条件、最大 50 個の宛先ゾーン条件、最大 50 個の送信元ネットワーク条件などを追加できます。

手順

ステップ 1 [デバイス（Devices）] > [NAT]を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入入力します。

ステップ 5 ルールの [タイプ（Type）] を指定します。

ステップ 6 ルールに追加する条件タイプに対応したタブをクリックします。

ステップ 7 次のいずれかの操作を行います。

- 表示されている条件を、すでに選択済みの条件のリストに追加するには、表示されている条件をクリックします。
- 表示されている条件をすべて選択するには、条件のいずれかの行を右クリックし、[すべて選択（Select All）] をクリックします。
- 表示されている条件の一部またはフィルタされた条件を選択するには、[検索（Search）] フィールド内をクリックし、検索のための文字列を入力します。入力していくと、リストが更新されて一致する項目が表示されます。
  オブジェクト名およびオブジェクトに設定されている値を検索対象にできます。たとえば `Texas Office` という名前の個別ネットワーク オブジェクトがあり、`192.168.3.0/24` という値が設定されていて、`US Offices` というグループ オブジェクトに含まれる場合、`Tex` などの部分的または完全な検索文字列を入力するか、または `3` などの値を入力することにより、両方のオブジェクトを表示できます。
- 表示されている条件を検索中、またはフィルタ中に検索文字列をクリアするには、検索フィールドの上のリロード アイコン（）または検索フィールド内のクリア アイコン（  ）をクリックします。
- 表示されている条件リストからゾーンの条件を選択し、選択済みの送信元または宛先の条件リストに追加するには、[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。
- 表示されている条件リストからネットワークとポートの条件を選択し、選択済みの元または変換済みの条件リストに追加するには、[元に追加（Add to Original）] または [変換済みに追加（Add to Translated）] をクリックします。

- 表示されている条件を選択済み条件のリストにドラッグ アンド ドロップするには、選択済み条件をクリックし、選択済み条件のリストにドラッグ アンド ドロップします。
- リテラルフィールドを使用し、選択済み条件のリストにリテラル条件を追加するには、クリックしてリテラルフィールドからのプロンプトを削除し、リテラル条件を入力し、[追加（Add）]をクリックします。ネットワーク条件は、リテラル条件を追加するためのフィールドを提供します。
- ドロップダウン リストを使用し、選択済み条件のリストにリテラル条件を追加するには、ドロップダウン リストから条件を選択し、[追加（Add）]をクリックします。ポート条件には、リテラル条件を追加するためのドロップダウン リストがあります。
- 個々のオブジェクトまたは条件フィルタを追加して、条件リストからそれを選択できるよう表示させるには、追加アイコン（  ）をクリックします。
- 選択済み条件のリストから条件を1つだけ削除するには、条件の横にある削除アイコン（  ）をクリックします。
- 選択済み条件のリストから条件を削除するには、選択済み条件のリストの行を右クリックして強調表示し、[削除（Delete）] をクリックします。

ステップ 8 設定を保存するには、[追加（Add）] をクリックします。

NAT ルールのリテラル条件

次の条件タイプについて、元のおよび変換後の条件のリストにリテラル値を追加できます。

- ネットワーク
- ポート

ネットワーク条件の場合、元のまたは変換後の条件リストの下にある設定フィールドにリテラル値を入力します。

ポート条件では、ドロップダウン リストからプロトコルを選択します。プロトコルが `All`、または `TCP` または `UDP` である場合、設定フィールドにポート番号を入力します。

該当するそれぞれの条件ページには、リテラル値を追加するために必要なコントロールがあります。設定フィールドに入力した値が無効である場合や、まだ有効と認識されていない場合は、赤いテキストとして表示されます。入力時に有効と認識された値は青色に変わります。有効な値が認識されると、グレー表示の [追加（Add）] ボタンがアクティブになります。追加したリテラル値は、選択済み条件リストにただちに表示されます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

NAT ルールの条件のオブジェクト

オブジェクトマネージャ（[オブジェクト（Objects）]>[オブジェクト管理（Object Management）]）で作成されたオブジェクトは、使用可能なNATルール条件の関連リストからすぐに選択可能になります。

NAT ポリシーから直接オブジェクトを作成することもできます。該当する条件ページ上のコントロールでは、オブジェクト マネージャでの設定コントロールと同じ機能を利用できます。

直接作成された個別のオブジェクトは使用可能なオブジェクトのリストにすぐに表示されます。それらを現在のルールと他の既存および将来のルールに追加できます。該当する条件ページとポリシー編集ページで、ポインタを 1 つの個別オブジェクトの上に置くとそのオブジェクトの内容が表示され、グループ オブジェクトの上に置くと、グループ内の個々のオブジェクトの数が表示されます。

NAT ルール内のゾーン条件

システムのセキュリティ ゾーンは、管理対象デバイス上のインターフェイスから構成されています。NATルールに追加するゾーンは、それらのゾーン内にルーテッドインターフェイスまたはハイブリッドインターフェイスを持つ、ネットワーク上のデバイスにそのルールをターゲットします。NAT ルールの条件として、ルーテッド インターフェイスまたはハイブリッド インターフェイスを持つセキュリティ ゾーンのみを追加できます。

現在仮想ルータに割り当てられているゾーンまたはスタンドアロン インターフェイスのどちらかを NAT ルールに追加できます。デバイス設定が展開されていないデバイスがある場合、[ゾーン（Zones）]ページの使用可能なゾーン リストの上に警告アイコン（⚠）が表示され、展開済みのゾーンとインターフェイスだけが表示されることが示されます。ゾーンの横にある矢印アイコン（▷）をクリックして、ゾーンを縮小または展開し、そのインターフェイスを非表示または表示することができます。

インターフェイスがハイ アベイラビリティペアの 7000 または 8000 シリーズ デバイス上にある場合、使用可能なゾーンのリストに、そのインターフェイスからの追加のブランチが表示されると共に、そのハイ アベイラビリティ ペアの他のインターフェイスがそのハイ アベイラビリティ ペアのアクティブデバイスのプライマリインターフェイスの子として表示されます。矢印アイコン（▷）をクリックして、ペアになったデバイス インターフェイスを縮小または展開し、そのインターフェイスを非表示または表示することもできます。

（注） 無効にされたインターフェイスを持つポリシーを保存して展開できますが、ルールではそれらのインターフェイスが有効になるまで変換を提供できません。

右側の 2 つのリストは、NAT ルールによって照合目的に使用される送信元ゾーンと宛先ゾーンです。すでにルールに値が設定されている場合、ルールを編集する際、これらのリストには既存の値が表示されます。送信元ゾーンのリストが空の場合、ルールは任意のゾーンまたはインターフェイスからのトラフィックを照合します。宛先ゾーンのリストが空の場合、ルールは任意のゾーンまたはインターフェイス宛てのトラフィックを照合します。

対象のデバイスでトリガーされることがないゾーンの組み合わせを持つルールに対しては警告が表示されます。

（注） これらのゾーンの組み合わせを持つポリシーを保存して展開できますが、ルールでは変換を提供しません。

ゾーン内の項目を選択するか、またはスタンドアロン インターフェイスを選択することによって、個別のインターフェイスを追加できます。ゾーン内のインターフェイスを追加できるのは、それらのインターフェイスが割り当てられるゾーンがまだ送信元ゾーンまたは宛先ゾーンのリストに追加されていない場合のみです。これらの個別に選択されたインターフェイスは、それらのインターフェイスを削除して別のゾーンに追加した場合でも、各ゾーンに対する変更の影響を受けません。インターフェイスがハイ アベイラビリティ ペアのプライマリ メンバーで、ダイナミック ルールを設定する場合、そのプライマリ インターフェイスだけを送信元ゾーンまたは宛先ゾーンのリストに追加できます。スタティック ルールの場合、個別のハイ アベイラビリティ ペアのメンバー インターフェイスを送信元ゾーンのリストに追加できます。ハイ アベイラビリティ ペアのプライマリ インターフェイスは、その子がまったく追加されていない場合にだけ、リストに追加できます。また、個別のハイアベイラビリティペアのインターフェイスは、プライマリが追加されていない場合にだけ追加できます。

ゾーンを追加すると、ルールではそのゾーンに関連付けられているすべてのインターフェイスを使用します。ゾーンに対してインターフェイスを追加または削除すると、インターフェイスが存在するデバイスにデバイス設定が再度展開されるまで、ルールでは更新されたバージョンのゾーンを使用しません。

（注） スタティック NAT ルールでは、送信元ゾーンのみを追加できます。ダイナミック NAT ルールでは、送信元ゾーンと宛先ゾーンの両方を追加できます。

NAT ルールへのゾーン条件の追加

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

手順

ステップ 1 [デバイス（Devices）] > [NAT]を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入力します。

ステップ 5 ルールの [タイプ（Type）] を指定します。

ステップ 6 [ゾーン（Zones）] タブをクリックします。

ステップ 7 [使用可能なゾーン（Available Zones）] リスト内のゾーンまたはインターフェイスをクリックします。

ステップ 8 次の選択肢があります。

- 送信元ゾーンによりトラフィックを照合するには、[送信元に追加（Add to Source）] をクリックします。
- 宛先ゾーンによりトラフィックを照合するには、[宛先に追加（Add to Destination）] をクリックします。

（注） スタティック NAT ルールには送信元ゾーンのみを追加できます。さらに、無効になっているインターフェイスを NAT ルールに追加できますが、ルールは変換を実現しません。

ステップ 9 [追加（Add）] をクリックして新しいルールを保存します。

ステップ 10 [保存（Save）] をクリックして、変更したポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ダイナミック NAT ルールの送信元ネットワーク条件

パケットの送信元IPアドレスの照合値と変換値を設定します。元の送信元ネットワークが設定されていない場合、すべての送信元 IP アドレスがダイナミック NAT ルールに一致します。スタティックNATルールの送信元ネットワークは設定できないことに注意してください。パケットがNATルールに一致すると、システムは変換後の送信元ネットワークの値を使用して、送信元IPアドレスの新しい値を割り当てます。ダイナミック ルール用に少なくとも 1 つの値を持つ変換後の送信元ネットワークを設定する必要があります。

注意 ネットワーク オブジェクトまたはオブジェクト グループがNATルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

ダイナミック NAT ルールに、次の種類の送信元ネットワーク条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのネットワーク オブジェクト
- 送信元ネットワーク条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のネットワーク オブジェクト
- リテラル、単一 IP アドレス、範囲、またはアドレス ブロック

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ネットワーク条件のダイナミック NAT ルールへの追加

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

展開されているポリシーで使用中のダイナミック ルールのネットワーク条件を更新すると、既存の変換済みアドレス プールを使用しているネットワーク セッションがドロップされます。

手順

ステップ 1 [デバイス（Devices）] > [NAT]を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入入力します。

ステップ 5 ルールのダイナミック [タイプ（Type）] を指定します。

- ダイナミック IP 専用
- ダイナミック IP およびポート

ステップ 6 [送信元ネットワーク（Source Network）] タブをクリックします。

ステップ 7 必要に応じて、リストの上にある追加アイコン（）をクリックし、[使用可能なネットワーク（Available Networks）] リストへ個々のネットワーク オブジェクトを追加します。
各ネットワーク オブジェクトに複数の IP アドレス、CIDR ブロック、およびプレフィクス長を追加できます。

ステップ 8 [使用可能なネットワーク（Available Networks）] リスト内の条件をクリックします。

ステップ 9 次の選択肢があります。

- 元の送信元ネットワークによりトラフィックを照合するには、[元に追加（Add to Original）] をクリックします。
- 変換後の送信元ネットワークと照合するトラフィックの変換値を指定するには、[変換後に追加（Add to Translated）] をクリックします。

ステップ 10 リテラル IP アドレス、範囲、アドレスブロックを追加するには、

a) [元の送信元ネットワーク（Original Source Network）] または [変換後の送信元ネットワーク（Translated Source Network）] リストの下にある [IP アドレス入力（Enter an IP address）] プロンプトをクリックします。

b) IP アドレス、範囲、アドレスブロックを入力します。
範囲は、下位の IP アドレス - 上位の IP アドレスの形式で追加します。たとえば、`179.13.1.1-179.13.1.10` です。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

c）入力した値の横にある [追加（Add）] をクリックします。

ステップ 11 [追加（Add）] をクリックしてルールを保存します。

ステップ 12 [保存（Save）] をクリックして、変更したポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

NAT ルールの宛先ネットワーク条件

パケットの宛先 IP アドレスの照合値と変換値を設定します。ダイナミック NAT ルールでは変換済み宛先ネットワークは設定できないことに注意してください。

スタティック NAT ルールは 1 対 1 変換であるため、[利用可能なネットワーク（Available Networks）] リストには単一の IP アドレスのみを含むネットワーク オブジェクトおよびグループのみが含まれます。スタティック変換では、[元の宛先ネットワーク（Original Destination Network）] リストと [変換済み宛先ネットワーク（Translated Destination Network）] リストにそれぞれ追加できるオブジェクトまたはリテラル値は 1 つのみです。

注意 ネットワーク オブジェクトまたはオブジェクト グループが NAT ルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

NAT ルールに、次の種類の宛先ネットワーク条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのネットワーク オブジェクト
- [宛先ネットワーク（Destination Network）] 条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のネットワーク オブジェクト
- リテラル、単一 IP アドレス、範囲、またはアドレス ブロック

  スタティック NAT ルールでは、リストにまだ値がない場合に限り、CIDR とサブネット マスク `/32` のみを追加できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

NAT ルールへの宛先ネットワーク条件の追加

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

展開されているポリシーで使用中のダイナミック ルールのネットワーク条件を更新すると、既存の変換済みアドレス プールを使用しているネットワーク セッションがドロップされます。

手順

ステップ 1 [デバイス（Devices）] > [NAT]を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入力します。

ステップ 5 ルールの [タイプ（Type）] を指定します。

ステップ 6 [宛先ネットワーク（Destination Network）] タブをクリックします。

ステップ 7 必要に応じて、リストの上にある追加アイコン（）をクリックし、[使用可能なネットワーク（Available Networks）] リストへ個々のネットワーク オブジェクトを追加します。
ダイナミック ルールの場合、各ネットワーク オブジェクトに複数の IP アドレス、CIDR ブロック、およびプレフィクス長を追加できます。スタティック ルールの場合、単一の IP アドレスのみを追加できます。

ステップ 8 [使用可能なネットワーク（Available Networks）] リスト内の条件またはオブジェクトをクリックします。

ステップ 9 次の選択肢があります。

- 元の宛先ネットワークによりトラフィックを照合するには、[元に追加（Add to Original）] をクリックします。
- 変換後の宛先ネットワークと照合するトラフィックの変換値を指定するには、[変換後に追加（Add to Translated）] をクリックします。

ステップ 10 オプションで、[元の宛先ネットワーク（Original Destination Network）] リストまたは [変換後の宛先ネットワーク（Translated Destination Network）] リストの下の [IP アドレス入力（Enter an IP

address）] プロンプトをクリックし、次に、IP アドレスまたはアドレス ブロックを入力して、[追加（Add）] をクリックします。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 [保存（Save）] をクリックし、ポリシーの変更内容を保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

NAT ルールでのポート条件

ルールにポート条件を追加することで、元の宛先ポートと変換後の宛先ポートおよび変換用の転送プロトコルに基づいてネットワーク トラフィックを照合できます。元のポートが設定されていない場合、すべての宛先ポートがルールと照合されます。パケットを NAT ルールと照合し変換後の宛先ポートが設定されていた場合、システムはその値にポートを変換します。ダイナミック ルールでは元の宛先ポートのみを指定できることに注意してください。スタティック ルールの場合、変換後の宛先ポートを定義できますが、元の宛先ポート オブジェクトまたはリテラル値と同じプロトコルを持つオブジェクトでのみ可能です。

システムは宛先ポートを、スタティック ルールの元の宛先ポート リスト内のポート オブジェクトまたはリテラル ポートの値、またはダイナミック ルールの複数の値と照合します。

スタティック NAT ルールは 1 対 1 変換であるため、[利用可能なポート（Available Ports）] リストには単一のポートのみを含むポート オブジェクトおよびグループのみが含まれます。スタティック変換では、単一のオブジェクトまたはリテラル値のみを [元のポート（Original Port）] リストと [変換済みポート（Translated Port）] リストの両方に追加できます。

ダイナミック ルールの場合は、ポートの範囲を追加できます。たとえば、元の宛先ポートを指定する場合、リテラル値として `1000-1100` を追加できます。

注意 ポート オブジェクトまたはオブジェクト グループが NAT ルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

NAT ルールには、次の種類のポート条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのポート オブジェクト
- 宛先ポート条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のポート オブジェクト
- TCP、UDP、またはすべて（TCP および UDP）の転送プロトコルとポートから構成されるリテラル ポート値

NAT ルールへのポートの条件の追加

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

手順

ステップ 1 [デバイス（Devices）] > [NAT]を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入力します。

ステップ 5 ルールの [タイプ（Type）] を指定します。

ステップ 6 [宛先ポート（Destination Port）] タブをクリックします。

ステップ 7 必要に応じて、[使用可能なポート（Available Ports）] リストの上にある追加アイコン（）をクリックし、リストに個別のポートオブジェクトを追加します。

追加する各ポート オブジェクトの 1 つのポートまたはポート範囲を指定できます。その後、ルールの条件として追加するオブジェクトを選択できます。スタティック ルールの場合、単一のポートを持つポート オブジェクトのみを使用できます。

ステップ 8 [使用可能なポート（Available Ports）] リスト内の条件をクリックします。

ステップ 9 次の選択肢があります。

- [元に追加（Add to Original）] をクリックします。
- [変換後に追加（Add to Translated）] をクリックします。
- 使用可能なポートをリストにドラッグ アンド ドロップします。

ステップ 10 リテラルポートを追加するには、次の手順を実行します。

a) [元のポート（Original Port）] または [変換後のポート（Translated Port）] リストの下にある [プロトコル（Protocol）] ドロップダウンリストからエントリを選択します。

b) ポートを入力します。

c) [追加（Add）] をクリックします。

ダイナミック ルールの場合、単一のポートまたは範囲を指定できます。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 [保存（Save）] をクリックし、ポリシーの変更内容を保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 X 部

7000 および 8000 シリーズの高度な導入オプション

第 29 章

仮想スイッチのセットアップ

以下のトピックでは、Firepower システムで仮想スイッチをセットアップする方法について説明します。

仮想スイッチ

レイヤ 2 展開の 7000 または 8000 シリーズ デバイスは、2 つ以上のネットワーク間でパケット スイッチングを提供するように設定できます。レイヤ 2 展開では、仮想スイッチをスタンドアロン ブロードキャスト ドメインとして機能させ、ネットワークを論理セグメントに分割するように設定できます。仮想スイッチでは、ホストからの Media Access Control（MAC）アドレスを使用して、パケットの送信先を判断します。

仮想スイッチを設定すると、スイッチはまず、スイッチ上の使用可能なすべてのポートからパケットをブロードキャストします。時間の経過とともに、スイッチはタグ付きのリターン トラフィックを使用して、各ポートに接続されたネットワーク上に存在する各ホストを学習していきます。

仮想スイッチには、トラフィックを処理するためのスイッチドインターフェイスが 2 つ以上含まれている必要があります。仮想スイッチごとに、トラフィックはスイッチドインターフェイスとして設定されたポートのセットに限定されてきます。たとえば、4 つのスイッチドインターフェイスのある仮想スイッチを設定した場合、ブロードキャスト用の 1 つのポートを介して送入されたパケットは、そのスイッチ上の残る 3 つのポートからのみ送出可能です。

物理スイッチドインターフェイスを設定する際は、仮想スイッチにそれを割り当てる必要があります。また、必要に応じて、物理ポート上に追加の論理スイッチドインターフェイスを定義することもできます。複数の物理インターフェイスを Link Aggregation Group（LAG）と呼ばれる単一の論理スイッチドインターフェイスにグループ化できます。この単一の集約論理リンクによって、帯域幅と冗長性の向上と、2つのエンドポイント間でのロードバランシングが実現されます。

注意 レイヤ2展開に何らかの理由で障害が発生した場合、デバイスはトラフィックを転送しなくなります。

スイッチドインターフェイスの設定

物理設定または論理設定を備えるよう、スイッチ型インターフェイスをセットアップできます。タグなしVLANトラフィックを処理するよう物理スイッチ型インターフェイスを設定できます。また、VLANタグが指定されたトラフィックを処理するよう論理スイッチ型インターフェイスを作成することもできます。

レイヤ2展開では、外部の物理インターフェイス上でトラフィックを受信した場合、それを待機しているスイッチ型インターフェイスがなければ、システムはそのトラフィックをドロップします。システムがVLANタグなしのパケットを受信した場合、該当するポートに物理スイッチドインターフェイスが設定されていなければ、パケットはドロップされます。システムがVLANタグ付きのパケットを受信した場合、論理スイッチドインターフェイスが設定されていなければ、同じくパケットはドロップされます。

スイッチドインターフェイスでVLANタグ付きで受信されたトラフィックをシステムが処理するときには、ルールの評価や転送の決定を行う前に、入力における最も外側のVLANタグを取り除きます。VLANタグ付き論理スイッチ型インターフェイスを介してデバイスから出るパケットは、出力において関連するVLANタグ付きでカプセル化されます。

親の物理インターフェイスをインラインまたはパッシブに変更すると、システムは関連するすべての論理インターフェイスを削除することに注意してください。

スイッチ型インターフェイスの設定メモ

管理対象デバイス上の1つ以上の物理ポートはスイッチ型インターフェイスとして設定できます。トラフィックを処理できるようにするには、その前に、物理スイッチ型インターフェイスを仮想スイッチに割り当てる必要があります。リンク モード設定およびMDI/MDIX設定は、銅線インターフェイスにのみ設定できます。

（注） 8000シリーズアプライアンスのインターフェイスは、半二重オプションをサポートしません。

物理スイッチ型インターフェイスごとに、複数の論理スイッチ型インターフェイスを追加できます。物理インターフェイスで受信したVLANタグ付きのトラフィックは、各論理インターフェイスにその特定のタグが関連付けられていなければ処理されません。トラフィックを処理するには、論理スイッチ型インターフェイスを仮想スイッチに割り当てる必要があります。

スイッチ型インターフェイスを設定する場合、設定可能なMTUの範囲は、Firepowerシステムのデバイスのモデルとインターフェイスのタイプによって異なる可能性があります。

MTU値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

既存の論理スイッチ型インターフェイスを編集するには、インターフェイスの横にある編集アイコン（[ ]）をクリックします。

論理スイッチ型インターフェイスを削除すると、それが存在する物理インターフェイスから、および関連付けられている仮想スイッチとセキュリティ ゾーンからそれが削除されます。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

物理スイッチド インターフェイスの設定

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

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 スイッチドインターフェイスを設定するデバイスの横にある編集アイコン（ ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 スイッチドインターフェイスとして設定するインターフェイスの横にある編集アイコン（ ）をクリックします。

ステップ 4 [スイッチド（Switched）] タブをクリックします。

ステップ 5 セキュリティゾーンをスイッチドインターフェイスに関連付けるには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して、新しいセキュリティ ゾーンを追加します。セキュリティ ゾーン オブジェクトの作成, （392 ページ）を参照してください。

ステップ 6 仮想スイッチをスイッチド インターフェイスに関連付けるには、次のいずれかを実行します。

- [仮想スイッチ（Virtual Switch）] ドロップダウン リストから既存の仮想スイッチを選択します。
- [新規（New）] を選択して、新しい仮想スイッチを追加します。仮想スイッチの追加, （686 ページ）を参照してください。

ステップ 7 [有効化（Enabled）]チェックボックスをオンにして、スイッチドインターフェイスがトラフィックを処理することを許可します。

（注） このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8 [モード（Mode）] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [自動ネゴシエーション（Auto Negotiation）] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。
モード設定は銅線インターフェイスにのみ使用できます。

8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

ステップ 9 [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または自動 MDIX のいずれかを指定するオプションを選択します。
デフォルトでは、[MDI/MDIX] は [自動 MDIX（Auto-MDIX）] に設定され、MDI と MDIX の間の切り替えを自動的に処理してリンクを確立します。

ステップ 10 [MTU] フィールドに、最大伝送ユニット（MTU）を入力して、パケットの最大許容サイズを入力します。
MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

ステップ 11 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲，（495 ページ）
Snort® の再起動シナリオ，（324 ページ）

論理スイッチドインターフェイスの追加

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

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 スイッチドインターフェイスを追加するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インターフェイスの追加（Add Interface）] をクリックします。

ステップ 4 [スイッチド（Switched）] をクリックします。

ステップ 5 [インターフェイス（Interface）] ドロップダウン リストから、VLAN タグ付きトラフィックを受信する物理インターフェイスを選択します。

ステップ 6 [VLAN タグ（VLAN Tag）] フィールドで、このインターフェイス上のインバウンド/アウトバウンド トラフィックに割り当てるタグ値を入力します。
このタグの値には、1 ～ 4094 の任意の整数を指定できます。

ステップ 7 セキュリティゾーンをスイッチドインターフェイスに関連付けるには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して、新しいセキュリティ ゾーンを追加します。セキュリティ ゾーン オブジェクトの作成，（392 ページ）を参照してください。

ステップ 8 仮想スイッチをスイッチド インターフェイスに関連付けるには、次のいずれかを実行します。

- [仮想スイッチ（Virtual Switch）] ドロップダウン リストから既存の仮想スイッチを選択します。
- [新規（New）] を選択して、新しい仮想スイッチを追加します。仮想スイッチの追加, （686 ページ）を参照してください。

ステップ 9 スイッチドインターフェイスにトラフィックを処理させるには、[有効（Enabled）]チェックボックスをオンにします。
このチェックボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。物理インターフェイスを無効にする場合、それに関連付けられているすべての論理インターフェイスも無効にします。

ステップ 10 [MTU] フィールドに、最大伝送ユニット（MTU）を入力して、パケットの最大許容サイズを指定します。
MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

ステップ 11 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

論理スイッチド インターフェイスの削除

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

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 削除するスイッチドインターフェイスが含まれる管理対象デバイスの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 削除する論理スイッチドインターフェイスの横にある削除アイコン（  ）をクリックします。

ステップ 4 入力を求められた場合、インターフェイスを削除することを確認します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

仮想スイッチの設定

レイヤ 2 展開でスイッチドインターフェイスを使用できるようにするには、その前に仮想スイッチを設定し、スイッチドインターフェイスをその仮想スイッチに割り当てる必要があります。仮想スイッチとは、ネットワークを通過するインバウンドトラフィックとアウトバウンドトラフィックを処理する複数のスイッチドインターフェイスからなるグループのことです。

仮想スイッチの設定に関する注意事項

仮想スイッチは、[デバイス管理（Device Management）]ページの[仮想スイッチ（Virtual Switches）]タブから追加することができます。[仮想スイッチ（Virtual Switches）]タブには、デバイス上で設定済みのすべての仮想スイッチのリストが表示されます。このページには、各スイッチのサマリ情報が表示されます。

表 *64*：仮想スイッチ テーブル ビューのフィールド

フィールド	説明
[名前（Name）]	仮想スイッチの名前。
インターフェイス	仮想スイッチに割り当てられたすべてのスイッチ型インターフェイス。[インターフェイス（Interfaces）]タブで無効にしたインターフェイスは表示されません。
ハイブリッド インターフェイス（Hybrid Interface）	仮想スイッチを仮想ルータに結合する、オプション設定のハイブリッド インターフェイス。

フィールド	説明
ユニキャスト パケット（Unicast Packets）	次の項目を含む、仮想スイッチのユニキャスト パケット統計： • 受信されたユニキャスト パケット • 転送されたユニキャスト パケット（ホストによるドロップを除く） • 誤ってドロップされたユニキャスト パケット
ブロードキャスト パケット（Broadcast Packets）	次の項目を含む、仮想スイッチのブロードキャスト パケット統計： • 受信されたブロードキャスト パケット • 転送されたブロードキャスト パケット • 誤ってドロップされたブロードキャスト パケット

また、スイッチ型インターフェイスを設定するときにスイッチを追加することもできます。仮想スイッチには、スイッチ型インターフェイスだけ割り当てることができます。管理対象デバイス上でスイッチ型インターフェイスを設定する前に仮想スイッチを作成する必要がある場合は、空の仮想スイッチを作成し、後でその仮想スイッチにインターフェイスを追加できます。

ヒント

既存の仮想スイッチを編集するには、スイッチの横にある編集アイコン（）をクリックします。

仮想スイッチの追加

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

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 仮想スイッチを追加するデバイスの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想スイッチ（Virtual Switches）] タブをクリックします。

ステップ 4 [仮想スイッチの追加（Add Virtual Switch）] をクリックします。

ステップ 5 [名前（Name）] フィールドに名前を入力します。

ステップ 6 [使用可能（Available）] リストから、仮想スイッチに追加される 1 つ以上のスイッチド インターフェイスを選択します。

ヒント [インターフェイス（Interfaces）] タブですでに無効にしたインターフェイスは使用できません。インターフェイスを追加した後で無効にすると、設定からそれが削除されます。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 仮想ルータに仮想スイッチを結びつけるには、[ハイブリッドインターフェイス（Hybrid Interface）] ドロップダウン リストからハイブリッド インターフェイスを選択します。

ステップ 9 必要に応じて、スイッチの詳細設定を行います。以下を参照してください。仮想スイッチの詳細設定, （687 ページ）

ステップ 10 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

論理ハイブリッド インターフェイス, （749 ページ）

仮想スイッチの詳細設定

スタティック MAC エントリを追加する（Adding Static MAC Entries）

仮想スイッチは、ネットワークからのリターン トラフィックにタグを付けることで、時間の経過と共にMACアドレスを学習します。手動でスタティックMACエントリを追加できます。そのようにすることで、MACアドレスが特定のポート上にあることを指定します。そのポートからトラフィックを受信するかどうかに関わらず、MAC アドレスはテーブル内でスタティック アドレスとして保持されます。仮想スイッチごとに 1 つ以上のスタティック MAC アドレスを指定できます。

スパニング ツリー プロトコル（STP）を有効にしてブリッジ プロトコル データ ユニット（BPDU）をドロップする（Enabling Spanning Tree Protocol (STP) and Dropping Bridge Protocol Data Units (BPDU)）

STP は、ネットワーク ループを防止するために使用されるネットワーク プロトコルです。BPDU は、ネットワークを介して交換され、ネットワーク ブリッジに関する情報を伝送します。ネットワーク内に冗長リンクがある場合、プロトコルはBPDUを使用して最も高速なネットワーク リンクを識別し、選択します。ネットワーク リンクで障害が発生した場合、スパニング ツリーは既存の代替リンクにフェールオーバーします。

（注） Cisco では、高可用性ペアで 7000 または 8000 シリーズ デバイスに展開する予定の仮想スイッチを設定する場合は、STP を有効にすることを強く推奨しています。仮想スイッチが複数のネットワーク インターフェイス間のトラフィックを切り替える場合は、STP のみを有効にします。

仮想スイッチが複数の VLAN 間のトラフィックをルーティングする場合、ルータ オン ア スティックと同様に、BPDU はさまざまな論理スイッチド インターフェイスを介してデバイスを出入りしますが、物理スイッチド インターフェイスは同じです。その結果、STP はデバイスを冗長ネットワーク ループと見なします。特定のレイヤ 2 展開では、これによって問題が発生する場合があります。それを防ぐため、トラフィックのモニタリング時にデバイスが BPDU をドロップするようにドメイン レベルで仮想スイッチを設定することができます。STP を無効にする場合は、BPDU をドロップするしかありません。

（注） 仮想スイッチが 1 つの物理インターフェイス上の VLAN 間でトラフィックをルーティングする場合にのみ、BPDU をドロップしてください。

厳格な TCP 強制を有効にする（Enabling Strict TCP Enforcement）

最大限の TCP セキュリティを実現するため、厳格な強制を有効にすることができます。この機能は、3 ウェイ ハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
- 応答側が SYN-ACK を送信する前に TCP 接続の発信側から送信された非 SYN/RST パケット
- SYN の後、セッションの確立前に TCP 接続のレスポンダから送信された非 SYN-ACK/RST パケット
- イニシエータまたはレスポンダから確立された TCP 接続の SYN パケット

仮想スイッチを論理ハイブリッド インターフェイスに関連付けると、そのスイッチでは、論理ハイブリッド インターフェイスに関連付けられている仮想ルータと同じ厳格な TCP 強制設定が使用されることに注意してください。その場合、スイッチで厳格な TCP 強制を指定することはできません。

仮想スイッチの詳細設定の設定

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

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 編集する仮想スイッチが含まれるデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想スイッチ（Virtual Switches）] タブをクリックします。

ステップ 4 編集する仮想スイッチの横にある編集アイコン（  ）をクリックします。

ステップ 5 [Advanced] タブをクリックします。

ステップ 6 スタティック MAC エントリを追加するには、[追加（Add）] をクリックします。

ステップ 7 [MAC アドレス（MAC Address）] フィールドで、2 桁の 16 進数 6 組をコロンで区切った標準形式を使用して、アドレスを入力します（たとえば 01:23:45:67:89:AB）。
（注） ブロードキャスト アドレス（00:00:00:00:00:00 と FF:FF:FF:FF:FF:FF）をスタティック MAC アドレスとして追加することはできません。

ステップ 8 [インターフェイス（Interface）] ドロップダウン リストから、MAC アドレスを割り当てるインターフェイスを選択します。

ステップ 9 [OK] をクリックします。

ステップ 10 スパニング ツリー プロトコルを有効にする場合は、[スパニング ツリー プロトコルを有効にする（Enable Spanning Tree Protocol）] チェックボックスをオンにします。

ステップ 11 厳密な TCP 強制を有効にするには、[厳密な TCP 強制（Strict TCP Enforcement）] チェックボックスをオンにします。
仮想スイッチを論理ハイブリッド インターフェイスに関連付けると、このオプションは表示されず、論理ハイブリッド インターフェイスに関連付けられた仮想ルータと同じ設定がスイッチで使用されます。

ステップ 12 ドメイン レベルで BPDU をドロップするには、[BPDU のドロップ（Drop BPDUs）] チェックボックスをオンにします。

ステップ 13 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

仮想スイッチの削除

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

仮想スイッチを削除すると、そのスイッチに割り当てられたスイッチドインターフェイスを別のスイッチに含めることができるようになります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 削除する仮想スイッチが含まれる管理対象デバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想スイッチ（Virtual Switches）] タブをクリックします。

ステップ 4 削除する仮想スイッチの横にある削除アイコン（  ）をクリックします。

ステップ 5 プロンプトが表示されたら、仮想スイッチを削除することを確認します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 30 章

仮想ルータのセットアップ

以下のトピックでは、Firepower システムで仮想ルータをセットアップする方法について説明します。

仮想ルータ

レイヤ 3 展開の管理対象デバイスは、2 つ以上のインターフェイス間のトラフィックをルーティングするように設定できます。トラフィックをルーティングするには、IP アドレスを各インター

フェイスに割り当ててから、これらのインターフェイスを仮想ルータに割り当てる必要があります。仮想ルータに割り当てるインターフェイスは、物理インターフェイス、論理インターフェイス、または Link Aggregation Group（LAG）インターフェイスのいずれかにできます。

システムは、宛先アドレスに従ってパケット転送の決定を行うことで、パケットをルーティングするように設定できます。ルーテッド インターフェイスとして設定されたインターフェイスは、レイヤ 3 トラフィックを受信し、転送します。ルータは転送基準に基づいて発信インターフェイスから宛先を取得し、アクセス コントロール ルールが、適用するセキュリティ ポリシーを指定します。

レイヤ3展開では、スタティック ルートを定義できます。また、Routing Information Protocol（RIP）およびOpen Shortest Path First（OSPF）のダイナミック ルーティング プロトコルを設定できます。さらに、スタティック ルートと RIP、またはスタティック ルートと OSPF の組み合わせを設定することもできます。

7000 または 8000 シリーズ デバイス上には、仮想ルータ、物理ルーテッド インターフェイス、または論理ルーテッド インターフェイスしか設定できないことに注意してください。

注意 レイヤ3展開に何らかの理由で障害が発生した場合、デバイスはトラフィックを転送しなくなります。

関連トピック

LAG 設定, （732 ページ）

ルーテッド インターフェイス

物理的設定または論理的設定のいずれかでルーテッド インターフェイスをセットアップできます。タグのない VLAN トラフィックを処理するために、物理的ルーテッドインターフェイスを設定できます。指定された VLAN タグのあるトラフィックを処理するために、論理的ルーテッドインターフェイスも作成できます。

レイヤ 3 の展開では、システムは待機しているルーテッド インターフェイスのない外部の物理的インターフェイスから受信したトラフィックをドロップします。このシステムでは、以下の場合パケットをドロップします。

- VLAN タブのないパケットを受信した場合、そのポート向けにルーテッドインターフェイスを設定したことがない場合。
- VLAN タグ付きパケットを受信した場合、そのポートの論理的ルーテッドインターフェイスを設定したことがない場合。

このシステムでは、ルールを評価するか、決定を転送する前にイングレスの最も外側の VLAN タグを削除して、スイッチ インターフェイス上で VLAN タグで受信したトラフィックを処理します。VLAN タグ付きの論理的ルーテッド インターフェイスを介してデバイスに残っているパケットは、イーグレスの関連付けられた VLAN タブによりカプセル化します。このシステムでは、削除プロセスの完了後、VLAN タブで受信したトラフィックをドロップします。

スタティック Address Resolution Protocol（ARP）エントリをルーテッド インターフェイスに追加できます。外部ホストは、トラフィックの送信先となるローカル ネットワーク上の宛先IPアドレスの MAC アドレスを知る必要がある場合は、ARP 要求を送信します。スタティック ARP エントリを設定する場合、仮想ルータは IP アドレスや関連付けられた MAC アドレスに応答します。

論理ルーテッド LAG インターフェイスの [ICMP 有効応答（ICMP Enable Responses）] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑制されるわけではありません。宛先 IP がルーテッド インターフェイスの IP で、プロトコルが ICMP であるパケットをドロップするように、アクセス コントロール ポリシーにネットワークベースのルールを追加できます。

管理対象デバイスの [ローカル ルータ トラフィックを検査する（Inspect Local Router Traffic）] オプションを有効にすると、システムは、ホストに到着する前にパケットをドロップし、これによっていかなる応答も阻止できます。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

上位の物理的インターフェイスをインラインまたはパッシブに変更する場合、システムでは、関連付けられた論理的インターフェイをすべて削除します。

関連トピック

デバイスの詳細設定, （469 ページ）
7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

物理ルーテッド インターフェイスの設定

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

ルーテッド インターフェイスとして管理対象デバイスの 1 つ以上の物理ポートを設定できます。トラフィックをルーティングする前に、物理ルーテッド インターフェイスを仮想ルータに割り当てる必要があります。

注意 ルーテッド インターフェイス ペアを 7000 または 8000 シリーズ デバイスに追加すると、設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 変更するインターフェイスの横にある編集アイコン（  ）をクリックします。

ステップ 4 [ルーテッド（Routed）] をクリックして、ルーテッド インターフェイス オプションを表示します。

ステップ 5 セキュリティ ゾーンを適用するには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して、新しいセキュリティ ゾーンを追加します。セキュリティ ゾーン オブジェクトの作成, （392 ページ）を参照してください。

ステップ 6 仮想ルータを指定するには、次のいずれかを実行します。

- [仮想ルータ（Virtual Router）] ドロップダウン リストから既存の仮想ルータを選択します。
- [新規（New）] を選択して、新しい仮想ルータを追加します。仮想ルータの追加, （703 ページ）を参照してください。

ステップ 7 [有効化（Enabled）]チェックボックスをオンにして、ルーテッドインターフェイスがトラフィックを処理することを許可します。このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8 [モード（Mode）] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [自動ネゴシエーション（Auto Negotiation）] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。
モード設定は銅線インターフェイスにのみ使用できます。

8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

ステップ 9 [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または自動 MDIX のいずれかを指定するオプションを選択します。

通常、[MDI/MDIX] は [自動 MDIX（Auto-MDIX）] に設定します。これにより、MDI と MDIX の間の切り替えが自動的に処理され、リンクが確立されます。

[MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。

ステップ 10 [MTU] フィールドに、最大伝送ユニット（MTU）を入力して、パケットの最大許容サイズを指定します。
MTU はレイヤ 2 MTU/MRU であり、レイヤ 3 MTU ではありません。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

ステップ 11 [ICMP] の横にある [応答を有効にする（Enable Responses）] チェックボックスをオンにして、インターフェイスを ping や traceroute などの ICMP トラフィックに応答可能にします。

ステップ 12 [IPv6 NDP] の横にある [ルータ アドバタイズメントの有効化（Enable Router Advertisement）] チェックボックスをオンにして、インターフェイスがルータ アドバタイズメントを伝送できるようにします。

ステップ 13 IP アドレスを追加するには、[追加（Add）] をクリックします。

ステップ 14 [アドレス（Address）] フィールドに、ルーテッド インターフェイスの IP アドレスとサブネット マスクを CIDR 表記で入力します。
次の点に注意してください。

- ネットワークおよびブロードキャスト アドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 15 組織が IPv6 アドレスを使用している場合、インターフェイスの IP アドレスを自動的に設定するには、[IPv6] フィールドの横の [アドレス自動設定（Address Autoconfiguration）] チェックボックスをオンにします。

ステップ 16 [タイプ（Type）] には、[標準（Normal）] または [SFRP] を選択します。
SFRP オプションの詳細についてはSFRP の設定, （700 ページ）を参照してください。

ステップ 17 [OK] をクリックします。

- IP アドレスを編集するには、編集アイコン（  ）をクリックします。
- IP アドレスを削除するには、削除アイコン（  ）をクリックします。

（注） IP アドレスを 7000 または 8000 シリーズ デバイスのルーテッド インターフェイスに追加する場合、ハイアベイラビリティ ペア ピアのルーテッド インターフェイスに対応する IP アドレスを追加する必要があります。

ステップ 18 スタティック ARP エントリを追加するには、[追加（Add）] をクリックします。

ステップ 19 [IP アドレス（IP Address）] フィールドに、スタティック ARP エントリの IP アドレスを入力します。

ステップ 20 [MAC アドレス（MAC Address）] フィールドに、IP アドレスに関連付ける MAC アドレスを入力します。2 桁の 16 進数の 6 個のグループをコロンで区切る標準アドレス形式を使用します（たとえば、01:23:45:67:89:AB）。

ステップ 21 [OK] をクリックします。

ヒント スタティック ARP エントリを編集するには、編集アイコン（  ）をクリックします。
スタティック ARP エントリを削除するには、削除アイコン（  ）をクリックします。

ステップ 22 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

論理ルーテッドインターフェイスの追加

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

各物理ルーテッド インターフェイスで、複数の論理ルーテッド インターフェイスを追加できます。物理インターフェイスで受信した VLAN タグ付きのトラフィックは、各論理インターフェイスにその特定のタグが関連付けられていなければ処理されません。トラフィックをルーティングするには、論理ルーテッド インターフェイスを仮想ルータに割り当てる必要があります。

注意 7000 または 8000 シリーズ デバイス 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。 でのルーテッド インターフェイス ペアの追加

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インターフェイスの追加（Add Interface）] をクリックします。

ステップ 4 [ルーテッド（Routed）] をクリックして、ルーテッド インターフェイス オプションを表示します。

ステップ 5 [インターフェイス（Interface）] ドロップダウン リストから、論理インターフェイスを追加する物理インターフェイスを選択します。

ステップ 6 [VLAN タグ（VLAN Tag）] フィールドで、このインターフェイス上のインバウンド/アウトバウンド トラフィックに割り当てるタグ値を入力します。この値には、1 ～ 4094 の任意の整数を指定できます。

ステップ 7 セキュリティ ゾーンを適用するには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して、新しいセキュリティ ゾーンを追加します。セキュリティ ゾーン オブジェクトの作成, （392 ページ）を参照してください。

ステップ 8 仮想ルータを指定するには、次のいずれかを実行します。

- [仮想ルータ（Virtual Router）] ドロップダウン リストから既存の仮想ルータを選択します。
- [新規（New）] を選択して、新しい仮想ルータを追加します。仮想ルータの追加, （703 ページ）を参照してください。

ステップ 9 ルーテッドインターフェイスにトラフィックを処理させるには、[有効（Enabled）]チェックボックスをオンにします。
このチェックボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。物理インターフェイスを無効にする場合、それに関連付けられているすべての論理インターフェイスも無効にします。

ステップ 10 [MTU] フィールドに、最大伝送ユニット（MTU）を入力して、パケットの最大許容サイズを指定します。
MTU はレイヤ 2 MTU/MRU であり、レイヤ 3 MTU ではありません。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

ステップ 11 [ICMP] の横にある [応答を有効にする（Enable Responses）] チェックボックスをオンにして、他のルータ、中間デバイス、またはホストに更新またはエラー情報を伝送します。

ステップ 12 [IPv6 NDP] の横にある [ルータ アドバタイズメントを有効にする（Enable Router Advertisement）] チェックボックスをオンにして、インターフェイスがルータ アドバタイズメントを伝送できるようにします。

ステップ 13 IP アドレスを追加するには、[追加（Add）] をクリックします。

ステップ 14 [アドレス（Address）] フィールドに、IP アドレスを CIDR 表記で入力します。
次の点に注意してください。

- ネットワークおよびブロードキャスト アドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 15 IPv6 を使用した環境で、インターフェイスの IP アドレスを自動設定するには、[IPv6] フィールドの横にある [アドレスの自動設定（Address Autoconfiguration）] チェックボックスを選択します。

ステップ 16 [タイプ（Type）] には、[普通（Normal）] または [SFRP] を選択します。
SFRP オプションの詳細についてはSFRP の設定, （700 ページ）を参照してください。

ステップ 17 [OK] をクリックします。

- IP アドレスを編集するには、編集アイコン（  ）をクリックします。
- IP アドレスを削除するには、削除アイコン（  ）をクリックします。

（注） IP アドレスを 7000 または 8000 シリーズ デバイスの高可用性ペアのルーテッド インターフェイスに追加する場合、高可用性ペアピアのルーテッド インターフェイスに対応する IP アドレスを追加する必要があります。

ステップ 18 スタティック ARP エントリを追加するには、[追加（Add）] をクリックします。

ステップ 19 [IP アドレス（IP Address）] フィールドに、スタティック ARP エントリの IP アドレスを入力します。

ステップ 20 [MAC アドレス（MAC Address）] フィールドに、IP アドレスに関連付ける MAC アドレスを入力します。2 桁の 16 進数の 6 個のグループをコロンで区切る標準アドレス形式を使用します（たとえば、01:23:45:67:89:AB）。

ステップ 21 [OK] をクリックします。スタティック ARP エントリが追加されます。

ヒント スタティック ARP エントリを編集するには、編集アイコン（  ）をクリックします。
スタティック ARP エントリを削除するには、削除アイコン（  ）をクリックします。

ステップ 22 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

論理ルーテッド インターフェイスの削除

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

論理ルーテッド インターフェイスを削除すると、帰属する物理インターフェイスのほか、割り当てられた仮想ルータおよびセキュリティ ゾーンからも削除されます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 削除する論理ルーテッド インターフェイスの横にある削除アイコン（）をクリックします。

ステップ 4 入力を求められた場合、インターフェイスを削除することを確認します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

SFRP

シスコの冗長プロトコル（SFRP）を設定すると、7000 または 8000 シリーズ デバイスの高可用性ペアまたは個別のデバイスのいずれかで、高可用性を得るためにネットワークの冗長性を実現できます。SFRP は IPv4 と IPv6 の両方のアドレスのゲートウェイ冗長性を提供します。ルーテッド インターフェイスおよびハイブリッド インターフェイスの SFRP を設定できます。

インターフェイスが個別のデバイスに設定される場合、同じブロードキャスト ドメインに存在する必要があります。インターフェイスのうち少なくとも 1 つをマスターに指定し、同じ数をバックアップとして指定する必要があります。システムは IP アドレスごとに 1 つのマスターと 1 つのバックアップのみをサポートします。ネットワーク接続が失われた場合、システムは自動的にバックアップをマスターに昇格し、接続を維持します。

SFRP に設定するオプションは、SFRP インターフェイス グループのすべてのインターフェイスで同じにする必要があります。グループ内の複数の IP アドレスのマスターとバックアップの状態は同じである必要があります。そのため、IP アドレスを追加または編集する場合、そのアドレスに設定する状態はグループ内のすべてのアドレスに適用されます。セキュリティのために、グループ内のインターフェイス間で共有される [グループ ID（Group ID）] と [共有秘密（Shared Secret）] の値を入力する必要があります。

仮想ルータの SFRP の IP アドレスを有効にするには、少なくとも 1 つの非 SFRP IP アドレスを設定する必要があります。

高可用性ペアの 7000 または 8000 シリーズ デバイスの場合、共有秘密を指定すると、SFRP の IP 設定とともに高可用性ペアのピアにコピーされます。共有秘密は、ピアのデータを認証します。

関連トピック

7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて, （515 ページ）

SFRP の設定

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

Cisco 冗長プロトコル（SFRP）を設定して、7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアまたは個別のデバイスのハイ アベイラビリティを得るためのネットワーク冗長性を実現できます。SFRP は IPv4 と IPv6 の両方のアドレスのゲートウェイ冗長性を提供します。ルーテッド インターフェイスおよびハイブリッド インターフェイスの SFRP を設定できます。

（注） 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアのルーティングされたインターフェイスまたはハイブリッド インターフェイスで SFRP IP アドレスがすでに 1 つ構成されている場合、複数の非 SFRP IP アドレスを有効にすることは推奨しません。7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアがスタンバイ モードでフェールオーバーした場合、NAT は実行されません。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 SFRP を設定するインターフェイスの横にある編集アイコン（）をクリックします。

ステップ 4 SFRP を設定するインターフェイスのタイプ（[ルーテッド（Routed）] または [ハイブリッド（Hybrid）]）を選択します。

ステップ 5 IP アドレスを追加または編集するときに SFRP を設定できます。[追加（Add）] をクリックして、IP アドレスを追加します。IP アドレスを編集するには、編集アイコン（）をクリックします。

ステップ 6 [タイプ（Type）] に [SFRP] を選択して SFRP オプションを表示します。

ステップ 7 [グループ ID（Group ID）] フィールドに、SFRP 用に設定されたマスターまたはバックアップ インターフェイス グループを指定する値を入力します。

ステップ 8 [優先順位（Priority）] で、[マスター（Master）] または [バックアップ（Backup）] のどちらかを選択して、優先するインターフェイスを指定します。

- 個別のデバイスの場合、1 つのデバイスにマスターへのインターフェイスを 1 個設定し、2 番目のデバイスにバックアップへのインターフェイスを設定する必要があります。
- 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアの場合、マスターとして 1 個のインターフェイスを設定すると、もう 1 個のインターフェイスは自動的にバックアップになります。

ステップ 9 [共有秘密（Shared Secret）] フィールドに、共有秘密を入力します。
[共有秘密（Shared Secret）] フィールドには、7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペア内のグループに関するデータが自動的に入力されます。

ステップ 10 [アドバタイズメントの間隔：（Advertisement Interval:）] フィールドに、レイヤ 3 トラフィックのルート アドバタイズメントの間隔を入力します。

ステップ 11 [OK] をクリックします。

ステップ 12 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて，（515 ページ）

仮想ルータ設定

注意 7000 または 8000 シリーズ デバイスで仮想ルータを追加した場合 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作，（326 ページ）を参照してください。

レイヤ 3 配置でルーテッド インターフェイスを使用する前に、仮想ルータを設定し、ルーテッド インターフェイスを割り当てる必要があります。仮想ルータは、レイヤ3トラフィックをルーティングするルーテッド インターフェイスのグループです。

1 つの仮想ルータに割り当てることができるのは、ルーテッド インターフェイスとハイブリッド インターフェイスのみです。

最大限の TCP セキュリティを実現するため、厳格な強制を有効にすることができます。この機能は、3 ウェイ ハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
- 応答側が SYN-ACK を送信する前に TCP 接続の発信側から送信された非 SYN/RST パケット
- SYN の後、セッションの確立前に TCP 接続のレスポンダから送信された非 SYN-ACK/RST パケット
- 発信側または応答側のどちらかから送信された、確立された TCP 接続の SYN パケット

レイヤ 3 インターフェイスの設定を非レイヤ 3 インターフェイスに変更したり、仮想ルータからレイヤ 3 インターフェイスを削除したりすると、ルータは無効な状態になる場合があることに注意してください。たとえば、DHCPv6 で使用されている場合、アップストリームとダウンストリームの不一致が生じることがあります。

仮想ルータの追加

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

[デバイス管理（Device Management）] ページの [仮想ルータ（Virtual Routers）] タブから仮想ルータを追加できます。ルーテッド インターフェイスを設定するときに、ルータを追加することもできます。

管理対象デバイスのインターフェイスを設定する前に仮想ルータを作成する場合は、空の仮想ルータを作成し、後でインターフェイスを追加できます。

注意 7000 または 8000 シリーズ デバイスで仮想ルータを追加した場合 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。
ヒント デバイスが高可用性ペアのスタックにある場合、[選択済みデバイス（Selected Device）] ドロップダウン リストから、変更するスタックを選択します。

ステップ 4 [仮想ルータの追加（Add Virtual Router）] をクリックします。

ステップ 5 [名前（Name）] フィールドに仮想ルータの名前を入力します。英数字とスペースを使用できます。

ステップ 6 [IPv6 サポート（IPv6 Support）] チェックボックスをオンまたはオフにして、仮想ルータで IPv6 スタティック ルーティング、OSPFv3 と RIPng を設定します。

ステップ 7 TCP の厳密な適用をやめるには、[TCP の厳密な適用（Strict TCP Enforcement）] チェックボックスをオフにします。このオプションは、デフォルトで有効です。

ステップ 8 [インターフェイス（Interfaces）] の [使用可能（Available）] リストから 1 つまたは複数のインターフェイスを選択し、[追加（Add）] をクリックします。

[使用可能（Available）] リストには、仮想ルータに割り当てることが可能なデバイス上のすべての有効なレイヤ 3 インターフェイス（ルーテッドおよびハイブリッド）が含まれます。

ヒント 仮想ルータからルーテッドまたはハイブリッド インターフェイスを削除するには、削除アイコン（）をクリックします。[インターフェイス（Interfaces）] タブで、設定したインターフェイスを無効にすることによっても削除できます。

ステップ 9 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

DHCP リレー

DHCP はインターネット ホストに設定パラメータを提供します。IP アドレスを未取得の DHCP クライアントは、ブロードキャスト ドメインの外にある DHCP サーバと直接通信できません。DHCP クライアントが DHCP サーバと通信できるようにするには、クライアントがサーバと同じブロードキャスト ドメイン内にない状況に対応できるように DHCP リレー インスタンスを設定します。

ユーザは、設定するそれぞれの仮想ルータに対して DHCP リレーを設定できます。デフォルトでは、この機能は無効になっています。DHCPv4 リレーまたは DHCPv6 リレーのどちらかを有効にできます。

（注） 同じデバイスで実行中の複数の仮想ルータを介して DHCPv6 リレー チェーンを実行することはできません。

DHCPv4 リレーの設定

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

次の手順は、仮想ルータで DHCPv4 リレーを設定する方法について説明します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [DHCPv4（DHCPv6）] チェックボックスをオンにします。

ステップ 6 [サーバ（Servers）] フィールドに、サーバの IP アドレスを入力します。

ステップ 7 [追加（Add）] をクリックします。
最大 4 台の DHCP サーバを追加できます。

ステップ 8 [最大ホップ（Max Hops）] フィールドに 1 ～ 255 の最大ホップ カウントを入力します。

ステップ 9 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

DHCPv6 リレーの設定

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

同じデバイスで実行中の複数の仮想ルータを介して DHCPv6 リレー チェーンを実行することはできません。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 DHCP リレーを設定する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [DHCPv6] チェックボックスをオンにします。

ステップ 6 [インターフェイス（Interfaces）] フィールドで、仮想ルータに割り当てられている 1 つ以上のインターフェイスの横にあるチェックボックスをオンにします。

ヒント DHCPv6 リレー用に設定されているインターフェイスは、[インターフェイス（Interfaces）] タブから無効にできません。最初に [DHCPv6 リレー インターフェイス（DHCPv6 Relay interfaces）] チェックボックスをオフにして、設定を保存する必要があります。

ステップ 7 選択したインターフェイスの横にあるドロップダウン アイコンをクリックし、インターフェイスが DHCP 要求をリレーする方式として、[アップストリーム（Upstream）]、[ダウンストリーム（Downstream）]、または [両方（Both）] を選択します。

（注） 少なくとも 1 つのダウンストリーム インターフェイスと 1 つのアップストリーム インターフェイスを含める必要があります。[両方（Both）] を選択することは、インターフェイスがダウンストリームとアップストリームの両方であることを意味します。

ステップ 8 [最大ホップ（Max Hops）] フィールドに 1 ～ 255 の最大ホップ カウントを入力します。

ステップ 9 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

スタティック ルート

スタティック ルーティングにより、ルータを通過するトラフィックの IP アドレスに関するルールを作成することができます。これはネットワークの現在のトポロジに関して他のルータとの通信がないため、仮想ルータのパス選択を設定する最も簡単な方法です。

スタティック ルート テーブルには次の表に示すように、各ルートに関するサマリー情報が含まれます。

表 *65* : スタティック ルート テーブル ビュー フィールド

フィールド	説明
[有効（Enabled）]	このルートが現在有効であるか、無効であるかを示します。
[名前（Name）]	スタティック ルートの名前。
[接続先（Destination）]	トラフィックがルーティングされる宛先ネットワーク。

フィールド	説明
タイプ（Type）	このルートに対して実行するアクションを指定します。次のいずれかです。 • [IP]：パケットが、隣接ルータのアドレスに転送されることを指定します。 • [インターフェイス（Interface）]：そのインターフェイスを介してトラフィックが直接接続されたネットワーク上のホストにルーティングされるインターフェイスにパケットが転送されることを指定します。 • [破棄（Discard）]：スタティック ルートでパケットをドロップすることを指定します。
ゲートウェイ（Gateway）	スタティック ルートのタイプとしてIPを選択した場合はターゲットIPアドレス、またはスタティック ルート タイプとしてインターフェイスを選択した場合はインターフェイス。
優先順位（Preference）	ルート選択を決定します。同じ宛先に対する複数のルートが存在する場合、より高い優先順位のルートが選択されます。

静的ルート テーブルの表示

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

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 表示するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 静的ルートを表示する仮想ルータの横にある編集アイコン（  ）をクリックします。
代わりに表示アイコン（）が表示される場合、設定は子孫ドメインに属しているか、設定を変更する権限がありません。

ステップ 5 [静的（Static）] タブをクリックします。

スタティック ルートの追加

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

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 スタティック ルートを追加するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 スタティック ルートを追加する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [静的（Static）] をクリックして、スタティック ルートのオプションを表示します。

ステップ 6 [静的ルートの追加（Add Static Route）] をクリックします。

ステップ 7 [ルート名（Route Name）] フィールドに、スタティック ルートの名前を入力します。英数字とスペースを使用できます。

ステップ 8 [有効（Enabled）] チェックボックスをオンにして、ルートが現在有効であることを指定します。

ステップ 9 [優先（Preference）] フィールドに、ルート選択を決定するための 1 ～ 65535 の数値を入力します。
（注） 同じ宛先に対する複数のルートが存在する場合、より高い優先順位のルートが使用されます。

ステップ 10 [タイプ（Type）] ドロップダウン リストから、設定するスタティック ルートのタイプを選択します。

ステップ 11 [宛先（Destination）] フィールドに、トラフィックがルーティングされる宛先ネットワークの IP アドレスを入力します。

ステップ 12 [ゲートウェイ（Gateway）] フィールドでは、次の 2 つの選択肢があります。

- スタティック ルート タイプとして [IP] を選択した場合は、IP アドレスを選択します。
- スタティック ルート タイプとして [インターフェイス（Interface）] を選択した場合は、ドロップダウン リストから有効なインターフェイスを選択します。

  ヒント [インターフェイス（Interfaces）] タブから無効にしたインターフェイスは使用できません。追加したインターフェイスを無効にすると、設定から削除されます。

ステップ 13 [OK] をクリックします。

ステップ 14 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ダイナミック ルーティング

ダイナミックつまり適応型のルーティングは、ルーティング プロトコルを使用して、ルートが取るパスをネットワーク条件の変化に応じて変更します。この適応は、できるだけ多くのルートの有効性を維持し、変更に応じて宛先に到達可能とすることを目的としたものです。このため、他のパスを選択できる限り、ネットワークはノードまたはノード間の接続の損失といった障害を「迂回」することができます。ダイナミック ルーティングなしでルータを設定することも、Routing Information Protocol（RIP）または Open Shortest Path First（OSPF）のルーティング プロトコルを設定することもできます。

RIP コンフィギュレーション

Routing Information Protocol（RIP）はホップ カウントを使用してルートを決定する、小規模な IP ネットワーク向けのダイナミック ルーティング プロトコルです。最適なルートは最小数のホップを使用します。RIP で許可されるホップの最大数は 15 です。このホップ制限により、RIP がサポートできるネットワークのサイズも制限されます。

RIP 設定のインターフェイスの追加

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

RIP を設定する際、RIP を設定する仮想ルータにすでに含まれているインターフェイスを選択する必要があります。無効になっているインターフェイスを使用することはできません。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（ ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [インターフェイス（Interfaces）] の下で、追加アイコン（  ）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、RIP を設定するインターフェイスを選択します。

ヒント [インターフェイス（Interfaces）] タブから無効にしたインターフェイスは使用できません。追加したインターフェイスを無効にすると、設定から削除されます。

ステップ 9 [メトリック（Metric）] フィールドに、インターフェイスのメトリックを入力します。異なる RIP インスタンスからのルートを使用可能で、すべてが同じ設定である場合、メトリックが最小のルートが優先ルートになります。

ステップ 10 [モード（Mode）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- [マルチキャスト（Multicast）]：RIP が指定されたアドレスですべての隣接ルータにルーティング テーブル全体をマルチキャストするデフォルトのモード。
- [ブロードキャスト（Broadcast）]：マルチキャスト モードが可能な場合でも、RIP にブロードキャスト（RIPv1 など）の使用を強制します。
- [送信なし（Quiet）]：RIP は、このインターフェイスに定期メッセージを送信しません。
- [リッスンなし（No Listen）]：RIP は、このインターフェイスに送信しますが、リッスンしません。

ステップ 11 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

RIP の認証設定

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

RIP 認証では、仮想ルータに設定した認証プロファイルの 1 つが使用されます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 RIP 認証プロファイルを追加する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [認証（Authentication）] で、[プロファイル（Profile）] ドロップダウン リストから既存の仮想ルータの認証プロファイルを選択するか、[なし（None）] を選択します。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

高度な RIP の設定

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

プロトコルの動作に影響するさまざまなタイムアウト値およびその他の機能に関していくつかの高度な RIP 設定を構成できます。

注意 不正な値に対する高度な RIP 設定を変更すると、ルータが他の RIP ルータと正常に通信することを妨げる場合があります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [優先順位（Preference）] フィールドに、ルーティング プロトコルの優先度の数値（高いほど優先される）を入力します。システムはスタティック ルートよりも RIP を使用して学習したルートを優先します。

ステップ 8 [期間（Period）] フィールドに、定期的な更新間隔（秒単位）を入力します。低い数値は高速なコンバージェンスを示しますが、ネットワーク負荷が大きくなります。

ステップ 9 [タイムアウト時間（Timeout Time）] フィールドに、到達不能とみなされるまでのルートの存続時間（秒単位）を指定する数値を入力します。

ステップ 10 [ガベージ時間（Garbage Time）] フィールドに、破棄されるまでのルートの存続時間（秒単位）を指定する数値を入力します。

ステップ 11 [無限（Infinity）] フィールドに、コンバージェンスの計算で無限間隔の値を指定する数値を入力します。値が大きいほど、プロトコル コンバージェンスが遅くなります。

ステップ 12 [実行（Honor）] ドロップダウン リストから、ルーティング テーブルをダンプする要求がいつ実行されるかを指定する、次のいずれかのオプションを選択します。

- [常時（Always）]：常に要求を実行する
- [ネイバー（Neighbor）]：直接接続されたネットワーク上のホストから送信された要求のみを実行する
- [なし（Never）]：要求を実行しない

ステップ 13 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

RIP 設定へのインポート フィルタの追加

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

ルート テーブルに対して RIP からの受け入れまたは拒否を行うルートを指定するために、インポート フィルタを追加できます。インポート フィルタはテーブルに表示される順に適用されます。

インポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。

ヒント

RIP インポート フィルタを編集するには、編集アイコン（）をクリックします。RIP インポート フィルタを削除するには、削除アイコン（）をクリックします。

はじめる前に

- 仮想ルータの追加, （703 ページ） の説明に従い、仮想ルータを追加します。
- 仮想ルータのフィルタの設定, （725 ページ） の説明に従い、仮想ルータにフィルタを設定します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 RIP 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [インポート フィルタ（Import Filters）] の下で、追加アイコン（）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、インポート フィルタとして追加するフィルタを選択します。

ステップ 9 [アクション（Action）] の横にある [承認（Accept）] または [拒否（Reject）] を選択します。

ステップ 10 [OK] をクリックします。

ヒント インポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（）または下へ移動するアイコン（）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

RIP 設定へのエクスポート フィルタの追加

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

ルート テーブルから RIP に対しての受け入れまたは拒否を行うルートを定義するために、エクスポート フィルタを追加できます。エクスポート フィルタはテーブルに表示される順に適用されます。

エクスポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 RIP 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [エクスポート フィルタ（Export Filters）] の下で、追加アイコン（）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、エクスポート フィルタとして追加するフィルタを選択します。

ステップ 9 [アクション（Action）] の横にある [承認（Accept）] または [拒否（Reject）] を選択します。

ステップ 10 [OK] をクリックします。

ヒント エクスポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（）または下へ移動するアイコン（）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

OSPF の設定

Open Shortest Path First（OSPF）は、他のルータから情報を取得し、リンク ステート アドバタイズメントを使用してルートを他のルータにアドバタイズすることで、ルートを動的に定義する適応型ルーティング プロトコルです。ルータは、それ自体と宛先との間のリンクに関する情報を維持し、ルーティングを決定します。OSPF は、各ルーテッドインターフェイスにコストを割り当て、コストが最低のルータを最適であるとみなします。

OSPF ルーティング エリア

OSPF ネットワークは、管理を簡略化し、トラフィックおよびリソースの使用を最適化するために、ルーティング エリアに構造化つまり分割することができます。エリアは、単純な 10 進数またはよく使用されるオクテットベースのドット付き 10 進数表記のいずれかで表現される 32 ビットの数字により識別されます。

慣習により、エリア ゼロつまり 0.0.0.0 は OSPF ネットワークのコアまたはバックボーン エリアを表します。他のエリアも指定できます。多くの場合、管理者はエリアのメイン ルータの IP アドレスをエリア ID として選択します。追加の各エリアはバックボーンの OSPF エリアに直接または仮想接続できる必要があります。そうした接続は、エリア境界ルータ（ABR）と呼ばれる相互接続ルータによって保持されます。ABR は、管轄する各エリアの個々のリンクステート データベースを管理し、ネットワーク内のすべてのエリアの集約ルートを保守します。

OSPF エリアの追加

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

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（ ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF] をクリックして、OSPF オプションを表示します。

ステップ 7 [エリア（Areas）] の下で、追加アイコン（  ）をクリックします。

ステップ 8 [エリア ID（Area Id）] フィールドに、エリアを表す数値を入力します。この値には整数または IPv4 アドレスを指定できます。

ステップ 9 オプションで、[スタブネット（Stubnet）] チェックボックスをオンにし、エリアが自律システムの外部のルータ アドバタイズメントを受信せず、エリア内のルーティングは完全にデフォルト ルートに基づくことを指定します。チェックボックスをオフにすると、このエリアはバックボーン エリアになります。それ以外の場合は、非スタブ エリアになります。

ステップ 10 [デフォルト コスト（Default cost）] フィールドに、エリアのデフォルト ルートに関連付けられたコストを入力します。

ステップ 11 [スタブネット（Stubnets）] の下で、追加アイコン（  ）をクリックします。

ステップ 12 [IP アドレス（IP Address）] フィールドに、IP アドレスを CIDR 表記で入力します。

ステップ 13 [非表示（Hidden）]チェックボックスを選択して、スタブネットが非表示であることを示します。非表示のスタブネットは別のエリアに伝播されません。

ステップ 14 [サマリ（Summary）] チェックボックスを選択して、このスタブネットのサブネットワークであるデフォルトのスタブネットが非表示となるように指定します。

ステップ 15 [スタブ コスト（Stub cost）] フィールドに、このスタブ ネットワークへのルーティングに関連付けられたコストを定義する値を入力します。

ステップ 16 [OK] をクリックします。

ステップ 17 ネットワークを追加するには [ネットワーク（Networks）] の下の追加アイコン（  ）をクリックします。

ステップ 18 [IP アドレス（IP Address）] フィールドに、ネットワークの IP アドレスを CIDR 表記で入力します。

ステップ 19 [非表示（Hidden）] チェックボックスをオンにして、ネットワークが非表示であることを示します。非表示のネットワークは別のエリアに伝播されません。

ステップ 20 [OK] をクリックします。

ステップ 21 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

OSPF エリア インターフェイス

OSPF用に仮想ルータに割り当てられたインターフェイスのサブセットを設定できます。次のリストに、各インターフェイスで指定できるオプションを示します。

インターフェイス

OSPFを設定するインターフェイスを選択します。[インターフェイス（Interfaces）]タブから無効にしたインターフェイスは使用できません。

タイプ（Type）

次のオプションから、OSPFインターフェイスのタイプを選択します。

- [ブロードキャスト（Broadcast）]：ブロードキャスト ネットワークでは、フラッディングおよびhelloメッセージはマルチキャストを使用し、すべてのネイバーに対して1つのパケットで送信されます。このオプションは、ルータがリンク ステート データベースと同期し、ネットワーク リンク ステート アドバタイズメントを発信するように指定します。このネットワーク タイプは、物理的なノンブロードキャスト マルチプル アクセス（NBMP）ネットワークと適切なIPプレフィクスなしのアンナンバード ネットワークには使用できません。
- [ポイントツーポイント（PtP）（Point-to-Point (PtP)）]：ポイントツーポイント ネットワークでは、2台のルータのみを接続します。選定は実行されず、ネットワーク リンク ステート アドバタイズメントは発生しないので、より単純かつ高速に確立されます。このネットワーク タイプは物理的なPtPインターフェイスだけでなく、PtPリンクとして使用されるブロードキャスト ネットワークにも役立ちます。このネットワーク タイプは物理的なNBMPネットワークでは使用できません。
- [ノンブロードキャスト（Non-Broadcast）]：NBMPネットワークで、パケットはマルチキャスト機能がないために各ネイバーに別々に送信されます。ブロードキャスト ネットワークと同様に、このオプションはリンク ステート アドバタイズメント伝播で中心的な役割を果たすルータを指定します。このネットワーク タイプはアンナンバード ネットワークでは使用できません。
- [自動検出（Autodetect）]：システムは指定されたインターフェイスに基づいて正しいタイプを判別します。

コスト

インターフェイスの出力コストを指定します。

Stub

インターフェイスがOSPFトラフィックをリッスンし、独自のトラフィックを送信する必要があるかどうかを指定します。

[プライオリティ（Priority）]

指定ルータの選定に使用される優先度を示す数値を入力します。多重アクセス ネットワークごとに、システムはルータおよびバックアップ ルータを指定します。これらのルータには、フラッディング プロセスでの特別な機能があります。優先度を高くすると、この選定での優先順位が上がります。優先度 0 でルータを設定することはできません。

[ノンブロードキャスト（Nonbroadcast）]

hello パケットが任意の未定義のネイバーに送信されるかどうかを指定します。このスイッチは、任意の NBMA ネットワークでは無視されます。

認証

仮想ルータに設定した認証プロファイルの 1 つからこのインターフェイスが使用する OSPF 認証プロファイルを選択するか、または [なし（None）] を選択します。認証プロファイルの設定に関する詳細については、仮想ルータ認証プロファイルの追加, （727 ページ）を参照してください。

[Hello 間隔（Hello Interval）]

hello メッセージの送信間隔（秒単位）を入力します。

[ポーリング（Poll）]

NBMA ネットワーク上の一部のネイバーに対する hello メッセージの送信間隔（秒単位）を入力します。

[再送間隔（Retrans Interval）]

確認応答されていないアップデートの再送信間隔（秒単位）を入力します。

[再送遅延（Retrans Delay）]

インターフェイス経由でのリンクステートアップデートパケットの送信に要する推定秒数を入力します。

待ち時間（Wait Time）

ルータが選定の開始と隣接関係の構築の間で待機する秒数を入力します。

[デッド間隔（Dead Interval）]

ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を入力します。この値が定義されている場合、dead カウントから計算された値はオーバーライドされます。

[無レスポンス カウント（Dead Count）]

hello 間隔と乗算されるときに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を指定する、数値を入力します。

OSPF エリア インターフェイスを編集するには、編集アイコン（  ）をクリックします。OSPF エリアインターフェイスを削除するには、削除アイコン（  ）をクリックします。[インターフェイス（Interfaces）] タブで設定されたインターフェイスを無効にすると削除されます。

OSPF エリア インターフェイスの追加

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

OSPF 用に仮想ルータに割り当てられたインターフェイスのサブセットを設定できます。

OSPF エリアで使用するインターフェイスは 1 つのみ選択できます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 OSPF インターフェイスを追加するデバイスの横にある編集アイコン（  ）をクリックします。マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 OSPFインターフェイスを追加する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）]をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF] をクリックして、OSPF オプションを表示します。

ステップ 7 [エリア（Areas）] の下で、追加アイコン（  ）をクリックします。

ステップ 8 [インターフェイス（Interfaces）] をクリックします。

ステップ 9 追加アイコン（  ）をクリックします。

ステップ 10 OSPF エリア インターフェイス，（717 ページ）で説明されているアクションのいずれかを実行します。

ステップ 11 ネットワークを追加するには [ネットワーク（Networks）] の下の追加アイコン（  ）をクリックします。

ステップ 12 [IP アドレス（IP address）] フィールドに、このインターフェイスから非ブロードキャスト ネットワークの hello メッセージを受信するネイバーの IP アドレスを入力します。

ステップ 13 [資格あり（Eligible）] チェックボックスをオンにして、ネイバーがメッセージを受け取る資格があることを示します。

ステップ 14 [OK] をクリックします。

ヒント ネイバーを編集するには、編集アイコン（  ）をクリックします。ネイバーを削除するには、削除アイコン（  ）をクリックします。

ステップ 15 [OK] をクリックします。

ステップ 16 [保存（Save）] をクリックします。

ステップ 17 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

OSPF エリア vlink の追加

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

OSPF 自律システムのすべてのエリアは、物理的にバックボーン エリアと接続されている必要があります。この物理接続が不可能である場合は、vlink を使用して、非バックボーンエリアを経由してバックボーンに接続できます。また vlink を使用して、非バックボーン エリアを経由し、分割されたバックボーンの 2 つの部分を接続することもできます。

vlink を追加するには、最低 2 つの OSPF エリアを追加しておく必要があります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF] をクリックして、OSPF オプションを表示します。

ステップ 7 [エリア（Areas）] の下で、追加アイコン（  ）をクリックします。

ステップ 8 [Vlinks] をクリックします。

ステップ 9 追加アイコン（  ）をクリックします。

ステップ 10 [ルータ ID（Router ID）] フィールドに、ルータの IP アドレスを入力します。

ステップ 11 [認証（Authentication）] ドロップダウン リストから、vlink が使用する認証プロファイルを選択します。

ステップ 12 [Hello インターバル（Hello Interval）] フィールドに、hello メッセージの送信間隔（秒単位）を入力します。

ステップ 13 [再送信間隔（Retrans Interval）] フィールドに、確認応答されていないアップデートの再送信間隔（秒単位）を入力します。

ステップ 14 [待機時間（Wait Time）] フィールドに、ルータが選定の開始と隣接関係の構築の間で待機する秒数を入力します。

ステップ 15 [Dead 間隔（Dead Interval）] フィールドに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を入力します。この値が定義されている場合、dead カウントから計算された値はオーバーライドされます。

ステップ 16 [Dead 回数（Dead Count）] フィールドに、hello 間隔と乗算されるときに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を指定する、数値を入力します。

ステップ 17 [OK] をクリックします。

ステップ 18 [保存（Save）] をクリックします。

ステップ 19 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

OSPF 設定へのインポート フィルタの追加

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

ルート テーブルに対して OSPF からの受け入れまたは拒否を行うルートを定義するために、インポート フィルタを追加できます。インポート フィルタはテーブルに表示される順に適用されます。

インポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] をクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF] をクリックして、OSPF オプションを表示します。

ステップ 7 [インポート フィルタ（Import Filters）] の下で、追加アイコン（）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、インポート フィルタとして追加するフィルタを選択します。

ステップ 9 [アクション（Action）] の横にある [承認（Accept）] または [拒否（Reject）] を選択します。

ステップ 10 [OK] をクリックします。

ヒント インポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（）または下へ移動するアイコン（）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

OSPF 設定へのエクスポート フィルタの追加

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

ルート テーブルから OSPF に対しての受け入れまたは拒否を行うルートを定義するために、エクスポート フィルタを追加できます。エクスポート フィルタはテーブルに表示される順に適用されます。

エクスポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 OSPF 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] タブをクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF] をクリックして、OSPF オプションを表示します。

ステップ 7 [エクスポート フィルタ（Export Filters）] の下で、追加アイコン（）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、エクスポート フィルタとして追加するフィルタを選択します。

ステップ 9 [アクション（Action）] の横にある [承認（Accept）] または [拒否（Reject）] を選択します。

ステップ 10 [OK] をクリックします。

ヒント エクスポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（）または下へ移動するアイコン（）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

仮想ルータのフィルタ

フィルタは、仮想ルータのルートテーブルへのインポートおよびルートのダイナミック プロトコルへのエクスポートを行うために、ルートを照合する方法を提供します。フィルタのリストを作成および管理できます。各フィルタは特定の基準を定義し、静的に定義されるか、またはダイナミック プロトコルから受信したルートを検索します。

仮想ルータ フィルタ テーブルには、仮想ルータに設定した各フィルタのサマリ情報が表示されます（次の表を参照してください）。

表 *66*：仮想ルータ フィルタ テーブル ビューのフィールド

フィールド	説明
[名前（Name）]	フィルタの名前。
プロトコル	ルートが発生するプロトコル。 • [スタティック（Static）]：ルートはローカル スタティック ルートとして発生します。 • [RIP]：ルートはダイナミックな RIP 設定から発生します。 • [OSPF]：ルートはダイナミックな OSPF 設定から発生します。
ルータから（From Router）	このフィルタがルートで一致を試みるルータの IP アドレス。スタティック フィルタおよび RIP フィルタに対してこの値を入力する必要があります。
Next Hop（ネクスト ホップ）	このルートを使用するパケットが転送されるネクスト ホップ。スタティック フィルタおよび RIP フィルタに対してこの値を入力する必要があります。
接続先タイプ（Destination Type）	パケットが送信される宛先のタイプ。 • ルータ • Device • 廃棄（Discard）
宛先ネットワーク（Destination Network）	このフィルタがルートで一致を試みるネットワーク。
OSPF パス タイプ（OSPF Path Type）	OSPF プロトコルにのみ適用されます。パス タイプは次のいずれかです。 • Ext-1 • Ext-2 • エリア間（Inter Area） • 内部エリア（Intra Area）
OSPF ルータ ID（OSPF Router ID）	OSPF プロトコルにのみ適用されます。ルート/ネットワークをアドバタイズするルータのルータ ID。

仮想ルータ フィルタの表示

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

仮想ルータ エディタの[フィルタ（Filter）]タブには、仮想ルータに設定したすべてのフィルタを含むテーブルが表示されます。テーブルには、各フィルタに関するサマリー情報が含まれています。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 表示するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 フィルタを表示する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [フィルタ（Filter）] タブをクリックします。

仮想ルータのフィルタの設定

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

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [フィルタ処理（Filter）] タブをクリックします。

ステップ 6 [フィルタの追加（Add Filter）] をクリックします。

ステップ 7 [名前（Name）] フィールドにフィルタの名前を入力します。英数字のみを使用できます。

ステップ 8 [プロトコル（Protocol）] で、[すべて（All）] を選択するか、フィルタに適用するプロトコルを選択します。

ステップ 9 [プロトコル（Protocol）] として [すべて（All）]、[スタティック（Static）]、または [RIP] を選択した場合は、[ルータから（From Router）] で、このフィルタがルートで一致を試みるルータ IP アドレスを入力します。

（注） IPv4 アドレスに対する /32 の CIDR ブロックと IPv6 アドレスに対する /128 のプレフィクス長も入力可能です。他のすべてのアドレス ブロックは、このフィールドでは無効です。

ステップ 10 [追加（Add）] をクリックします。

ステップ 11 [プロトコル（Protocol）] として [すべて（All）]、[スタティック（Static）]、または [RIP（RIP）] を選択した場合は、[ネクストホップ（Next Hop）] で、このフィルタがルートで一致を試みるゲートウェイの IP アドレスを入力します。

（注） IPv4 アドレスに対する /32 の CIDR ブロックと IPv6 アドレスに対する /128 のプレフィクス長も入力可能です。他のすべてのアドレス ブロックは、このフィールドでは無効です。

ステップ 12 [追加（Add）] をクリックします。

ステップ 13 [送信先のタイプ（Destination Type）] で、フィルタに適用するオプションを選択します。

ステップ 14 [宛先ネットワーク（Destination Network）] で、このフィルタがルートで一致を試みるネットワークの IP アドレスを入力します。

ステップ 15 [追加（Add）] をクリックします。

ステップ 16 [プロトコル（Protocol）] として [すべて（All）] または [OSPF] を選択した場合は、[パスのタイプ（Path Type）] で、フィルタに適用するオプションを選択します。少なくとも 1 つのパス タイプを選択する必要があります。

ステップ 17 [プロトコル（Protocol）] として [OSPF] を選択した場合は、[ルータ ID（Router ID）] で、ルート/ネットワークをアドバタイズするルータのルータ ID の役割を持つ IP アドレスを入力します。

ステップ 18 [追加（Add）] をクリックします。

ステップ 19 [OK] をクリックします。

ステップ 20 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

仮想ルータ認証プロファイルの追加

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

RIP および OSPF の設定で使用する認証プロファイルをセットアップできます。簡易パスワードを設定するか、共有暗号キーを指定できます。簡易パスワードでは、すべてのパケットが 8 バイトのパスワードを伝送できます。システムはこのパスワードが欠如している受信パケットを無視します。暗号キーでは検証が可能で、パスワードから生成される 16 バイト長のダイジェストがすべてのパケットに付加されます。

OSPF の場合、各エリアは異なる認証方式を使用できることに注意してください。そのため、多くのエリア間で共有できる認証プロファイルを作成します。OSPFv3 の認証は追加できません。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [認証プロファイル（Authentication Profile）] をクリックします。

ステップ 6 [認証プロファイルの追加（Add Authentication Profile）] をクリックします。

ステップ 7 [認証プロファイル名（Authentication Profile Name）] フィールドに、認証プロファイルの名前を入力します。

ステップ 8 [認証タイプ（Authentication Type）] ドロップダウン リストから、[単純（simple）] または [暗号化（cryptographic）] を選択します。

ステップ 9 [パスワード（Password）] フィールドに、安全なパスワードを入力します。

ステップ 10 確認のために [パスワードの確認（Confirm Password）] フィールドにもう一度パスワードを入力します。

ステップ 11 [OK] をクリックします。

ステップ 12 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

仮想ルータ統計情報の表示

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

各仮想ルータの実行時統計情報を表示できます。統計情報にはユニキャスト パケット、ドロップされたパケット、IPv4 および IPv6 アドレスの個別のルーティング テーブルが表示されます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 統計情報を表示するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 ルータ統計情報を表示する仮想ルータの横にある表示アイコン（  ）をクリックします。

仮想ルータの削除

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

仮想ルータを削除すると、ルータに割り当てられているすべてのルーテッド インターフェイスを他のルータに含めることができるようになります。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 削除する仮想ルータの横にある削除アイコン（  ）をクリックします。

ステップ 5 入力を求められた場合、仮想ルータを削除することを確認します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 31 章

集約インターフェイスと LACP

以下のトピックでは、集約インターフェイスの設定について、および管理対象デバイスでLACPがどのように機能するかについて説明します。

集約インターフェイスについて

Firepower システムでは、管理対象デバイスがレイヤ 2（ネットワーク間でパケット スイッチングを行う）、またはレイヤ 3（インターフェイス間でトラフィックをルーティングする）に展開されている場合、複数の物理イーサネット インターフェイスを管理対象デバイス上で 1 つの論理リンクにグループ化できます。このように 1 つに集約された論理リンクは、帯域幅と冗長性の向上および、2 つのエンドポイント間でのロードバランシングを実現します。

集約リンクを作成するには、スイッチドまたはルーテッド Link Aggregation Group（LAG）を作成します。集約グループを作成すると、集約インターフェイスと呼ばれる論理インターフェイスが作成されます。上位層エンティティである LAG は単一の論理リンクに似ており、データ トラフィックは集約インターフェイスを介して送信されます。集約リンクは、複数のリンクの帯域幅をまとめて追加することによって帯域幅を増加させます。また、使用可能なすべてのリンクのトラフィックをロードバランシングすることで、冗長性を実現します。リンクの 1 つで障害が発生すると、トラフィックは残りのリンク全体にロードバランシングされます。

LAG のエンドポイントは、7000 または 8000 シリーズ デバイス（上記の図を参照）が 2 つの場合もあれば、一方がサードパーティ アクセス スイッチまたはルータに接続されている 7000 または 8000 シリーズ デバイスの場合もあります。2 つのデバイスは一致している必要はありませんが、同じ物理構成で、IEEE 802.ad リンク アグリゲーション標準規格をサポートしている必要があります。LAG の通常の展開では、2 つの管理対象デバイス間のアクセス リンクを集約するか、管理対象デバイスとアクセス スイッチまたはルータ間にポイントツーポイント接続を確立します。

NGIPSv デバイスや ASA FirePOWER モジュールでは集約インターフェイスを設定することはできません。

LAG 設定

集約インターフェイスには次の 2 種類があります。

- スイッチド：レイヤ 2 集約インターフェイス
- ルーテッド：レイヤ 3 集約インターフェイス

リンク集約は、リンク集約グループ（LAG）を使用して実装します。LAG を設定するには、集約スイッチドまたはルーテッド インターフェイスを作成して、一連の物理インターフェイスをリンクに関連付けます。すべての物理インターフェイスは同じ速度とメディアでなければなりません。

集約リンクは動的または静的に作成します。動的リンク集約では、IEEE 802.ad リンク集約標準のコンポーネットである Link Aggregation Control Protocol（LACP）が使用されますが、静的リンク集約では使用されません。LACP は、LAG の両端の各デバイスでリンクおよびシステムの情報を交換できるようにして、集約でアクティブに使用するリンクを決定します。静的 LAG 構成では、手動でリンク集約を維持し、ロードバランシング ポリシーとリンク選択ポリシーを展開する必要があります。

スイッチドまたはルーテッド集約インターフェイスを作成すると、同じタイプのリンク集約グループが自動的に作成され、それに番号が付けられます。たとえば、最初の LAG（スイッチドまたはルーテッド）を作成すると、その集約インターフェイスは、管理対象デバイスの [インターフェイス（Interfaces）] タブの lag0 ラベルによって識別できます。物理インターフェイスと論理インターフェイスをこの LAG に関連付けると、それらは階層ツリー メニューのプライマリ LAG の下にネスト表示されます。ただし、スイッチド LAG にはスイッチド物理インターフェイスのみを含めることができ、ルーテッド LAG にはルーテッド物理インターフェイスのみを含めることができます。

LAG を設定する際は、以下の要件を考慮してください。

- Firepower システムは、最大 14 の LAG をサポートし、各 LAG インターフェイスに 0 ～ 13 の一意の ID を割り当てます。LAG ID は設定できません。
- リンクの両側に LAG を設定し、どちらの側のインターフェイスも同じ速度に設定する必要があります。

- 各 LAG ごとに少なくとも 2 つの物理インターフェイスを関連付ける必要があります（最大 8 つ）。物理インターフェイスは複数の LAG に属することはできません。
- LAG の物理インターフェイスは、他の動作モードでインラインまたはパッシブとして使用できず、タグ付きトラフィックの別の論理インターフェイスの一部として使用することもできません。
- LAG の物理インターフェイスは複数の NetMods にまたがることが可能ですが、複数のセンサーにまたがることはできません（すべての物理インターフェイスが同じデバイス上に存在する必要があります）。
- LAG にはスタック構成の NetMod を含めることができません。

スイッチド インターフェイスの集約

管理対象デバイスの 2 ～ 8 つの物理ポートを組み合わせて、スイッチド LAG インターフェイスを作成できます。トラフィックを処理できるようにするには、その前に、スイッチド LAG インターフェイスを仮想スイッチに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

ルーテッド インターフェイスの集約

7000 または 8000 シリーズ デバイスの 2 ～ 8 つの物理ポートを組み合わせて、ルーテッド LAG インターフェイスを作成できます。トラフィックをルーティングする前に、ルーテッド LAG インターフェイスを仮想ルータに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

ルーテッド LAG インターフェイスにスタティック Address Resolution Protocol（ARP）エントリを追加できます。外部ホストは、トラフィックの送信先となるローカルネットワーク上の宛先 IP ア

ドレスの MAC アドレスを知る必要がある場合は、ARP 要求を送信します。スタティック ARP エントリを設定する場合、仮想ルータは IP アドレスや関連付けられた MAC アドレスに応答します。

ルーテッド LAG インターフェイスの [ICMP 対応の応答数（ICMP Enable Responses）] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑制されるわけではありません。引き続き、アクセス コントロール ルールを使用して、宛先 IP がルーテッド インターフェイスの IP であり、プロトコルが ICMP である接続を処理することができます。ポートおよび ICMP コードの条件, （347 ページ）を参照してください。

[ローカル ルータ トラフィックを検査する（Inspect Local Router Traffic）] オプションを有効にすると、パケットはホストに到達する前にドロップされるため、あらゆる応答が抑制されます。ローカル ルータ トラフィックの検査の詳細については、デバイスの詳細設定, （469 ページ）を参照してください。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

論理集約インターフェイス

各スイッチドまたはルーテッド集約インターフェイスごとに、複数の論理スイッチド インターフェイスを追加できます。論理 LAG インターフェイスで受信した VLAN タグ付きトラフィックを処理するには、各論理 LAG インターフェイスをその特定のタグに関連付ける必要があります。物理スイッチドまたはルーテッド インターフェイスに追加するのと同じ方法で、論理インターフェイスをスイッチドまたはルーテッド集約インターフェイスに追加します。

（注） LAG インターフェイスを作成すると、デフォルトで「タグなし」論理インターフェイスが作成されます。このインターフェイスは **lag*n.0*** ラベルによって識別されます（***n*** は 0 ～ 13 の整数）。動作させるには、各 LAG にこの論理インターフェイスが少なくとも 1 つ必要です。LAG に追加の論理インターフェイスを関連付けて、VLAN タグ付きトラフィックを処理できます。追加する各論理インターフェイスには固有の VLAN タグが必要です。Firepower System は 1 ～ 4094 の VLAN タグをサポートします。

論理ルーテッドインターフェイスには、シスコ冗長プロトコル（SFRP）を設定することもできます。SFRP では、指定した IP アドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。

論理ルーテッド LAG インターフェイスの [ICMP 有効応答（ICMP Enable Responses）] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑制されるわけではありません。宛先 IP がルーテッド インターフェイスの IP で、プロトコルが ICMP であるパケットをドロップするように、アクセス コントロール ポリシーにネットワークベースのルールを追加できます。

管理対象デバイスの詳細設定である [ローカル ルータ トラフィックの検閲（Inspect Local Router Traffic）] オプションを有効にした場合、パケットはホストに到達する前にドロップされるため、すべての応答を防ぐことができます。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

関連トピック

SFRP, （700 ページ）
デバイスの詳細設定, （469 ページ）
7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

ロード バランシング アルゴリズム

LAG バンドルのメンバー リンクへのトラフィックの分散方法を決定する出口ロード バランシング アルゴリズムを LAG に割り当てます。ロード バランシング アルゴリズムは、レイヤ 2 MAC アドレス、レイヤ 3 IP アドレス、レイヤ 4 ポート番号（TCP/UDP トラフィック）など、さまざまなパケット フィールドの値に基づいてハッシュを決定します。選択したロード バランシング アルゴリズムは、LAG バンドルのメンバー リンクすべてに適用されます。

LAG を設定する場合は、次のオプションから展開シナリオに対応するロード バランシング アルゴリズムを選択します。

- 宛先 IP（Destination IP）
- [宛先 MAC（Destination MAC）]
- [接続先ポート（Destination Port）]

- ソース IP
- [送信元 MAC（Source MAC）]
- 送信元ポート
- [送信元/宛先 IP（Source and Destination IP）]
- [送信元/宛先 MAC（Source and Destination MAC）]
- [送信元/宛先ポート（Source and Destination Port）]

（注） LAG の両端に同じロードバランシング アルゴリズムを設定する必要があります。必要に応じて、上位層のアルゴリズムが下位層のアルゴリズムにバックオフされます（例：ICMP トラフィックに対してレイヤ 3 にバックオフされるレイヤ 4 アルゴリズムなど）。

リンク セレクション ポリシー

リンク アグリゲーションでは、両方のエンドポイントで各リンクの速度とメディアが同じである必要があります。リンク プロパティを動的に変更できるので、リンク選択ポリシーは、システムによるリンク選択プロセスの管理方法を決定する上で役立ちます。最大ポート数を最大化するリンク選択ポリシーはリンク冗長性をサポートし、総帯域幅を最大化するリンク選択ポリシーを全体的なリンク速度をサポートします。安定したリンク選択ポリシーは、リンク状態の過剰な変更を最小限に抑えようとします。

（注） LAG の両端に同じリンク選択ポリシーを設定する必要があります。

次のオプションから展開シナリオに対応するリンク選択ポリシーを選択します。

- [最大ポート数（Highest Port Count）]：冗長性を向上させる最大アクティブ ポート数を割り当てるには、このオプションを選択します。
- [最大合計帯域幅（Highest Total Bandwidth）]：集約リンクに最大合計帯域幅を割り当てるには、このオプションを選択します。
- [安定（Stable）]：最大の課題がリンクの安定性と信頼性である場合は、このオプションを選択します。LAG を設定すると、アクティブ リンクは、ポート数や帯域幅が追加された場合ではなく、どうしても必要な場合（リンク障害などの場合）にのみ変更されます。
- [LACP 優先順位（LACP Priority）]：LAG でアクティブにするリンクを LACP アルゴリズムにより決定するには、このオプションを選択します。この設定は、展開目標が未定義の場合や、LAG の一端のデバイスが Firepower Management Center によって管理されていない場合に適しています。

LACP は、動的リンク アグリゲーションをサポートするリンク選択方式の自動化における主要部分です。LACP を有効にすると、LACP の優先度に基づいたリンク選択ポリシーは LACP の次のプロパティを使用します。

LACP システム プライオリティ

リンク アグリゲーションにおいて優位なデバイスを判断するには、LACP を実行している各パートナー デバイスにこの値を設定します。値が小さいシステムほど、システム プライオリティが高くなります。動的リンク アグリゲーションでは、最初に、LACP システム優先順位の高いシステム側でメンバー リンクに選択された状態が設定され、次に、優先順位の低いシステムでメンバー リンクが適宜設定されます。0 ～ 65535 を指定できます。値を指定しない場合、デフォルトの優先順位は 32768 になります。

LACP リンク優先順位。

集約グループに属する各リンクにこの値を設定します。リンク優先順位によって、LAG におけるアクティブ リンクとスタンバイ リンクが決まります。値が小さいリンクほど優先順位が高くなります。アクティブ リンクがダウンすると、最も優先順位の高いスタンバイ リンクが選択され、ダウンしたリンクと交換されます。ただし、複数のリンクの LACP リンク優先順位が同じである場合は、物理ポート番号が最も小さいリンクがスタンバイ リンクとして選択されます。0 ～ 65535 を指定できます。値を指定しない場合、デフォルトの優先順位は 32768 になります。

リンク集約制御プロトコル（LACP）

IEEE 802.3ad のコンポーネントであるリンク集約制御プロトコル（LACP）は、LAG バンドルを作成して維持するためにシステムおよびポートの情報を交換する 1 つの方式です。LACP を有効にすると、LAG の両端の各デバイスは LACP を使用して、集約においてアクティブに使用されているリンクを特定します。LACP は、リンク間で LACP パケット（または制御メッセージ）を交換することによって、アベイラビリティと冗長性を実現します。このプロトコルは、リンクの能力を動的に学習し、他のポートに通知します。LACP は、適合するリンクを特定すると、それらのリンクを LAG にグループ化します。あるリンクで障害が発生した場合、トラフィックは他のリンクで継続されます。リンクを機能させるには、LAG の両端で LACP を有効にする必要があります。

LACP

LACP を有効にする場合は、LAG の両端で転送モードを指定して、ペアになったデバイス間での LACP パケットの交換方法を指定する必要があります。LACP モードには次の 2 つのオプションがあります。

- [アクティブ（Active）] : デバイスをアクティブ ネゴシエーション ステートにするにはこのモードを選択します。このモードでは、デバイスは LACP パケットを送信することにより、リモート リンクとのネゴシエーションを開始します。

- [パッシブ（Passive）]：デバイスをパッシブ ネゴシエーション ステートにするにはこのモードを選択します。このモードでは、デバイスは受信した LACP パケットには応答しますが、LACP ネゴシエーションを開始しません。

（注） どちらのモードでも、LACPはリンク間でネゴシエートして、それらのリンクがポート速度などの基準に基づいてリンク バンドルを形成可能かどうかを判定できます。ただし、パッシブ対パッシブの構成は避けるようにしてください。そのような構成では、基本的にLAGの両端がリスニング モードになります。

LACPには、デバイス間でのLACPパケットの送信頻度を定義するタイマーがあります。LACPは次のレートでパケットを交換します。

- [低速（Slow）]：30 秒
- [高速（Fast）]：1 秒

このオプションが適用されたデバイスは、LAG の反対側のパートナー デバイスからこの頻度で LACP パケットを受信することを予期します。

（注） LAG がデバイス スタック内の管理対象デバイスに設定されている場合は、プライマリ デバイスだけがパートナー システムとのLACP通信に参加します。すべてのセカンダリ デバイスは、LACP メッセージをプライマリ デバイスに転送します。プライマリ デバイスは、動的な LAG の変更をセカンダリ デバイスにリレーします。

集約スイッチド インターフェイスの追加

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

管理対象デバイスの 2 ～ 8 つの物理ポートを組み合わせて、スイッチドLAGインターフェイスを作成できます。トラフィックを処理できるようにするには、その前に、スイッチドLAGインターフェイスを仮想スイッチに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 スイッチド LAG インターフェイスを設定するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [追加（Add）] ドロップダウン メニューから [集約インターフェイスの追加（Add Aggregate Interface）] を選択します。

ステップ 4 [スイッチド（Switched）] をクリックして、スイッチド LAG インターフェイスのオプションを表示します。

ステップ 5 セキュリティ ゾーンを適用するには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] をクリックして新しいセキュリティ ゾーンを追加します。セキュリティ ゾーン オブジェクトの作成, （392 ページ） を参照してください。

ステップ 6 仮想スイッチを指定します。

- [仮想スイッチ（Virtual Switch）] ドロップダウン リストから既存の仮想スイッチを選択します。
- [新規（New）] を選択して新しい仮想スイッチを追加します。仮想スイッチの追加, （686 ページ） を参照してください。

ステップ 7 [有効（Enabled）] チェックボックスをオンにして、スイッチド LAG インターフェイスがトラフィックを処理できるようにします。
このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8 [モード（Mode）] からリンク モードを指定するオプションを選択するか、または [Autonegotiation] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。
モード設定は銅線インターフェイスにのみ使用できます。

8000 シリーズアプライアンスのインターフェイスは、半二重オプションをサポートしません。リンクが自動的に速度をネゴシエートする場合は、同じ速度設定に基づいて LAG のすべてのアクティブ リンクが選択されます。

ステップ 9 [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または Auto-MDIX のいずれかを指定するオプションを選択します。
[MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。

デフォルトでは、MDI/MDIX は自動 MDI に設定され、MDI と MDIX の間のスイッチングを自動的に処理してリンクを確立します。

ステップ 10 [MTU] フィールドに最大伝送ユニット（MTU）を入力します。
設定可能な MTU の範囲は、Firepower System のデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）を参照してください。

ステップ 11 [リンク アグリゲーション（Link Aggregation）] で、LAG バンドルに追加する物理インターフェイスを [使用できるインターフェイス（Available Interfaces）] から 1 つまたは複数選択します。

ヒント LAG バンドルから物理インターフェイスを削除するには、1つ以上の物理インターフェイスを選択して、選択項目の削除アイコン（  ）をクリックします。LAG バンドルからすべての物理インターフェイスを削除するには、すべてを削除アイコン（）をクリックします。[インターフェイス（Interfaces）] タブから LAG インターフェイスを削除すると、そのインターフェイスも削除されます。

ステップ 12 [ロードバランシング アルゴリズム（Load-Balancing Algorithm）] ドロップダウン リストからオプションを選択します。

ステップ 13 ドロップダウンリストから [リンク選択ポリシー（Link Selection Policy）] を選択します。

ヒント Firepower System デバイスとサードパーティ製ネットワーク デバイスとの間に集約インターフェイスを設定する場合は、[LACP 優先（LACP Priority）] を選択します。

ステップ 14 [リンク選択ポリシー（Link Selection Policy）] に [LACP 優先（LACP Priority）] を選択した場合は、[システム優先度（System Priority）] に値を割り当て、[インターフェイスの優先度の設定（Configure Interface Priority）] リンクをクリックして優先度の値を LAG の各インターフェイスに割り当てます。

ステップ 15 [トンネルレベル（Tunnel Level）] ドロップダウン リストから [内部（Inner）] または [外部（Outer）] を選択します。

（注） レイヤ 3 ロードバランシングが設定されている場合、トンネル レベルは IPv4 トラフィックにのみ適用されます。外部トンネルは常に、レイヤ 2 と IPv6 トラフィックに使用されます。[トンネル レベル（Tunnel Level）] が明示的に設定されていない場合、デフォルトは [外部（Outer）] になります。

ステップ 16 [LACP] で [有効（Enabled）] チェックボックスをオンにして、スイッチド LAG インターフェイスがリンク集約制御プロトコルを使用してトラフィックを処理できるようにします。
このチェックボックスをオフにすると、LAG インターフェイスは静的設定になり、Firepower System は選択されたすべての物理インターフェイスを集約に使用します。

ステップ 17 [レート（Rate）] オプション ボタンをクリックし、パートナー デバイスから LACP 制御メッセージを受信する頻度を設定します。

- パケットを 30 秒ごとに受信するには、[遅い（Slow）] をクリックします。
- パケットを 1 秒ごとに受信するには、[速い（Fast）] をクリックします。

ステップ 18 [モード（Mode）] オプション ボタンをクリックし、デバイスのリスニング モードを設定します。

- パートナー デバイスに LACP パケットを送信してリモート リンクとのネゴシエーションを開始するには、[アクティブ（Active）] をクリックします。

- 受信した LACP パケットに応答するには、[パッシブ（Passive）] をクリックします。

ステップ 19 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

集約ルーテッド インターフェイスの追加

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

管理対象デバイスの 2 ～ 8 つの物理ポートを組み合わせて、ルーテッド LAG インターフェイスを作成できます。トラフィックをルーティングする前に、ルーテッド LAG インターフェイスを仮想ルータに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

注意 7000 または 8000 シリーズ デバイス 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。 でのルーテッド インターフェイス ペアの追加

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 ルーテッド LAG インターフェイスを設定するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [追加（Add）] ドロップダウン メニューから [集約インターフェイスの追加（Add Aggregate Interface）] を選択します。

ステップ 4 [Routed] をクリックして、ルーテッド LAG インターフェイス オプションを表示します。

ステップ 5 セキュリティ ゾーンを適用するには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して新しいセキュリティ ゾーンを追加します。セキュリティ ゾーン オブジェクトの作成, （392 ページ） を参照してください。

ステップ 6 仮想ルータを指定します。

- [仮想ルータ（Virtual Router）] ドロップダウン リストから既存の仮想ルータを選択します。
- [新規（New）] を選択して新しい仮想ルータ 仮想ルータの追加, （703 ページ）を追加します。

ステップ 7 [有効（Enabled）] チェックボックスをオンにして、ルーテッド LAG インターフェイスがトラフィックを処理できるようにします。
このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8 [モード（Mode）] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [Autonegotiation] を選択して、速度とデュプレックス設定を自動的にネゴシエートするよう LAG インターフェイスを設定します。
モード設定は銅線インターフェイスにのみ使用できます。

8000 シリーズアプライアンスのインターフェイスは、半二重オプションをサポートしません。リンクが自動的に速度をネゴシエートする場合は、同じ速度設定に基づいて LAG のすべてのアクティブ リンクが選択されます。

ステップ 9 [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または Auto-MDIX のいずれかを指定するオプションを選択します。
[MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。

デフォルトでは、MDI/MDIX は自動 MDI に設定され、MDI と MDIX の間のスイッチングを自動的に処理してリンクを確立します。

ステップ 10 [MTU] フィールドに最大伝送ユニット（MTU）を入力します。
MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

ステップ 11 LAG インターフェイスが ping や traceroute のような ICMP トラフィックに応答できるようにするには、[ICMP] の横にある [応答を有効にする（Enable Responses）] チェックボックスをオンにします。

ステップ 12 LAG インターフェイスがルータアドバタイズメントをブロードキャストできるようにするには、[IPv6 NDP] の横にある [ルータアドバタイズメントを有効にする（Enable Router Advertisement）] チェックボックスをオンにします。

ステップ 13 [追加（Add）] をクリックして、IP アドレスを追加します。

ステップ 14 [アドレス（Address）] フィールドで、CIDR 表記を使用して、ルーテッド LAG インターフェイスの IP アドレスとサブネット マスクを入力します。
次の点に注意してください。

- ネットワークおよびブロードキャスト アドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 15 IPv6 を使用した環境で、LAG インターフェイスの IP アドレスを自動設定するには、[IPv6] フィールドの横にある [アドレスの自動設定（Address Autoconfiguration）] チェックボックスをオンにします。

ステップ 16 [タイプ（Type）] には、[普通（Normal）] または [SFRP] を選択します。

ステップ 17 [タイプ（Type）] に SFRP を選択した場合は、SFRP, （700 ページ）の説明に従いオプションを設定してください。

ステップ 18 [OK] をクリックします。

（注） IP アドレスを 7000 または 8000 シリーズデバイスの高可用性ペアのルーテッド インターフェイスに追加する場合、高可用性ピアのルーテッド インターフェイスに対応する IP アドレスを追加する必要があります。

ステップ 19 [追加（Add）] をクリックして、スタティック ARP エントリを追加します。

ステップ 20 [IP アドレス（IP Address）] フィールドに IP アドレスを入力します。

ステップ 21 [MAC アドレス（MAC Address）] フィールドに IP アドレスに関連付ける MAC アドレスを入力します。標準形式を使用します（たとえば、01:23:45:67:89:AB）。

ステップ 22 [OK] をクリックします。

ステップ 23 [リンク アグリゲーション（Link Aggregation）] で、LAG バンドルに追加する物理インターフェイスを [使用できるインターフェイス（Available Interfaces）] から 1 つまたは複数選択します。

ヒント　LAGバンドルから物理インターフェイスを削除するには、1つ以上の物理インターフェイスを選択して、選択項目の削除アイコン（  ）をクリックします。LAG バンドルからすべての物理インターフェイスを削除するには、すべてを削除アイコン（  ）をクリックします。[インターフェイス（Interfaces）] タブから LAG インターフェイスを削除すると、そのインターフェイスも削除されます。

ステップ 24　ドロップダウンリストから [ロードバランシング アルゴリズム（Load-Balancing Algorithm）] を選択します。

ステップ 25　ドロップダウンリストから [リンク選択ポリシー（Link Selection Policy）] を選択します。

ヒント　Firepower System デバイスとサードパーティ製ネットワーク デバイスとの間に集約インターフェイスを設定する場合は、[LACP 優先（LACP Priority）] を選択します。

ステップ 26　[リンク選択ポリシー（Link Selection Policy）] に [LACP 優先（LACP Priority）] を選択した場合は、[システム優先度（System Priority）] に値を割り当て、[インターフェイスの優先度の設定（Configure Interface Priority）] リンクをクリックして優先度の値を LAG の各インターフェイスに割り当てます。

ステップ 27　[トンネルレベル（Tunnel Level）] ドロップダウン リストから [内部（Inner）] または [外部（Outer）] を選択します。

（注）　レイヤ 3 ロードバランシングが設定されている場合、トンネル レベルは IPv4 トラフィックにのみ適用されます。外部トンネルは常に、レイヤ 2 と IPv6 トラフィックに使用されます。[トンネル レベル（Tunnel Level）] が明示的に設定されていない場合、デフォルトは [外部（Outer）] になります。

ステップ 28　[LACP] で [有効（Enabled）] チェックボックスをオンにして、ルーテッド LAG インターフェイスがリンク集約制御プロトコルを使用してトラフィックを処理できるようにします。
このチェックボックスをオフにすると、LAGインターフェイスは静的設定になり、Firepower System はすべての物理インターフェイスを集約に使用します。

ステップ 29　[レート（Rate）] オプション ボタンをクリックし、パートナー デバイスから LACP 制御メッセージを受信する頻度を設定します。

- パケットを 30 秒ごとに受信するには、[遅い（Slow）] をクリックします。
- パケットを 1 秒ごとに受信するには、[速い（Fast）] をクリックします。

ステップ 30　[モード（Mode）] オプション ボタンをクリックし、デバイスのリスニング モードを設定します。

- パートナー デバイスに LACP パケットを送信してリモート リンクとのネゴシエーションを開始するには、[アクティブ（Active）] をクリックします。
- 受信した LACP パケットに応答するには、[パッシブ（Passive）] をクリックします。

ステップ 31　[保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

デバイスの詳細設定，（469 ページ）

論理集約インターフェイスの追加

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

各スイッチドまたはルーテッド集約インターフェイスごとに、複数の論理インターフェイスを追加できます。論理 LAG インターフェイスで受信した VLAN タグ付きトラフィックを処理するには、各論理LAGインターフェイスをその特定のタグに関連付ける必要があります。物理スイッチドまたはルーテッド インターフェイスに追加するのと同じ方法で、論理インターフェイスをスイッチドまたはルーテッド集約インターフェイスに追加します。

（注） LAG インターフェイスを作成すると、デフォルトで「タグなし」論理インターフェイスが作成されます。このインターフェイスは **lag*n.0*** ラベルによって識別されます（***n*** は 0 ～ 13 の整数）。動作させるには、各LAGにこの論理インターフェイスが少なくとも1つ必要です。LAG に追加の論理インターフェイスを関連付けて、VLANタグ付きトラフィックを処理できます。追加する各論理インターフェイスには固有の VLAN タグが必要です。Firepower System は 1 ～ 4094 の VLAN タグをサポートします。

注意 7000 または 8000 シリーズ デバイス 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作，（326 ページ）を参照してください。 でのルーテッド インターフェイス ペアの追加

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 論理 LAG インターフェイスを追加するデバイスの横にある、編集アイコン（ ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [追加（Add）] ドロップダウン メニューから、[論理インターフェイスの追加（Add Logical Interface）] を選択します。

ステップ 4 [スイッチド（Switched）]をクリックしてスイッチドインターフェイス オプションを表示するか、[ルーテッド（Routed）] をクリックしてルーテッド インターフェイス オプションを表示します。

ステップ 5 [インターフェイス（Interface）] ドロップダウン リストから使用可能な LAG を選択します。集約インターフェイスは **lag*n*** ラベルによって識別されます（***n*** は 0 ～ 13 の整数）。

ステップ 6 選択したインターフェイスのタイプに適した残りの設定を行います。

- スイッチド：スイッチドインターフェイスへの論理インターフェイスの追加方法の詳細については、論理スイッチドインターフェイスの追加, （683 ページ）を参照してください。
- ルーテッド：ルーテッドインターフェイスへの論理インターフェイスの追加方法の詳細については、論理ルーテッドインターフェイスの追加, （696 ページ）を参照してください。

関連トピック

SFRP, （700 ページ）
デバイスの詳細設定, （469 ページ）
7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

集約インターフェイス統計情報の表示

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

各集約インターフェイスのプロトコルおよびトラフィックの統計情報を表示できます。統計情報には、LACP キーとパートナー情報などの LACP プロトコル情報、受信パケット、転送パケット、ドロップパケットが表示されます。統計情報は、メンバーインターフェイスごとに詳細化されており、ポート単位でトラフィックとリンクの情報が表示されます。

集約インターフェイス情報は、事前定義されたウィジェットを介してダッシュボードにも表示されます。[現在のインターフェイス ステータス（Current Interface Status）] ウィジェットは、有効になっているか未使用のアプライアンスのすべてのインターフェイスのステータスを示します。Interface Traffic ウィジェットには、ダッシュボードの時間範囲においてアプライアンスのインターフェイスで送受信された受信（Rx）トラフィックと送信（Tx）トラフィックの割合が示されます。定義済みダッシュボード ウィジェット, （227 ページ）を参照してください。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 論理集約インターフェイス統計情報を表示するデバイスの横にある、編集アイコン（）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 インターフェイス統計情報を表示するインターフェイスの横にある、表示アイコン（  ）をクリックします。

集約インターフェイスの削除

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

集約インターフェイスは **lag*n*** ラベルによって識別できます（***n*** は 0 ～ 13 の整数）。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 集約インターフェイスを削除するデバイスの横にある、編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 削除する集約インターフェイスの横にある、削除アイコン（  ）をクリックします。

ステップ 4 プロンプトが表示されたら、集約インターフェイスを削除することを確認します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

第 32 章

ハイブリッド インターフェイス

次のトピックでは、ローカル ハイブリッド インターフェイスの設定方法を示します。

ハイブリッド インターフェイスについて

管理対象デバイス上に論理ハイブリッドインターフェイスを設定することで、Firepower システムが仮想ルータと仮想スイッチの間でトラフィックをブリッジできるようになります。仮想スイッチのインターフェイスで受信した IP トラフィックの宛先が、そのスイッチに関連付けられた論理ハイブリッドインターフェイスの MAC アドレスとなっている場合、システムは、そのトラフィックをレイヤ 3 トラフィックとして処理し、宛先 IP アドレスに応じてトラフィックをルーティングするかトラフィックに応答します。それ以外の宛先が設定されたトラフィックを受信した場合、システムはそのトラフィックをレイヤ 2 トラフィックとして処理し、適切なスイッチングを行います。NGIPSv デバイス上で論理ハイブリッド インターフェイスを設定することはできません。

仮想スイッチと仮想ルータの両方に関連付けられていないハイブリッド インターフェイスは、ルーティングに使用できず、トラフィックを生成することも、トラフィックに応答することもありません。

論理ハイブリッド インターフェイス

レイヤ 2 とレイヤ 3 の間でトラフィックを中継するには、論理ハイブリッド インターフェイスを仮想ルータと仮想スイッチに関連付ける必要があります。仮想スイッチに関連付けることができるハイブリッドインターフェイスは 1 つだけです。一方、仮想ルータには複数のハイブリッドインターフェイスを関連付けることができます。

論理ハイブリッドインターフェイスには、シスコ冗長プロトコル（SFRP）を設定することもできます。SFRP では、指定した IP アドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。

ハイブリッド インターフェイスの [ICMP 有効応答（ICMP Enable Responses）] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑止されるわけではありません。宛先 IP がハイブリッドインターフェイスの IP で、プロトコルが ICMP であるパケットをドロップするように、アクセス コントロール ポリシーにネットワークベースのルールを追加できます。

管理対象デバイスの [ローカル ルータ トラフィックの検閲（Inspect Local Router Traffic）] オプションを有効にした場合、パケットはホストに到達する前にドロップされるため、すべての応答を防ぐことができます。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

関連トピック

SFRP の設定, （700 ページ）
デバイスの詳細設定, （469 ページ）
7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

論理ハイブリッドインターフェイスの追加

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

注意 7000 または 8000 シリーズ デバイス 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。 でのルーテッド インターフェイス ペアの追加

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 ハイブリッドインターフェイスを追加するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [追加（Add）] ドロップダウン メニューから、[論理インターフェイスの追加（Add Logical Interface）] を選択します。

ステップ 4 [ハイブリッド（Hybrid）] をクリックして、ハイブリッド インターフェイス オプションを表示します。

ステップ 5 [名前（Name）] フィールドに、インターフェイスの名前を入力します。

ステップ 6 [仮想ルータ（Virtual Router）] ドロップダウン リストから既存の仮想ルータを選択し、[なし（None）] を選択するか、または [新規（New）] を選択して新しい仮想ルータを追加します。
（注） 新しい仮想ルータを追加する場合は、ハイブリッド インターフェイスのセットアップが完了した後に、[デバイス管理（Device Management）] ページで、その仮想ルータを設定する必要があります。仮想ルータの追加, （703 ページ）を参照してください。

ステップ 7 [仮想スイッチ（Virtual Switch）] ドロップダウン リストから既存の仮想スイッチを選択し、[なし（None）] を選択するか、または [新規（New）] を選択して新しい仮想スイッチを追加します。
（注） 新しい仮想スイッチを追加する場合は、ハイブリッド インターフェイスのセットアップが完了した後に、[デバイス管理（Device Management）] ページで、その仮想スイッチを設定する必要があります。仮想スイッチの追加, （686 ページ）を参照してください。

ステップ 8 ハイブリッド インターフェイスにトラフィックを処理させるには、[有効（Enabled）] チェックボックスをオンにします。
（注） このチェックボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。

ステップ 9 [MTU] フィールドに、最大伝送ユニット（MTU）を入力して、パケットの最大許容サイズを指定します。
MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

ステップ 10 [ICMP] の横にある [応答を有効にする（Enable Responses）] チェックボックスをオンにして、インターフェイスを ping や traceroute などの ICMP トラフィックに応答可能にします。

ステップ 11 [IPv6 NDP] の横にある [ルータ アドバタイズメントを有効にする（Enable Router Advertisement）] チェックボックスをオンにして、インターフェイスがルータ アドバタイズメントを伝送できるようにします。このオプションを有効にできるのは、IPv6 アドレスを追加した場合のみです。

ステップ 12 IP アドレスを追加するには、[追加（Add）] をクリックします。

ステップ 13 [アドレス（Address）] フィールドに、IP アドレスとサブネット マスクを入力します。次の点に注意してください。

- ネットワークおよびブロードキャスト アドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 14 IPv6 アドレスがある場合、オプションで、[IPv6] フィールドの横にある [アドレスの自動設定（Address Autoconfiguration）] チェックボックスをオンにして、インターフェイスの IP アドレスを自動的に設定します。

ステップ 15 [タイプ（Type）] には、[普通（Normal）] または [SFRP] を選択します。

ステップ 16 [タイプ（Type）] に SFRP を選択した場合は、SFRP, （700 ページ）の説明に従いオプションを設定してください。

ステップ 17 [OK] をクリックします。

ステップ 18 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲, （495 ページ）
Snort® の再起動シナリオ , （324 ページ）

論理ハイブリッド インターフェイスの削除

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

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）]を選択します。

ステップ 2 論理ハイブリッドインターフェイスを削除するデバイスの横にある編集アイコン（  ）をクリックします。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 削除する論理ハイブリッドインターフェイスの横にある削除アイコン（  ）をクリックします。

ステップ 4 入力を求められた場合、インターフェイスを削除することを確認します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 33 章

ゲートウェイ VPN

次のトピックでは、VPN 展開を管理する方法について説明します。

ゲートウェイ VPN の基本

バーチャルプライベートネットワーク（VPN）は、インターネットや他のネットワークなどのパブリック ソースを介したエンドポイント間でセキュアなトンネルを確立するネットワーク接続です。Firepower管理対象デバイスの仮想ルータ間にセキュアVPNトンネルを確立するようにFirepowerシステムを設定できます。システムは、インターネットプロトコルセキュリティ（IPsec）プロトコル スイートを使用してトンネルを構築します。

VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストはセキュアな VPN トンネルを介して、リモート ゲートウェイの背後にあるホストに接続することができます。接続は、2 つのゲートウェイの IP アドレスとホスト名、その背後のサブネット、および相互認証のための 2 つのゲートウェイの共有秘密で構成されます。

VPN エンドポイントは、Internet Key Exchange（IKE）のバージョン 1 またはバージョン 2 のいずれかのプロトコルを使用して相互に認証し、トンネルに対してセキュリティ アソシエーションを作成します。システムは IPsec Authentication Header（AH）プロトコルまたは IPsec Encapsulating Security Payload（ESP）プロトコルのいずれかを使用して、トンネルに入るデータを認証します。ESP プロトコルは、AH と同じ機能を提供する他にデータの暗号化も行います。

展開にアクセス コントロール ポリシーが存在する場合、システムは、VPN トラフィックがアクセス コントロールを通過するまで VPN トラフィックを送信しません。さらに、システムは、トンネルがダウンしている場合は、トンネル トラフィックをパブリックなソースに送信しません。

VPN を Firepower 用に設定して展開するには、展開先の各管理対象デバイスで VPN ライセンスを有効にしておく必要があります。また、VPN 機能は 7000 および 8000 シリーズ デバイスでのみ使用できます。

IPsec

IPsec プロトコル スイートは、VPN トンネルにおいて、IP パケットが ESP または AH セキュリティ プロトコルでどのようにハッシュ、暗号化、およびカプセル化されるかを定義します。Firepower システムはハッシュ アルゴリズムおよび Security Association（SA）の暗号キーを使用しますが、これは、Internet Key Exchange（IKE）プロトコルによって 2 つのゲートウェイ間で確立されています。

セキュリティ アソシエーション（SA）は2つのデバイス間で共有のセキュリティ属性を確立し、VPN エンドポイントがセキュアな通信をサポートできるようにします。SA は、2 つの VPN エンドポイントが、VPN トンネルがどのようにセキュアにされているかを表すパラメータを処理することができます。

システムは、IPsec 接続のネゴシエーションの最初の段階で Internet Security Association and Key Management Protoco（ISAKMP）を使用し、エンドポイントと認証キー交換の間で VPN を確立します。IKE プロトコルは ISAKMP 内にあります。

AHセキュリティプロトコルは、パケット見出しとデータを保護しますが、暗号化はできません。ESP はパケットを暗号化および保護しますが、最も外側の IP 見出しをセキュアにすることはできません。多くの場合、この保護は必要なく、大半の VPN 展開は、（暗号化の機能により）AH よりも頻繁に ESP を使用します。VPN はトンネル モードのみで動作するため、システムはレイヤ 3 からのパケット全体を暗号化および認証し、ESP プロトコル内で稼動します。トンネル モードの ESP は、後者の暗号化機能だけでなく、データを暗号化します。

IKE

Firepower システムは IKE プロトコルを使用して、トンネルに対して SA をネゴシエートする他に、2つのゲートウェイを相互に認証します。プロセスは、次の2つのフェーズで構成されます。

IKE フェーズ 1 では、Diffie-Hellman キー交換によってセキュアに認証された通信チャネルを確立し、その後の IKE 通信を暗号化するために事前共有キーを生成します。このネゴシエーションにより、双方向の ISAKMP セキュリティ アソシエーションが生じます。ユーザは、事前共有キーを使用して認証を行うことができます。フェーズ 1 はメイン モードで機能します。このフェーズでは、ネゴシエーションの間にすべてのデータを保護しようとしますが、ピアのアイデンティティも保護します。

IKE フェーズ 2 では、IKE ピアが、フェーズ 1 で確立されたセキュアなチャネルを使用して、IPsec の代わりにセキュリティ アソシエーションにネゴシエートします。ネゴシエーションにより、最低 2 つの単方向セキュリティ アソシエーション（一方は着信、他方は発信）が生じます。

VPN 展開

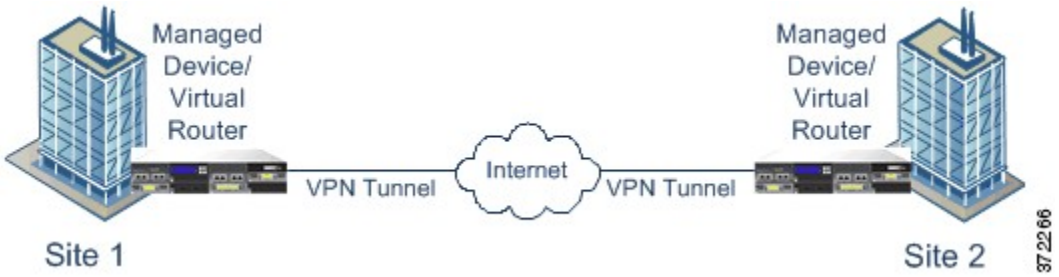
VPN展開は、VPNに含まれているエンドポイントおよびネットワークを指定し、またそれらが相互にどのように接続しているかを指定します。VPN 展開を Firepower Management Center に設定すると、次に管理対象デバイス、または別の Firepower Management Center によって管理されているデバイスにその VPN 展開を導入できます。

システムでは、ポイントツーポイント、スター、およびメッシュという 3 つのタイプの VPN 展開がサポートされています。

ポイントツーポイントの VPN 展開

ポイントツーポイントの VPN 展開では、2 つのエンドポイントが相互に直接通信します。2 つのエンドポイントをピア デバイスとして設定し、いずれかのデバイスでセキュアな接続を開始することができます。この設定の各デバイスは、VPN 対応の管理対象デバイスであることが必要です。

次の図は、一般的なポイントツーポイントの VPN 展開を示しています。



スター VPN 導入

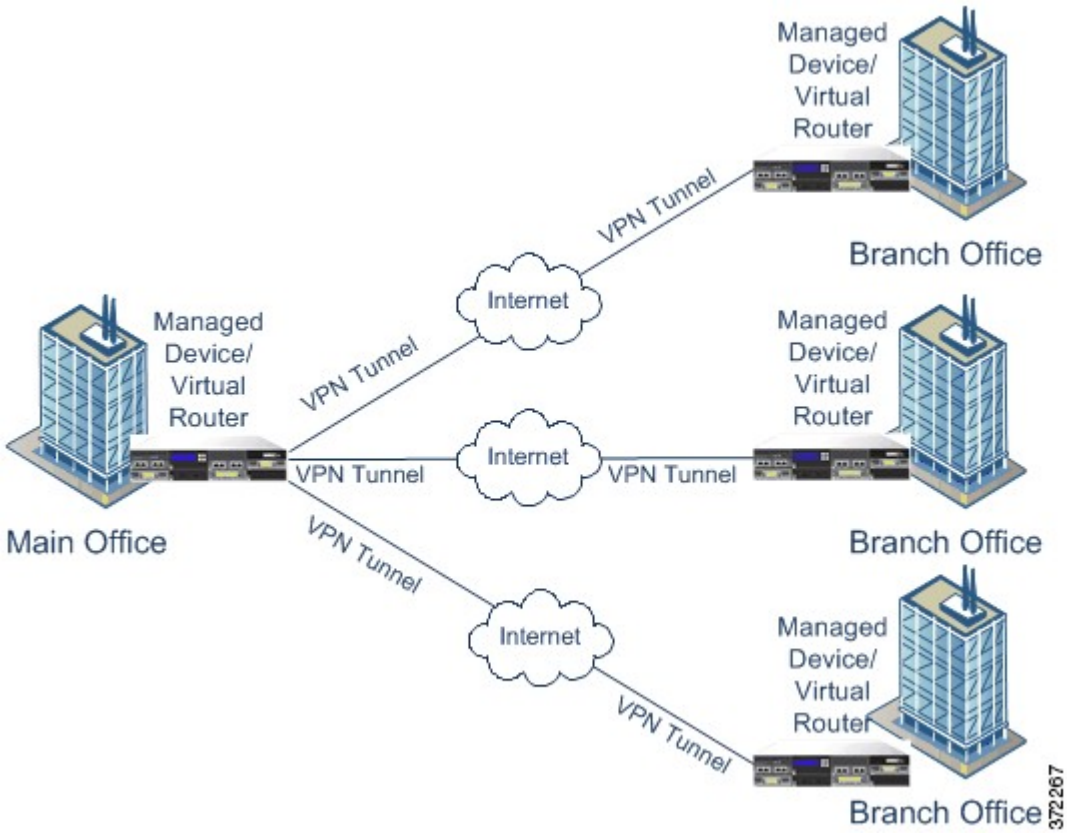
スター VPN 導入では、中央のエンドポイント（ハブ ノード）が、複数のリモート エンドポイント（リーフ ノード）とのセキュアな接続を確立します。ハブ ノードと個々のリーフ ノード間のそれぞれの接続は、別の VPN トンネルです。いずれかのリーフ ノードの背後にあるホストは、ハブ ノードを介して互いに通信できます。

スター型の展開は一般的に、インターネットや他のサードパーティのネットワークを介してセキュアな接続を使用している組織の本店と支店を接続する VPN を表します。スター VPN 導入は、すべての従業員に対して、組織のネットワークへのコントロールされたアクセスを提供します。

一般的なスター型の導入では、ハブ ノードは本社に配置します。リーフ ノードは支社に配置します。トラフィックの大部分は、これらのリーフ ノードから開始されます。各ノードは、VPN 対応の管理対象デバイスであることが必要です。

スター型の導入は、IKE バージョン 2 のみをサポートします。

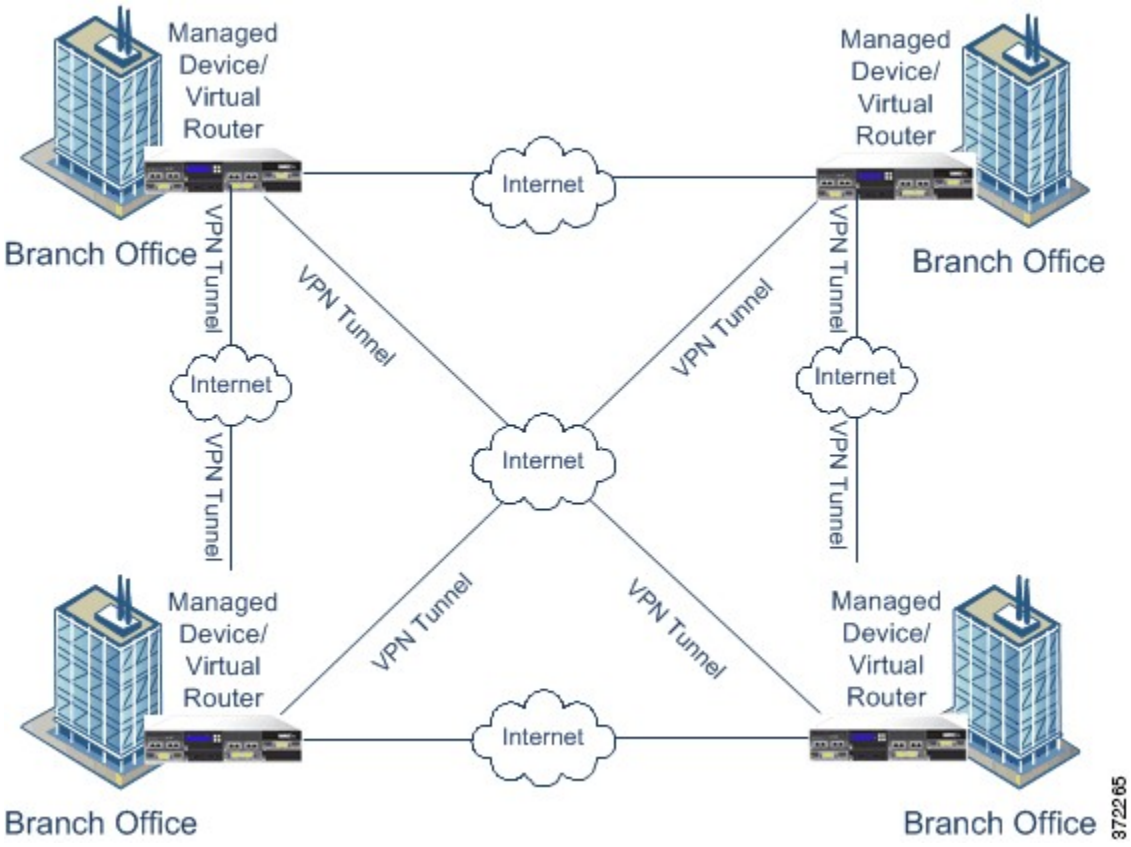
次の図は、一般的なスター VPN 導入を示しています。



メッシュ VPN 展開

メッシュ VPN 展開では、すべてのエンドポイントが個々の VPN トンネルによって他のエンドポイントと通信できます。メッシュ型の展開では 1 つのエンドポイントで障害が発生しても残りのエンドポイントが相互に通信できるように、冗長性を備えています。このタイプの展開は一般的に、分散した支店が配置されたグループを接続する VPN を表します。この設定で展開する VPN 対応の管理対象デバイスの数は、必要な冗長性のレベルによって異なります。各エンドポイントは、VPN 対応の管理対象デバイスであることが必要です。

次の図は、一般的なメッシュ VPN 展開を示しています。



VPN 展開の管理

[VPN] ページ（[デバイス（Devices）] > [VPN]）で、現行のすべての VPN 展開を、展開に含まれている名前およびエンドポイントごとに表示することができます。このページ内のオプションを使用して、VPN 展開のステータスを表示する、新しい展開を作成する、管理対象デバイスに展開する、展開を修正または削除する、といった操作を実行することができます。

デバイスを Firepower Management Center に登録すると、登録中に、展開済みの VPN が Firepower Management Center と同期されることに注意してください。

関連トピック

VPN 展開の管理, （767 ページ）

VPN 展開オプション

新しい VPN 展開を作成する場合には、最小限の処理として、一意の名前と展開のタイプを指定し、事前共有キーを指定する必要があります。次の 3 つのタイプの展開から選択することができ、それぞれの展開には VPN トンネルが含まれています。

- ポイントツーポイント（PTP）型の展開は、2 つのエンドポイント間で VPN トンネルを確立します。

- スター型の展開は VPN トンネルのグループを確立し、ハブ エンドポイントをリーフ エンドポイントのグループに接続します。
- メッシュ型の展開は、エンドポイントのセット内でVPNトンネルのグループを確立します。

VPN 展開でエンドポイントとして使用できるのは、Cisco の管理対象デバイスのみです。サードパーティ製のエンドポイントはサポートされません。

VPN 認証に対して事前共有キーを定義する必要があります。展開内で生成したすべての VPN 接続で使用するデフォルトのキーを指定できます。ポイントツーポイント型の展開では、各エンドポイントのペアに事前共有キーを指定できます。

マルチドメイン展開では、ドメイン間でVPN展開を構成できます。つまり、異なるドメインに属するデバイスにエンドポイントを割り当てることができます。このような場合は、関連する子孫ドメインで先祖の展開を表示できますが、変更することはできません。ドリルダウンして展開の詳細を表示すると、現在のドメインに属するデバイスの情報のみが表示されます。

ポイントツーポイント VPN 展開オプション

ポイントツーポイント VPN 展開を設定する場合は、エンドポイント ペアのグループを定義し、各ペアの 2 つのノード間に VPN を作成します。

次に、展開で指定できるオプションについて示します。

[名前（Name）]

展開の一意の名前を指定します。

タイプ（Type）

ポイントツーポイント型の展開を設定するには、[PTP] をクリックします。

事前共有キー（Pre-Shared Key）

認証に対して一意の事前共有キーを定義します。各エンドポイント ペアに対して事前共有キーを指定しない場合は、システムで展開内のすべての VPN に対してこのキーが使用されます。

Device

展開のエンドポイントとして、デバイス スタックやデバイス高可用性ペアなどの管理対象デバイスを選択できます。使用している Firepower Management Center で管理されていないシスコの管理対象デバイスの場合は、[その他（Other）] を選択し、エンドポイントの IP アドレスを指定します。

[仮想ルータ（Virtual Router）]

エンドポイントとして管理対象デバイスを選択する場合は、選択したデバイスに現在適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

インターフェイス（Interface）

エンドポイントとして管理対象デバイスを選択した場合は、指定した仮想ルータに割り当てられているルーテッド インターフェイスを選択します。

[IPアドレス（IP Address）]

- エンドポイントとして管理対象デバイスを選択する場合は、指定されたルーテッド インターフェイスに割り当てられている IP アドレスを選択します。
- 管理対象デバイスがデバイス高可用性ペアの場合は、SFRP IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスが Firepower Management Center で管理されて**いない**場合は、エンドポイントに IP アドレスを指定します。

[保護されたネットワーク（Protected Networks）]

暗号化された展開でネットワークを指定します。各ネットワークに対して CIDR ブロックでサブネットを入力します。IKE バージョン 1 は、保護された単一のネットワークのみサポートしています。

VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイント ペアの保護されたネットワークは重複することはできないことに注意してください。エンドポイントについて保護されたネットワークのリストに 1 つ以上の IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ（IPv4 または IPv6）のエントリを少なくとも 1 つ持っていることが必要です。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です。（IPv4 については /32 CIDR アドレスを使用し、IPv6 については /128 CIDR アドレス ブロックを使用します）。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

[内部 IP（Internal IP）]

エンドポイントが、ネットワーク アドレス変換を備えたファイアウォールの背後に配置されている場合は、このチェックボックスをオンにします。

[パブリック IP（Public IP）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、ファイアウォールに対してパブリック IP アドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

[パブリック IKE ポート（Public IKE Port）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、内部のエンドポイントにポート転送されているファイアウォール上の UDP ポートに対して、1 ～ 65535 の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが 500 または 4500 ではない場合、この値を指定する必要があります。

[実装キーを使用する（Use Deployment Key）]

展開に対して定義されている事前共有キーを使用する場合は、チェックボックスをオンにします。このエンドポイント ペアに対して VPN 認証の事前共有キーを指定するには、チェックボックスをオフにします。

事前共有キー（Pre-Shared Key）

[実装キーを使用する（Use Deployment Key）] チェックボックスをオフにした場合は、このフィールドに事前共有キーを指定します。

関連トピック

ポイントツーポイント VPN 展開の設定, （768 ページ）

スター VPN の展開オプション

スター VPN 展開を設定する場合は、1 つのハブ ノード エンドポイント、およびリーフ ノード エンドポイントのグループを定義します。展開を設定するには、ハブ ノードエンドポイントと、少なくとも 1 つのリーフ ノード エンドポイントを定義する必要があります。

次に、展開で指定できるオプションについて示します。

[名前（Name）]

展開の一意の名前を指定します。

タイプ（Type）

スター型の展開を設定するには、[スター（Star）] をクリックします。

事前共有キー（Pre-Shared Key）

認証に対して一意の事前共有キーを定義します。

Device

展開のエンドポイントとして、デバイス スタックやデバイス高可用性ペアなどの管理対象デバイスを選択できます。使用している Firepower Management Center で管理されていないシスコの管理対象デバイスの場合は、[その他（Other）] を選択し、エンドポイントの IP アドレスを指定します。

[仮想ルータ（Virtual Router）]

エンドポイントとして管理対象デバイスを選択する場合は、選択したデバイスに現在適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

インターフェイス（Interface）

エンドポイントとして管理対象デバイスを選択する場合は、選択した仮想ルータに割り当てられているルーテッド インターフェイスを選択します。

[IPアドレス（IP Address）]

- エンドポイントとして管理対象デバイスを選択する場合は、指定されたルーテッド インターフェイスに割り当てられている IP アドレスを選択します。
- 管理対象デバイスがデバイス高可用性ペアの場合は、SFRP IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスが Firepower Management Center で管理されて**いない**場合は、エンドポイントに IP アドレスを指定します。

[保護されたネットワーク（Protected Networks）]

暗号化された展開でネットワークを指定します。各ネットワークに対してCIDRブロックでサブネットを入力します。

VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイント ペアの保護されたネットワークは重複することはできないことに注意してください。エンドポイントについて保護されたネットワークのリストに 1 つ以上の IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ（IPv4 または IPv6）のエントリを少なくとも 1 つ持っていることが必要です。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です。（IPv4 については /32 CIDR アドレスを使用し、IPv6 については /128 CIDR アドレス ブロックを使用します）。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

[内部 IP（Internal IP）]

エンドポイントが、ネットワーク アドレス変換を備えたファイアウォールの背後に配置されている場合は、このチェックボックスをオンにします。

[パブリック IP（Public IP）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、ファイアウォールに対してパブリック IP アドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

[パブリック IKE ポート（Public IKE Port）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、内部のエンドポイントにポート転送されているファイアウォール上の UDP ポートに対して、1 ～ 65535 の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが 500 または 4500 ではない場合、この値を指定する必要があります。

関連トピック

スター VPN 展開の設定, （768 ページ）

メッシュ VPN 展開オプション

メッシュ VPN 展開を設定する場合は、VPN のグループを定義して、特定のエンドポイント セットに任意の 2 つのポイントをリンクさせます。

次に、展開で指定できるオプションについて示します。

[名前（Name）]

展開の一意の名前を指定します。

タイプ（Type）

メッシュ型の展開を設定するには、[メッシュ（Mesh）] をクリックします。

事前共有キー（Pre-Shared Key）

認証に対して一意の事前共有キーを定義します。

Device

展開のエンドポイントとして、デバイス スタックやデバイス高可用性ペアなどの管理対象デバイスを選択できます。使用している Firepower Management Center で管理されていないシスコの管理対象デバイスの場合は、[その他（Other）] を選択し、エンドポイントの IP アドレスを指定します。

[仮想ルータ（Virtual Router）]

エンドポイントとして管理対象デバイスを選択した場合は、指定したデバイスに適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

インターフェイス（Interface）

エンドポイントとして管理対象デバイスを選択した場合は、指定した仮想ルータに割り当てられているルーテッド インターフェイスを選択します。

[IPアドレス（IP Address）]

- エンドポイントとして管理対象デバイスを選択した場合は、選択したルーテッド インターフェイスに割り当てられている IP アドレスを選択します。
- 管理対象デバイスがデバイス高可用性ペアの場合は、SFRP IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスが Firepower Management Center で管理されて**いない**場合は、エンドポイントに IP アドレスを指定します。

[保護されたネットワーク（Protected Networks）]

暗号化された展開でネットワークを指定します。各ネットワークに対してCIDRブロックでサブネットを入力します。IKEバージョン1は、保護された単一のネットワークのみサポートしています。

VPNエンドポイントは同じIPアドレスを持つことはできません。また、VPNエンドポイントペアの保護されたネットワークは重複することはできないことに注意してください。エンドポイントについて保護されたネットワークのリストに1つ以上のIPv4またはIPv6エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ（IPv4またはIPv6）のエントリを少なくとも1つ持っていることが必要です。このようなエントリを持っていない場合、他のエンドポイントのIPアドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です。（IPv4については/32 CIDRアドレスを使用し、IPv6については/128 CIDRアドレスブロックを使用します）。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

[内部 IP（Internal IP）]

エンドポイントが、ネットワークアドレス変換を備えたファイアウォールの背後に配置されている場合は、このチェックボックスをオンにします。

[パブリック IP（Public IP）]

[内部IP（Internal IP）]チェックボックスをオンにした場合は、ファイアウォールに対してパブリックIPアドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

[パブリック IKE ポート（Public IKE Port）]

[内部IP（Internal IP）]チェックボックスをオンにした場合は、内部のエンドポイントにポート転送されているファイアウォール上のUDPポートに対して、1～65535の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが500または4500ではない場合、この値を指定する必要があります。

関連トピック

メッシュ VPN 展開の設定, （769 ページ）

VPN 展開の詳細オプション

VPNの展開には、展開のVPNで共有できる共通設定がいくつか含まれています。各VPNでは、デフォルトの設定を使用するか、またはそのデフォルトの設定を上書きすることができます。通常、詳細設定はほとんど、あるいはまったく変更する必要がありません。詳細設定は導入環境ごとに異なります。

次に、展開で指定できる詳細オプションについて説明します。

許可されるその他のアルゴリズム（Other Algorithm Allowed）

このチェックボックスをオンにすると、[アルゴリズム（Algorithm）] リストに含まれていないがリモート ピアによって提案されるアルゴリズムについて、自動ネゴシエーションが有効になります。

アルゴリズム（SNMP (v3) Auth. Alrorithm）

展開でデータのセキュリティを確保するため、フェーズ 1 とフェーズ 2 のアルゴリズムの提案を指定します。両方のフェーズに対して、[暗号（Cipher）]、[ハッシュ（Hash）]、および [Diffie-Hellman (DH)]グループ認証メッセージを選択します。

IKE ライフタイム（IKE Life Time）

IKE SA の最大ネゴシエーション間隔について、数値を指定し、時間単位を選択します。最小 15 分、最大 30 日を指定できます。

IKE v2

システムで IKE バージョン 2 を使用する場合は、このチェックボックスをオンにします。このバージョンでは、スター型の展開と複数の保護ネットワークがサポートされます。

ライフタイム（Life Time）

SA の最大ネゴシエーション間隔について、数値を指定し、時間単位を選択します。最小 5 分、最大 24 時間を指定できます。

ライフ パケット数（Life Packets）

有効期限までに IPsec SA を介して伝送できるパケット数を指定します。0 ～ 18446744073709551615 の整数を使用できます。

ライフ バイト（Life Bytes）

有効期限までに IPsec SA を介して伝送できるバイト数を指定します。0 ～ 18446744073709551615 の整数を使用できます。

AH

保護対象のデータに対して認証ヘッダー セキュリティ プロトコルを使用するように指定する場合は、このチェックボックスをオンにします。暗号化サービス ペイロード（ESP）プロトコルを使用する場合は、このチェックボックスをオフにします。

関連トピック

高度な VPN 展開を設定する方法, （770 ページ）

VPN 展開の管理

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

注意 7000 または 8000 シリーズ デバイス上の VPN を追加または削除して、設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作，（326 ページ）を参照してください。

手順

ステップ 1 [デバイス（Devices）] > [VPN]を選択します。

ステップ 2 VPN の展開を管理します。

- 追加：新しい VPN の展開を作成するには、[VPN の追加（Add VPN）] > [Firepower デバイス（Firepower Device）] をクリックして、展開タイプに応じて次の手順を実行します。
  - メッシュ VPN 展開の設定，（769 ページ）
  - ポイントツーポイント VPN 展開の設定，（768 ページ）
  - スター VPN 展開の設定，（768 ページ）
- 編集：既存の VPN 展開の設定を変更するには、編集アイコン（  ）をクリックします。VPN 展開の編集，（771 ページ）を参照してください。
- 削除：VPN 展開を削除するには、削除アイコン（  ）をクリックします。
- 展開：[展開（Deploy）] をクリックします（設定変更の導入，（320 ページ） を参照）。
- VPN ステータスの表示：既存の VPN 展開のステータスを表示するには、ステータス アイコンをクリックします。VPN ステータスの表示，（772 ページ）を参照してください。

関連トピック

Snort® の再起動シナリオ，（324 ページ）

ポイントツーポイント VPN 展開の設定

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

手順

ステップ 1 [デバイス（Devices）] > [VPN]を選択します。

ステップ 2 [VPN の追加（Add VPN）] > [Firepower デバイス（Firepower Device）] をクリックします。

ステップ 3 一意の名前を入力します。

ステップ 4 [タイプ（Type）] として [PTP] が選択されていることを確認します。

ステップ 5 一意の事前共有キーを入力します。

ステップ 6 [ノード ペア（Node Pairs）] の隣の追加アイコン（  ）をクリックします。

ステップ 7 ポイントツーポイント VPN 展開オプション，（760 ページ）で説明されている VPN 展開オプションを設定します。

ステップ 8 [ノード A（Node A）] の下の [保護されたネットワーク（Protected Networks）] の隣にある追加アイコン（  ）をクリックします。

ステップ 9 保護されたネットワークの CIDR ブロックを入力します。

ステップ 10 [OK] をクリックします。

ステップ 11 [ノード B（Node B）] に対して手順 8 ～ 10 を繰り返します。

ステップ 12 [保存（Save）] をクリックします。
エンドポイント ペアが展開に追加されます。

ステップ 13 [保存（Save）] をクリックして、展開の設定を終了します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

スター VPN 展開の設定

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

手順

ステップ 1 [デバイス（Devices）] > [VPN]を選択します。

ステップ 2 [VPN の追加（Add VPN）] > [Firepower デバイス（Firepower Device）] をクリックします。

ステップ 3 一意の名前を入力します。

ステップ 4 [スター（Star）] をクリックしてタイプを指定します。

ステップ 5 一意の事前共有キーを入力します。

ステップ 6 [ハブ ノード（Hub Node）] の隣の編集アイコン（  ）をクリックします。

ステップ 7 スター VPN の展開オプション, （762 ページ）で説明されている VPN 展開オプションを設定します。

ステップ 8 [保護されたネットワーク（Protected Networks）] の隣の追加アイコン（  ）をクリックします。

ステップ 9 保護されたネットワークの IP アドレスを入力します。

ステップ 10 [OK] をクリックします。

ステップ 11 [保存（Save）] をクリックします。ハブ ノードが展開に追加されます。

ステップ 12 [リーフ ノード（Leaf Nodes）] の隣の追加アイコン（  ）をクリックします。

ステップ 13 リーフ ノードを完了するには、手順 7 ～ 10 を繰り返します。これにより、ハブ ノードと同じオプションが設定されます。

ステップ 14 [保存（Save）] をクリックします。
リーフ ノードが展開に追加されます。

ステップ 15 [保存（Save）] をクリックして、展開の設定を終了します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

メッシュ VPN 展開の設定

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

手順

ステップ 1 [デバイス（Devices）] > [VPN]を選択します。

ステップ 2 [VPN の追加（Add VPN）] > [Firepower デバイス（Firepower Device）] をクリックします。

ステップ 3 一意の名前を入力します。

ステップ 4 [メッシュ（Mesh）] をクリックして [タイプ（Type）] を指定します。

ステップ 5 一意の事前共有キーを入力します。

ステップ 6 [ノード（Nodes）] の隣の追加アイコン（  ）をクリックします。

ステップ 7 メッシュ VPN 展開オプション, （764 ページ）で説明されている VPN 展開オプションを設定します。

ステップ 8 [保護されたネットワーク（Protected Networks）] の隣の追加アイコン（  ）をクリックします。

ステップ 9 保護されたネットワークの CIDR ブロックを入力します。

ステップ 10 [OK] をクリックします。
保護されたネットワークが追加されます。

ステップ 11 [保存（Save）] をクリックします。
展開にエンドポイントが追加されます。

ステップ 12 エンドポイントをさらに追加するには、ステップ 6 ～ 11 を繰り返します。

ステップ 13 [保存（Save）] をクリックして展開を完了します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

高度な VPN 展開を設定する方法

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

マルチドメイン展開では、現在のドメインで作成されたVPN展開が表示されます。これは編集できます。また、エンドポイント デバイスの 1 つがドメインに属している場合は、先祖ドメインで作成された VPN 展開も表示されます。先祖ドメインで作成された VPN 展開は編集できません。下位のドメインで作成された VPN 展開を表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [デバイス（Devices）] > [VPN]を選択します。

ステップ 2 編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 VPN 展開の詳細オプション, （765 ページ）の説明に従って、詳細設定を行います。

ステップ 5 [アルゴリズム（Algorithms）] の隣の追加アイコン（）をクリックします。

ステップ 6 両方のフェーズに対して、[暗号（Cipher）]、[ハッシュ（Hash）]、および[Diffie-Hellman]（[DH]）グループ認証のメッセージを選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

VPN 展開の編集

注意 2 人のユーザが同じ展開について同時に編集**してはいけません**。ただし、Web インターフェイスでは同時編集を防止していないことに注意してください。

マルチドメイン展開では、現在のドメインで作成されたVPN展開が表示されます。これは編集できます。また、エンドポイント デバイスの 1 つがドメインに属している場合は、先祖ドメインで作成された VPN 展開も表示されます。先祖ドメインで作成された VPN 展開は編集できません。下位のドメインで作成された VPN 展開を表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [デバイス（Devices）] > [VPN]を選択します。

ステップ 2 編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 必要な設定を変更します。

- [詳細設定（Advanced）] の設定。高度な VPN 展開を設定する方法, （770 ページ）を参照してください。
- メッシュ展開の設定。メッシュ VPN 展開の設定, （769 ページ）を参照してください。
- ポイントツーポイント型の展開の設定。ポイントツーポイント VPN 展開の設定, （768 ページ）を参照してください。
- スター型の展開の設定。スター VPN 展開の設定, （768 ページ）を参照してください。

ヒント 展開を最初に保存した後で、展開のタイプを編集することはできません。展開のタイプを変更するには、展開を削除してから新しい展開を作成する必要があります。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

VPN 展開のステータス

VPN 展開を設定した後で、設定した VPN トンネルのステータスを表示できます。VPN ページには、各 VPN 展開の展開後に、その展開のステータス アイコンが表示されます。

- （  ）アイコンは、すべての VPN エンドポイントが稼動していることを表します。
- （  ）アイコンは、すべての VPN エンドポイントが停止していることを表します。
- （  ）アイコンは、稼動しているエンドポイントと停止しているエンドポイントがあることを表します。

ステータス アイコンをクリックして、展開のステータス、および展開内のエンドポイントに関する基本情報（エンドポイント名やIPアドレスなど）を表示することができます。VPNステータスは、毎分、または（エンドポイントが停止した、または稼動したなど）ステータスの変更が生じた場合に更新されます。

関連トピック

VPN ステータスの表示, （772 ページ）

VPN ステータスの表示

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

マルチドメイン展開では、システムは現在のドメインで作成された VPN 展開を表示します。また、エンドポイント デバイスの 1 つがドメインに属している場合は、先祖ドメインで作成された VPN 展開も表示されます。下位のドメインで作成された VPN 展開を表示するには、そのドメインに切り替えます。

手順

ステップ 1 [デバイス（Devices）] > [VPN]を選択します。

ステップ 2 ステータスを表示する展開の隣にある、VPN ステータス アイコンをクリックします。

ステップ 3 [OK] をクリックします。

VPN の統計およびログ

VPN 展開を設定した後で、設定した VPN トンネルを通過するデータの統計を表示することができます。また、各エンドポイントについて最新の VPN システムと IKE ログを表示することができます。

システムには、次の統計情報が表示されます。

エンドポイント（Endpoint）

VPN エンドポイントとして指定されたルーテッドインターフェイスおよび IP アドレスへのデバイス パス。

ステータス

VPN 接続の状態（稼動または停止のどちらか）。

プロトコル

暗号化で使用されるプロトコル（ESP または AH）。

受信パケット数（Packets received）

IPsec SA ネゴシエーション中に VPN トンネルが受信する、インターフェイスあたりのパケット数。

転送パケット数（Packets Forwarded）

IPsec SA ネゴシエーション中に VPN トンネルが送信する、インターフェイスあたりのパケット数。

受信バイト数（Bytes Received）

IPsec SA ネゴシエーション中に VPN トンネルが受信する、インターフェイスあたりのバイト数。

転送バイト数（Bytes Forwarded）

IPsec SA ネゴシエーション中に VPN トンネルが送信する、インターフェイスあたりのバイト数。

作成時刻（Time Created）

VPN 接続が作成された日時。

最終使用時刻（Time Last Used）

ユーザが最後に VPN 接続を開始した時間。

NAT トラバーサル（NAT Traversal）

[はい（Yes）] が表示されている場合、ネットワーク アドレス変換を備えたデバイスの背後に少なくとも 1 つの VPN エンドポイントが存在します。

IKE 状態（IKE State）

IKE SA の状態（接続、確立、削除、または廃棄）。

IKE イベント（IKE Event）

IKE SA イベント（再認証、またはキー再生成）。

IKE イベント時間（IKE Event Time）

次のイベントが発生する時間（秒）。

IKE アルゴリズム（IKE Algorithm）

VPN 展開で使用されている IKE アルゴリズム。

IPSec 状態（IPSec State）

IPSec SA の状態（インストール中、インストール済み、更新中、キー再生成、削除、および廃棄）。

IPSec イベント（IPSec Event）

IPSec SA イベントがキーを再生成するタイミングの通知。

IPSec イベント時間（IPSec Event Time）

次のイベントが発生するまでの時間（秒）。

IPSec アルゴリズム（IPSec Algorithm）

VPN 展開で使用されている IPSec アルゴリズム。

関連トピック

VPN 統計情報およびログの表示, （775 ページ）

VPN 統計情報およびログの表示

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

マルチドメイン展開では、システムは現在のドメインで作成された VPN 展開を表示します。また、エンドポイント デバイスの 1 つがドメインに属している場合は、先祖ドメインで作成された VPN 展開も表示されます。下位のドメインで作成された VPN 展開を表示するには、そのドメインに切り替えます。

手順

ステップ 1 [デバイス（Devices）] > [VPN]を選択します。

ステップ 2 統計情報を表示する展開の隣にある、VPN ステータス アイコンをクリックします。

ステップ 3 統計情報の表示アイコン（  ）をクリックします。

ステップ 4 オプションで、[更新（Refresh）] をクリックして、VPN の統計情報を更新することもできます。

ステップ 5 オプションで、[最新のログの表示（View Recent Log）] をクリックして、各エンドポイントの最新のデータ ログを表示することもできます。ハイ アベイラビリティ ペアの 7000 または 8000 シリーズ デバイスおよびスタック デバイスのログを表示するには、アクティブ/プライマリ、またはバックアップ/セカンダリのいずれかのデバイスへのリンクをクリックします。

第 XI 部

アクセス制御

第 34 章

アクセス コントロール ポリシーの開始

ここでは、アクセス コントロール ポリシーの使用を開始する方法について説明します。

アクセス制御の概要

アクセス制御は、（非高速パスを通る）ネットワーク トラフィックの指定、検査、ロギングが可能な階層型ポリシーベースの機能です。アクセス コントロール ポリシーはネストすることができ、これはマルチドメイン展開で特に有用です。このポリシーでは各ポリシーが先祖（または基本）ポリシーからルールや設定を継承します。この継承を強制することもできますが、下位のポリシーによる先祖ポリシーの上書きを許可することもできます。各管理対象デバイスは 1 つのアクセス コントロール ポリシーのターゲットにすることができます。

ポリシーのターゲットデバイスがネットワーク トラフィックについて収集したデータは、以下に基づいてそのトラフィックのフィルタや制御に使用できます。

- トランスポート層およびネットワーク層の特定しやすい単純な特性（送信元と宛先、ポート、プロトコルなど）
- レピュテーション、リスク、ビジネスとの関連性、使用されたアプリケーション、または訪問した URL などの特性を含む、トラフィックに関する最新のコンテキスト情報
- レルム、ユーザ、ユーザ グループ、または ISE の属性

- 暗号化されたトラフィックの特性（このトラフィックを復号してさらに分析することもできます）
- 暗号化されていないトラフィックまたは復号されたトラフィックに、禁止されているファイル、検出されたマルウェア、または侵入の試みが存在するかどうか

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

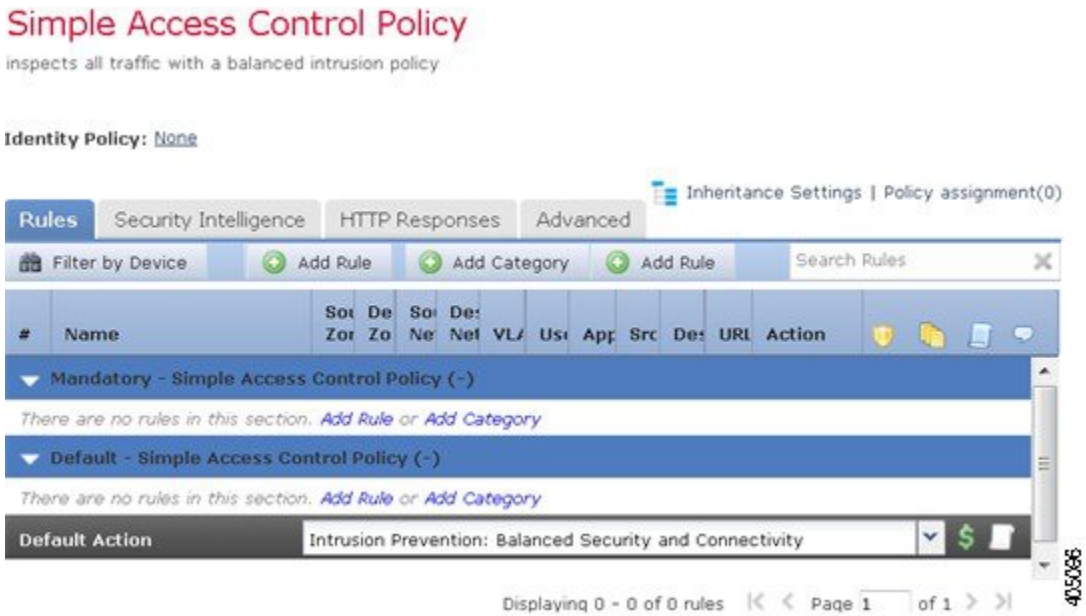
展開のライセンスを取得せずにシステムを設定することはできますが、多くの機能では、展開する前に適切なライセンスを有効にする必要があります。また、一部の機能は、特定のデバイス モデルでのみ使用できます。サポートされていない機能は、警告アイコンおよび確認ダイアログ ボックスに示されます。

（注） システムがトラフィックに影響を与えるためには、ルーテッド、スイッチド、トランスペアレント インターフェイスまたはインライン インターフェイスのペアを使用して関連する設定を管理対象デバイスに展開する必要があります。場合によっては、タップ モードのインライン デバイスを含むパッシブに展開されたデバイスにインライン設定を展開することがシステムによって阻害されます。それ以外の場合、ポリシーは正常に展開されますが、パッシブに展開されたデバイスを使用してトラフィックのブロックや変更を試みると、予期しない結果になる可能性があります。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

アクセス コントロール ポリシーのコンポーネント

新しく作成したアクセス コントロール ポリシーは、デフォルト アクションを使用して、すべてのトラフィックを処理するようにターゲット デバイスに指示します。

次の図で、デフォルトアクションはトラフィックが最終接続先に到達する前に、[バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] に基づく侵入ポリシー使用してトラフィックを検査します。



次のリストに、簡単なポリシーの作成後に変更可能な設定を示します。

（注） 現在のドメインで作成されたアクセス コントロール ポリシーのみ編集できます。また、先祖アクセス コントロール ポリシーによってロックされている設定は編集できません。

名前（Name）と説明（Description）

各アクセス コントロール ポリシーには一意の名前が必要です。説明は任意です。

継承設定（Inheritance Settings）

ポリシー継承により、アクセス コントロール ポリシーの階層を作成することができます。親（または基本）ポリシーは子孫のデフォルト設定を定義、実行します。これはマルチドメイン導入環境で特に有効です。

ポリシーの継承設定で基本ポリシーを選択できます。また、現在のポリシーで設定をロックすることで、子孫にも同じ設定を継承させることできます。ロック解除された設定については、子孫ポリシーによる上書きが可能です。

ポリシー割り当て

各アクセス コントロール ポリシーがそのポリシーを使用するデバイスを識別します。1 つのデバイスに適用されるアクセス コントロール ポリシーは 1 つのみです。マルチドメイン導入環境では、1 ドメイン内のすべてのデバイスで同じ基本ポリシーを使用させることができます。

ルール（Rule）

アクセス コントロール ルールは、ネットワーク トラフィックをきめ細かく処理する方法を提供します。先祖ポリシーから継承したルールを含むアクセス コントロール ポリシーのルールには、1から始まる番号が付いています。システムは、ルール番号の昇順で上から順に、アクセス コントロール ルールをトラフィックと照合します。

通常、システムは、ルールのすべての条件がトラフィックに一致する最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。条件は単純または複雑にできます。条件の使用は特定のライセンスによって異なります。

デフォルト アクション（Default Action）

デフォルト アクションは、他のアクセス制御設定で処理されないトラフィックをどのように処理し、ロギングするかを定義します。デフォルト アクションにより、追加のインスペクションなしですべてのトラフィックをブロックまたは信頼することができます。また、侵入およびディスカバリ データの有無についてトラフィックを検査することもできます。

アクセス コントロール ポリシーのデフォルト アクションは先祖ポリシーから継承することもできますが、継承を強制的に実施することはできません。

セキュリティ インテリジェンス（Security Intelligence）

セキュリティ インテリジェンスは、悪意のあるインターネット コンテンツに対する最初の防衛ラインです。この機能により、最新の IP アドレス、URL、ドメイン名レピュテーション インテリジェンスをもとに接続をブラックリストに登録（ブロック）することができます。重要なリソースへの継続的なアクセスを確保するために、ブラックリストはカスタム ホワイトリストで上書きできます。

HTTP 応答（HTTP Responses）

システムによりユーザの Web サイト リクエストがブロックされた場合、システム提供の汎用的な応答ページを表示するか、カスタム ページを表示させることができます。ユーザに警告するページを表示するものの、ユーザが最初に要求したサイトに進めるようにすることもできます。

アクセス コントロールの詳細オプション（Advanced Access Control Options）

通常、アクセス コントロール ポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。多くの場合、デフォルト設定が適切です。詳細設定では、トラフィックの前処理、SSL インスペクション、ID、種々のパフォーマンス オプションなどを変更できます。

アクセス コントロール ポリシーのデフォルト アクション

単純なアクセス コントロール ポリシーでは、デフォルト アクションは、ターゲット デバイスがすべてのトラフィックをどう処理するかを指定します。より複雑なポリシーでは、デフォルト アクションは次のトラフィックを処理します。

- インテリジェント アプリケーション バイパスで信頼されないトラフィック
- セキュリティ インテリジェンスによってブラックリスト登録されていないトラフィック
- SSL インスペクションによってブロックされていないトラフィック（暗号化トラフィックのみ）
- ポリシー内のどのルールにも一致しないトラフィック（トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く）

アクセス コントロール ポリシーのデフォルト アクションにより、追加のインスペクションなしでトラフィックをブロックまたは信頼することができます。また、侵入およびディスカバリ データの有無についてトラフィックを検査することもできます。

（注） デフォルト アクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行**できません**。デフォルト アクションで処理される接続のロギングは、初期設定では無効ですが、有効にすることもできます。

ポリシーを継承している場合、最下位の子孫のデフォルト アクションによってトラフィックの最終的な処理が決まります。アクセス コントロール ポリシーのデフォルト アクションは基本ポリシーから継承することもできますが、継承したデフォルト アクションを強制的に実施することはできません。

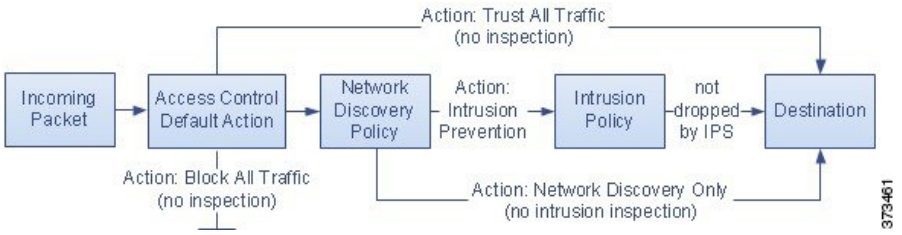
次の表に各デフォルト アクションが処理するトラフィックに対して実施可能なインスペクションの種類を示します。

表 *67*：アクセス コントロール ポリシーのデフォルト アクション

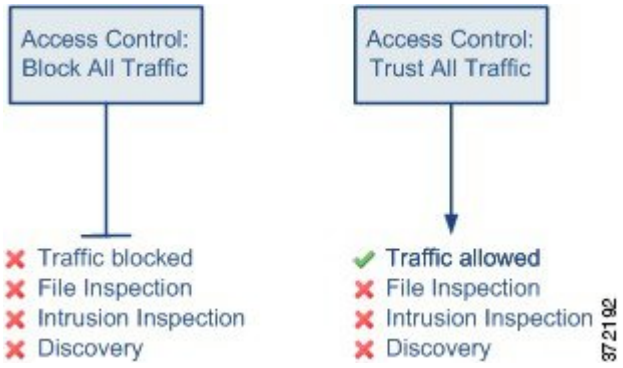
デフォルト アクション	トラフィックに対して行う処理	インスペクション タイプとポリシー
アクセス コントロール：すべてのトラフィックをブロック	それ以上のインスペクションは行わずにブロックする	none
アクセス コントロール：すべてのトラフィックを信頼	信頼（追加のインスペクションなしで最終宛先に許可）	none
侵入防御（Intrusion Prevention）	ユーザが指定した侵入ポリシーに合格する限り、許可する	侵入、指定した侵入ポリシーおよび関連する変数セットを使用、および 検出（discovery）、ネットワーク検出ポリシーを使用
ネットワーク検出のみ（Network Discovery Only）	許可（allow）	検出のみ（discovery only）、ネットワーク検出ポリシーを使用

デフォルト アクション	トラフィックに対して行う処理	インスペクション タイプとポリシー
基本ポリシーから継承	基本ポリシーで定義	基本ポリシーで定義

次の図は、表を図で表したものです。



次の図は、[すべてのトラフィックをブロック（Block All Traffic）] および [すべてのトラフィックを信頼（Trust All Traffic）] のデフォルト アクションを示しています。



次の図は、[侵入防御（Intrusion Prevention）] および [ネットワーク検出のみ（Network Discovery Only）] のデフォルト アクションを説明しています。

ヒント [ネットワーク検出のみ（Network Discovery Only）] の目的は、検出のみの展開でパフォーマンスを向上させることです。侵入検知および防御のみを目的としている場合は、さまざまな設定でディスカバリを無効にできます。

アクセス コントロール ポリシーの継承

アクセス制御は、マルチテナンシーを補完する階層型ポリシーベース実装となっています。ドメイン階層を作成するのと同様に、対応するアクセス コントロール ポリシーの階層を作成できます。子孫（あるいは子）アクセスコントロールポリシーは、直接の親（あるいは基本）ポリシーからルールや設定を継承します。この基本ポリシーにもさらに親ポリシーがあり、その親ポリシーにもさらに、というようにルールや設定が継承されている場合もあります。

アクセス コントロール ポリシーのルールは、親ポリシーの [強制（Mandatory）] ルール セクションと [デフォルト（Default）] のルール セクションの間にネストされています。この実装により、先祖ポリシーの [強制（Mandatory）] ルールは実施される一方、先祖ポリシーの [デフォルト（Default）] ルールは現在のポリシーでプリエンプション処理することが可能です。

次の設定をロックすることで、すべての子孫ポリシーに設定を実行させることができます。ロック解除された設定については、子孫ポリシーによる上書きが可能です。

- セキュリティ インテリジェンス：最新の IP アドレス、URL、ドメイン名レピュテーション インテリジェンスをもとに接続をブラックリストに登録（ブロック）します。
- HTTP 応答ページ：ユーザの Web サイト リクエストをブロックした際、カスタム応答ページあるいはシステム提供の応答ページを表示します。
- 詳細設定：関連するサブポリシー、ネットワーク分析設定、パフォーマンス設定、その他の一般設定オプションを指定します。

アクセス コントロール ポリシーのデフォルト アクションは先祖ポリシーから継承することもできますが、継承を強制的に実施することはできません。

ポリシーの継承とマルチテナンシー

通常のマルチドメイン導入環境では、アクセスコントロールポリシーの階層がドメイン構造に対応しており、管理対象デバイスに最下位レベルのアクセスコントロールポリシーを適用します。この実装により、ドメインの上層レベルでは選択的にアクセス制御を実施しながらも、ドメインの下層レベルの管理者は展開ごとに設定を調整することが可能です（子孫ドメインの管理者を制限するには、ポリシー継承と適用だけでなく、ロールによる制限を行う必要があります）。

たとえば、所属している部門のグローバル ドメイン管理者は、グローバル レベルのアクセス コントロールポリシーを作成できます。そして、そのグローバル レベルのポリシーを基本ポリシーとして、機能別にサブドメインに分けられたすべてのデバイスで使用するよう要求することがことが可能です。

サブドメインの管理者がFirepower Management Centerにログインしてアクセス制御を設定する際、グローバル レベルのポリシーはそのまま展開できます。あるいは、グローバル レベルのポリシーの範囲内の子孫アクセス コントロール ポリシーを作成、展開することも可能です。

（注） アクセス制御の継承および適用が最も有効に実装されるのは、マルチテナンシーを補完する場合ですが、1 つのドメイン内においてもアクセス制御ポリシーを階層化することが可能です。また、任意のレベルでアクセス コントロール ポリシーを割り当て、展開することもできます。

アクセス コントロール ポリシーの管理

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

Firepower システムでは、システム付属のアクセス コントロール ポリシーの編集と、カスタム アクセス コントロール ポリシーの作成が可能です。デバイスの初期設定に応じて、システム付属のポリシーには次のものが含まれます。

- デフォルト アクセス制御：詳細な検査なしで、すべてのトラフィックをブロックします。
- デフォルト侵入防御：すべてのトラフィックを許可しますが、Balanced Security and Connectivity 侵入ポリシーおよびデフォルトの侵入変数セットを使用して検査も実行します。
- デフォルト ネットワーク検出：すべてのトラフィックを許可すると同時に検出データについて検査しますが、侵入やエクスプロイトについては検査しません。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] を選択します。

ステップ 2 アクセス コントロール ポリシーを管理します。

- コピー：コピー アイコン（）をクリックします。
- 作成：[新規ポリシー（New Policy）] をクリックします。基本的なアクセス コントロール ポリシーの作成, （787 ページ）を参照してください。

- 削除：削除アイコン（  ）をクリックします。
- 展開：[展開（Deploy）] をクリックします（設定変更の導入, （320 ページ） を参照）。
- 編集：編集アイコン（  ）をクリックします。次を参照してください。アクセス コントロール ポリシーの編集, （789 ページ）
- 継承：子孫を持つポリシーの横にあるプラスアイコン（  ）をクリックすると、ポリシーの階層ビューが展開されます。
- インポート/エクスポート：[インポート/エクスポート（Import/Export）] をクリックします。コンフィギュレーションのインポートとエクスポート, （187 ページ）を参照してください。
- [レポート（Report）]：レポート アイコン（  ）をクリックします（現在のポリシー レポートの生成, （333 ページ） を参照）。

基本的なアクセス コントロール ポリシーの作成

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

新規アクセス コントロール ポリシーを作成する場合は、少なくとも、デフォルト アクションを選択する必要があります。

ほとんどの場合、デフォルト アクションにより処理される接続のロギングは最初は無効になっています。例外は、マルチドメイン導入でサブポリシーを作成する場合です。この場合、継承されたデフォルト アクションのロギング設定に応じて、接続のロギングが有効になります。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力し、オプションで [説明（Description）] を入力します。

ステップ 4 オプションで、[基本ポリシーの選択（Select Base Policy）] ドロップダウンリストから基本ポリシーを選択します。
ドメインにアクセス コントロール ポリシーが適用されている場合は、この手順はオプションではありません。適用されているポリシーまたはその子孫のいずれかを基本ポリシーとして選択する必要があります。

ステップ 5 初期デフォルト アクションを指定します。

- 基本ポリシーを選択すると、新しいポリシーではそのデフォルト アクションが継承されます。ここで変更することはできません。
- [すべてのトラフィックをブロック（Block All Traffic）] を選択すると、[アクセス コントロール：すべてのトラフィックをブロック（Access Control: Block All Traffic）] をデフォルト アクションとするポリシーが作成されます。
- [侵入防御（Intrusion Prevention）] を選択すると、[侵入防御：セキュリティと接続性のバランス（Intrusion Prevention: Balanced Security and Connectivity）] をデフォルト アクションとし、デフォルトの侵入変数セットが関連付けられたポリシーが作成されます。
- [ネットワーク検出（Network Discovery）] を選択すると、[ネットワーク検出のみ（Network Discovery Only）] をデフォルト アクションとするポリシーが作成されます。

ヒント デフォルトですべてのトラフィックを信頼するか、基本ポリシーを選択しデフォルト アクションは継承しないようにする場合は、後でデフォルト アクションを変更できます。

注意 アクセス コントロール ポリシーによって使用される侵入ポリシーの総数の変更 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。 現在使用されていない侵入ポリシーを追加するか、侵入ポリシーの最後のインスタンスを削除することで、侵入ポリシーの総数を変更します。アクセス コントロール ルールで侵入ポリシーをデフォルトのアクションまたはデフォルトの侵入ポリシーとして使用できます。

ステップ 6 必要に応じて、ポリシーを展開する [使用可能なデバイス（Available Devices）] を選択し、[ポリシーに追加（Add to Policy）] をクリック（またはドラッグ アンド ドロップ）して、選択したデバイスを追加します。表示されるデバイスを絞り込むには、[検索（Search）] フィールドに検索文字列を入力します。
このポリシーをすぐに展開するには、この手順を実行する必要があります。

ステップ 7 [保存（Save）] をクリックします。

次の作業

- 必要に応じて、アクセス コントロール ポリシーの編集, （789 ページ）の説明に従って、さらに新しいポリシーを設定します。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

アクセス コントロール ポリシーの編集

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

ポリシーの編集は、1 つのブラウザ ウィンドウを使用して、一度に 1 人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシー エディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] を選択します。

ステップ 2 編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 アクセス コントロール ポリシーを編集します。

- 名前と説明：いずれかのフィールドをクリックし、新しい情報を入力します。
- デフォルト アクション：[デフォルト アクション（Default Action）] ドロップダウン リストから値を選択します。

注意 アクセス コントロール ポリシーによって使用される侵入ポリシーの総数の変更 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。 現在使用されていない侵入ポリシーを追加するか、侵入ポリシーの最後のインスタンスを削除することで、侵入ポリシーの総数を変更します。アクセス コントロール ルールで侵入ポリシーをデフォルトのアクションまたはデフォルトの侵入ポリシーとして使用できます。

- デフォルト アクションの変数セット：[侵入防御（Intrusion Prevention）] のデフォルト アクションに関連付けられている変数セットを変更するには、変数アイコン（）をクリックします。表示されるポップアップ ウィンドウで、新しい変数セットを選択して [OK] をクリックします。また、編集アイコン（）をクリックして、選択した変数セットを新しいウィン

ドウで編集することもできます。詳細については、変数の管理，（414 ページ）を参照してください。

- デフォルト アクションのロギング：デフォルト アクションで処理される接続のロギングを設定するには、ロギングアイコン（  ）をクリックします。ポリシーのデフォルトアクションによる接続のロギング，（1919 ページ）を参照してください。
- HTTP 応答：システムが Web サイトの要求をブロックする際にブラウザに表示される情報を指定するには、[HTTP 応答（HTTP Responses）] タブをクリックします。HTTP 応答ページの選択，（826 ページ）を参照してください。
- 継承：基本ポリシーの変更：このポリシーの基本アクセス コントロール ポリシーを変更するには、[継承設定（Inheritance Settings）] をクリックします。基本アクセス コントロール ポリシーの選択，（792 ページ）を参照してください。
- 継承：子孫での設定のロック：このポリシーの設定を子孫ポリシーに適用するには、[継承設定（Inheritance Settings）] をクリックします。子孫アクセス コントロール ポリシーのロックの設定，（793 ページ）を参照してください。
- ポリシー割り当て：ターゲット：このポリシーの対象となっている管理対象デバイスを特定するには、[ポリシー割り当て（Policy Assignment）] をクリックします。アクセス コントロール ポリシーのターゲット デバイスの設定，（795 ページ）を参照してください。
- ポリシー割り当て：ドメインで必須：このポリシーをサブドメインに適用するには、[ポリシー割り当て（Policy Assignment）] をクリックします。ドメインでのアクセス コントロール ポリシーの強制，（794 ページ）を参照してください。
- ルール：アクセス コントロール ルールを管理し、侵入とファイル ポリシーを使用して悪意のあるトラフィックを検査およびブロックするには、[ルール（Rules）] タブをクリックします。アクセス コントロール ルールの作成および編集，（807 ページ）を参照してください。
- セキュリティ インテリジェンス：最新のレピュテーション インテリジェンスに基づいてすぐに接続をブラックリストに載せる（ブロックする）には、[セキュリティ インテリジェンス（Security Intelligence）] タブをクリックします。セキュリティ インテリジェンスの設定，（834 ページ）を参照してください。
- 詳細オプション：前処理、SSL インスペクション、アイデンティティ、パフォーマンス、およびその他の詳細オプションを設定するには、[詳細（Advanced）] タブをクリックします。アクセス コントロール ポリシーの詳細設定，（796 ページ）を参照してください。
- 警告：アクセス コントロール ポリシー（およびその子孫ポリシーと関連ポリシー）の警告またはエラーのリストを表示するには、[警告の表示（Show Warnings）] をクリックします。警告とエラーによって、トラフィック分析やフローに悪影響を及ぼしたり、ポリシーの展開を妨げたりする構成がマークされます。警告がない場合、ボタンは表示されません。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

アクセス コントロール ポリシーの継承の管理

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

手順

ステップ 1 変更する継承設定を持つアクセス コントロール ポリシーを編集します。アクセス コントロール ポリシーの編集，（789 ページ）を参照してください。

ステップ 2 ポリシーの継承を管理します。

- 基本ポリシーの変更：このポリシーの基本アクセス コントロール ポリシーを変更するには、[継承設定（Inheritance Settings）] をクリックして、基本アクセス コントロール ポリシーの選択，（792 ページ）で説明する手順を実行します。
- 子孫の設定のロック：このポリシーの設定を子孫ポリシーで強制適用するには、[継承設定（Inheritance Settings）] をクリックして、子孫アクセス コントロール ポリシーのロックの設定，（793 ページ）で説明する手順を実行します。
- ドメインで必須：このポリシーをサブドメインで強制適用するには、[ポリシーの割り当て（Policy Assignment）] をクリックして、ドメインでのアクセス コントロール ポリシーの強制，（794 ページ）で説明する手順を実行します。
- 基本ポリシーからの設定の継承：基本アクセス コントロール ポリシーから設定を継承するには、[セキュリティ インテリジェンス（Security Intelligence）] タブ、[HTTP 応答（HTTP Responses）] タブ、または [詳細（Advanced）] タブをクリックして、基本ポリシーからのアクセス コントロール ポリシー設定の継承，（792 ページ）で説明する手順を実行します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

基本アクセス コントロール ポリシーの選択

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

1 つのアクセス コントロール ポリシーを別の基本（親）として使用できます。デフォルトでは、子のポリシーが基本ポリシーから設定を継承します。ロック解除された設定を変更することも可能です。

既存のアクセスコントロールポリシーの基本ポリシーを変更すると、システムで現在のポリシー設定が新しい基本ポリシーの任意のロックされた設定に更新されます。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、[継承設定（Inheritance Settings）] をクリックします。

ステップ 2 [基本ポリシーの選択（Select Base Policy）] ドロップダウンリストからポリシーを選択します。マルチドメイン展開では、アクセスコントロールポリシーが既存のドメインで必要になることがあります。基本ポリシーとして、強制ポリシーまたはその子孫ポリシーの一つを選択できます。

ステップ 3 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

基本ポリシーからのアクセス コントロール ポリシー設定の継承

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

新しい子ポリシーは、基本ポリシーから多数の設定を継承します。これらの設定は、基本ポリシーでロックされていない場合はオーバーライドできます。

基本ポリシーから後で設定を再継承すると、システムによって基本ポリシーの設定が表示され、コントロールが淡色表示されます。ただし、オーバーライドした内容はシステムによって保存され、その内容は継承を再度無効にすると復元されます。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス（Security Intelligence）] タブ、[HTTP 応答（HTTP Responses）] タブまたは [詳細（Advanced）] タブをクリックします。

ステップ 2 継承する設定ごとに、[基本ポリシーから継承（Inherit from base policy）] チェックボックスをオンにします。
コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。

ステップ 3 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

子孫アクセス コントロール ポリシーのロックの設定

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

アクセス コントロール ポリシーの設定をロックして、すべての子孫ポリシーで設定を適用します。子孫ポリシーでは、ロックされていない設定をオーバーライドできます。

設定をロックするときに、すでに子孫ポリシーで実行されていたオーバーライドを保存して、設定のロックを再度解除したときにオーバーライドを復元できるようにします。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[設定の継承（Inheritance Settings）] をクリックします。

ステップ 2 [子ポリシーの継承設定（Child Policy Inheritance Settings）] 領域で、ロックする設定をオンにします。
コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。

ステップ 3 [OK] をクリックして継承設定を保存します。

ステップ 4 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ドメインでのアクセス コントロール ポリシーの強制

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

ドメイン内の各デバイスが同一の基本アクセス コントロール ポリシーまたは、そのポリシーの子孫ポリシーの 1 つを使用するように強制できます。

はじめる前に

- 少なくとも 1 つのグローバル ドメイン以外のドメインを設定します。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[ポリシーの割り当て（Policy Assignments）] をクリックします。

ステップ 2 [ドメインに強制（Required on Domains）] タブをクリックします。

ステップ 3 ドメイン リストを作成します。

- 追加：現在のアクセス コントロール ポリシーを強制適用するドメインを選択して [追加（Add）] をクリックするか、選択したドメインのリストにドラッグアンドドロップします。
- 削除：リーフ ドメインの横にある削除アイコン（）をクリックするか、先祖ドメインを右クリックして [選択項目の削除（Delete Selected）] を選択します。
- 検索：検索フィールドに検索文字列を入力します。クリア アイコン（）をクリックして、検索をクリアします。

ステップ 4 [OK] をクリックしてドメインに強制適用する設定を保存します。

ステップ 5 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

アクセス コントロール ポリシーのターゲット デバイスの設定

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

アクセス コントロール ポリシーは、それを使用するデバイスを指定します。それぞれのデバイスは、1 つのアクセス コントロール ポリシーのみのターゲットに設定できます。マルチドメイン展開では、ドメイン内のすべてのデバイスが同一の基本ポリシーを使用するように強制できます。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[ポリシーの割り当て（Policy Assignments）] をクリックします。

ステップ 2 [ターゲット デバイス（Targeted Devices）] タブで、ターゲット リストを作成します。

- 追加：1 つ以上の [使用可能なデバイス（Available Devices）] を選択して、[ポリシーに追加（Add to Policy）] をクリックするか、[選択したデバイス（Selected Devices）] のリストにドラッグ アンド ドロップします。
- 削除：1 つのデバイスの横にある削除アイコン（  ）をクリックするか、複数のデバイスを選択して、右クリックしてから [選択済み項目の削除（Delete Selected）] を選択します。
- 検索：検索フィールドに検索文字列を入力します。クリアアイコン（  ）をクリックして、検索をクリアします。

[影響を受けるデバイス（Impacted Devices）] の下に、割り当てられたアクセス コントロール ポリシーが現在のポリシーの子であるデバイスが一覧表示されます。現在のポリシーを変更すると、これらのデバイスに影響します。

ステップ 3 必要に応じて、[ドメインで強制（Required on Domains）] タブをクリックして、選択したサブドメイン内のすべてのデバイスが同じ基本ポリシーを使用するように強制します。ドメインでのアクセス コントロール ポリシーの強制，（794 ページ）を参照してください。

ステップ 4 [OK] をクリックしてターゲット デバイス設定を保存します。

ステップ 5 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

アクセス コントロール ポリシーの詳細設定

通常、アクセス コントロール ポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。デフォルト設定は、ほとんどの展開環境に適しています。侵入ルールの更新, （157 ページ）で説明しているように、アクセス コントロール ポリシーの前処理およびパフォーマンスの詳細オプションの多くは、ルールの更新によって変更される可能性があることに注意してください。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

注意 Snort プロセスを再起動し、トラフィック インスペクションを一時的に中断する詳細設定変更のリストについては、展開またはアクティブ化された際に Snort プロセスを再起動する設定, （327ページ）を参照してください。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort® の再起動によるトラフィックの動作, （326 ページ）も参照してください。

全般設定

ユーザが要求した各 URL に対して保存する文字数をカスタマイズするには、長い URL のロギングの制限, （1920 ページ）を参照してください。

ユーザが最初のブロックをバイパスした後に Web サイトを再度ブロックするまでの時間間隔をカスタマイズするには、ブロックされた Web サイトのユーザ バイパス タイムアウトの設定, （829 ページ）を参照してください。

[URL キャッシュ ミス ルックアップを再試行する（Retry URL cache miss lookup）] を無効にすると、カテゴリがキャッシュされない場合には、クラウド ルックアップを使用せずに、すぐにトラフィックが URL に渡されるようにすることができます。クラウド ルックアップで別のカテゴリが用意されるまで、クラウド ルックアップを必要とする URL は未分類の URL として処理されます。

特定の設定で Snort プロセスを再起動する必要がない限り設定の変更を展開する場合にトラフィックを検査するには、必ず、[ポリシーの適用時にトラフィックを検査する（Inspect traffic during policy apply）] がデフォルト値（有効）に設定してください。このオプションを有効にすると、リソースの需要が高まった場合にいくつかのパケットが検査なしでドロップされることがあります。詳細については、Snort® の再起動シナリオ , （324 ページ）を参照してください。

関連するポリシー

詳細設定を使用して、サブポリシー（SSL、ID、）をアクセス制御に関連付けます。アクセス制御への他のポリシーの関連付け，（798 ページ）を参照してください。

ネットワーク分析ポリシーと侵入ポリシー

ネットワーク分析ポリシーおよび侵入ポリシーの詳細設定によって、以下が可能になります。

- システムがトラフィックを検査する方法を正確に決定する前に、最初にそのトラフィックを検査するために使用される、アクセス コントロール ポリシーのデフォルトの侵入ポリシーと関連付けられている変数セットの変更。
- 多くの前処理オプションを制御する、アクセス コントロール ポリシーのデフォルト ネットワーク分析ポリシーの変更。
- カスタム ネットワーク分析ルールおよびネットワーク分析ポリシーを使用した、特定のセキュリティ ゾーン、ネットワーク、および VLAN に対する前処理オプションの調整。

詳細については、ネットワーク分析/侵入ポリシーのための高度なアクセス制御の設定，（1259 ページ）を参照してください。

ファイルおよびマルウェアの設定

ファイルとマルウェアのインスペクション パフォーマンスとストレージの調整，（987 ページ）に、ファイル制御と AMP for Firepower のパフォーマンス オプションに関する情報が記載されています。

インテリジェント アプリケーション バイパスの設定

インテリジェント アプリケーション バイパス（IAB）は、トラフィックがインスペクション パフォーマンスとフローしきい値の組み合わせを超過したときにバイパスするアプリケーションを指定する、または、バイパスに関するテストを行うための、エキスパート レベルの設定です。詳細については、インテリジェント アプリケーション バイパス，（855 ページ）を参照してください。

トランスポート層とネットワーク層のプリプロセッサの設定

トランスポート層とネットワーク層のプリプロセッサの詳細設定は、アクセス コントロール ポリシーが展開されるすべてのネットワーク、ゾーン、VLAN にグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。詳細については、トランスポート/ネットワーク プリプロセッサの詳細設定，（1366 ページ）を参照してください。

検出拡張の設定

検出拡張の詳細設定を行うことで、アダプティブ プロファイルを使用して、ホストのオペレーティング システムに基づき、パッシブ展開におけるパケット フラグメントと TCP ストリームのリアセンブルを向上させることができます。詳細については、適応型プロファイル，（1429 ページ）を参照してください。

パフォーマンス設定および遅延ベースのパフォーマンス設定

侵入防御のパフォーマンス チューニングについて，（1241 ページ） では、侵入行為についてトラフィックを分析する際にシステムのパフォーマンスを向上させるための情報を提供しています。

遅延ベースのパフォーマンス設定固有の情報については、パケットおよび侵入ルールの遅延しきい値構成，（1246 ページ）を参照してください。

アクセス制御への他のポリシーの関連付け

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

次のサブポリシーのいずれかとアクセス コントロール ポリシーとを関連付けるには、アクセス コントロール ポリシーの詳細設定を使用します。

- SSL ポリシー：セキュア ソケット レイヤ（SSL）または Transport Layer Security（TLS）で暗号化されたアプリケーション層プロトコル トラフィックをモニタ、復号化、ブロック、または許可します。

注意 SSL ポリシーを追加または削除すると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作，（326 ページ）を参照してください。

- アイデンティティ ポリシー：トラフィックに関連付けられているレルムと認証方式に基づいて、ユーザ認証を実行します。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 適切な [ポリシー設定（Policy Settings）] 領域の編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 3 ドロップダウン リストからポリシーを選択します。

ユーザが作成したポリシーを選択する場合は、表示される編集アイコンをクリックしてポリシーを編集できます。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 35 章

アクセス コントロール ルール

次の各トピックでは、アクセス コントロール ルールの設定方法について説明します。

アクセス コントロール ルールの概要

アクセス コントロール ポリシー内では、アクセス コントロール ルールによって複数の管理対象デバイスでネットワーク トラフィックを処理するきめ細かい制御方法が提供されます。

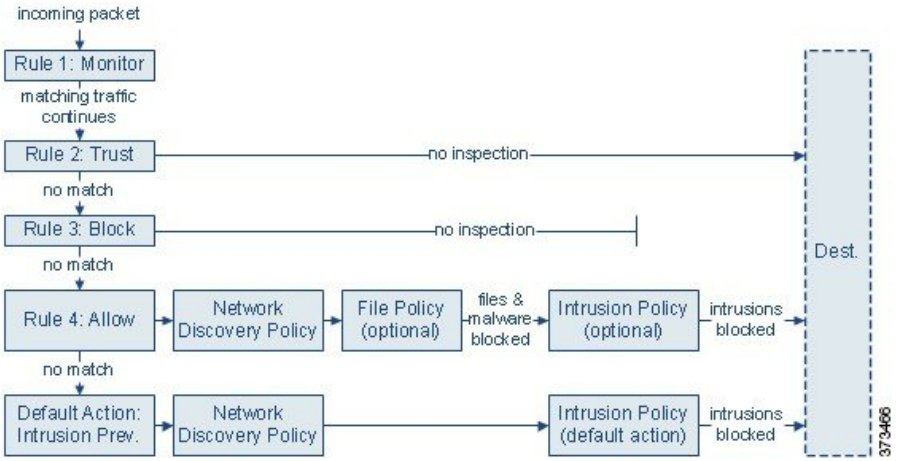
（注） アクセス コントロール ルールがネットワーク トラフィックを評価する前に、8000 シリーズ高速パス、セキュリティ インテリジェンスのフィルタリング、SSL インスペクション、ユーザの識別、および一部の復号と前処理が発生します。

システムは、指定した順にアクセスコントロールルールをトラフィックと照合します。ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。

また、各ルールにはアクションがあり、これによって一致するトラフィックをモニタ、信頼、ブロック、または許可するかを決定します。トラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したり

ネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

次のシナリオでは、インラインの侵入防御展開環境で、アクセスコントロールルールによってトラフィックを評価できる方法を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **ルール 1**：**モニタ**はトラフィックを最初に評価します。モニタ ルールはネットワーク トラフィックを追跡してログに記録しますが、トラフィック フローには影響しません。システムは引き続きトラフィックを追加のルールと照合し、許可するか拒否するかを決定します。
- **ルール 2**：**信頼**はトラフィックを 2 番目に評価します。一致するトラフィックは追加のインスペクションなしで宛先まで通過することが許可されますが、引き続きアイデンティティの要件との対象となります。一致しないトラフィックは、引き続き次のルールと照合されます。
- **ルール 3**：**ブロック**はトラフィックを 3 番目に評価します。一致するトラフィックは、追加のインスペクションなしでブロックされます。一致しないトラフィックは、引き続き最後のルールと照合されます。
- **ルール 4**：**許可**は最後のルールです。このルールの場合、一致したトラフィックは許可されますが、トラフィック内の禁止ファイル、マルウェア、侵入、エクスプロイトは検出されてブロックされます。残りの禁止されていない悪意のないトラフィックはで宛先まで通過することが許可されますが、引き続きアイデンティティの要件との対象となります。ファイルインスペクションのみを実行する、または侵入インスペクションのみを実行する、もしくは両方とも実行しない許可ルールを設定できます。
- **デフォルトアクション**は、いずれのルールにも一致しないすべてのトラフィックを処理します。このシナリオでは、デフォルトアクションは、悪意のないトラフィックの通過を許可する前に侵入防御を実行します。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルト アクションを割り当てることもあります。（デフォルトアクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません。）

アクセス コントロール ルールまたはデフォルト アクションによって許可したトラフィックは、自動的にホスト、アプリケーション、およびユーザ データについてネットワーク検出ポリシーによるインスペクションの対象になります。ディスカバリを拡張することや無効化することはできますが、明示的に有効にはしません。ただし、トラフィックを許可しても、ディスカバリ データ収集が自動的に保証されるわけではありません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。また、アプリケーション検出は、暗号化されたセッションに限定されます。

暗号化されたトラフィックの通過が SSL インスペクション設定で許可される場合、または SSL インスペクションが設定されていない場合は、そのトラフィックがアクセス コントロール ルールによって処理されることに注意してください。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、システムは暗号化ペイロードの侵入およびファイル インスペクションを無効にしています。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

アクセス コントロール ルールの管理

アクセス コントロール ポリシー エディタの [ルール（Rules）] タブでは、編集中のポリシーのアクセス コントロール ルールの追加、編集、分類、検索、移動、有効化、無効化、削除、その他の管理が行えます。

ポリシー エディタでは、各アクセス コントロール ルールに対してルールの名前、条件の概要、ルール アクションが表示され、さらにルールのインスペクション オプションや状態を示すアイコンが表示されます。各アイコンの意味は次のとおりです。

- 侵入ポリシー オプション（  ）
- ファイル ポリシー オプション（  ）
- ロギング オプション（  ）
- コメント（  ）
- 警告（  ）
- エラー（  ）
- 重要な情報（  ）

無効なルールはグレー表示され、ルール名の下に [（無効）（(disabled)）] というマークが付きます。

ルールを作成または編集するには、アクセス コントロール ルール エディタを使用します。次の操作を実行できます。

- エディタの上部で、ルールの名前、状態、位置、アクションなどの基本的なプロパティを設定します。

- エディタの左下にあるタブを使用して、条件を追加します。
- インスペクションおよびロギングのオプションを設定し、さらにルールにコメントを追加するには、右下にあるタブを使用します。便宜上、どのタブを表示しているかに関係なく、エディタにはルールのインスペクションおよびロギングのオプションがリストされます。

（注） アクセス コントロール ルールの適切な作成と順序付けは複雑なタスクですが、効果的な展開を構築するためには不可欠です。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、追加のライセンスが必要となったり、ルールに無効な設定が含まれる場合があります。システムが想定どおりにトラフィックを確実に処理できるように、アクセス コントロール ポリシー インターフェイスにはルールに対する強力な警告およびエラーのフィードバック システムがあります。

アクセス コントロール ルールのコンポーネント

一意の名前に加え、各アクセス コントロール ルールには次の基本コンポーネントがあります。

状態（State）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置（Position）

アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。ポリシー継承を使用する場合、ルール 1 は再外部ポリシーの 1 番目のルールです。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。モニタ ルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

また、ルールはセクションおよびカテゴリに属していることがあります。これは、単に整理のためであり、ルールの位置に影響しません。ルールの位置は、すべてのセクションとカテゴリにまたがって設定されます。

セクションおよびカテゴリ

アクセス コントロール ルールの整理に役立つように、アクセス コントロール ポリシーには、システムで用意されている 2 つのルール セクションとして「必須（Mandatory）」と「デフォルト（Default）」があります。アクセス コントロール ルールをさらに細かく整理するため、「必須（Mandatory）」セクション内と「デフォルト（Default）」セクション内にカスタム ルール カテゴリを作成することができます。

ポリシーの継承を使用する場合、現在のポリシーのルールは、その親ポリシーの「必須（Mandatory）」セクションと「デフォルト（Default）」セクションの間にネストされます。

条件（Conditions）

条件は、ルールが処理する特定のトラフィックを指定します。条件には単純なものと複雑なものがあり、ライセンスによって用途が異なります。

アクション（Action）

ルールのアクションによって、一致したトラフィックの処理方法が決まります。一致したトラフィックをモニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。信頼できるトラフィック、ブロックされたトラフィック、または暗号化されたトラフィックに対しては、詳細な検査は実行されません。

インスペクション（Inspection）

詳細検査オプションは、悪意のあるトラフィックをどのように検査してブロックし、それ以外のものは許可するかを決定します。ルールを使用してトラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出たりする前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

ログ

ルールのロギング設定によって、システムが記録する処理済みトラフィックのレコードを管理します。1 つのルールに一致するトラフィックのレコードを 1 つ保持できます。一般的に、接続の開始時または終了時（あるいは、その両方）にセッションをログに記録できます。接続のログは、データベースの他に、システム ログ（Syslog）または SNMP トラップ サーバに記録できます。

説明

アクセス コントロール ルールで変更を保存するたびに、コメントを追加できます。

アクセス コントロール ルールの順序

アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で先頭から順にアクセス コントロール ルールをトラフィックと照合します。

ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。モニタ ルール（トラフィックをログに記録するが、トラフィック フローには影響しないルール）を除き、いずれかのルールとトラフィックが一致した後、システムは優先順位の低い追加ルールに対してトラフィックの評価を継続しません。

アクセス コントロール ルールの整理に役立つように、アクセス コントロール ポリシーには、システムで用意されている 2 つのルール セクションとして「必須（Mandatory）」と「デフォルト（Default）」があります。さらに細かく整理するため、「必須（Mandatory）」セクション内や「デフォルト（Default）」セクション内にカスタム ルール カテゴリを作成することができます。カテゴリは、作成した後に移動することはできません。ただし、カテゴリを削除または名前変更したり、ルールをカテゴリ内またはカテゴリ間で移動したりすることはできます。システムはセクションとカテゴリに横断的にルール番号を割り当てます。

ポリシーの継承を使用する場合、現在のポリシーのルールは、その親ポリシーの「必須（Mandatory）」ルール セクションと「デフォルト（Default）」ルール セクションの間にネストされます。ルール 1 は、現在のポリシーではなく、最外部ポリシーの 1 番目のルールです。ルールの番号は、すべてのポリシー、セクション、カテゴリにまたがって割り当てられます。

アクセス コントロール ポリシーの変更を許可する定義済みユーザ ロールによって、ルールのカテゴリ内またはカテゴリ間でアクセス コントロール ルールを移動および変更することもできます。しかし、ユーザがルールを移動および変更することを制限するには、カスタム ロールを作成できます。アクセス コントロール ポリシーの変更権限が割り当てられているユーザは、制限なく、カスタム カテゴリにルールを追加することや、カテゴリ内のルールを変更することができます。

ヒント アクセス コントロール ルールの順序を適切に設定することで、ネットワーク トラフィック処理に必要なリソースを削減して、ルールのプリエンプションを回避できます。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

アクセス制御ルール カテゴリの追加

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

アクセス コントロール ポリシーの必須ルール セクションとデフォルト ルール セクションをカスタム カテゴリに分割できます。カテゴリを作成した後は、そのカテゴリの削除と名前の変更に加え、カテゴリへのルールの挿入、ルールの削除、カテゴリ内またはカテゴリ間のルールの移動はできますが、カテゴリ自体の移動はできません。システムはセクションとカテゴリに横断的にルール番号を割り当てます。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[カテゴリの追加（Add Category）] をクリックします。

ヒント ポリシーにルールがすでに含まれている場合は、既存のルールの行の空白部分をクリックして、新しいカテゴリを追加する前にその位置を設定できます。既存のルールを右クリックし、[新規カテゴリの挿入（Insert new category）] を選択することもできます。

ステップ 2 名前を入力します。

ステップ 3 [挿入（Insert）] ドロップダウン リストから、カテゴリを追加する先を選択します。

- カテゴリをセクションのすべての既存カテゴリの下に挿入するには、[必須ルール内（Into Mandatory）] または [デフォルトルール内（into Default）] を選択します。
- 既存のカテゴリの上に挿入するには、[カテゴリの上（above category）] を選択した後、カテゴリを選択します。
- アクセス制御ルールの上または下に挿入するには、[ルールの上（above rule）] または [ルールの下（below rule）] を選択した後、既存のルール番号を入力します。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

アクセス コントロール ルールの作成および編集

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

注意 アクセス コントロール ポリシーによって使用される侵入ポリシーの総数の変更 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。 現在使用されていない侵入ポリシーを追加するか、侵入ポリシーの最後のインスタンスを削除することで、侵入ポリシーの総数を変更します。アクセス コントロール ルールで侵入ポリシーをデフォルトのアクションまたはデフォルトの侵入ポリシーとして使用できます。

手順

ステップ 1 アクセス コントロール ポリシー エディタには、以下のオプションがあります。

- 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- 既存のルールを編集するには、編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ 2 名前を入力します。

ステップ 3 以下のルール コンポーネントを設定するか、デフォルトを受け入れます。

- [有効（Enabled）] : ルールを有効にするかどうかを指定します。
- [位置（Position）] : ルールの位置を指定します。アクセス コントロール ルールの順序, （805 ページ）を参照してください。
- [アクション（Action）] : ルールの [アクション（Action）] を選択します。アクセス コントロール ルールのアクション, （810 ページ）を参照してください。
- [条件（Conditions）] : 追加する条件に対応するタブをクリックします。詳細は、ルール条件タイプ, （341 ページ）を参照してください。
- [ディープインスペクション（Deep Inspection）] : 許可ルールおよびインタラクティブ ブロック ルールの場合、侵入調査アイコン（  ）またはファイルおよびマルウェア調査アイコン（  ）をクリックして、ルールの [インスペクション（Inspection）] オプションを設定します。アイコンが淡色表示の場合、そのタイプのポリシーがルールに選択されていません。詳細については、侵入ポリシーとファイル ポリシーを使用したアクセス制御, （815 ページ）を参照してください。
- [ロギング（Logging）] : アクティブな（青の）ロギング アイコン（  ）をクリックして、[ロギング（Logging）] オプションを指定します。アイコンが淡色表示の場合、接続ロギングがそのルールで無効になっています。詳細については、接続ロギング ストラテジー, （1908 ページ）を参照してください。
- [コメント（Comments）] : コメント列の数字をクリックして、[コメント（Comments）] を追加します。数字は、ルールにすでに含まれているコメントの数を示します。詳細については、アクセス コントロール ルールのコメント, （813 ページ）を参照してください。

ステップ 4 ルールを保存します。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

アクセス コントロール ルールの有効化と無効化

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

アクセスコントロールルールを作成すると、そのルールはデフォルトで有効になります。ルールを無効にすると、システムはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。アクセス コントロール ポリシーのルール リストを表示したときに、無効なルールはグレー表示されますが、変更は可能です。

ヒント また、ルール エディタを使用してアクセス コントロール ルールを有効化または無効化することもできます。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、ルールを右クリックし、ルールの状態を選択します。

代わりに表示アイコン（）がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ 2 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

アクセス コントロール ルールの配置

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

既存のルールは、アクセス コントロール ポリシー内で移動できますが、アクセス コントロール ポリシー間では移動できません。カテゴリにルールを追加または移動すると、そのルールはシステムによってカテゴリの最後に配置されます。

ヒント　複数のルールを一度に移動するには、移動するルールを選択し、右クリック メニューを使用してカット アンド ペーストします。

手順

ステップ 1　アクセス制御ルール エディタには、次のオプションがあります。

- 新しいルールを追加する場合は、[挿入（Insert）] ドロップダウンリストを使用します。
- 既存のルールを編集する場合、[移動（Move）] をクリックします。

ステップ 2　ルールを移動またはルールを挿入する場所を選択します。

- [必須に挿入（into Mandatory）] または [デフォルトに挿入（into Default）] を選択します。
- [カテゴリに挿入（into Category）] を選択して、ユーザ定義カテゴリを選択します。
- [ルールの上（above rule）] または [ルールの下（below rule）] を選択してから、適切なルール番号を入力します。

ステップ 3　[保存（Save）] をクリックします。

ステップ 4　[保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

アクセス コントロール ルールのアクション

アクセス コントロール ルールには、システムが一致するトラフィックをどのように処理し、ロギングするのかを指定するアクションがあります。モニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。

アクセス コントロール ポリシーのデフォルト アクションは、モニタ アクセス コントロール ルール以外のどの条件にも一致しないトラフィックを処理します。

アクセス コントロール ルールのモニタ アクション

モニタ アクションはトラフィック フローに影響を与えません。つまり、一致するトラフィックがただちに許可または拒否されることはありません。その代わり、追加のルールに照らしてトラ

フィックが照合され、許可/拒否が決定されます。モニタ ルール以外の一致する最初のルールが、トラフィック フローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、システムはデフォルト アクションを使用します。

モニタ ルールの主な目的はネットワーク トラフィックのトラッキングなので、システムはモニタ対象トラフィックの接続終了イベントを自動的にログに記録します。つまり、トラフィックが他のルールに一致せず、デフォルト アクションでロギングが有効になっていない場合でも、接続はログに記録されます。

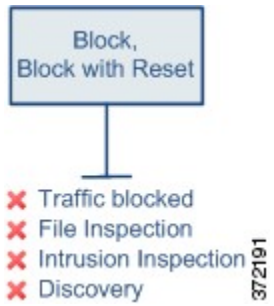
（注） ローカル内トラフィックがレイヤ 3 展開のモニタ ルールに一致する場合、そのトラフィックはインスペクションをバイパスすることがあります。トラフィックのインスペクションを確実に実行するには、トラフィックをルーティングしている管理対象デバイスの詳細設定で [ローカル ルータ トラフィックの検査（Inspect Local Router Traffic）] を有効にします。

アクセス コントロール ルールの信頼アクション

[信頼（Trust）]アクションは、ディープインスペクションやネットワーク検出をせずにトラフィックを通過させます。信頼処理されたトラフィックも、ID 条件およびの対象です。

アクセス コントロール ルールのブロック アクション

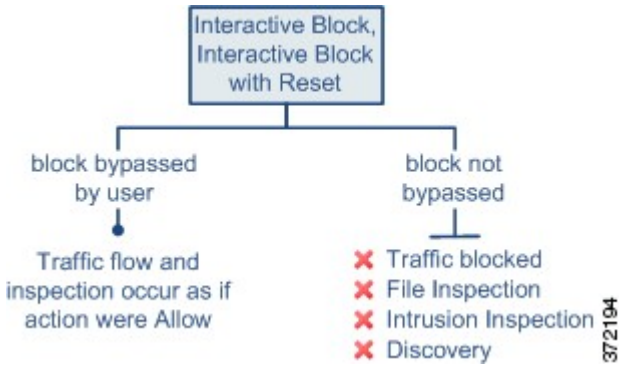
ブロック アクションおよびリセットしてブロック アクションはトラフィックを拒否し、いかなる追加のインスペクションも行われません。リセットしてブロック ルールでは接続のリセットも行います。



Web リクエストをブロックした際、*HTTP* 応答ページを表示できます。HTTP 応答ページとインタラクティブ ブロッキング，（825 ページ）を参照してください。

アクセス コントロール ルール インタラクティブ ブロック アクション

インタラクティブ ブロック アクションおよびリセット付きインタラクティブ ブロック アクションを使用すると、ユーザはカスタマイズ可能な警告ページ（*HTTP* 応答ページと呼ばれます）をクリック スルーすることで、Web サイトのブロックをバイパスできます。リセット付きインタラクティブ ブロック ルールでは接続のリセットも行います。詳細については、HTTP 応答ページとインタラクティブ ブロッキング，（825 ページ）を参照してください。



ユーザがブロックをバイパスする場合、ルールは許可ルールを模倣します。したがって、ユーザは、どちらかのタイプのインタラクティブ ブロック ルールをファイル ポリシーと侵入ポリシーに関連付け、このユーザ許可されたトラフィックを検査できます。システムがネットワーク検出で検査することもできます。

ユーザがブロックをバイパスしない（できない）場合は、ルールはブロック ルールを模倣します。一致するトラフィックは、追加のインスペクションなしで拒否されます。

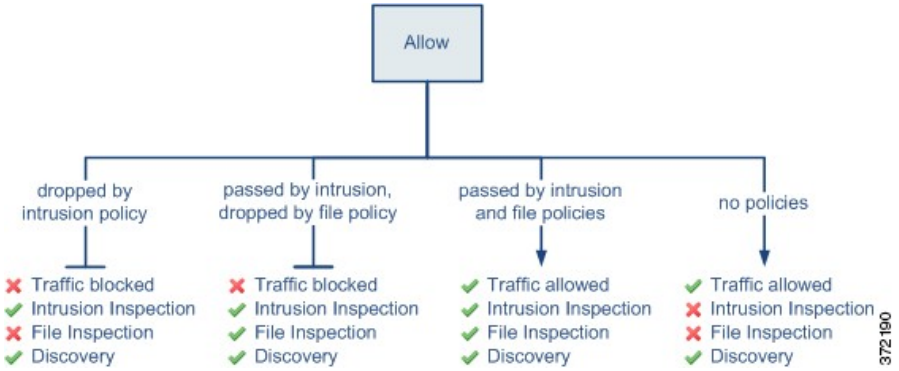
アクセス コントロール ルールの許可アクション

[許可（Allow）] アクションは、一致するトラフィックを通過させます。ただし、引き続き ID 条件およびの対象となります。

任意で、ディープ インスペクションを行い、トラフィックが接続先に到達する前に暗号化されていないトラフィックや復号されたトラフィックを検査、ブロックすることも可能です。

- 侵入ポリシーでは、侵入検知と防御設定に応じてネットワーク トラフィックを分析し、設定内容に応じて違反パケットをドロップすることが可能です。
- ファイル ポリシーでは、ファイルの制御ができます。ファイル制御により、ユーザが特定のアプリケーション プロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出およびブロックすることができます。
- ファイル ポリシーでは、ネットワークベースの高度なマルウェア防御（AMP）を実行することもできます。AMP for Firepower は設定に応じて、マルウェアがないかファイルを検査し、検出したマルウェアをブロックします。

下の図は、許可ルールの条件（またはユーザによりバイパスされるインタラクティブ ブロック ルール）を満たすトラフィックに対して実行されるインスペクションの種類を示しています。侵入インスペクションの前にファイル インスペクションが行われることに注意してください。そこでブロックされたファイルに対しては、侵入関連のエクスプロイトについては検査されません。



シンプルにするために、この図では、侵入ポリシーとファイル ポリシーの両方がアクセス コントロール ルールに関連付けられている状態（またはどちらも関連付けられていない状態）のトラフィック フローを示しています。ただし、どちらか 1 つだけを設定することも可能です。ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーによって決定されます。侵入ポリシーがない場合、トラフィック フローはファイル ポリシーによって決定されます。

トラフィックが侵入ポリシーとファイル ポリシーのどちらかによって検査またはドロップされるかどうかに関わらず、システムはネットワーク検出を使ってトラフィックを検査できます。ただし、トラフィックを許可しても、ディスカバリ検査が自動的に保証されるわけではありません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。また、アプリケーション検出は、暗号化されたセッションに限定されます。

アクセス コントロール ルールのコメント

アクセス コントロール ルールを作成または編集するときは、コメントを追加できます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。あるルールの全コメントのリストを表示し、各コメントを追加したユーザやコメント追加日を確認することができます。

ルールを保存すると、最後に保存してから追加されたすべてのコメントは読み取り専用になります。

アクセス制御ルールへのコメントの追加

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

手順

ステップ 1 アクセス コントロール ルール エディタで、[コメント（Comments）] タブをクリックします。

ステップ 2 [New Comment] をクリックします。

ステップ 3 コメントを入力し、[OK] をクリックします。ルールを保存するまでこのコメントを編集または削除できます。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 36 章

侵入ポリシーとファイル ポリシーを使用したアクセス制御

次の各トピックでは、侵入ポリシーとファイル ポリシーを使用するようにアクセス コントロール ポリシーを設定する方法について説明します。

ディープ インスペクションについて

侵入ポリシーとファイル ポリシーは、トラフィックが宛先に対して許可される前の最後のとりでとして連携して動作します。

- 侵入ポリシーは、システムの侵入防御機能を制御します。
- ファイル ポリシーは、システムのファイル制御と AMP for Firepower の機能を管理します。

アクセス コントロールはディープ インスペクションの前に発生し、アクセス コントロール ルールおよびアクセスコントロールのデフォルトアクションによって、侵入ポリシーおよびファイル ポリシーで検査されるトラフィックが決まります。

侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセスコントロールルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイル ポリシー（またはその両方）を使ってトラフィックを検査するよう、システムに指示できます。

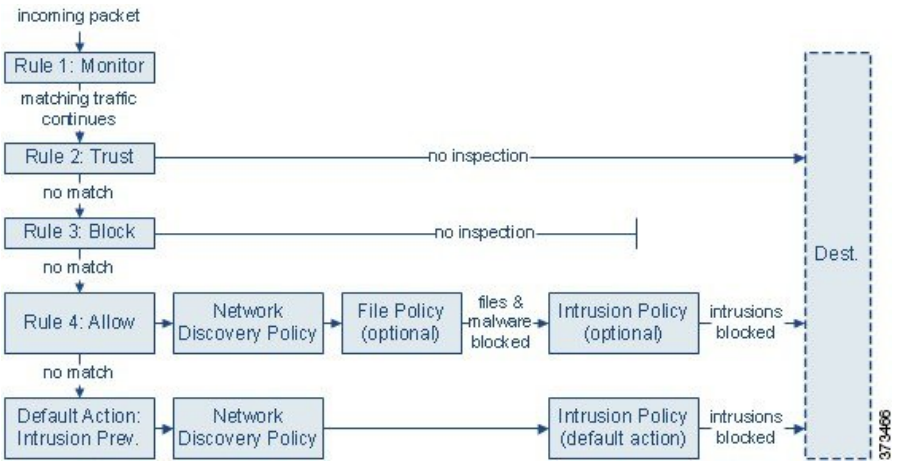
（注） デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイルインスペクションは無効になっています。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

システムは、AMP クラウドからエンドポイント向け AMP データを受信し、このデータを任意の AMP for Firepower データと一緒に表示できます。

アクセス コントロール トラフィック処理

アクセス コントロール ルールは、複数の管理対象デバイスでネットワーク トラフィックを処理する詳細な方法を提供します。システムは、指定した順にアクセス コントロール ルールをトラフィックと照合します。ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。アクセスコントロールルールのアクションによって、システムが一致するトラフィックをどのように処理するかが決まります。一致したトラフィックをモニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。

次の図は、4 つの異なるタイプのアクセス コントロール ルールとデフォルト アクションを含むアクセス コントロール ポリシーによって制御されている、インラインの侵入防御と AMP for Firepower の展開におけるトラフィックのフローを示します。



上記のシナリオでは、ポリシー内の最初の 3 つのアクセス コントロール ルール（モニタ、信頼およびブロック）は一致するトラフィックを検査できません。モニタ ルールはネットワーク トラフィックの追跡とロギングを行いますが検査はしないので、システムは引き続きトラフィックを追加のルールと照合し、許可または拒否を決定します。信頼ルールおよびブロック ルールは、どのような種類のインスペクションも追加で行うことなく一致するトラフィックを処理しますが、一致しないトラフィックは引き続き次のアクセス コントロール ルールに照合されます。

ポリシー内の 4 番目と最後のルールである許可ルールは、次の順序で他のさまざまなポリシーを呼び出し、一致するトラフィックを検査および処理します。

- **ディスカバリ**：**ネットワーク検出ポリシー**：最初に、ネットワーク検出ポリシーがトラフィックのディスカバリ データの有無を検査します。ディスカバリはパッシブ分析で、トラフィックのフローに影響しません。明示的にディスカバリを有効にしなくても、それを拡張または無効にできます。ただし、トラフィックを許可しても、ディスカバリ データ収集が自動的に保証されるわけではありません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。
- **AMP for Firepower とファイル制御**：**ファイル ポリシー**：システムは、トラフィックがディスカバリによって検査された後、トラフィックの禁止ファイルやマルウェアを検査できます。AMP for Firepower は、PDF、Microsoft Office 文書など多数のファイル タイプに潜むマルウェアを検出し、オプションでブロックできます。部門がマルウェア ファイル伝送のブロックに加えて、（ファイルにマルウェアが含まれるかどうかにかかわらず）特定のタイプのすべてのファイルをブロックする必要がある場合は、ファイル制御機能により、特定のファイル タイプの伝送についてネットワーク トラフィックをモニタし、ファイルをブロックまたは許可することができます。
- **侵入防御**：**侵入ポリシー**：ファイルインスペクションの後、システムは侵入およびエクスプロイトについてトラフィックを検査できます。侵入ポリシーは、復号されたパケットの攻撃をパターンに基づいて調査し、悪意のあるトラフィックをブロックしたり、変更したりします。侵入ポリシーは変数セットとペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映することができます。
- **接続先**：前述のすべてのチェックを通過したトラフィックは、その接続先に渡されます。

インタラクティブブロック ルール（この図には表示されていません）には、許可ルールと同じインスペクション オプションがあります。これにより、あるユーザが警告ページをクリック スルーすることによってブロックされた Web サイトをバイパスした場合に、悪意のあるコンテンツがないかトラフィックを検査できます。

ポリシー内のモニタ以外のアクセス コントロール ルールのいずれにも一致しないトラフィックは、デフォルト アクションによって処理されます。このシナリオでは、デフォルト アクションは侵入防御アクションとなり、トラフィックは指定された侵入ポリシーを通過する限りその最終接続先に許可されます。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルト アクションが割り当てられている場合もあります。システムはデフォルト アクションによって許可されたトラフィックに対しディスカバリ データおよび侵入の有無を検査できますが、禁止されたファイルまたはマルウェアの有無は検査できないことに注意してください。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

（注） 場合によっては、接続がアクセス コントロール ポリシーによって分析される場合、システムはトラフィックを処理するアクセス コントロール ルール（存在する場合）を決定する前に、その接続の最初の数パケットを処理し**通過を許可する**必要があります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。

ファイル インスペクションおよび侵入インスペクションの順序

アクセス コントロール ポリシーで、複数の許可ルールとインタラクティブ ブロック ルールを異なる侵入ポリシーおよびファイルポリシーに関連付けて、インスペクションプロファイルをさまざまなタイプのトラフィックに照合できます。

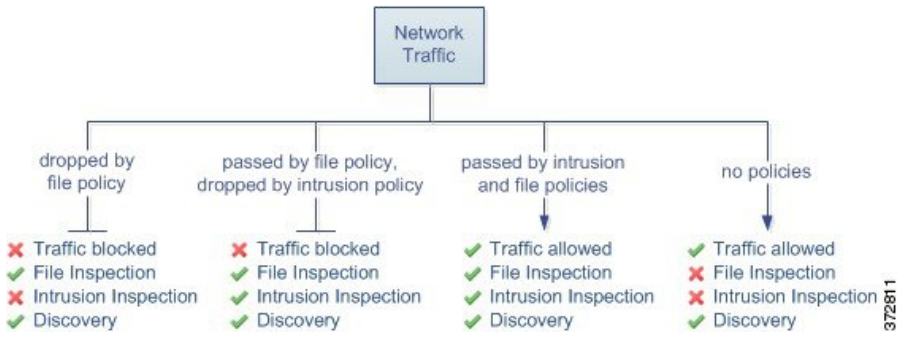
（注） 侵入防御またはネットワーク検出のみのデフォルトアクションによって許可されたトラフィックは、検出データおよび侵入の有無について検査されますが、禁止されたファイルまたはマルウェアの有無については検査されません。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

同じルールでファイル インスペクションと侵入インスペクションの両方を実行する必要はありません。許可ルールまたはインタラクティブ ブロック ルールに一致する接続の場合：

- ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーによって決まります
- 侵入ポリシーがない場合、トラフィック フローはファイル ポリシーによって決まります
- どちらもない場合、許可されたトラフィックはネットワーク検出のみで検査されます。

ヒント システムは、信頼されたトラフィックに対してはどんなインスペクションも実行しません。侵入ポリシーもファイル ポリシーも含めずに許可ルールを設定すると、信頼ルールの場合と同様にトラフィックが通過しますが、許可ルールでは一致するトラフィックに対して検出を実行できます。

以下の図は、「許可」アクセス コントロール ルール、またはユーザによりバイパスされた「インタラクティブ ブロック」アクセス コントロール ルールのどちらかの条件を満たすトラフィックに対して実行できるインスペクションの種類を示しています。単純化のために、侵入/ファイル ポリシーの両方が 1 つのアクセス コントロール ルールに関連付けられている（またはどちらも関連付けられていない）状態でのトラフィック フローを図に示しています。



アクセス コントロール ルールによって処理される単一接続の場合、ファイル インスペクションは侵入インスペクションの前に行われます。つまり、システムは侵入のためファイル ポリシーによってブロックされたファイルを検査しません。ファイル インスペクション内では、タイプによ

る単純なブロッキングの方が、マルウェア インスペクションおよびブロッキングよりも優先されます。

たとえば、アクセス コントロール ルールで定義された特定のネットワーク トラフィックを正常に許可するシナリオを考えてください。ただし、予防措置として、実行可能ファイルのダウンロードをブロックし、ダウンロードされたPDFのマルウェアインスペクションを行って検出された場合はブロックし、トラフィックに対して侵入インスペクションを実行する必要があるとします。

一時的に許可するトラフィックの特性に一致するルールを持つアクセスコントロールポリシーを作成し、それを侵入ポリシーとファイルポリシーの両方に関連付けます。ファイルポリシーはすべての実行可能ファイルのダウンロードをブロックし、マルウェアを含むPDFも検査およびブロックします。

- まず、システムはファイル ポリシーで指定された単純なタイプ マッチングに基づいて、すべての実行可能ファイルのダウンロードをブロックします。これはすぐにブロックされるため、これらのファイルは、マルウェアインスペクションの対象にも侵入インスペクションの対象にもなりません。
- 次に、システムは、ネットワーク上のホストにダウンロードされたPDFに対するマルウェアクラウドルックアップを実行します。マルウェアの性質を持つPDFはすべてブロックされ、侵入インスペクションの対象にはなりません。
- 最後に、システムはアクセス コントロール ルールに関連付けられている侵入ポリシーを使用して、ファイルポリシーでブロックされなかったファイルを含む残りのトラフィック全体を検査します。

（注） ファイルがセッションで検出されブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

ファイル制御およびマルウェア保護のためのアクセス コントロール ルールの設定

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールをファイル ポリシーに関連付けることができます。ファイル インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なるファイルおよびマルウェアのインスペクション プロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムはファイル ポリシーの設定に従って禁止されたファイル（マルウェアを含む）を検出すると、イベントをFirepower Management Centerデータベースに自動的にロギングします。ログファイルまたはマルウェア イベントが必要ない場合は、アクセス コントロール ルールごとにこのロギングを無効にできます。

また、システムは、呼び出し元のアクセスコントロールルールのロギング設定にかかわらず、関連付けられた接続の終了を Firepower Management Center データベースにロギングします。

ファイル制御および AMP を実行するアクセス コントロール ルールの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（ファイル制御） マルウェア（AMP）	保護（ファイル制御） マルウェア（AMP）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

注意 [ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] を選択、[ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] ルールで [ファイルの保存（Store files）] または無効化、または [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] または [マルウェア ブロック（Block Malware）] ファイル ルール アクションを分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[動的分析（Dynamic Analysis）]、または [ローカル マルウェア分析（Local Malware Analysis）]）またはファイルの保存オプション（[マルウェア（Malware）]、[不明（Unknown）]、[正常（Clean）]、または [カスタム（Custom）]）と結合する最初のファイル ルールを追加または最後のファイル ルールを削除すると、設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

はじめる前に

- AMP を含むファイル制御をアクセス コントロール ルールで実行するためには、適応型プロファイルの設定, （1431 ページ） で説明されているように、アダプティブ プロファイルを有効にする**必要があります**。

手順

ステップ 1 アクセス コントロール ルール エディタで、[許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] の [アクション（Action）] を選択します。

ステップ 2 [インスペクション（Inspection）] タブをクリックします。

ステップ 3 アクセス コントロール ルールに一致するトラフィックを検査する場合は [マルウェア ポリシー（Malware Policy）]（ファイル ポリシー）を選択し、または一致するトラフィックに対するファイル インスペクションを無効にする場合は [なし（None）] を選択します。

ステップ 4 （オプション）[ロギング（Logging）] タブをクリックし、[ログ ファイル（Log Files）] チェックボックスをオフにして、一致する接続のファイルまたはマルウェア イベントのロギングを無効にします。

（注） シスコでは、ファイル イベントおよびマルウェア イベントのロギングを有効のままにすることを推奨しています。

ステップ 5 ルールを保存します。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

侵入防御のためのアクセス コントロール ルールの設定

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールを侵入ポリシーに関連付けることができます。侵入インスペクションを許可アクセスコントロールルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なる侵入インスペクション プロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セット使用します。セット内の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

ヒント システム提供の侵入ポリシーを使用する場合であっても、正確にネットワーク環境を反映するためにシステムの侵入変数を設定することを**強く**推奨します。少なくとも、デフォルト セットにあるデフォルトの変数を変更します。

システムによって提供される侵入ポリシーとカスタム侵入ポリシーについて

Firepowerシステムには複数の侵入ポリシーが付属しています。システム提供の侵入ポリシーを使用することで、Cisco Talos Security Intelligence and Research Group（Talos）の経験を活用できます。これらのポリシーでは、Talos が侵入ルールおよびプリプロセッサ ルールの状態を設定し、詳細設定の初期設定も提供します。システムによって提供されるポリシーをそのまま使用するか、またはカスタムポリシーのベースとして使用できます。カスタムポリシーを作成すれば、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。

接続イベントおよび侵入イベントのロギング

アクセスコントロールルールによって呼び出された侵入ポリシーが侵入を検出すると、侵入イベントを生成し、そのイベントを Firepower Management Center に保存します。また、システムはアクセス コントロール ルールのロギング設定に関係なく、侵入が発生した接続の終了を Firepower Management Center データベースに自動的にロギングします。

アクセス コントロール ルールの設定と侵入ポリシー

ユーザが独自に作成するカスタム侵入ポリシーに加え、初期インライン ポリシーと初期パッシブ ポリシーの 2 つのカスタム ポリシーがシステムで用意されています。これらの 2 つの侵入ポリシーは、ベースとして Balanced Security and Connectivity 侵入ポリシーを使用します。両者の唯一の相違点は、[インライン時にドロップ（Drop When Inline）] 設定です。インライン ポリシーではドロップ動作が有効化され、パッシブ ポリシーでは無効化されています。

1 つのアクセス コントロール ポリシーで使用可能な固有の侵入ポリシーの数は、ターゲット デバイスのモデルによって異なります。より強力なデバイスは、より多数のポリシーを処理できます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。異なる侵入ポリシーと変数セットのペアをそれぞれの許可ルールおよびインタラクティブ ブロック ルール（およびデフォルトアクション）と関連付けることができますが、ターゲットデバイスが設定されたとおりに検査を実行するのに必要なリソースが不足している場合は、アクセス コントロール ポリシーを展開できません。

侵入防御を実行するアクセス コントロール ルールの設定

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

注意 アクセス コントロール ポリシーによって使用される侵入ポリシーの総数の変更 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作，（326 ページ）を参照してください。 現在使用されていない侵入ポリシーを追加するか、侵入ポリシーの最後のインスタンスを削除することで、侵入ポリシーの総数を変更します。アクセス コントロール ルールで侵入ポリシーをデフォルトのアクションまたはデフォルトの侵入ポリシーとして使用できます。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、新しいルールを作成するか、既存のルールを編集します。アクセス コントロール ルールのコンポーネント，（804 ページ）を参照してください。

ステップ 2 ルール アクションが [許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定されていることを確認します。

ステップ 3 [削除インスペクション タブを選択します。

ステップ 4 システムによって提供されるまたはカスタムの侵入ポリシーを選択するか、またはアクセス コントロール ルールに一致するトラフィックに対する侵入インスペクションを無効にするには [なし（None）] を選択します。

ステップ 5 侵入ポリシーに関連付けられた変数セットを変更するには、[変数セット（Variable Set）] ドロップダウン リストから値を選択します。

ステップ 6 [保存（Save）] をクリックしてルールを保存します。

ステップ 7 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

第 37 章

HTTP応答ページとインタラクティブブロッキング

ここでは、システムが Web 要求をブロックしたときに表示されるカスタム ページの設定方法について説明します。

HTTP 応答ページについて

アクセス制御の一部として、アクセス コントロール ルールあるいはアクセス コントロール ポリシーのデフォルト アクションを使って、システムが Web リクエストをブロックしたときに表示する *HTTP* 応答ページを設定できます。

システム提供の汎用応答ページを選択するか、カスタム HTML を入力できます。表示される応答ページはセッションのブロック方法によって異なります。

- ブロックまたはリセット付きブロックの場合、ブロックされたセッションはタイムアウトするかリセットされます。ブロック応答ページにより、接続が拒否されたことを示すデフォルトのブラウザ ページまたはサーバ ページは上書きされます。
- インタラクティブ ブロックまたはリセット付きインタラクティブ ブロックの場合、システムはインタラクティブ ブロック応答ページを表示してユーザに警告しますが、ユーザはボタンをクリック（あるいはページを更新）して要求したサイトをロードできます。応答ページをバイパスした後、ロードされなかったページの要素をロードするために、ページを更新しなければならない場合があります。

システムが Web トラフィックをブロックしたときに必ず HTTP 応答ページが表示されるわけではありません。HTTP 応答ページの制限，（826 ページ）を参照してください。

HTTP 応答ページの制限

システムが Web トラフィックをブロックする場合に、常に、HTTP 応答ページが表示されるわけではありません。

アクセス コントロール ルール以外の設定

システムは、アクセス コントロール ルールまたはアクセス コントロール ルールのデフォルト アクションのいずれかによってブロックされた（またはインタラクティブにブロックされた）暗号化されていない接続または復号された接続の場合にのみ、応答ページを表示します。次の場合、システムは応答ページを表示しません。

- セキュリティ インテリジェンスによってブラックリストに載せられた接続
- SSL ポリシーによってブロックされた暗号化接続

プロモートされたアクセス コントロール ルール

Web トラフィックがプロモートされたアクセス コントロール ルール（単純なネットワーク条件のみの早期に適用されたブロッキング ルール）の結果としてブロックされている場合、システムは応答ページを表示しません。

URL 識別の前

システムは、システムが要求された URL を識別する前にトラフィックがブロックされた場合は、応答ページを表示しません。URL フィルタリングの制限, （362 ページ）を参照してください。

暗号化されたトラフィック

システムは、セッションが暗号化されている、または暗号化されていた場合は、応答ページを表示しません。

HTTP 応答ページの選択

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

HTTP 応答ページを確実に表示できるかは、ネットワーク設定、トラフィック負荷、およびページのサイズによって異なります。ページが小さいほど、正常に表示される傾向にあります。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、[HTTP 応答（HTTP Responses）] タブをクリックします。
コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 2 [応答ページをブロック（Block Response Page）] および [応答ページのインタラクティブ ブロック（Interactive Block Response Page）] を選択します。

- [System-provided]：一般的な応答が表示されます。表示アイコン（  ）をクリックすると、このページのコードが表示されます。
- [Custom]：カスタム応答ページが作成されます。ポップアップ ウィンドウが表示されます。このウィンドウに事前入力されているシステムによって提供されるコードを編集アイコン（  ）をクリックして置換または変更できます。カウンタで使用した文字数が表示されます。
- [None]：応答ページを無効にして、インタラクションや説明なしでセッションをブロックします。アクセス コントロール ポリシー全体でインタラクティブ ブロッキングを無効にするには、このオプションを選択します。

ステップ 3 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

HTTP 応答ページでのインタラクティブ ブロッキング

インタラクティブ ブロッキングを設定すると、ユーザは警告を読んだ後に当初要求したサイトを読み込むことができます。応答ページをバイパスした後、ロードされなかったページの要素をロードするために、ページを最新表示しなければならない場合があります。

ヒント アクセス コントロール ポリシー全体に対してインタラクティブ ブロッキングを素早く無効にするには、システム提供のページもカスタム ページも表示しないでください。そうすると、システムにより操作なしですべての接続がブロックされます。

ユーザがインタラクティブ ブロックをバイパスしない場合、一致するトラフィックは拒否され、追加のインスペクションは行われません。ユーザがインタラクティブ ブロックをバイパスするとアクセス コントロール ルールはトラフィックを許可しますが、引き続きトラフィックはディープ インスペクションやブロッキングの対象となる場合があります。

デフォルトでは、ユーザのバイパスは後続のアクセスで警告ページを表示することなく、10 分（600 秒）間有効です。期間を 1 年に設定したり、ユーザに毎回ブロックをバイパスするように強制できます。この制限は、ポリシー内のすべてのインタラクティブブロック ルールに適用されます。ルールごとに制限を設定することはできません。

インタラクティブブロックされるトラフィックに関するロギング オプションは、許可されたトラフィックに関するオプションと同じですが、ユーザがインタラクティブ ブロックをバイパスしない場合、システムがログに記録できるのは接続開始イベントだけです。システムが最初にユーザに警告すると、ロギングされた接続開始イベントはシステムにより [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションでマークされます。ユーザがブロックをバイパスすると、セッションが記録される追加の接続イベントに [許可（Allow）] アクションが付きます。

インタラクティブ ブロッキングの設定

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

手順

ステップ 1 アクセス コントロールの一部として、Web トラフィックと一致するアクセス コントロール ルールを設定します。アクセス コントロール ルールの作成および編集, （807 ページ）を参照してください。

- アクション：ルール アクションを [インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定します。アクセス コントロール ルール インタラクティブ ブロック アクション, （812 ページ）を参照してください。
- 条件：URL 条件を使用して、インタラクティブにブロックする Web トラフィックを指定します。URL 条件（URL フィルタリング）, （356 ページ）を参照してください。
- ロギング：ユーザがブロックをバイパスすると想定し、それに応じてロギング オプションを選択します。許可された接続のロギング, （1915 ページ）を参照してください。

- インスペクション：ユーザがブロックをバイパスすると想定し、それに応じてディープインスペクション オプションを選択します。侵入ポリシーとファイル ポリシーを使用したアクセス制御，（815 ページ）を参照してください。

ステップ 2 （オプション）アクセス コントロール ポリシーの [HTTP 応答（HTTP Responses）] タブで、カスタム インタラクティブ ブロックの HTTP 応答ページを選択します。HTTP 応答ページの選択，（826 ページ）を参照してください。

ステップ 3 （オプション）アクセス コントロール ポリシーの [詳細（Advanced）] タブで、ユーザのバイパス タイムアウトを変更します。ブロックされた Web サイトのユーザ バイパス タイムアウトの設定，（829 ページ）を参照してください。
ユーザはブロックをバイパスした後、そのページを参照でき、タイムアウト期間が経過するまで警告は表示されません。

ステップ 4 アクセス コントロール ポリシーを保存します。

ステップ 5 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

ブロックされた Web サイトのユーザ バイパス タイムアウトの設定

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

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [全般設定（General Settings）] の横にある編集アイコン（  ）をクリックします。
代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 3 [ブロックをバイパスするためのインタラクティブ ブロックを許可する期間（秒）（Allow an Interactive Block to bypass blocking for (seconds)）] フィールドに、ユーザ バイパスの期限が切れるまでの経過時間を秒数で入力します。ゼロを指定すると、ユーザはブロックを毎回強制的にバイパスします。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 38 章

セキュリティ インテリジェンス ブラックリスト

以下のトピックでは、セキュリティ インテリジェンスの概要（トラフィックのブラックリストとホワイトリストの使用、基本設定など）を示します。

セキュリティ インテリジェンスについて

悪意のあるインターネットコンテンツに対する防御の前線として、セキュリティインテリジェンスは疑わしいIPアドレス、URL、ドメイン名が関連する接続をレピュテーションインテリジェンスを使用して迅速にブロックします。これは、セキュリティインテリジェンスブラックリスト登録と呼ばれます。

セキュリティ インテリジェンスはアクセス制御の最初のフェーズであり、大量のリソースを消費する評価をシステムが実行する前に行われます。ブラックリスト登録により、インスペクションの必要がないトラフィックを迅速に除外することで、パフォーマンスが向上します。

（注） FastPath が適用されたトラフィックをブラックリストに登録することはできません。8000 シリーズの FastPath 適用は、セキュリティ インテリジェンスによるフィルタリングの前に行われます。FastPath が適用されたトラフィックは、セキュリティインテリジェンスを含め、以降のすべての評価をバイパスします。

カスタムブラックリストを設定することはできますが、CIscoは定期的に更新されるインテリジェンス フィードへのアクセスを提供しています。マルウェア、スパム、ボットネット、フィッシン

グなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。

セキュリティ インテリジェンスのブラックリスト登録を改良するには、ホワイトリストとモニタ専用ブラックリストを併せて使用するという方法があります。これらのメカニズムは、トラフィックをブラックリストに登録しないようにしますが、一致するトラフィックを自動的に信頼したりFastPathを適用したりすることは**しません**。ホワイトリストに登録されたトラフィックや、セキュリティインテリジェンスの段階でモニタされるトラフィックは、意図的に残りのアクセスコントロールによる分析が適用されます。

セキュリティ インテリジェンスの設定

特定のIPアドレス、URL、ドメイン名をホワイトリストまたはブラックリストに登録したりモニタしたりするためには、カスタム オブジェクト、リスト、またはフィードを設定する必要があります。次の選択肢があります。

- ネットワーク、URL、DNS フィールドを設定するには、セキュリティ インテリジェンス フィードの作成, （424 ページ）を参照してください。
- ネットワーク、URL、DNS リストを設定するには、セキュリティ インテリジェンス リストの更新, （428 ページ）を参照してください。
- ネットワーク オブジェクトとオブジェクト グループを設定するには、ネットワーク オブジェクトの作成, （389 ページ）を参照してください。
- URL オブジェクトとオブジェクト グループを設定するには、URL オブジェクトの作成, （395 ページ）を参照してください。

DNSリストまたはフィードに基づくトラフィックのブラックリスト/ホワイトリスト登録あるいはモニタリングには、以下の条件もあります。

- DNS ポリシーを作成します。詳細については、基本 DNS ポリシーの作成, （842 ページ）を参照してください。
- DNS リストまたはフィードを参照する DNS ルールを設定します。詳細については、DNS ルールの作成および編集, （845 ページ）を参照してください。

DNS ポリシーはアクセス コントロール ポリシーの一部として展開するため、両方のポリシーを関連付ける必要があります。詳細については、DNSポリシーの展開, （854ページ）を参照してください。

セキュリティ インテリジェンス戦略

セキュリティ インテリジェンス戦略では、次の要素を使用します。

- Cisco提供のフィード：Ciscoでは、定期的に更新されるインテリジェンス フィードへのアクセスを提供しています。マルウェア、スパム、ボットネット、フィッシングなど、セキュリ

ティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。

- サードパーティのフィード：Cisco 提供のフィードをサードパーティのフィードで補完できます。これらのフィードは、Firepower Management Center が定期的にインターネットからダウンロードする動的リストです。
- グローバルおよびカスタムブラックリスト：特定の IP アドレス、URL、ドメイン名をブラックリストに登録します。パフォーマンスを向上させるために、スパムのブラックリスト登録を電子メール トラフィックを処理するセキュリティ ゾーンに制限するなどして、適用対象を絞り込むこともできます。
- 誤検出をなくすためのホワイトリスト：ブラックリストの範囲が広すぎる場合、または残りのアクセス コントロールでさらに分析するトラフィックを前もってブロックしてしまう場合は、ブラックリストをカスタム ホワイトリストでオーバーライドできます。
- ブラックリスト登録に代わるモニタリング：特にパッシブ展開や、フィードを実装する前にテストする場合に有用です。違反しているセッションをブロックする代わりに単にモニタしてログに記録し、接続終了イベントを生成できます。

（注） パッシブ展開環境では、パフォーマンスを最適化するために、Cisco では常にモニタ専用の設定を使用することを推奨しています。パッシブに展開された管理対象デバイスはトラフィック フローに影響を与えることができないため、トラフィックをブロックするようにシステムを構成しても何のメリットもありません。また、ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

例：ホワイトリスト登録

信頼できるフィードにより、重要なリソースへのアクセスが不適切にブロックされたものの、そのフィードが全体としては組織にとって有用である場合は、そのフィード全体をブラックリストから削除するのではなく、不適切に分類された IP アドレスだけをホワイトリストに登録するという方法を取ることができます。

例：ゾーンを使用したセキュリティ インテリジェンス

不適切に分類された IP アドレスをホワイトリストに登録した後、組織内でそれらの IP アドレスにアクセスする必要があるユーザが使用しているセキュリティ ゾーンによりホワイトリストのオブジェクトを制限するという方法が考えられます。この方法では、ビジネス ニーズを持つユーザだけが、ホワイトリストに登録された URL にアクセスできます。あるいは、サードパーティのスパム フィードを使用して、電子メール サーバのセキュリティ ゾーンのトラフィックをブラックリスト登録するという方法もあります。

例：モニタ専用のブラックリスト登録

たとえば、サードパーティのフィードを使用したブロッキングを実装する前に、そのフィードをテストする必要があるとします。フィードをモニタ専用に設定すると、ブロックされるはずの接続をシステムで詳細に分析できるだけでなく、そのような接続のそれぞれをログに記録して、評価することもできます。

セキュリティ インテリジェンスの設定

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

各アクセス コントロール ポリシーには、セキュリティ インテリジェンス オプションがあります。ネットワーク オブジェクト、URL オブジェクトとリスト、およびセキュリティ インテリジェンス フィードとリストをホワイトリストまたはブラックリストに追加でき、これらはすべてセキュリティ ゾーンによって制約できます。アクセス コントロール ポリシーに DNS ポリシーを関連付け、ドメイン名をホワイトリストまたはブラックリストに追加することもできます。

注意 アクセス コントロール ポリシーの [セキュリティ インテリジェンス（Security Intelligence）] タブからホワイトリストまたはブラックリストに複数のオブジェクトを追加したり、複数のオブジェクトを削除したりします。設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。Snort プロセスが再起動するかどうかは、インスペクションに使用できるメモリに応じて、デバイスごとに異なる場合があることに注意してください。

ホワイトリストとブラックリストには、合計 255 個までのネットワーク オブジェクトおよび合計 32767 個までの URL オブジェクトとリストを追加できます。つまり、ホワイトリスト内のオブジェクトの数とブラックリスト内の数の合計が 255 個のネットワーク オブジェクトまたは 32767 個の URL オブジェクトとリストを超えることはできません。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

はじめる前に

- パッシブ展開の場合、またはモニタのみにセキュリティ インテリジェンス フィルタリングを設定する場合は、ロギングを有効にします。セキュリティ インテリジェンスによる接続のロギング, （1917 ページ）を参照してください。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス（Security Intelligence）] タブをクリックします。
コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 2 次の選択肢があります。

- [ネットワーク（Networks）] タブをクリックして、ネットワーク オブジェクトを追加します。
- [URL（URLs）] タブをクリックして、URL オブジェクトを追加します。

ステップ 3 ホワイトリストまたはブラックリストに追加する利用可能なオブジェクトを探します。次の選択肢があります。

- [名前または値で検索（Search by name or value）] フィールドに入力して、利用可能なオブジェクトを検索します。[リロード（reload）]（  ）または[クリア（clear）]（  ）をクリックして、検索文字列をクリアします。
- 既存のリストまたはフィードがニーズを満たしていない場合は、追加アイコン（  ）をクリックし、[新規ネットワーク リスト（New Network List）] または [新規 URL リスト（New URL List）] を選択し、セキュリティ インテリジェンス フィードの作成, （424 ページ）または新しいセキュリティ インテリジェンス リストの Firepower Management Center へのアップロード, （427 ページ）の説明に従って続行します。
- 既存のオブジェクトがニーズを満たしていない場合は、追加アイコン（  ）をクリックし、[新規ネットワーク オブジェクト（New Network Object）] または [新規 URL オブジェクト（New URL Object）] を選択し、ネットワーク オブジェクトの作成, （389 ページ）の説明に従って続行します。

セキュリティ インテリジェンスは、/0 ネットマスクを使用して、IP アドレス ブロックを無視します。

ステップ 4 追加する 1 つ以上の利用可能なオブジェクトを選択します。

ステップ 5 オプションで、[利用可能なゾーン（Available Zone）] を選択して、選択したオブジェクトをゾーンごとに制約します。

システムが提供するセキュリティ インテリジェンス リストをゾーンで制約することはできません。

ステップ 6 [ホワイトリストに追加（Add to Whitelist）] または [ブラックリストに追加（Add to Blacklist）] をクリックするか、選択したオブジェクトをクリックしていずれかのリストにドラッグします。

ホワイトリストまたはブラックリストからオブジェクトを削除するには、その削除アイコン（  ）をクリックします。複数のオブジェクトを削除するには、オブジェクトを選択し、右クリックして [選択項目の削除（Delete Selected）] を選択します。

ステップ 7 オプションで、ブラックリスト登録されたオブジェクトをモニタ専用に設定するには、[ブラックリスト（Blacklist）] にリストされている該当するオブジェクトを右クリックし、[モニタ専用（ブロックしない）（Monitor-only (do not block)）] を選択します。

システムが提供するセキュリティインテリジェンスリストをモニタ専用に設定することはできません。

ステップ 8 [DNS ポリシー（DNS Policy）] ドロップダウン リストから DNS ポリシーを選択します。DNS ポリシーの概要, （839 ページ） を参照してください。

ステップ 9 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

セキュリティ インテリジェンス オプション

アクセス制御ポリシー エディタのセキュリティ インテリジェンス タブを使用して、ネットワーク（IP アドレス）と URL セキュリティ インテリジェンスを設定し、アクセス制御ポリシーを DNS ポリシーに関連付けます。

オブジェクト、ゾーン、ブラックリスト アイコン

アクセス制御ポリシー エディタのセキュリティ インテリジェンス タブで、オブジェクトまたはゾーンのそれぞれのタイプを別のアイコンと区別します。

ブラックリストでは、ブロックに設定したオブジェクトにはブロック アイコン（  ）を付け、監視対象のみのオブジェクトには、監視アイコン（  ）を付けます。監視のみの場合には、アクセス制御を使用して、ブラックリストの IP アドレスと URL を含む接続を処理し、ブラックリストに一致する接続をロギングします。

ホワイトリストがブラックリストをオーバーライドするため、両方のリストに同じオブジェクトを追加すると、ブラックリスト登録されたオブジェクトに取り消し線が表示されます。

ゾーンの制約

システムが提供したグローバル リスト以外、ゾーンごとにセキュリティ インテリジェンス フィルタリングを制約できます。複数のゾーンでオブジェクトのセキュリティインテリジェンスフィ

ルタリングを適用するには、ゾーンのそれぞれについて、オブジェクトをホワイトリストまたはブラックリストに追加する必要があります。

ログ

デフォルトで有効になっているセキュリティ インテリジェンス ロギングは、アクセス制御ポリシー対象のデバイスが処理するブロックされ、監視対象である接続はすべてロギングされます。ただし、システムはホワイトリストの一致はロギングしません。ホワイトリストに登録された接続のロギングは、その接続の最終的な傾向によって異なります。ブラックリストの接続については、ブラックリスト対象のオブジェクトを監視のみに設定する前にロギングを有効にする必要があります。

セキュリティ インテリジェンス カテゴリ

セキュリティインテリジェンス カテゴリ	説明
Attacker	アクティブ スキャナと悪意のある発信アクティビティが知られているブラックリストのホスト。
Bogon	Bogon ネットワークおよび割り当てられていない IP アドレス
Bots	バイナリ マルウェア ドロッパを有するサイト
CnC	botnets 用のホスト C & C サーバを有するサイト
Dga	C&Cサーバのランデブー ポイントとして機能するさまざまなドメイン名を生成するために使用されるマルウェア アルゴリズム
Exploitkit	クライアントのソフトウェアの脆弱性を特定するために設計されたソフトウェア キット
Malware	マルウェアバイナリまたはエクスプロイト キットを有するサイト
OpenProxy	匿名の web ブラウジングが可能な公開プロキシ
OpenRelay	スパム用に使用されることが既知のオープン メール リレー
Phishing	フィッシング ページを有するサイト
応答	悪意があるか疑わしいアクティブに積極的に参加している IP アドレスと URL
Spam	スパムを送信することが知られているメール ホスト
Suspicious	疑いがあり、既知のマルウェアと同様の特性を持つようなファイル

セキュリティ インテリジェンス カテゴリ	説明
TorExitNode	Tor exit ノード

第 39 章

DNS ポリシー

次のトピックでは、DNS ポリシーと DNS ルールについて、および管理対象デバイスに DNS ポリシーを導入する方法について説明します。

DNS ポリシーの概要

DNSベースのセキュリティインテリジェンスにより、クライアントが要求したドメイン名に基づいて、トラフィックをホワイトリスト/ブラックリストに登録できるようになります。シスコが提供するドメイン名のインテリジェンスを使用して、トラフィックをフィルタリングできます。また、環境に合わせて、ドメイン名のカスタム リストやフィードを設定することも可能です。

DNS ポリシーによってブラックリスト登録されたトラフィックは即座にブロックされるため、他のさらなるインスペクションの対象にはなりません（侵入、エクスプロイト、マルウェアなどについてだけでなくネットワーク検出についても）。ブラックリストをホワイトリストで上書きしてアクセス コントロール ルールによる評価を強制することができます。また、セキュリティ インテリジェンス フィルタリングに「モニタ専用」設定を使用でき、パッシブ展開環境ではこの設定が推奨されます。この設定では、ブラックリスト登録されたであろう接続をシステムが分析できるだけでなく、ブラックリストに一致する接続がログに記録され、接続終了セキュリティ インテリジェンス イベントが生成されます。

（注） 期限切れのため、またはクライアントの DNS キャッシュやローカル DNS サーバのキャッシュがクリアされているか、期限切れであるために、DNS サーバでドメイン キャッシュが削除されない場合に、DNS ベースのセキュリティ インテリジェンスが意図したとおりに機能しないことがあります。

DNS ポリシーおよび関連付けられた DNS ルールを使用して DNS ベースのセキュリティ インテリジェンスを設定します。デバイスにこれを展開するには、アクセス コントロール ポリシーに DNS ポリシーを関連付けてから管理対象デバイスに設定を展開する必要があります。

DNS ポリシーのコンポーネント

DNS ポリシーにより、ドメイン名に基づいて、接続をホワイトリストまたはブラックリストに登録できます。次のリストに、DNS ポリシーの作成後に変更可能な設定を示します。

名前（Name）と説明（Description）

各 DNS ポリシーには固有の名前が必要です。説明は任意です。

マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

ルール（Rule）

ルールは、ドメイン名に基づいてネットワーク トラフィックを処理する詳細な方法を提供します。DNS ポリシーのルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、トラフィックを DNS ルールと上から順に照合します。

DNS ポリシーを作成すると、システムはこれをデフォルトのグローバル DNS ホワイトリスト ルールおよびデフォルトのグローバル DNS ブラックリスト ルールに入力します。両方のルールは、それぞれのカテゴリで先頭の位置に固定されます。これらのルールは変更できませんが無効にすることはできます。

マルチドメイン展開では、子孫 DNS ホワイトリスト ルールおよび子孫 DNS ブラックリスト ルールも先祖ドメインの DNS ポリシーに追加されます。これらのルールは、それぞれのカテゴリの 2 番目の位置に固定されます。

（注） Firepower Management Center でマルチテナンシーが有効になっている場合、システムは先祖ドメインと子孫ドメインを含むドメインの階層に編成されます。これらのドメインは、DNS 管理で使用されるドメイン名とは別になります。

子孫のリストには、Firepower システムのサブドメイン ユーザによってホワイトリストまたはブラックリストに登録されたドメインが含まれます。先祖ドメインから、子孫のリストの内容を表示することはできません。サブドメイン ユーザをホワイトリストまたはブラックリストに登録しない場合は、次を実行します。

- 子孫のリストのルールを無効にします。
- アクセス コントロール ポリシーの継承設定を使用してセキュリティ インテリジェンスを適用します。

ルールはシステムにより次の順序で評価されます。

- グローバル DNS ホワイトリスト ルール（有効な場合）
- 子孫 DNS ホワイトリスト ルール（有効な場合）
- ホワイトリスト ルール
- グローバル DNS ブラックリスト ルール（有効な場合）
- 子孫 DNS ブラックリスト ルール（有効な場合）
- ブラックリスト ルールおよびモニタ ルール

通常、システムによる DN ベースのネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。トラフィックに一致する DNS ルールがない場合、システムは、関連付けられたアクセス コントロール ポリシー ルールに基づいてトラフィックの評価を続行します。DNS ルール条件は単純または複雑のどちらでも構いません。

基本 DNS ポリシーの作成

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

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [DNS]を選択します。

ステップ 2 [DNS ポリシーの追加（Add DNS Policy）] をクリックします。

ステップ 3 [名前（Name）] に一意のポリシー名を入力し、オプションで [説明（Description）] にポリシーの説明を入力します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 必要に応じて、セキュリティインテリジェンスによる接続のロギング，（1917ページ）の説明に従って、さらに新しいポリシーを設定します。
- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

DNS ポリシーの編集

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

DNS ポリシーの編集は、1 つのブラウザ ウィンドウを使用して、一度に 1 人のみで行う必要があります。複数のユーザが同じポリシーを保存を試みた場合、最初に保存された一連の変更だけが保持されます。

セッションのプライバシーを保護するために、ポリシー エディタで 30 分間操作が行われないと警告が表示されます。60 分後には、システムにより変更が破棄されます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [DNS]を選択します。

ステップ 2 編集する DNS ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 DNS ポリシーを編集します。

- 名前と説明：名前または説明を変更するには、フィールドをクリックして新しい情報を入力します。
- ルール：DNS ルールを追加、分類、有効化、無効化、または管理する場合は、[ルール（Rules）] タブをクリックして、DNS ルールの作成および編集, （845 ページ）の説明に従って続行します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

DNS ポリシーの管理

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

[DNS ポリシー（DNS Policy）] ページ（[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [DNS]）を使用して、DNS のカスタム ポリシーを管理します。自分で作成したカスタム ポリシーに加えて、システムにはデフォルトの DNS ポリシーが用意されています。このポリシーは、デフォルトのブラックリストとホワイトリストを使用します。このシステム付属のカスタムポリシーは編集して使用できます。マルチドメイン展開では、このデフォルトポリシーはデフォルトのグローバル DNS ブラックリスト、グローバル DNS ホワイトリスト、子孫 DNS ブラックリスト、および子孫 DNS ホワイトリストを使用します。また、このポリシーはグローバル ドメインでのみ編集できます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [DNS]を選択します。

ステップ 2 DNS ポリシーを以下のように管理します。

- 比較：DNS ポリシーを比較するには、[ポリシーの比較（Compare Policies）] をクリックして、ポリシーの比較, （331 ページ）で説明する手順を実行します。
- コピー：DNS ポリシーをコピーするには、コピー アイコン（  ）をクリックして、DNS ポリシーの編集, （842 ページ）で説明する手順を実行します。
- 作成：新しい DNS ポリシーを作成するには、[DNS ポリシーの追加（Add DNS Policy）] をクリックし、基本 DNS ポリシーの作成, （842 ページ）で説明する手順を実行します。
- 削除：DNS ポリシーを削除するには、削除アイコン（  ）をクリックし、ポリシーの削除を確認します。
- 編集：既存の DNS ポリシーを変更するには、編集アイコン（  ）をクリックし、DNS ポリシーの編集, （842 ページ）で説明する手順を実行します。

DNS ルール

DNS ルールは、ホストが要求するドメイン名に基づいてトラフィックを処理します。セキュリティ インテリジェンスの一部として、この評価は、トラフィックの復号の後、アクセス コントロール評価の前に適用されます。

システムは指定した順序でトラフィックをDNSルールと照合します。ほとんどの場合、システムによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。DNS ルールを作成すると、システムは、モニタ ルールとブラックリスト ルールの前にホワイトリスト ルールを配置し、最初にホワイトリスト ルールに対してトラフィックを評価します。

各 DNS ルールには、一意の名前以外にも、次の基本コンポーネントがあります。

状態（State）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置（Position）

DNS ポリシーのルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で上から順に、トラフィックをルールと照合します。モニタ ルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

条件（Conditions）

条件は、ルールが処理する特定のトラフィックを指定します。DNS ルールには、DNS フィードまたはリスト条件が含まれている必要があり、セキュリティ ゾーン、ネットワーク、または VLAN によってトラフィックと照合することができます。

操作（Action）

ルールのアクションによって、一致したトラフィックの処理方法が決まります。

- ホワイトリストに登録されたトラフィックは許可され、アクセス コントロールによるさらなるインスペクションの対象になります。
- モニタ対象のトラフィックは、残りの DNS ブラックリスト ルールにより、さらなる評価の対象となります。DNS ブラックリスト ルールに一致しないトラフィックは、アクセス コントロール ルールに検査されます。そのトラフィックのセキュリティ インテリジェンス イベントは、システムにより記録されます。
- ブラックリストに登録されたトラフィックは、追加のインスペクションなしでドロップされます。[検出されないドメイン（Domain Not Found）] 応答を返すか、シンクホール サーバに DNS クエリをリダイレクトすることもできます。

関連トピック

セキュリティ インテリジェンスについて, （831 ページ）

DNS ルールの作成および編集

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

DNS ポリシーでは、ホワイトリスト ルールおよびブラックリスト ルールに合計 32767 個まで DNS リストを追加できます。つまり、DNS ポリシーのリストの数が 32767 を超えることはできません。

手順

ステップ 1 DNS ポリシー エディタには、以下のオプションがあります。

- 新しいルールを追加するには、[DNS ルールの追加（Add DNS Rule）] をクリックします。
- 既存のルールを編集するには、編集アイコン（  ）をクリックします。

ステップ 2 名前を入力します。

ステップ 3 以下のルール コンポーネントを設定するか、デフォルトを受け入れます。

- [アクション（Action）]：ルールの [アクション（Action）] を選択します。DNS ルールのアクション, （848 ページ）を参照してください。
- [条件（Conditions）]：ルールの条件を設定します。DNS ルールの条件, （849 ページ）を参照してください。
- [有効（Enabled）]：ルールを有効にするかどうかを指定します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

DNS ルールの管理

DNS ポリシー エディタの [ルール（Rules）] タブでは、ポリシー内の DNS ルールの追加、編集、移動、有効化、無効化、削除、その他の管理が行えます。

各ルールについて、ポリシーエディタでは、その名前、条件のサマリー、およびルールアクションが表示されます。他のアイコンにより、警告（  ）、エラー（  ）、その他の重要な情報（  ）が示されます。無効なルールはグレー表示され、ルール名の下に [無効（disabled）] というマークが付きます。

DNS ルールの有効化と無効化

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

作成したDNSルールは、デフォルトで有効になっています。ルールを無効にすると、システムはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。DNSポリシーのルール リストを表示すると、無効なルールはグレー表示されますが、変更は可能です。また、DNS ルール エディタを使用して DNS ルールを有効または無効にできることに注意してください。

手順

ステップ 1 DNS ポリシー エディタで、ルールを右クリックしてルール状態を選択します。

ステップ 2 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

DNS ルールの評価順序

DNS ポリシーのルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、DNS ルールを上から順にトラフィックと照合します。ほとんどの場合、システムによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。

- モニタ ルールでは、システムはまずトラフィックを記録し、その後、優先順位の低い DNS ブラックリスト ルールに対してトラフィックの評価を続行します。
- モニタ ルール以外では、トラフィックがルールに一致した後、システムは優先順位の低い追加の DNS ルールに対してトラフィックの評価は続行**しません**。

ルールの順序については、以下の点い注意してください。

- グローバル ホワイトリストは常に先頭で、他のすべてのルールよりも優先されます。
- 子孫 DNS ホワイトリスト ルールは、マルチドメイン展開の非リーフ ドメインでのみ表示されます。これは常に 2 番目であり、グローバル ホワイトリストを除き、他のすべてルールよりも優先されます。
- ホワイトリスト セクションはブラックリスト セクションよりも優先され、ホワイトリスト ルールは常に他のルールよりも優先されます。
- グローバル ブラックリストは常にブラックリスト セクションの先頭で、他のモニタ ルールおよびとブラックリスト ルールよりも優先されます。
- 子孫 DNS ブラックリスト ルールは、マルチドメイン展開の非リーフ ドメインでのみ表示されます。これは常にブラックリスト セクションの 2 番目であり、グローバル ブラックリストを除き、他のすべてのモニタ ルールおよびブラックリスト ルールよりも優先されます。
- ブラックリストセクションには、モニタ ルールおよびブラックリストルールが含まれます。

- 初めて DNS ルールを作成したときは、ホワイトリスト アクションを割り当てるとそれはシステムによりホワイトリストセクションの最後に配置され、他のアクションを割り当てるとブラックリスト セクションの最後に配置されます。

ルールをドラッグ アンド ドロップして、これらの順序を変更できます。

DNS ルールのアクション

すべてのDNSルールには、一致するトラフィックについて次のことを決定するアクションがあります。

- 処理：まずルールアクションは、システムがルールの条件に一致するトラフィックをホワイトリスト登録、モニタ、またはブラックリスト登録するかどうかを制御します。
- ロギング：ルールアクションによって、一致するトラフィックの詳細をいつ、どのようにログに記録できるかが決まります。

インラインで展開されたデバイスのみがトラフィックをブラックリスト登録できることに留意してください。パッシブに展開されたデバイスまたはタップ モードで展開されたデバイスは、トラフィックをホワイトリスト登録およびロギングできますが、トラフィックに影響を与えることはできません。

[ホワイトリスト（Whitelist）] アクション

[ホワイトリスト（Whitelist）]アクションにより、一致するトラフィックの通過が許可されます。トラフィックをホワイトリスト登録すると、そのトラフィックは、照合するアクセス コントロール ルール、またはアクセス コントロール ポリシーのデフォルト アクションによるさらなるインスペクションの対象になります。

システムは、ホワイトリストの一致はロギングしません。ただし、ホワイトリストに登録された接続のロギングは、接続の最終的な傾向によって異なります。

[モニタ（Monitor）] アクション

[モニタ（Monitor）]アクションはトラフィック フローに影響を与えません。つまり、一致するトラフィックがただちにホワイトリスト登録されたりブラックリスト登録されることはありません。その代わり、追加のルールに照らしてトラフィックが照合され、許可/拒否が決定されます。モニタ ルール以外の一致する最初の DNS ルールが、システムがトラフィックをブラックリスト登録するかどうかを決定します。一致する追加のルールがなければ、トラフィックはアクセス コントロール評価の対象となります。

DNSポリシーによってモニタされる接続については、システムは、接続終了セキュリティインテリジェンスと接続イベントを Firepower Management Center データベースにロギングします。

[ブラックリスト（Blacklist）] アクション

[ブラックリスト（Blacklist）]アクションは、いかなる種類のインスペクションなしで、トラフィックをブラックリスト登録します。

- [ドロップ（Drop）] アクションはトラフィックをドロップします。
- [検出されないドメイン（Domain Not Found）] アクションは、存在しないインターネット ドメインの応答を DNS クエリに返し、これによりクライアントが DNS 要求を解決することを防ぎます。
- [シンクホール（Sinkhole）] アクションは、応答内のシンクホール オブジェクトの IPv4 または IPv6 アドレスを DNS クエリに返します。シンクホール サーバは、IP アドレスへの後続の接続をロギングするか、またはロギングしてブロックすることができます。[シンクホール（Sinkhole）] アクションを設定する場合、シンクホール オブジェクトも設定する必要があります。

[ドロップ（Drop）] または [検出されないドメイン（Domain Not Found）] アクションに基づいてブラックリスト登録された接続については、システムは接続開始セキュリティ インテリジェンス イベントと接続イベントをロギングします。ブラックリスト登録されたトラフィックは追加のインスペクションなしですぐに拒否されるため、ログに記録できる固有の接続の終了イベントはありません。

[シンクホール（Sinkhole）] アクションに基づいてブラックリスト登録された接続については、ロギングはシンクホール オブジェクト設定によって異なります。シンクホール オブジェクトを、シンクホール接続をロギングのみするよう設定している場合、システムは、後続の接続の接続終了イベントをロギングします。シンクホール オブジェクトを、シンクホール接続をロギングしてブロックするよう設定している場合、システムは、後続の接続の接続開始イベントをロギングし、その後、その接続をブロックします。

（注） ASA FirePOWER デバイスでシンクホール アクションを使用して DNS ルールを設定し、トラフィックがルールに一致する場合、デフォルトでは ASA によって、後続のシンクホール接続がブロックされます。回避策として、ASA コマンド ラインから次のコマンドを実行します。

```
asa(config)# policy-map global_policy
asa(config-pmap)# class inspection_default
asa(config-pmap-c)# no inspect dns preset_dns_map
```

ASA が引き続き接続をブロックする場合は、サポートにお問い合わせください。

関連トピック

アクションと接続ロギング, （1912 ページ）

DNS ルールの条件

DNS ルールの条件によって、ルールが処理するトラフィックのタイプが識別されます。条件は単純または複雑のどちらでも構いません。DNS ルール内の DNS フィードまたはリスト条件を定義する必要があります。また、必要に応じてセキュリティ ゾーン、ネットワーク、または VLAN によってトラフィックを制御できます。

DNS ルールに条件を追加するときは、以下に留意してください。

- ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。
- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールの**すべての**条件に一致する必要があります。たとえば、DNS フィードまたはリスト条件およびネットワーク条件を含み、VLAN タグ条件を含まないルールは、セッション中の VLAN タグに関係なく、ドメイン名と送信元または宛先に基づいてトラフィックを評価します。
- ルールの条件ごとに、最大 50 の条件を追加できます。条件の基準の**いずれかに**一致するトラフィックはその条件を満たします。たとえば、単一ルールを使用して、最大 50 の DNS リストおよびフィードに基づいてトラフィックをブラックリスト登録できます。

DNS およびセキュリティ ゾーンに基づくトラフィックの制御

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

DNS ルール内のゾーン条件によって、その送信元および宛先セキュリティ ゾーン別にトラフィックを制御することができます。セキュリティ ゾーンは、複数のデバイス間に配置されている場合がある 1 つ以上のインターフェイスのグループです。検出モードと呼ばれる、デバイスの初期セットアップ時に選択するオプションによって、システムが最初にデバイスのインターフェイスをどのように設定するか、およびこれらのインターフェイスがセキュリティ ゾーンに属するかどうかが決定します。

手順

ステップ 1 DNS ルール エディタで、[ゾーン（Zones）] タブをクリックします。

ステップ 2 [利用可能なゾーン（Available Zones）] から追加するゾーンを見つけて選択します。追加するゾーンを検索するには、[利用可能なゾーン（Available Zones）] リストの上にある [名前で検索（Search by name）] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

ステップ 3 クリックして 1 つのゾーンを選択するか、右クリックして [すべて選択（Select All）] を選択します。

ステップ 4 [送信元に追加（Add to Source）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5 ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

DNS およびネットワークに基づくトラフィックの制御

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

DNSルール内のネットワーク条件によって、その送信元IPアドレス別にトラフィックを制御することができます。制御するトラフィックに対し、明示的に送信元 IP アドレスを指定できます。

手順

ステップ 1 DNS ルール エディタで、[ネットワーク（Networks）] タブをクリックします。

ステップ 2 [利用可能なネットワーク（Available Networks）] から、次のように追加するネットワークを見つけて選択します。

- ここでネットワーク オブジェクトを追加するには（後で条件に追加できます）、[利用可能なネットワーク（Available Networks）] リストの上にある追加アイコン（  ）をクリックし、ネットワーク オブジェクトの作成，（389 ページ）の説明に従って進みます。
- 追加するネットワーク オブジェクトを検索するには、[利用可能なネットワーク（Available Networks）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトのいずれかのコンポーネントのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 [送信元に追加（Add to Source）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 4 手動で指定する送信元 IP アドレスまたはアドレス ブロックを追加します。[送信元ネットワーク（Source Networks）] リストの下にある [IP アドレスの入力（Enter an IP address）] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [追加（Add）] をクリックします。
システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際のIPアドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ステップ 5 ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

DNS および VLAN に基づくトラフィックの制御

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

DNS ルールで VLAN 条件を設定すると、トラフィックの VLAN タグに応じてそのトラフィックを制御できます。システムは、最も内側の VLAN タグを使用して VLAN を基準にパケットを識別します。

VLAN ベースの DNS ルール条件を作成するときは、VLAN タグを手動で指定できます。または、VLAN タグ オブジェクトを使用して VLAN 条件を設定することもできます。VLAN タグ オブジェクトとは、いくつかの VLAN タグに名前を付けて再利用可能にしたものを指します。

手順

ステップ 1 DNS ルール エディタで、[VLAN タグ（VLAN Tags）] タブを選択します。

ステップ 2 [利用可能な VLAN タグ（Available VLAN Tags）] で、追加する VLAN を選択します。

- VLAN タグ オブジェクトをここで追加するには（後で条件に追加できます）、[利用可能な VLAN タグ（Available VLAN Tags）] リストの上にある追加アイコン（  ）をクリックし、VLAN タグ オブジェクトの作成，（394 ページ）の説明に従って進みます。
- 追加する VLAN タグ オブジェクトおよびグループを検索するには、[利用可能な VLAN タグ（Available VLAN Tags）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクト名またはオブジェクトの VLAN タグの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 4 手動で指定する VLAN タグを追加します。[選択した VLAN タグ（Selected VLAN Tags）] リストの下にある [VLAN タグの入力（Enter a VLAN Tag）] プロンプトをクリックし、VLAN タグまたはその範囲を入力して、[追加（Add）] をクリックします。1 から 4094 までの任意の VLAN タグを指定できます。VLAN タグの範囲を指定するにはハイフンを使用します。
システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の VLAN タグを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ステップ 5 ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

DNS リスト、フィード、またはカテゴリに基づくトラフィックの制御

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

DNS リスト、フィード、またはカテゴリがクライアントから要求されたドメイン名を含む場合、DNS ルール内の DNS 条件によりトラフィックを制御することができます。DNS ルール内の DNS 条件を定義する必要があります。

グローバルまたはカスタムのホワイトリストまたはブラックリストを DNS 条件に追加するかどうかに関わらず、システムは設定されたルール アクションをトラフィックに適用します。たとえばルールにグローバル ホワイトリストを追加し、[ドロップ（Drop）] アクションを設定すると、システムはホワイトリスト登録されている必要があるすべてのトラフィックをブラックリスト登録します。

手順

ステップ 1 DNS ルール エディタで、[DNS] タブをクリックします。

ステップ 2 次のように、[DNS リストおよびフィード（DNS Lists and Feeds）] から追加する DNS リストおよびフィードを検索して選択します。

- DNS リストまたはフィードをここで追加するには（後で条件に追加できます）、[DNS リストおよびフィード（DNS Lists and Feeds）] リストの上にある追加アイコン（  ）をクリックし、セキュリティ インテリジェンス フィードの作成, （424 ページ）の説明に従って進みます。
- 追加する DNS リスト、フィード、またはカテゴリを検索するには、[DNS リストおよびフィード（DNS Lists and Feeds）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 4 ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

DNS ポリシーの展開

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン
脅威（Threat）	Protection	任意（Any）	任意（Any）

DNS のポリシー設定の更新を終了した後に、アクセス コントロール設定の一部としてこれを展開する必要があります。

- セキュリティ インテリジェンスの設定，（834 ページ）で説明されているように、DNS ポリシーをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

第 40 章

インテリジェントアプリケーションバイパス

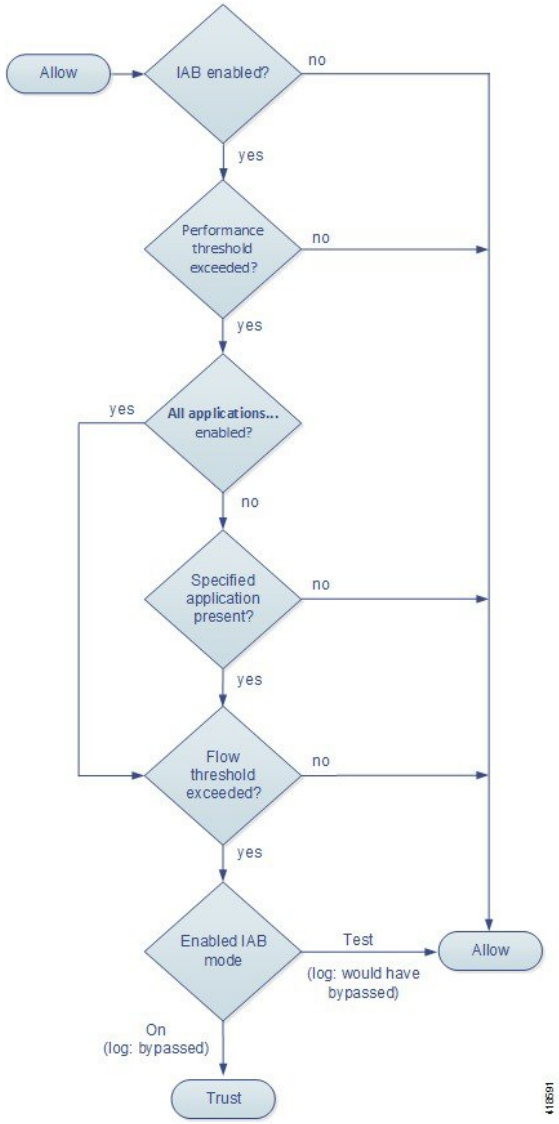
次のトピックでは、インテリジェント アプリケーション バイパス（IAB）を使用するようアクセス コントロール ポリシーを設定する方法について説明します。

IAB の概要

IABは、パフォーマンスとフローのしきい値を超過した場合に追加のインスペクションなしでネットワークを通過する信頼されるアプリケーションを特定します。たとえば、毎晩のバックアップがシステムパフォーマンスに大きく影響する場合、しきい値を超えてもバックアップアプリケーションが生成したトラフィックを信頼するように設定できます。オプションで、インスペクションパフォーマンスしきい値を超過したときに、IABが、いずれかのフロー バイパスしきい値を超えるすべてのトラフィックをアプリケーションのタイプに関係なく信頼するようにIABを設定できます。このオプションには、バージョン 6.0.1.4 か、後続の 6.0.1.x パッチが必要です。

IAB は、アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションによって許可されるトラフィックに対し、トラフィックが詳細なインスペクションの対象となる前に実行されます。テスト モードでは、しきい値を超過しているかどうか判断することと、しきい値を超過している場合、IAB を実際に有効化している状態（バイパス モードといいます）であればバイパスされたであろうアプリケーション フローを特定することが可能です。

次の図は、IAB の決定プロセスを示します。



IAB オプション

状態

IAB を有効または無効にします。

パフォーマンス サンプル インターバル（Performance Sample Interval）

システムが IAB パフォーマンスしきい値との比較のためにシステム パフォーマンス メトリックを収集する IAB パフォーマンス サンプリング スキャンの間隔を秒単位で指定します。値を 0 にすると、IAB が無効になります。

バイパス可能なアプリケーションとフィルタ（Bypassable Applications and Filters）

この機能には、相互に排他的な、次の 2 つのオプションがあります。

アプリケーション/フィルタ（Applications/Filters）

バイパス可能なアプリケーションおよびアプリケーション（フィルタ）のセットを指定できるエディタが提供されます。アプリケーション条件（アプリケーション制御），（350 ページ）を参照してください。

未確認アプリケーションを含むすべてのアプリケーション

インスペクション パフォーマンスしきい値を超過すると、アプリケーションのタイプに関係なく、いずれかのフロー バイパスしきい値を超過するすべてのトラフィックを信頼します。このオプションを使用するにはバージョン 6.0.1.4 またはそれ以降の 6.0.1.x パッチが必要です。

検査パフォーマンスしきい値（Inspection Performance Thresholds）

検査パフォーマンスしきい値は、侵入検査パフォーマンスの限界を提供し、これを超えるとフローしきい値の検査が開始されます。IAB は、0 に設定されている検査パフォーマンスしきい値を使用しません。

（注） インスペクション パフォーマンスしきい値とフロー バイパスしきい値は、デフォルトでは無効化されています。IAB がトラフィックを信頼するには、少なくともいずれか 1 つを有効化し、いずれか 1 つを超過している必要があります。インスペクション パフォーマンスしきい値またはフロー バイパスしきい値を複数有効にした場合、IAB がトラフィックを信頼するには、いずれか 1 つのみを超過する必要があります。

ドロップ率（Drop Percentage）

消費が激しい侵入ルール、ファイル ポリシー、圧縮解除などによってパフォーマンス過負荷となったためにパケットがドロップされた場合にドロップされたパケットが、パケット全体に占める割合の平均。侵入ルールのような通常の設定によってドロップされるパケットは含まれません。1 より大きい整数を指定すると、指定された割合のパケットがドロップされると IAB がアクティブになることに注意してください。1 を指定すると、0 ～ 1 の任意の割合によって IAB がアクティブになります。これにより、少数のパケットで IAB をアクティブにすることができます。

プロセッサ使用率（Processor Utilization Percentage）

プロセッサ リソースの平均使用率。

パケット遅延（Package Latency）

マイクロ秒単位の平均パケット遅延。

フロー レート（Flow Rate）

1秒あたりのフロー数で測定される、システムによるフロー処理率。このオプションでは、IABは、フローを件数ではなくレートで測定するように設定されることに注意が必要です。

フロー バイパスしきい値（Flow Bypass Thresholds）

フロー バイパスしきい値ではフロー制限が提供され、これを超えると、IABがバイパス モードでバイパス可能なアプリケーション トラフィックを信頼するようにトリガーされるか、またはテスト モードで追加の検査を受けるアプリケーション トラフィックが許可されます。IAB は、0 に設定されているフロー バイパスしきい値を使用しません。

（注） インスペクション パフォーマンスしきい値とフロー バイパスしきい値は、デフォルトでは無効化されています。IAB がトラフィックを信頼するには、少なくともいずれか 1 つを有効化し、いずれか 1 つを超過している必要があります。インスペクション パフォーマンスしきい値またはフロー バイパスしきい値を複数有効にした場合、IAB がトラフィックを信頼するには、いずれか 1 つのみを超過する必要があります。

フローあたりのバイト数

フローに含めることができる最大サイズ（KB）。

フローあたりのパケット数

フローに含めることができるパケットの最大個数。

フロー継続時間

フローをオープンのままにできる最長時間（秒）。

フロー速度

最大転送速度（KB/秒）。

IAB の設定

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

注意 すべての展開にIABが必要なわけではありません。IABを使用する展開では、限定的な方法でIABを使用する場合があります。ネットワーク トラフィック（特にアプリケーション トラフィック）とシステム パフォーマンス（予測可能なパフォーマンスの問題を含む）の専門知識がある場合を除き、IABを有効化しないでください。バイパス モードでIABを実行する前に、指定したトラフィックを信頼してもリスクが発生しないことを確認します。

手順

ステップ 1 アクセス コントロール ポリシー エディタで [詳細（Advanced）] タブをクリックし、[インテリジェント アプリケーション バイパス設定（Intelligent Application Bypass Settings）] の横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 2 IABのオプションを設定します。

- [状態（State）]：IABを [オフ（Off）] または [オン（On）]、あるいは [テスト（Test）] モードで有効にします。
- パフォーマンス サンプル間隔（Performance Sample Interval）：IABのパフォーマンス サンプリング スキャンの間隔を秒単位で入力します。IABを有効にした場合は、テスト モードであっても、ゼロ以外の値を入力します。0を入力すると、IABは無効になります。
- バイパス可能なアプリケーションとフィルタ（Bypassable Applications and Filters）：次のいずれかを実行します。
  - バイパスされるアプリケーションとフィルタの数をクリックし、トラフィックをバイパスするアプリケーションを指定します。アプリケーション条件とフィルタの設定，（351 ページ）を参照してください。
  - [未確認アプリケーションを含むすべてのアプリケーション（All applications including unidentified applications）] をクリックし、インスペクション パフォーマンスしきい値を超過したときに、IABが、いずれかのフロー バイパスしきい値を超えるすべてのトラフィックをアプリケーションのタイプに関係なく信頼するように設定します。このオプションを使用するにはバージョン6.0.1.4またはそれ以降の6.0.1.xパッチが必要です。
- [インスペクション パフォーマンスしきい値（Inspection Performance Thresholds）]：[設定（Configure）] をクリックし、1つ以上のしきい値を入力します。
- [フロー バイパスしきい値（Flow Bypass Thresholds）]：[設定（Configure）] をクリックし、1つ以上のしきい値を入力します。

少なくとも1つのインスペクション パフォーマンスしきい値と1つのフロー バイパスしきい値を指定する必要があります。IABがトラフィックを信頼するには、両方を超過している必要があり

ます。各タイプに複数のしきい値を入力した場合、いずれか 1 つのタイプのみを超過する必要があります。詳細については、IAB オプション，（856 ページ）を参照してください。

ステップ 3 [OK] をクリックして IAB 設定を保存します。

ステップ 4 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

IAB のロギングと分析

IAB は、接続ロギングを有効にしたかどうかを問わず、バイパスされたフローやバイパスされることが予想されるフローをロギングする接続終了イベントを強制します。接続イベントは、バイパスモードでバイパスされたフロー、またはテストモードでバイパスされることが予想されるフローを示します。接続イベントに基づいたカスタムのダッシュボード ウィジェットやレポートでは、バイパスされたフローおよびバイパスされることが予想されるフローの長期的な統計情報を表示できます。

IAB の接続イベント

アクション（Action）

[理由（Reason）] に [インテリジェント アプリケーション バイパス（Intelligent App Bypass）] が含まれる場合：

許可（Allow）：

適用された IAB 設定がテストモードであり、[アプリケーション プロトコル（Application Protocol）] によって指定されたアプリケーションのトラフィックが、インスペクション用に使用可能のままであることを示します。

信頼する（Trust）：

適用された IAB 設定がバイパス モードであり、[アプリケーション プロトコル（Application Protocol）] によって指定されたアプリケーションのトラフィックが信頼されているため、それ以上インスペクションが行われずにネットワークを通過することを示します。

理由（Reason）

[インテリジェント アプリケーション バイパス（Intelligent App Bypass）] は、IAB がバイパス モードまたはテスト モードでイベントをトリガーしたことを示します。

アプリケーション プロトコル（Application Protocol）

このフィールドには、イベントをトリガーしたアプリケーション プロトコルが表示されます。

例

次の省略された図では、一部のフィールドが省かれています。図は、2 つの別個のアクセス コントロール ポリシーの異なる IAB 設定から生成された 2 つの接続イベントの [アクション（Action）]、[理由（Reason）]、および [アプリケーション プロトコル（Application Protocol）] フィールドを示しています。

最初のイベントの場合、[信頼する（Trust）] アクションは、IAB がバイパス モードで有効にされており、Bonjour プロトコル トラフィックが信頼されているため、それ以上インスペクションが行われずに受け渡されることを示します。

2 番目のイベントの場合、[許可（Allow）] アクションは、IAB がテスト モードで有効にされているため、Ubuntu Update Manager トラフィックはさらにインスペクションが行われる必要がありますが、IAB がバイパス モードであればバイパスされることが予想されることを示します。

例

次の省略された図では、一部のフィールドが省かれています。2 番目のイベントのフローは両方とも（[アクション（Action）] : [信頼する（Trust）]、[理由（Reason）] : [インテリジェント アプリケーション バイパス（Intelligent App Bypass）]）をバイパスし、侵入ルール（[理由（Reason）] : [侵入モニタ（Intrusion Monitor）]）によって検査されました。[侵入モニタ（Intrusion Monitor）] の理由は、[イベントの生成（Generate Events）] に設定された侵入ルールが検出されたが、接続時にエクスプロイトをブロックしなかったことを示しています。この例では、これはアプリケーションが検出される前に発生しました。アプリケーションが検出された後、IAB は、アプリケーションがバイパス可能であると認識し、フローを信頼しました。

IAB のカスタム ダッシュボード ウィジェット

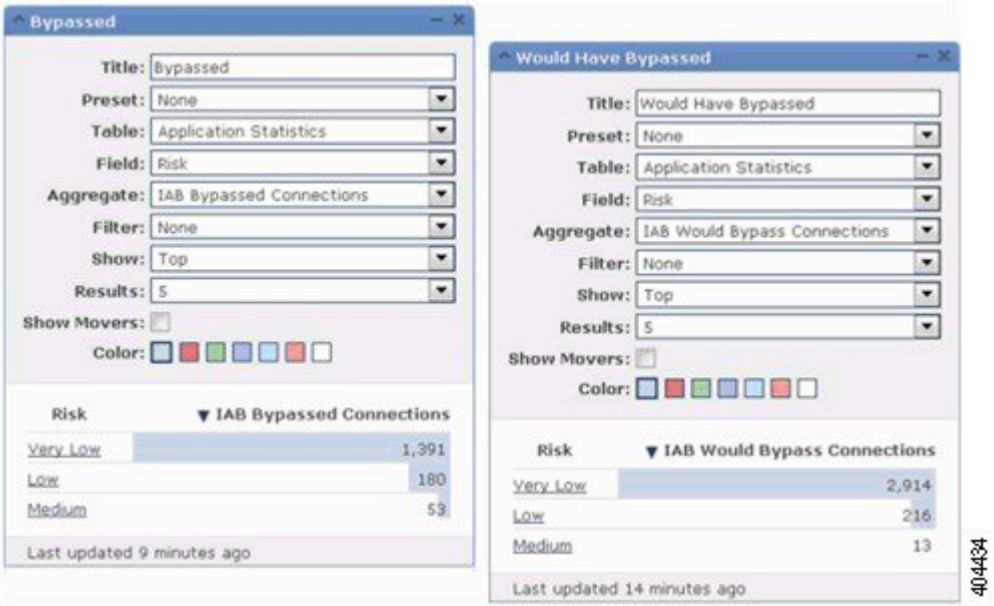
接続イベントに基づいて長期的な IAB の統計情報を表示するカスタム分析ダッシュボード ウィジェットを作成できます。ウィジェットを作成する際には、次の項目を指定します。

- プリセット（Preset）：なし（None）
- テーブル（Table）：アプリケーションの統計（Application Statistics）
- フィールド（Field）：任意（any）
- 集約（Aggregate）：次のいずれか
  - IAB が接続をバイパスした（IAB Bypassed Connections）
  - IAB が接続をバイパスすることが予想された（IAB Would Bypass Connections）
- フィールド（Field）：任意（any）

例

次のカスタム分析ダッシュボード ウィジェットの例では、次のようになっています。

- 「*Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてバイパス モードで有効になっているためにバイパスされたアプリケーション トラフィックの統計を示しています。
- 「*Would Have Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてテスト モードで有効になっているためにバイパスされることが予想されたアプリケーション トラフィックの統計を示しています。.



IAB のカスタム レポート

接続イベントに基づいて長期的な IAB の統計情報を表示するカスタム レポートを作成できます。レポートを作成する際には、次の項目を指定します。

- テーブル（Table）：アプリケーションの統計（Application Statistics）
- プリセット（Preset）：なし（None）
- フィールド（Field）：任意（any）
- X 軸（X-Axis）：任意（any）
- Y 軸（Y-Axis）：以下のいずれか
  - IAB が接続をバイパスした（IAB Bypassed Connections）
  - IAB が接続をバイパスすることが予想された（IAB Would Bypass Connections）

例

次の図は、2 つのレポートの例の抜粋を示します。

- 「*Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてバイパス モードで有効になっているためにバイパスされたアプリケーション トラフィックの統計を示しています。
- 「*Would Have Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてテスト モードで有効になっているためにバイパスされることが予想されたアプリケーション トラフィックの統計を示しています。

第 XII 部

暗号化トラフィックの処理

第 41 章

トラフィック復号の概要

以下のトピックではSSLインスペクションの概要を示し、SSLインスペクション設定の前提条件と詳細な導入シナリオについて説明します。

トラフィックの復号の概要

Firepowerシステムは、デフォルトではセキュア ソケット レイヤ（SSL）プロトコルまたはその後継である Transport Layer Security（TLS）プロトコルで暗号化されたトラフィックを検査できません。*SSL* インスペクション（検査）機能を使用すると、暗号化トラフィックのインスペクションを実行せずにブロックしたり、暗号化または復号されたトラフィックをアクセス コントロール（制御）を使用して検査したりできます。システムは、暗号化されたセッションを処理する際にトラフィックに関する詳細をログに記録します。暗号化トラフィックのインスペクションと暗号化セッションのデータ分析を組み合わせることで、ネットワーク内の暗号化されたアプリケーションやトラフィックをより詳細に把握したり制御したりできます。

SSLインスペクションは、ポリシーベースの機能です。FirePOWERシステムでは、アクセス コントロール ポリシーは、SSL ポリシーを含む、サブポリシーおよびその他の設定を呼び出すマスター設定です。アクセス コントロールと SSL ポリシーを関連付ければ、システムはアクセス コントロール ルールで評価する前に、その SSL ポリシーを使用して暗号化セッションを処理します。SSL インスペクションを設定していない場合、またはデバイスがサポートしていない場合、アクセス コントロール ルールは、すべての暗号化トラフィックを処理します。

暗号化されたトラフィックの通過がSSLインスペクション設定で許可される場合、そのトラフィックがアクセスコントロールルールによって処理されることにも注意してください。ただし、一部のアクセスコントロールルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、システムは暗号化ペイロードの侵入およびファイル インスペクションを無効にしています。

これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

システムでTCP接続でのSSLハンドシェイクが検出された場合、その検出されたトラフィックを復号できるかどうかが判定されます。復号できない場合は、設定されたアクションが適用されます。以下のアクションを設定できます。

- 暗号化トラフィックをブロックする
- 暗号化トラフィックをブロックし、TCP 接続をリセットする
- 暗号化されたトラフィックを復号しない

システムによるトラフィックの復号が可能な場合、システムでは、それ以上のインスペクションを行わずにトラフィックをブロックするか、復号されていないトラフィックをアクセス コントロールによって評価するか、または次のいずれかの方法を使用して復号します。

- 既知の秘密キーを使用して復号する。外部ホストがネットワーク上のサーバとのSSLハンドシェイクを開始すると、交換されたサーバ証明書とアプライアンスにアップロード済みのサーバ証明書が照合されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号します。
- サーバ証明書の再署名によって復号する。ネットワーク上のホストが外部サーバとのSSLハンドシェイクを開始すると、システムによって、交換されたサーバ証明書が、アップロード済みの認証局（CA）証明書で再署名されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号します。

復号されたトラフィックに対しては、はじめから暗号化されていないトラフィックと同じトラフィックの処理と分析（ネットワーク、レピュテーション、およびユーザベースの各アクセスコントロール、侵入検知と防御、Cisco Advanced Malware Protection（Cisco AMP）、およびディスカバリ（検出））が実行されます。システムで、復号されたトラフィックのポスト分析をブロックしない場合、トラフィックを再暗号化してから宛先ホストに渡します。

SSLインスペクションの要件

構成時の設定やライセンスに加え、アプライアンスをネットワーク上にどのように展開しているかにより、暗号化トラフィックの制御や復号化に適用できるアクションが異なります。最適な展開タイプを決定するときは、マッピングされたアクション、既存のネットワーク展開、および全体的な要件のリストを確認してください。

インライン、ルーティング、スイッチド、またはハイブリッドのインターフェイスで設定および展開されたデバイスでは、トラフィック フローの変更が可能です。これらのデバイスでは、着信および発信トラフィックのモニタリング、ブロック、許可、および復号を行うことができます。

パッシブまたはインライン（タップ モード）のインターフェイスで設定および展開されたデバイスでは、トラフィック フローを変更することはできません。これらのデバイスで行えるのは、着信トラフィックのモニタリング、許可、および復号だけです。パッシブ展開では、一時Diffie-Hellman（DHE）および楕円曲線 Diffie-Hellman（ECDHE）の暗号スイートを使用した暗号化トラフィックの復号はサポートされません。

SSL インスペクションの一部の機能では、公開キー証明書と秘密キーのペアが必要です。暗号化セッションの特性に応じてトラフィックを復号したり制御したりするためには、証明書および秘密キーのペアを Firepower Management Centerにアップロードする必要があります。

SSL ルール設定の前提条件に関する情報

SSL インスペクションは、サポートする公開キー インフラストラクチャ（PKI）の多くの情報に依存しています。照合ルールの条件を設定するときは、その組織におけるトラフィック パターンについて検討する必要があります。

表 *68*：*SSL* ルール条件の設定に必要な情報

一致対象	必要な情報
自己署名サーバ証明書を含む、検出されたサーバ証明書	サーバ証明書
信頼できるサーバ証明書	CA 証明書
検出されたサーバ証明書のサブジェクトまたは発行元	サーバ証明書のサブジェクト DN または発行元 DN

ルールの適用先となる暗号化トラフィックの復号、ブロック、モニタリングが不要かどうか、または復号が必要かどうかについて検討します。その結果を、SSL ルールのアクション、復号できないトラフィックのアクション、およびSSL ポリシーのデフォルト アクションに反映させます。

表 *69*：*SSL* 復号に必要な情報

復号の対象	必要な情報
制御対象のサーバへの着信トラフィック	サーバ証明書のファイルと秘密キー ファイルのペア
外部サーバへの発信トラフィック	CA 証明書のファイルと秘密キー ファイルのペア CA 証明書と秘密キーを生成することもできます。

これらの情報を収集したら、システムにアップロードして、再利用可能なオブジェクトを設定します。

関連トピック

識別名オブジェクト，（438 ページ）
PKI オブジェクト，（440 ページ）

SSL インスペクション アプライアンス導入シナリオ

ここでは Life Insurance Example, Inc.（LifeIns）という架空の生命保険会社で使われる複数のシナリオを例にして、同社のプロセス監査で利用されている暗号化トラフィックの SSL インスペクションについて解説します。LifeIns はそのビジネス プロセスに基づいて、以下の展開を計画しています。

- カスタマー サービス部門では、単一の 7000 または 8000 シリーズ デバイスをパッシブ展開する
- 契約審査部門では、単一の 7000 または 8000 シリーズ デバイスをインライン展開する
- 上記の両方のデバイスを単一のFirepower Management Centerで管理する

カスタマー サービスのビジネス プロセス

LifeIns はすでに顧客対応用の Web サイトを構築済みです。LifeIns は、保険契約に関する見込み顧客からの暗号化された質問や要求を、Web サイトや電子メールで受け取ります。LifeIns のカスタマー サービスは、これらの要求を処理して 24 時間以内に必要な情報を返信しなければなりません。カスタマー サービスでは、着信するコンタクト メトリックのコレクションを拡張したいと思っています。LifeIns では、すでにカスタマー サービスに対する内部監査用のレビューが確立されています。

また、LifeIns は暗号化された申請書もオンラインで受信します。カスタマー サービス部門は申請書を 24 時間以内に処理し、申請書類のファイルを契約審査部門に送信しなければなりません。カスタマーサービスでは、オンラインフォームからの不正な申請をすべて除外するようにしていますが、この作業が同部門での作業のかなりの部分を占めています。

契約審査部門のビジネス プロセス

LifeIns の契約審査担当者は、Medical Repository Example, LLC（MedRepo）という医療データ リポジトリに、オンラインで暗号化された医療情報要求を送信します。MedRepo はこれらの要求を評価し、LifeIns に暗号化されたレコードを 72 時間以内に送信します。その後は契約審査担当者が申請書類を査定し、保険契約および保険料に関連する判定を送信します。契約審査部門では、そのメトリック コレクションを拡張したいと思っています。

最近、不明な送信元からのスプーフィング（なりすまし）応答が LifeIns に送られてくるようになりました。LifeIns の契約審査担当者はインターネット使用に関する適切なトレーニングを受けていますが、LifeIns の IT 部門はまず、医療応答の形式で送られてくる暗号化トラフィックをすべて分析し、すべてのスプーフィング行為をブロックしたいと考えています。

LifeIns では、経験の浅い契約審査担当者に対して 6 ヵ月のトレーニング期間を設けています。最近、こうした契約審査担当者が MedRepo のカスタマーサービス部門への暗号化された医療規制リクエストの送信を正しく行わない事例がありました。そのため MedRepo から LifeIns に複数の苦情が提出されています。LifeIns は、新任の契約審査担当者用のトレーニング期間を延長し、契約審査担当者から MedRepo への要求についても監査を入れることを計画しています。

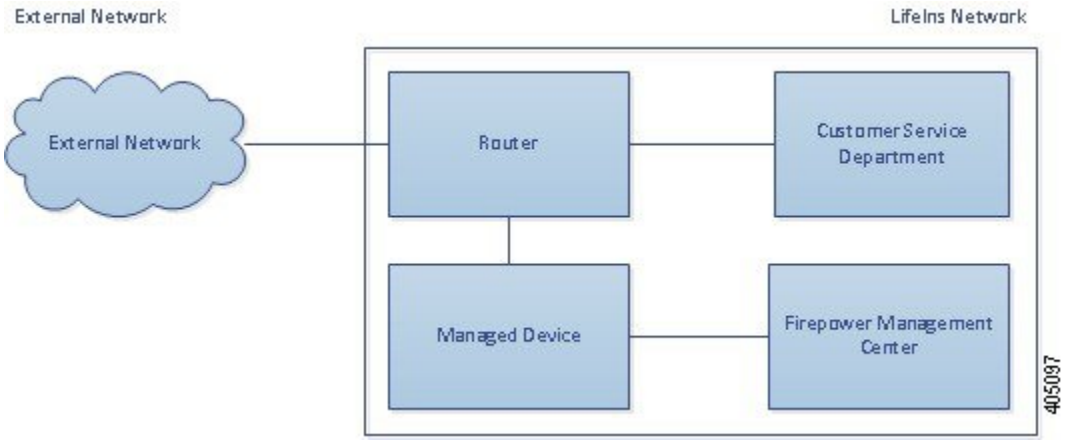
パッシブ展開でのトラフィックの復号

LifeIns のビジネス要件では、カスタマー サービスに次の要求をしています。

- すべての要求と申請書類を 24 時間以内に処理する
- 着信するコンタクト メトリックのコレクション プロセスを改善する
- 着信した不正な申請書類を特定して廃棄する

カスタマー サービス部門では、追加の監査用レビューを必要としません。

LifeIns ではカスタマー サービスの管理対象デバイスのパッシブ展開を計画しています。



外部ネットワークからのトラフィックは LifeIns のルータに送信されます。ルータはトラフィックをカスタマー サービス部門にルーティングし、検査用にトラフィックのコピーを管理対象デバイスにミラーリングします。

管理元の Firepower Management Center で、[アクセス コントロール（Access Control）] および [SSL エディタ（SSL Editor）] のカスタム ロールを持つユーザが、SSL インスペクションの設定を次のように行います。

- カスタマー サービス部門に送信された暗号化トラフィックをすべてログに記録する
- オンラインの申請フォームからカスタマーサービスに送信された暗号化トラフィックを復号する
- カスタマーサービスに送信された他の暗号化トラフィックは、オンライン リクエスト フォームからのトラフィックも含め、すべて復号しない

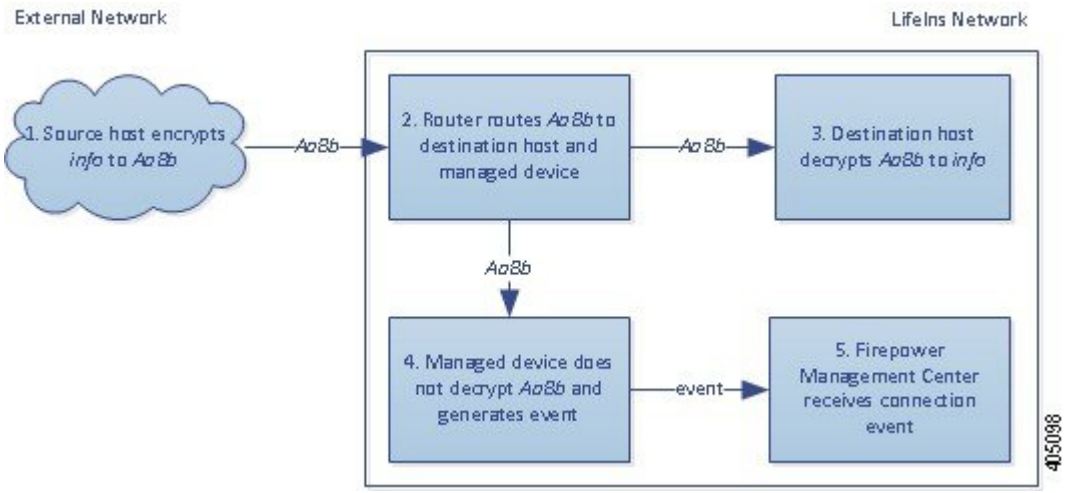
さらに、復号された申請フォーム トラフィック中に偽の申請データが含まれていないかを検査し、検出された場合はログに記録するためのアクセス コントロールも設定します。

次のシナリオでは、ユーザからカスタマーサービスにオンラインフォームが送信されます。ユーザのブラウザは、サーバとの TCP 接続を確立してから、SSL ハンドシェイクを開始します。管理対象デバイスが、このトラフィックのコピーを受信します。クライアントとサーバが SSL ハンド

シェイクを完了することで、暗号化されたセッションが確立されます。システムは、ハンドシェイクと接続の詳細に応じて、接続のログを記録し、暗号化トラフィックのコピーを処理します。

パッシブ展開での暗号化トラフィック モニタリング

管理対象デバイスは、カスタマー サービスに送信されるすべてのSSL暗号化トラフィックについて、接続のログを記録します。



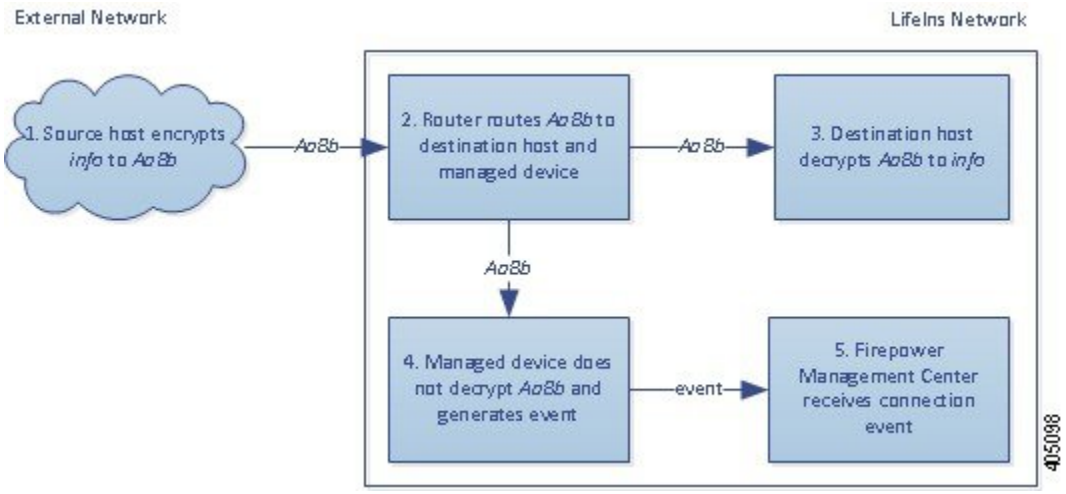
次のステップが実行されます。

1. ユーザがプレーンテキストの要求（`info`）を送信します。クライアントがこれを暗号化（`AaBb`）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeInsのルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（`AaBb`）を受信し、これをプレーン テキスト（`info`）に復号します。
4. 管理対象デバイスはトラフィックを復号しません。

   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、デバイスは接続イベントを生成します。
5. Firepower Management Centerが接続イベントを受信します。

パッシブ展開での復号されていない暗号化トラフィック

保険契約に関する要求を含むすべてのSSL暗号化トラフィックについては、管理対象デバイスはそのトラフィックを復号せずに許可し、接続のログを記録します。



次のステップが実行されます。

1. ユーザがプレーンテキストの要求（info）を送信します。クライアントがこれを暗号化（AaBb）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeInsのルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（AaBb）を受信し、これをプレーン テキスト（info）に復号します。
4. 管理対象デバイスはトラフィックを復号しません。

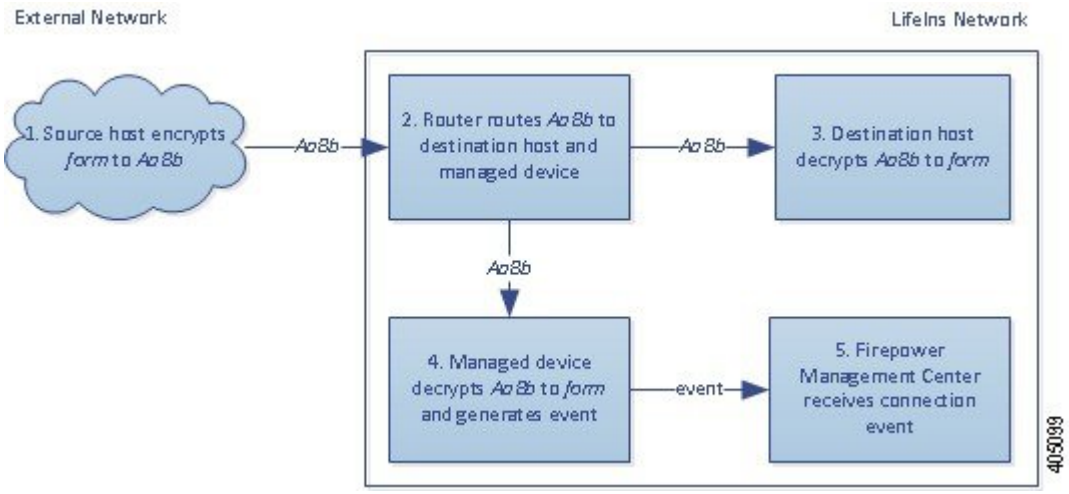
   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、デバイスは接続イベントを生成します。
5. Firepower Management Centerが接続イベントを受信します。

パッシブ展開での暗号化トラフィックの秘密キーによる検査

申請フォームのデータを含むすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。

（注） パッシブ展開の場合、DHEまたはECDHE暗号スイートで暗号化されたトラフィックは、既知の秘密キーを使って復号することはできません。

有効な申請フォームの情報を含むトラフィックについては、接続のログが記録されます。

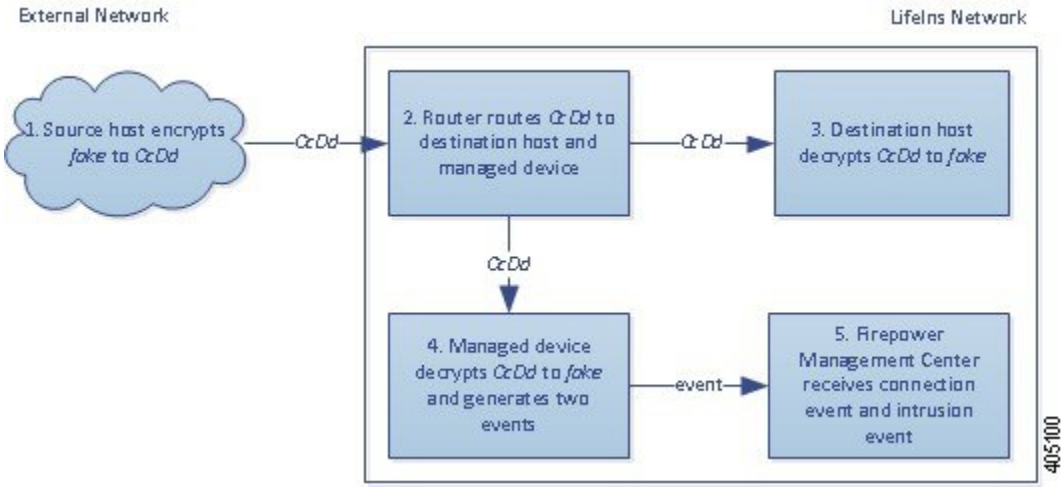


次のステップが実行されます。

1. ユーザがプレーンテキストの要求（form）を送信します。クライアントがこれを暗号化（AaBb）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeInsのルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（AaBb）を受信し、これをプレーン テキスト（form）に復号します。
4. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、暗号化トラフィックをプレーン テキスト（form）に復号化します。

   アクセス コントロール ポリシーは、復号されたトラフィックの処理を継続します。偽の申請書であることを示す情報は検出されません。セッション終了後、デバイスは接続イベントを生成します。
5. Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、復号されたトラフィックに偽の申請データが含まれていた場合、接続および偽のデータについてのログが記録されます。



次のステップが実行されます。

1 ユーザがプレーンテキストの要求（fake）を送信します。クライアントがこれを暗号化（CcDd）し、カスタマー サービスに暗号化トラフィックを送信します。

2 LifeInsのルータが暗号化トラフィックを受信し、カスタマーサービス部門のサーバにルーティングします。また、管理対象デバイスにそのトラフィックのコピーを送信します。

3 カスタマー サービス部門のサーバが、暗号化された情報の要求（CcDd）を受信し、これをプレーン テキスト（fake）に復号します。

4 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、暗号化トラフィックをプレーン テキスト（fake）に復号します。

アクセス コントロール ポリシーは、復号されたトラフィックの処理を継続して、偽の申請書であることを示す情報を検出します。デバイスが侵入イベントを生成します。セッション終了後、デバイスは接続イベントを生成します。

5 Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントおよび偽の申請データの侵入イベントを受信します。

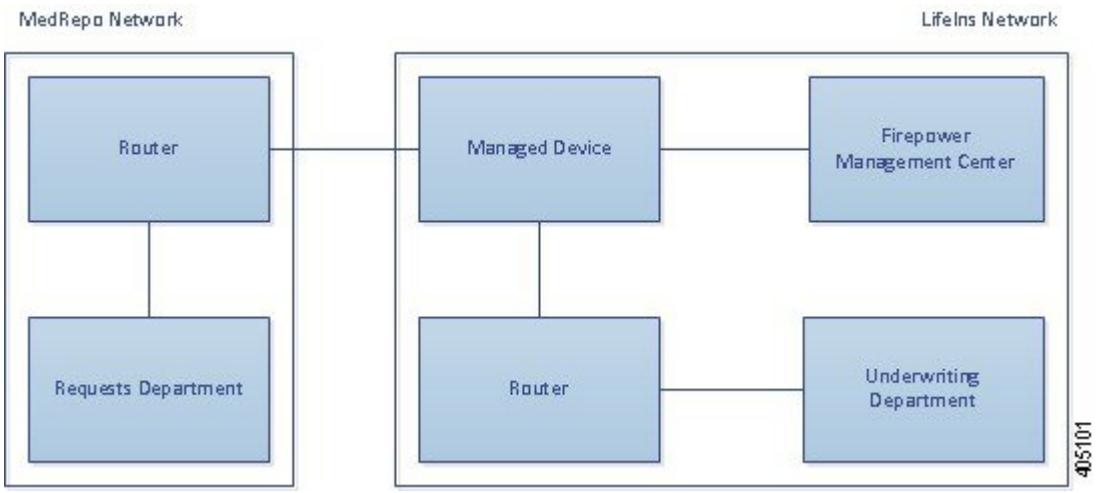
インライン展開でのトラフィックの復号

LifeIns のビジネス要件では、契約審査部門に次の要求をしています。

- 新採用および経験の浅い契約審査担当者を監査し、MedRepoへの情報要求が適切なすべての規則に準じていることを検証する
- その契約審査によるメトリック コレクション プロセスを改善する
- MedRepo が送信元と思われるすべての要求を調査し、スプーフィング行為を排除する
- 契約審査部門から MedRepo のカスタマー サービス部門へのすべての不適切な規制要求を排除する

- 経験豊富な契約審査担当者は監査しない

LifeIns の契約審査部門では、デバイスのインライン展開を計画しています。



MedRepo のネットワークからのトラフィックは、MedRepo のルータに流されます。そこから LifeIns のネットワークにトラフィックがルーティングされます。管理対象デバイスがそのトラフィックを受信し、許可されたトラフィックを LifeIns のルータに転送し、また管理元の Firepower Management Center にイベントを送信します。LifeIns のルータは、トラフィックを宛先ホストにルーティングします。

管理元の Firepower Management Center で、[アクセス コントロール（Access Control）] および [SSL エディタ（SSL Editor）] のカスタム ロールを持つユーザが、SSL アクセス コントロール ルールの設定を次のように行います。

- 契約審査部門に送信された暗号化トラフィックをすべてログに記録する
- LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信された暗号化トラフィックをすべてブロックする
- MedRepo から LifeIns の契約審査部門宛て、および LifeIns の経験の浅い契約審査担当者から MedRepo のリクエスト部門宛てに送信される暗号化トラフィックをすべて復号する
- 経験豊富な契約審査担当者から送信される暗号化トラフィックは復号しない

さらに、カスタムの侵入ポリシーと以下の設定を使用して、復号トラフィックを検査するアクセス コントロールを設定します。

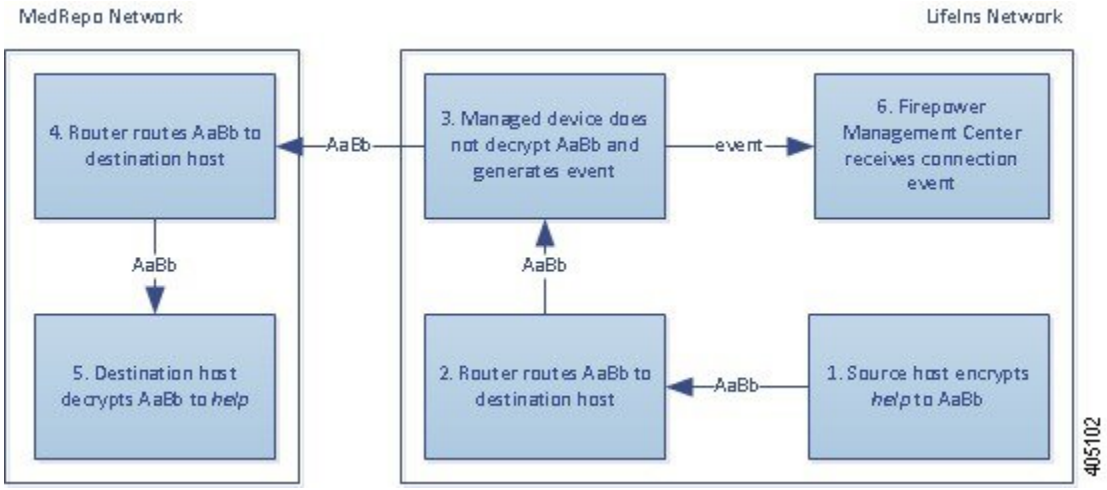
- 復号トラフィックでスプーフィング行為が検出された場合はそのトラフィックをブロックし、スプーフィング行為をログに記録する
- 規制に準拠しない情報を含んでいる復号トラフィックをブロックし、不適切な情報をログに記録する
- 他の暗号化および復号されたトラフィックをすべて許可する

許可された復号トラフィックは、再暗号化されて宛先ホストに転送されます。

次のシナリオでは、ユーザが情報をオンラインでリモート サーバに送信します。ユーザのブラウザは、サーバとの TCP 接続を確立してから、SSL ハンドシェイクを開始します。管理対象デバイスがこのトラフィックを受信し、ハンドシェイクと接続の詳細に基づいて、システムが接続のログへの記録とトラフィックの処理を行います。システムがトラフィックをブロックした場合、TCP 接続も切断されます。トラフィックがブロックされない場合、クライアントとサーバが SSL ハンドシェイクを完了することで、暗号化されたセッションが確立されます。

インライン展開での暗号化トラフィック モニタリング

契約審査部門で送受信されるすべての SSL 暗号化トラフィックについて、接続のログが記録されます。



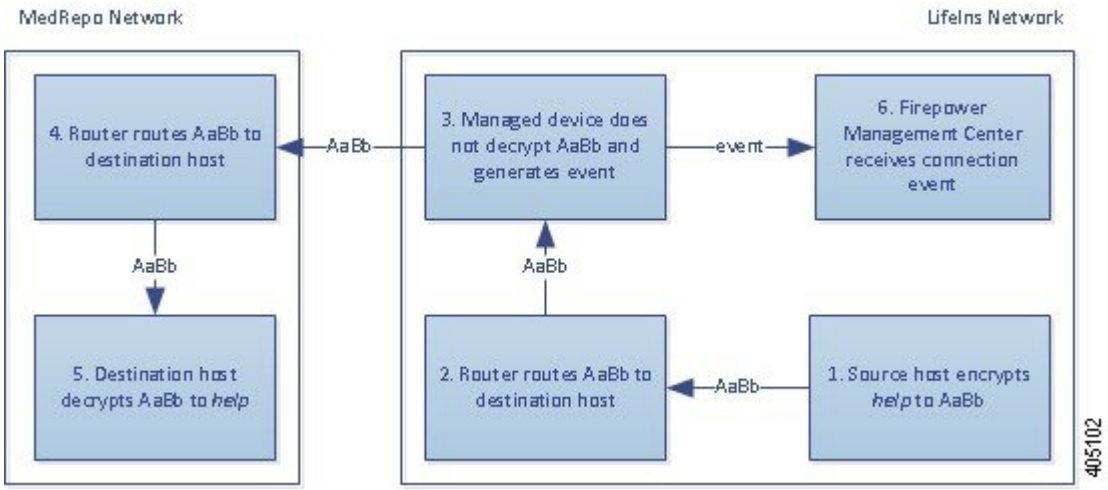
次のステップが実行されます。

1. ユーザがプレーンテキストの要求（help）を送信します。クライアントがこれを暗号化（AaBb）し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. 管理対象デバイスはトラフィックを復号しません。

   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. 契約審査部門のサーバは、暗号化された情報の要求（AaBb）を受信し、これをプレーンテキスト（help）に復号します。
6. Firepower Management Centerが接続イベントを受信します。

インライン展開での復号されていない暗号化トラフィック

経験豊富な契約審査担当者から送信されるすべての SSL 暗号化トラフィックについては、管理対象デバイスはそのトラフィックを復号せずに許可し、接続のログを記録します。



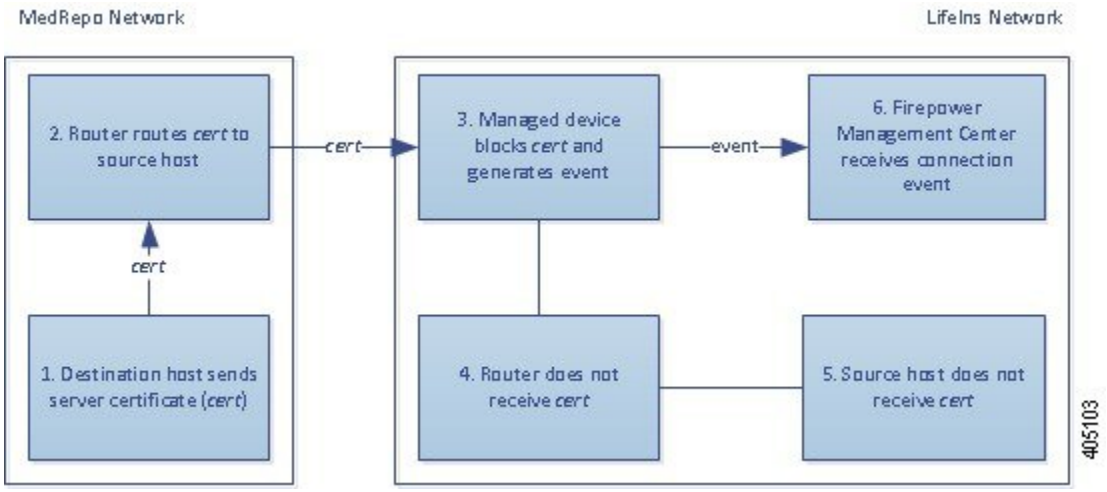
次のステップが実行されます。

1. ユーザがプレーンテキストの要求（help）を送信します。クライアントがこれを暗号化（AaBb）し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. 管理対象デバイスはこのトラフィックを復号しません。

   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. リクエスト部門のサーバは、暗号化された情報の要求（AaBb）を受信し、これをプレーンテキスト（help）に復号します。
6. Firepower Management Centerが接続イベントを受信します。

インライン展開での暗号化トラフィックのブロック

LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信されるすべての SMTPS 電子メール トラフィックは SSL ハンドシェイク時にブロックされ、追加の検査なしで接続のログが記録されます。

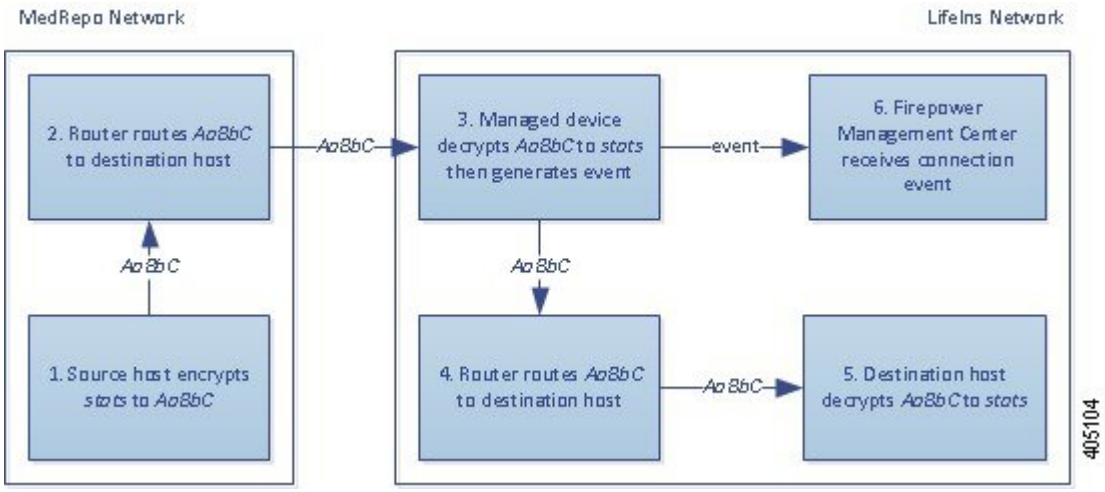


次のステップが実行されます。

1. カスタマー サービス部門のサーバは、クライアント ブラウザから SSL ハンドシェイクの確立要求を受信すると、SSLハンドシェイクの次のステップとして、サーバ証明書（cert）をLifeInsの契約審査担当者に送信します。
2. MedRepoのルータが証明書を受信し、これをLifeInsの契約審査担当者にルーティングします。
3. 管理対象デバイスは追加の検査を行わずにトラフィックをブロックし、TCP 接続を終了します。これにより、接続イベントが生成されます。
4. 内部ルータは、ブロックされたトラフィックを受信しません。
5. 契約審査担当者は、ブロックされたトラフィックを受信しません。
6. Firepower Management Centerが接続イベントを受信します。

インライン展開での暗号化トラフィックの秘密キーによる検査

MedRepoからLifeInsの契約審査部門に送信されるすべてのSSL暗号化トラフィックは復号され、接続のログが記録されます。復号には、アップロードされたサーバ秘密キーを使って取得されたセッション キーが使用されます。正規のトラフィックは許可され、再暗号化されて契約審査部門に送信されます。

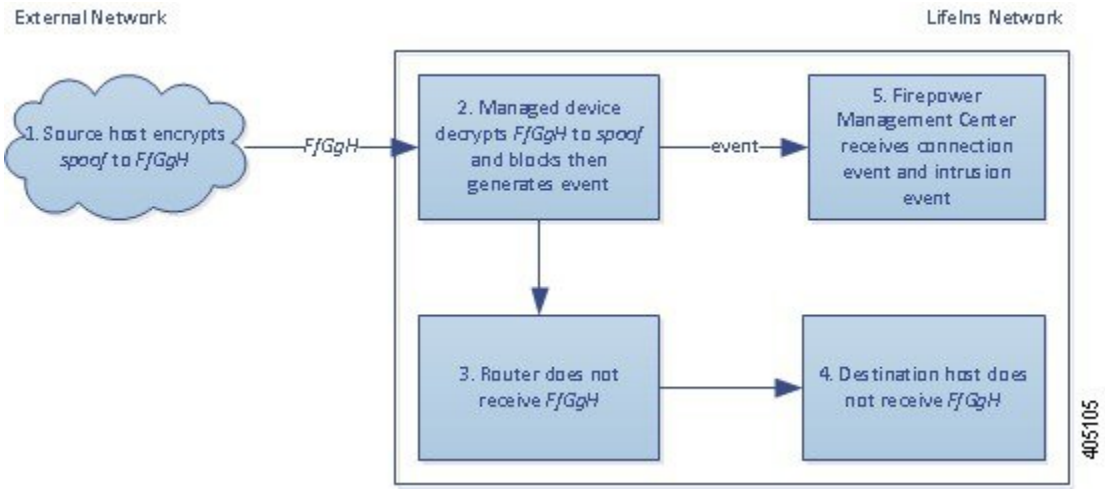


次のステップが実行されます。

1. ユーザがプレーン テキストの要求（stats）を送信します。クライアントがこれを暗号化（AaBbC）し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. 外部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
3. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（stats）に復号します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続します。スプーフィング行為は検出されません。デバイスは暗号化トラフィック（AaBbC）を転送し、セッション終了後に接続イベントを生成します。
4. 内部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
5. 契約審査部門のサーバは、暗号化された情報（AaBbC）を受信し、これをプレーン テキスト（stats）に復号します。
6. Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、スプーフィング行為の復号トラフィックはすべてドロップされ、接続およびスプーフィング行為についてのログが記録されます。



次のステップが実行されます。

1 ユーザがプレーン テキストの要求（spoof）を送信しますが、このトラフィックは改変されており、発信元が MedRepo, LLC であるかのように偽装されています。クライアントがこれを暗号化（FfGgH）し、契約審査部門のサーバに暗号化トラフィックを送信します。

2 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（spoof）に復号します。

アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続し、スプーフィング行為を検出します。デバイスはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。

3 内部ルータは、ブロックされたトラフィックを受信しません。

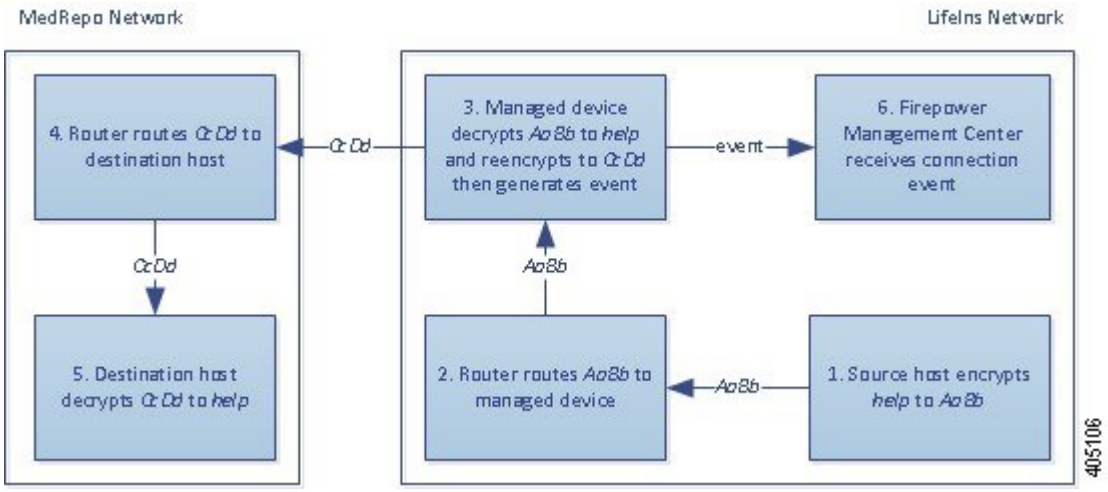
4 契約審査部門のサーバは、ブロックされたトラフィックを受信しません。

5 Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントおよびスプーフィング行為の侵入イベントを受信します。

インライン展開での暗号化トラフィックの再署名済み証明書による検査

新任および経験の浅い契約審査担当者から MedRepo のリクエスト部門に送信されるすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。復号には、再署名されたサーバ証明書を使って取得されたセッション キーが使用されます。正規のトラフィックは許可され、再暗号化されて MedRepo に送信されます。

（注） インライン展開においてサーバ証明書の再署名によりトラフィックを復号化する場合、デバイスは中間者（man-in-the-middle）として機能します。ここでは 2 つの SSL セッションが作成され、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間で使用されます。その結果、暗号セッションの詳細はセッションごとに異なります。



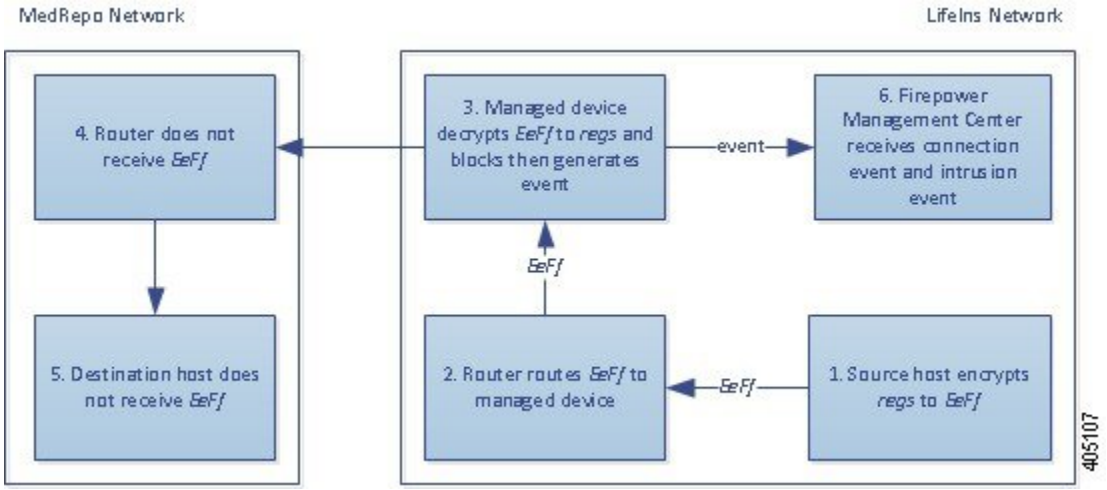
次のステップが実行されます。

1. ユーザがプレーンテキストの要求（help）を送信します。クライアントがこれを暗号化（AaBb）し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. 管理対象デバイスは、再署名されたサーバ証明書と秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（help）に復号します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続します。不適切な要求は検出されません。デバイスはトラフィックを再暗号化（CcDd）して、送信を許可します。セッション終了後、接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. リクエスト部門のサーバは、暗号化された情報（CcDd）を受信し、これをプレーン テキスト（help）に復号します。
6. Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。

（注） 再署名されたサーバ証明書で暗号化されたトラフィックにより、信頼できない証明書についての警告がクライアントのブラウザに表示されます。この問題を避けるには、組織のドメイン ルートにある信頼できる証明書ストアまたはクライアントの信頼できる証明書ストアにCA証明書を追加します。

これに対し、規制要件を満たさない情報を含んでいる復号トラフィックは、すべてドロップされます。接続および非準拠情報についてのログが記録されます。



次のステップが実行されます。

1 ユーザが規制要件に準拠していない要求をプレーンテキスト（regs）で送信します。クライアントがこれを暗号化（EeFf）し、リクエスト部門のサーバに暗号化トラフィックを送信します。

2 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。

3 管理対象デバイスは、再署名されたサーバ証明書と秘密キーで取得したセッションキーを使用して、このトラフィックをプレーン テキスト（regs）に復号します。

アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続し、不適切な要求を検出します。デバイスはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。

4 外部ルータは、ブロックされたトラフィックを受信しません。

5 リクエスト部門のサーバは、ブロックされたトラフィックを受信しません。

6 Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントおよび不適切な要求の侵入イベントを受信します。

第 42 章

SSL ポリシーの使用を開始するには

ここでは、SSL ポリシーの作成、設定、管理、およびロギングの概要を示します。

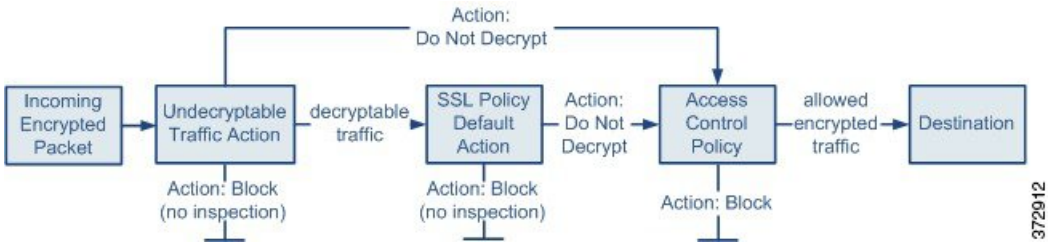
SSL ポリシーの概要

SSL ポリシーは、ネットワーク上の暗号化トラフィックをシステムがどのように処理するかを決定します。SSL ポリシーを、1 つまたは複数設定できます。SSL ポリシーをアクセス コントロール ポリシーに関連付け、そのアクセス コントロール ポリシーを管理対象デバイスに展開します。デバイスで TCP ハンドシェイクが検出されると、アクセス コントロール ポリシーは最初にトラフィックを処理して検査します。次に TCP 接続上で SSL 暗号化セッションが識別された場合は、SSL ポリシーが引き継いで、暗号化トラフィックの処理および復号を行います。

注意 SSL ポリシーを追加または削除すると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作，（326 ページ）を参照してください。

最も単純な SSL ポリシーは、次の図のように、単一のデフォルト アクションで暗号化トラフィックを処理するように展開先のデバイスに指示します。デフォルト アクションの設定では、それ以

上のインスペクションなしで復号可能トラフィックをブロックするか、復号されていない復号可能トラフィックをアクセス コントロールで検査するように指定できます。システムは、暗号化されたトラフィックを許可するか、またはブロックできます。デバイスは復号できないトラフィックを検出すると、トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号しないままにして、アクセス コントロールによる検査を行います。



より複雑な SSL ポリシーでは、各種の復号できないトラフィックをさまざまなアクションで処理できます。また、認証局（CA）が証明書を発行したか、または暗号化証明書を信頼するかどうかに応じてトラフィックを制御したり、SSL ルールを使ってきめ細かな暗号化トラフィックの制御およびログの記録を行ったりできます。これらのルールには、単純なものや複雑なものがあり、複数の基準を使用して暗号化トラフィックの照合および検査を行います。

関連トピック

SSL ルールの条件, （903 ページ）

SSL ポリシーのデフォルト アクション

SSL ポリシーのデフォルト アクションは、ポリシーのモニタ以外のルールと一致しない復号可能な暗号化トラフィックについてシステムがどのように処理するかを決定します。SSL ルールがまったく含まれない SSL ポリシーを適用する場合、ネットワーク上のすべての復号可能トラフィックの処理方法を、デフォルトアクションが決定します。デフォルトアクションでブロックされた暗号化トラフィックに対しては、システムはいかなる種類のインスペクションも行わないことに注意してください。

表 *70*：*SSL* ポリシーのデフォルト アクション

デフォルト アクション	暗号化トラフィックに対して行う処理
ブロック（Block）	それ以上のインスペクションは行わずに SSL セッションをブロックする
リセットしてブロック（Block with reset）	それ以上のインスペクションは行わずに SSL セッションをブロックし、TCP 接続をリセットする
復号しない（Do not decrypt）	アクセス コントロールを使用して暗号化トラフィックを検査する

復号できないトラフィックのデフォルト処理オプション

表 *71*：復号できないトラフィック タイプ

タイプ（**Type**）	説明	デフォルト アクション	使用可能なアクション
圧縮されたセッション（Compressed Session）	SSL セッションはデータ圧縮メソッドを適用します。	デフォルト アクションを継承する（Inherit default action）	復号しない（Do not decrypt） ブロック（Block） リセットしてブロック（Block with reset） デフォルト アクションを継承する（Inherit default action）
SSLv2 セッション（SSLv2 Session）	セッションは SSL バージョン 2 で暗号化されます。 トラフィックが復号可能となるのは、ClientHello メッセージが SSL 2.0 で、送信トラフィックの残りが SSL 3.0 であることに注意してください。	デフォルト アクションを継承する（Inherit default action）	復号しない（Do not decrypt） ブロック（Block） リセットしてブロック（Block with reset） デフォルト アクションを継承する（Inherit default action）
不明な暗号スイート（Unknown Cipher Suite）	システムが認識できない暗号スイートです。	デフォルト アクションを継承する（Inherit default action）	復号しない（Do not decrypt） ブロック（Block） リセットしてブロック（Block with reset） デフォルト アクションを継承する（Inherit default action）

タイプ（Type）	説明	デフォルト アクション	使用可能なアクション
サポートされていない暗号スイート（Unsupported Cipher Suite）	検出された暗号スイートに基づく復号を、システムはサポートしていません。	デフォルト アクションを継承する（Inherit default action）	復号しない（Do not decrypt） ブロック（Block） リセットしてブロック（Block with reset） デフォルト アクションを継承する（Inherit default action）
セッションが未キャッシュ（Session not cached）	SSLセッションでセッションの再利用が有効化されており、クライアントとサーバがセッションIDを使ってセッションを再確立しているが、システムでセッション IDがキャッシュされていません。	デフォルト アクションを継承する（Inherit default action）	復号しない（Do not decrypt） ブロック（Block） リセットしてブロック（Block with reset） デフォルト アクションを継承する（Inherit default action）
ハンドシェイク エラー（Handshake Errors）	SSLハンドシェイクのネゴシエーション中にエラーが発生しました。	デフォルト アクションを継承する（Inherit default action）	復号しない（Do not decrypt） ブロック（Block） リセットしてブロック（Block with reset） デフォルト アクションを継承する（Inherit default action）
復号エラー（Decryption Errors）	トラフィックの復号中にエラーが発生しました。	ブロック（Block）	ブロック（Block） リセットしてブロック（Block With Reset）

SSL ポリシーを最初に作成する場合、デフォルト アクションによって処理される接続のログは、デフォルトでは無効化されています。復号できないトラフィックの処理ではデフォルト アクションのログ設定も適用されるため、復号できないトラフィックのアクションで処理される接続のログは、デフォルトでは無効化されています。

ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号できないことに注意してください。このトラフィックはアクセスコントロールを使用して引き続き検査できるため、復号できないトラフィック アクションでは処理されません。このトラフィックを許可するには、サーバ証明書の共通名または識別名と一致させるために、[復号しない（Do not decrypt）] アクションを使用して SSL ルールを設定します。

（注） クライアントと管理対象デバイスの間に HTTP プロキシがあって、クライアントとサーバが CONNECT HTTP メソッドを使用してトンネル SSL 接続を確立する場合、システムはトラフィックを復号化できません。システムによるこのトラフィックの処理法は、ハンドシェイク エラー（Handshake Errors）の復号できないアクションが決定します。

SSL ポリシーの管理

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

SSL ポリシー エディタでは、次の操作を実行できます。

- ポリシーを設定する
- SSL ルールを追加、編集、削除、有効化、無効化、および編成する
- 信頼できる CA 証明書を追加する
- システムが復号できない暗号化トラフィックに対する処理を決定する
- デフォルト アクションおよび復号できないトラフィック アクションで処理されるトラフィックのログを記録する

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [SSL]を選択します。

ステップ 2 SSL ポリシーを管理します。

- 関連付け：アクセス コントロール ポリシーに SSL ポリシーを関連付ける場合は、アクセス制御への他のポリシーの関連付け, （798 ページ）を参照してください。

- [比較（Compare）]：[ポリシーの比較（Compare Policies）]をクリックします（ポリシーの比較，（331 ページ） を参照）。
- コピー：コピー アイコン（  ）をクリックします。
- 作成：[新規ポリシー（New Policy）]をクリックします。基本 SSL ポリシーの作成，（890 ページ）を参照してください。
- 削除：削除アイコン（  ）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 展開：[展開（Deploy）]をクリックします（設定変更の導入，（320 ページ） を参照）。
- 編集：編集アイコン（  ）をクリックします。SSL ポリシーの編集，（892 ページ）を参照してください。代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- インポート/エクスポート：コンフィギュレーションのインポート/エクスポートについて，（187 ページ）を参照してください。
- [レポート（Report）]：レポート アイコン（  ）をクリックします（現在のポリシー レポートの生成，（333 ページ） を参照）。

基本 SSL ポリシーの作成

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

SSL ポリシーの設定では、ポリシーに一意の名前を付け、デフォルト アクションを指定する必要があります。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [SSL]を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] に一意のポリシー名を入力し、オプションで [説明（Description）] にポリシーの説明を入力します。

ステップ 4 [デフォルト アクション（Default Action）] を指定します。SSL ポリシーのデフォルト アクション, （886 ページ）を参照してください。

ステップ 5 ポリシーのデフォルト アクションによる接続のロギング, （1919 ページ）の説明に従って、デフォルト アクションのロギング オプションを設定します。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- SSL ポリシーに追加するルールを設定します。SSL ルールの作成および変更, （900 ページ）を参照してください。
- 復号化できないトラフィックのデフォルト処理を設定します。復号できないトラフィックのデフォルト処理の設定, （891 ページ）を参照してください。
- 復号化できないトラフィックのデフォルト処理のロギング オプションを設定します。ポリシーのデフォルト アクションによる接続のロギング, （1919 ページ）を参照してください。
- アクセス制御への他のポリシーの関連付け, （798 ページ）の説明に従って、SSL ポリシーをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

復号できないトラフィックのデフォルト処理の設定

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

システムによる復号や検査ができない特定タイプの暗号化トラフィックの処理については、SSL ポリシー レベルで、復号できないトラフィックのアクションを設定できます。SSL ルールがまったく含まれない SSL ポリシーを展開する場合、ネットワーク上のすべての復号できない暗号化トラフィックの処理方法は、復号できないトラフィックのアクションによって決定されます。

復号できないトラフィックのタイプによって、次の選択ができます。

- 接続をブロックする
- 接続をブロックした後でリセットする
- アクセス コントロールを使用して暗号化トラフィックを検査する
- SSL ポリシーのデフォルト アクションを継承する

手順

ステップ 1 SSL ポリシー エディタで、[復号できないアクション（Undecryptable Actions）] タブをクリックします。

ステップ 2 各フィールドで、SSL ポリシーのデフォルト アクションを選択するか、復号できないタイプのトラフィックに対して実行する別のアクションを選択します。詳細については、復号できないトラフィックのデフォルト処理オプション，（887 ページ）と SSL ポリシーのデフォルト アクション，（886 ページ）を参照してください。

ステップ 3 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 復号できないトラフィックのアクションで処理される接続に関するデフォルト ロギングを設定します。ポリシーのデフォルト アクションによる接続のロギング，（1919 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

SSL ポリシーの編集

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

ポリシーの編集は、1 つのブラウザ ウィンドウを使用して、一度に 1 人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシー エディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [SSL]を選択します。

ステップ 2 設定する SSL ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 SSL ポリシーを設定します。

- 説明：SSL ポリシーの説明を更新するには、[説明（Description）] フィールドをクリックし、新しい説明を入力します。
- ログ：復号できないトラフィックの処理および SSL ルールに一致しないトラフィックについて接続を記録するには、ポリシーのデフォルト アクションによる接続のロギング, （1919 ページ）を参照してください。
- 名前の変更：SSL ポリシーの名前を変更するには、[名前（Name）] フィールドをクリックし、新しい名前を入力します。
- デフォルト アクションの設定：SSL ポリシーが SSL ルールに一致しないトラフィックをどのように処理するかを設定するには、SSL ポリシーのデフォルト アクション, （886 ページ）を参照してください。
- 復号できないトラフィックのデフォルト アクションの設定：SSL ポリシーが復号できないトラフィックをどのように処理するかを設定するには、復号できないトラフィックのデフォルト処理の設定, （891 ページ）を参照してください。
- 信頼：SSL ポリシーに信頼された CA 証明書を追加するには、外部認証局の信頼, （942 ページ）を参照してください。

ステップ 4 SSL ポリシー内のルールを編集します。

- 追加：ルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- コピー：ルールをコピーするには、選択したルールを右クリックして、[コピー（Copy）] を選択します。
- 切り取り：ルールを切り取るには、選択したルールを右クリックして、[切り取り（Cut）] を選択します。
- 削除：ルールを削除するには、ルールの横にある削除アイコン（  ）をクリックして、[OK] をクリックします。
- 無効化：有効なルールを無効にするには、選択したルールを右クリックして、[状態（State）] を選択し、[無効（Disable）] を選択します。
- 表示：特定のルール属性の設定ページを表示するには、ルールの行にある条件の列で名前、値、またはアイコンをクリックします。たとえば、[送信元ネットワーク（Source Networks）] カラムに示されている名前または値をクリックすると、選択したルールの [ネットワーク

（Networks）] ページが表示されます。詳細については、ネットワーク ベースの SSL ルールの条件, （918 ページ）を参照してください。

- 編集：ルールを編集するには、ルールの横にある編集アイコン（  ）をクリックします。
- 有効化：無効なルールを有効にするには、選択したルールを右クリックして、[状態（State）] を選択し、[有効（Enable）] を選択します。無効なルールはグレー表示され、ルール名の下に [（無効）（(disabled)）] というマークが付きます。
- 貼り付け：切り取られたルールまたはコピーされたルールを貼り付けるには、選択したルールを右クリックして、[上に貼り付け（Paste above）] または [下に貼り付け（Paste below）] を選択します。

ステップ 5 設定を保存または廃棄します。

- 変更を保存し、編集を続行する場合は、[保存（Save）] をクリックします。
- 変更を廃棄する場合は、[キャンセル（Cancel）] をクリックし、プロンプトが出たら [OK] をクリックします。

次の作業

- SSL ポリシーがアクセス コントロール ポリシーにまだ関連付けられていない場合は、アクセス制御への他のポリシーの関連付け, （798 ページ）の説明に従って関連付けます。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

SSL ルールの作成および変更, （900 ページ）

第 43 章

SSL ルールの使用を開始するには

ここでは、SSL ルールの作成、設定、管理、トラブルシューティングの概要を示します。

SSL ルールの概要

SSL ポリシー内に各種の *SSL* ルールを設定することで、それ以上のインスペクションなしでトラフィックをブロックする、トラフィックを復号せずにアクセス コントロールで検査する、あるいはアクセス コントロールの分析用にトラフィックを復号するなど、複数の管理対象デバイスをカバーしたきめ細かな暗号化トラフィックの処理メソッドを構築できます。

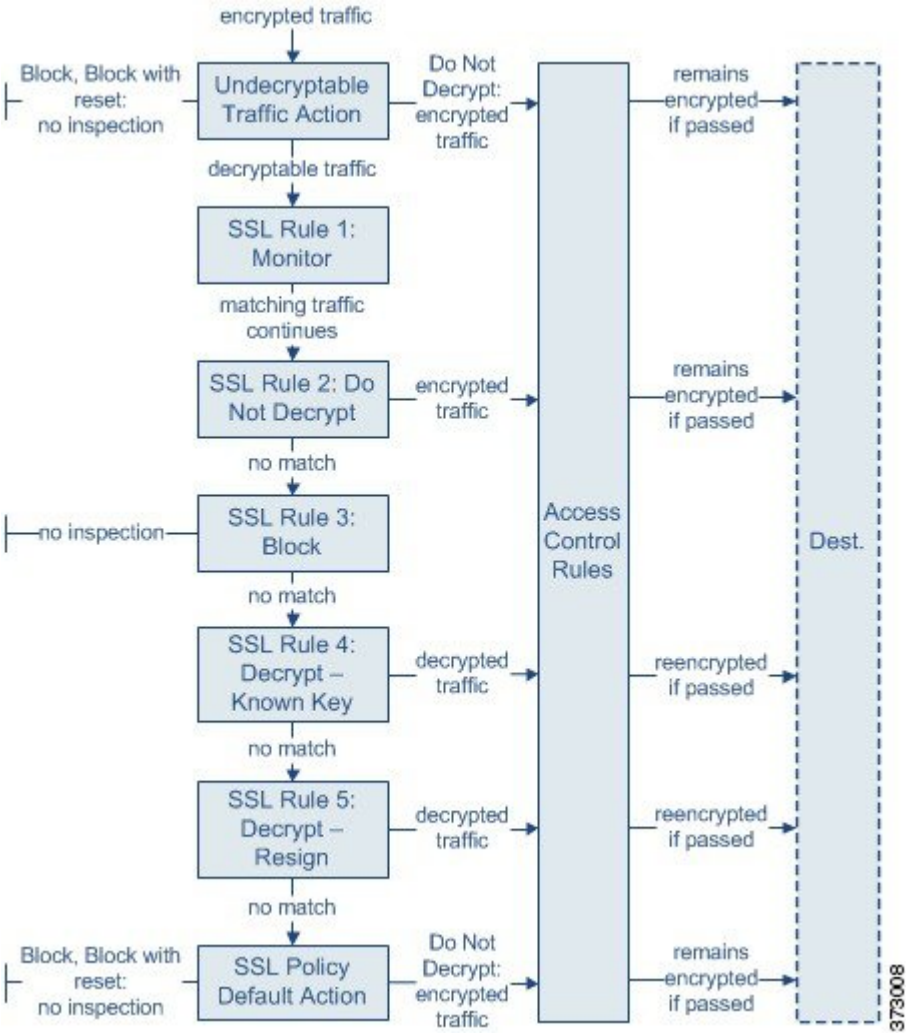
SSL ルールのトラフィック処理

システムは指定した順序で SSL ルールをトラフィックと照合します。ほとんどの場合、システムによる暗号化トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の SSL ルールに従って行われます。こうした条件には、単純なものと複雑なものがあります。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書の識別名、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを制御できます。

各ルールにはアクションも設定されます。アクションにより、アクセス制御と一致する暗号化または復号化トラフィックに対してモニタ、ブロック、検査のいずれを行うかが決まります。システムがブロックした暗号化トラフィックは、それ以上のインスペクションが**行われない**ことに注

意してください。暗号化されたトラフィックおよび復号できないトラフィックは、アクセス コントロールを使用して検査します。ただし、一部のアクセスコントロールルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、システムは暗号化ペイロードの侵入およびファイル インスペクションを無効にしています。

次のシナリオは、インライン展開での SSL ルールによるトラフィックの処理を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **復号できないトラフィック アクション（Undecryptable Traffic Action）**は、暗号化されたトラフィックを最初に評価します。復号できないトラフィックについては、システムはそれ以上のインスペクションを行わないでブロックするか、あるいはアクセス制御による検査に渡します。一致しなかった暗号化トラフィックは、次のルールへと進められます。
- **SSL ルール 1：モニタ（SSL Rule 1: Monitor）**は、暗号化トラフィックを次に評価します。モニタ ルールは、暗号化トラフィックのログ記録と追跡を行いますが、トラフィック フロー

には影響しません。システムは引き続きトラフィックを追加のルールと照合し、許可するか拒否するかを決定します。

- **SSL ルール 2**：**復号しない（SSL Rule 2: Do Not Decrypt**）は、暗号化トラフィックを 3 番目に評価します。一致したトラフィックは復号されません。システムはこのトラフィックをアクセス コントロールにより検査しますが、ファイルや侵入インスペクションは行いません。一致しないトラフィックは、引き続き次のルールと照合されます。
- **SSL ルール 3**：**ブロック（SSL Rule 3: Block**）は、暗号化トラフィックを 4 番目に評価します。一致するトラフィックは、追加のインスペクションなしでブロックされます。一致しないトラフィックは、引き続き次のルールと照合されます。
- **SSL ルール 4**：**復号 - 既知のキー（SSL Rule 4: Decrypt - Known Key**）は、暗号化トラフィックを 5 番目に評価します。ネットワークへの着信トラフィックで一致したものは、ユーザのアップロードする秘密キーを使用して復号されます。復号トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ルール 5**：**復号 - 再署名（SSL Rule 5: Decrypt - Resign**）は、最後のルールです。トラフィックがこのルールに一致した場合、システムはアップロードされた CA 証明書を使用してサーバ証明書を再署名してから、中間者（man-in-the-middle）としてトラフィックを復号します。復号トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ポリシーのデフォルト アクション（SSL Policy Default Action**）は、どの SSL ルールにも一致しなかったすべてのトラフィックを処理します。デフォルトアクションでは、暗号化トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号しないで、アクセス コントロールによる検査を行います。

暗号化トラフィック インスペクションの設定

暗号化セッションの特性に基づいた暗号化トラフィックの制御および暗号化トラフィックの復号には、再利用可能な公開キー インフラストラクチャ（PKI）オブジェクトの作成が必要です。この情報の追加は、信頼できる認証局（CA）の証明書の SSL ポリシーへのアップロード時、SSL ルール条件の作成時、およびプロセスでの関連オブジェクトの作成時に、臨機応変に実行できます。ただし、これらのオブジェクトを事前に設定しておくと、不適切なオブジェクトが作成される可能性を抑制できます。

証明書とキー ペアによる暗号化トラフィックの復号

セッション暗号化に使用するサーバ証明書と秘密キーをアップロードして内部証明書オブジェクトを設定しておくと、システムは着信する暗号化トラフィックを復号化できます。[復号 - 既知のキー（Decrypt - Known Key）] アクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、システムはアップロードされた秘密キーを使用してセッションを復号化します。

CA 証明書と秘密キーをアップロードして内部 CA オブジェクトを設定した場合、システムは発信トラフィックの復号化もできます。[復号 - 再署名（Decrypt - Resign）] アクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、システムはクライアント ブラウザに渡されたサーバ証明書を再署名した後、中間者（man-in-the-middle）としてセッションを復号します。オプションで、証明書全体ではなく自己署名証明書キーのみを置き換えることができます。この場合、ユーザはブラウザで自己署名証明書キー通知を確認します。

暗号化セッションの特性に基づいたトラフィック制御

システムによる暗号化トラフィックの制御は、セッション ネゴシエートに使用されたサーバ証明書または暗号スイートに基づいて実行できます。複数の異なる再利用可能オブジェクトの 1 つを設定し、SSL ルール条件でオブジェクトを参照してトラフィックを照合することができます。次の表に、設定できる再利用可能なオブジェクトのタイプを示します。

設定する内容	暗号化トラフィック制御に使用する条件
1 つまたは複数の暗号スイートが含まれる暗号スイートのリスト	暗号化セッションのネゴシエートに使用される暗号スイートが、暗号スイート リストにある暗号スイートのいずれかに一致する。
組織が信頼する CA 証明書のアップロードによる信頼できる CA オブジェクト	この信頼できる CA は、次のいずれかにより、セッションの暗号化に使用されたサーバ証明書を信頼する。 • CA が証明書を直接発行した。 • サーバ証明書を発行した中間 CA に CA が証明書を発行した。
サーバ証明書のアップロードによる外部証明書オブジェクト	セッションの暗号化に使用されたサーバ証明書が、アップロードされたサーバ証明書と一致する。
発行元の識別名または証明書サブジェクトを含む識別名オブジェクト	セッション暗号化に使用された証明書で、サブジェクトまたは発行元の共通名、国、組織、組織単位のいずれかが、設定された識別名と一致する。

関連トピック

暗号スイート リスト，（436 ページ）
識別名オブジェクト，（438 ページ）
PKI オブジェクト，（440 ページ）

SSL ルールのコンポーネント

各 SSL ルールには、一意の名前以外にも、次の基本コンポーネントがあります。

状態（State）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置（Position）

SSL ポリシーのルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。モニタ ルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

条件（Conditions）

条件は、ルールが処理する特定のトラフィックを指定します。こうした条件では、セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書のサブジェクトまたは発行元、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを照合できます。使用する条件は、ターゲット デバイスのライセンスによって異なります。

操作（Action）

ルールのアクションによって、一致したトラフィックの処理方法が決まります。暗号化された一致したトラフィックは、モニタ、許可、ブロック、または復号できます。復号および許可された暗号化トラフィックは、さらなる検査の影響下に置かれます。システムは、ブロックされた暗号化トラフィックに対してはインスペクションを実行**しない**ことに注意してください。

ログ

ルールのロギング設定によって、システムが記録する処理済みトラフィックのレコードを管理します。1 つのルールに一致するトラフィックのレコードを 1 つ保持できます。SSL ポリシーでの設定に従って、システムが暗号化セッションをブロックするか、あるいは復号なしで渡すことを許可するときに、その接続をログに記録できます。アクセス コントロール ルールに従ってより詳細な評価のために復号化した場合の接続ログを記録するようにシステムを強制することも可能で、これはその後でどのような処理やトラフィックの検査がされるかとは無関係です。接続のログは、Firepower Management Center のデータベースの他に、システム ログ（Syslog）または SNMP トラップ サーバに記録できます。

ヒント　SSL ルールを適切に作成し順序付けするのは複雑なタスクです。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、追加のライセンスが必要となったり、ルールに無効な設定が含まれる場合があります。予期したとおりにトラフィックが確実に処理されるようにするために、SSL ポリシー インターフェイスには、ルールに関する強力な警告およびエラーのフィードバック システムが用意されています。

関連トピック

セキュリティ ゾーンの条件, （343 ページ）
ネットワーク条件, （345 ページ）
VLAN 条件, （347 ページ）
ポートおよび ICMP コードの条件, （347 ページ）
アプリケーション条件（アプリケーション制御）, （350 ページ）
URL 条件（URL フィルタリング）, （356 ページ）
ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御）, （363 ページ）
ルールのパフォーマンスに関するガイドライン, （371 ページ）
SSL ルールのトラブルシューティング, （915 ページ）

SSL ルールの作成および変更

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

手順

ステップ 1　[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [SSL]を選択します。

ステップ 2　SSL ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3　次の選択肢があります。

- 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。

- 既存のルールを編集するには、編集アイコン（）をクリックします。

ステップ 4 名前を入力します。

ステップ 5 上記に要約されるようにルール コンポーネントを設定します。次の設定をするか、デフォルト設定をそのまま使用することができます。

- ルールを有効にするかどうかを指定します。
- ルールの位置を指定します。SSL ルールの順序の評価, （901 ページ） を参照してください。
- [アクション（Action）] で、ルールのアクションを選択します。SSL ルール アクションの設定, （909 ページ）を参照してください。
- ルールの条件を設定します。SSL ルールの条件タイプ, （904 ページ） を参照してください。
- [ログ（Logging）] オプションを指定します。SSL ルールによる復号可能接続のロギング, （1916 ページ） を参照してください。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

SSL ルールの順序の評価

SSL ルールを最初に作成するときに、ルール エディタの [挿入（Insert）] ドロップダウン リストを使用して、その位置を指定します。SSL ポリシーの SSL ルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、SSL ルールを上から順にトラフィックと照合します。

ほとんどの場合、システムによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の SSL ルールに従って行われます。モニタ ルール（トラフィックをログに記録するがトラフィック フローには影響しないルール）の場合を除き、システムは、そのトラフィックがルールに一致した後、追加の優先順位の低いルールに対してトラフィックを評価し続けることは**ありません**。

ヒント 適切な SSL ルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

番号ごとのルールの順序付けに加えて、カテゴリ別にルールをグループ化できます。デフォルトでは、3 つのカテゴリ（管理者、標準、ルート）があります。カスタム カテゴリを追加できますが、システム提供のカテゴリを削除したり、それらの順序を変更したりすることはできません。

関連トピック

ルールのパフォーマンスに関するガイドライン，（371 ページ）

ルール カテゴリへの SSL ルールの追加

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

手順

ステップ 1 SSL ルール エディタの [挿入（Insert）] ドロップダウン リストで [カテゴリ（Into Category）] を選択し、使用するカテゴリを選択します。

ステップ 2 [保存（Save）] をクリックします。

ヒント ルールを保存すると、そのカテゴリの最後に配置されます。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

番号による SSL ルールの配置

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

手順

ステップ 1 SSL ルール エディタの [挿入（Insert）] ドロップダウンリストで、[ルールの上（above rule）] または [ルールの下（below rule）] を選択して、適切なルール番号を入力します。

ステップ 2 [保存（Save）] をクリックします。

ヒント ルールを保存すると、指定した場所に配置されます。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

SSL ルールの条件

SSL ルールの条件は、ルールで処理する暗号化トラフィックのタイプを特定します。条件には、単純なものと複雑なものがあり、ルールごとに複数の条件タイプを指定できます。トラフィックにルールが適用されるのは、トラフィックがルールの条件をすべて満たしている場合だけです。

ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。たとえば、証明書の条件が設定され、バージョンの条件が設定されていないルールは、セッション SSL または TLS のバージョンにかかわりなく、セッションのネゴシエーションに使用されるサーバ証明書に基づいてトラフィックを評価します。

すべての SSL ルールには、一致する暗号化トラフィックに対して次の判定をする関連アクションがあります。

- 処理：まず第一に、ルールアクションはルールの条件に一致する暗号化トラフィックに対して、モニタ、信頼、ブロック、または復号化を行うかどうかを判定します。
- ロギング：ルールアクションは一致する暗号化トラフィックの詳細をいつ、どのようにログに記録するかを判定します。

SSL インスペクション設定では、次のように復号されたトラフィックの処理、検査、ログ記録を行います。

- SSL ポリシーの復号できないアクションは、システムが復号できないトラフィックを処理します。
- ポリシーのデフォルトアクションは、モニタ以外のどの SSL ルールの条件にも一致しないトラフィックを処理します。

システムが暗号化セッションを信頼またはブロックしたときに、接続イベントをログに記録できます。アクセスコントロールルールに従ってより詳細な評価のために復号化した場合の接続ログを記録するようにシステムを強制することも可能で、これはその後でどのような処理やトラフィックの検査がされるかとは無関係です。暗号化セッションの接続ログには、セッションの暗号化に使用される証明書など、暗号化の詳細が含まれます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続（[ブロック（Block）]、[リセットしてブロック（Block with reset）]）の場合、システムは即座にセッションを終了し、イベントを生成します。
- 信頼された接続（Do not decrypt）の場合、システムはセッション終了時にイベントを生成します。

SSL ルールの条件タイプ

SSL ルールを追加および編集するときは、ルール エディタ下部の左側にあるタブを使用して、ルール条件の追加と編集を行います。

表 *72* : *SSL* ルールの条件タイプ

条件	一致する暗号化トラフィック	詳細（Details）
ゾーン	特定のセキュリティ ゾーンでインターフェイスを介したデバイスへの着信またはデバイスからの発信	セキュリティ ゾーンは、ご使用の導入ポリシーおよびセキュリティ ポリシーに準じた 1 つ以上のインターフェイスの論理グループです。ゾーン内のインターフェイスは、複数のデバイスにまたがって配置される場合があります。
ネットワーク	その送信元または宛先 IP アドレス、国、または大陸による	IP アドレスを明示的に指定できます。位置情報機能を使用して、その送信元または宛先の国または大陸に基づいてトラフィックを制御できます。
VLAN タグ	VLAN のタグ	システムは、最も内側の VLAN タグを使用して VLAN を基準にパケットを識別します。
ポート	その送信元または宛先ポートによる	TCP ポートに基づいて暗号化トラフィックを制御できます。
Users	セッションに関与するユーザによる	暗号化されたモニタ対象セッションの関連ホストにログインしている LDAP ユーザに基づいて暗号化トラフィックを制御できます。Microsoft Active Directory サーバから取得された個別ユーザまたはグループに基づいてトラフィックを制御できます。
アプリケーション	セッションで検出されたアプリケーションによる	タイプ、リスク、ビジネスとの関連性、カテゴリの基本的な特性に従って、フィルタ アクセスまたは暗号化セッションの各アプリケーションへのアクセスを制御できます。
カテゴリ	証明書サブジェクトの識別名に基づいてセッションで要求される URL	URL の一般分類とリスク レベルに基づいて、ネットワークのユーザがアクセスできる Web サイトを制限できます。
識別名	暗号化セッションのネゴシエートに使用されたサーバ証明書のサブジェクトまたは発行元の識別名	サーバ証明書を発行した CA またはサーバ証明書ホルダーに基づいて、暗号化トラフィックを制御できます。
証明書（Certificates）	暗号化セッションのネゴシエートに使用されるサーバ証明書	暗号化セッションのネゴシエート用にユーザのブラウザに渡されるサーバ証明書に基づいて、暗号化されたトラフィックを制御できます。

条件	一致する暗号化トラフィック	詳細（Details）
証明書のステータス（Certificate Status）	暗号化セッションのネゴシエートに使用されるサーバ証明書のプロパティ	サーバ証明書のステータスに基づいて、暗号化トラフィックを制御できます。
暗号スイート	暗号化セッションのネゴシエートに使用する暗号スイート	暗号化セッションのネゴシエート用にサーバで選択された暗号スイートに基づいて、暗号化トラフィックを制御できます。
バージョン	セッションの暗号化に使用される SSL または TLS のバージョン	セッションの暗号化に使用される SSL または TLS のバージョンに基づいて、暗号化トラフィックを制御できます。

関連トピック

ネットワーク ベースの SSL ルールの条件, （918 ページ）
ユーザベースの SSL ルールの条件, （926 ページ）
暗号化トラフィックでのレピュテーションベースの URL ブロッキング, （934 ページ）
サーバ証明書ベースの SSL ルール条件, （936 ページ）

SSL ルールのアクション

SSL ルール：モニタ アクション

[モニタ（Monitor）]アクションは暗号化トラフィック フローに影響を与えません。つまり、一致するトラフィックがただちに許可または拒否されることはありません。その代わり、追加のルールが存在する場合はそのルールに照らしてトラフィックが照合され、信頼するか、ブロックするか、復号するかが決定されます。モニタ ルール以外の一致する最初のルールが、トラフィック フローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、システムはデフォルト アクションを使用します。

モニタ ルールの主要な目的はネットワーク トラフィックを追跡することであるため、ルールのロギング設定や、あとで接続を処理するデフォルトのアクションにかかわらず、システムはモニタ対象トラフィックの接続終了イベントを自動的に Firepower Management Center データベースに記録します。

SSL ルール：復号しないアクション

[復号しない（Do not decrypt）] アクションは、アクセス コントロール ポリシーのルールおよびデフォルトアクションに従って暗号化トラフィックを評価するため転送します。一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、こうしたトラフィックに一致するルール数が少なくなる場合があります。暗号化トラフィックに対しては、侵入やファイル インスペクションなどのディープ インスペクションを行うことはできません。

[復号しない（Do not decrypt）] ルールの一般的な理由は、以下のとおりです。

- SSL トラフィックの復号が法律によって禁止されている。
- 信頼できると判明しているサイトである。
- トラフィックを調べることによって中断できるサイト（Windows Update など）である。

詳細については、次を参照してください。復号できないトラフィックのデフォルト処理オプション，（887 ページ）

SSL ルール：ブロッキング アクション

[ブロック（Block）] および [リセットしてブロック（Block with reset）] アクションは、アクセスコントロール ルールの [ブロック（Block）] と [リセットしてブロック（Block with reset）] アクションに類似しています。これらのアクションは、クライアントとサーバによる SSL 暗号化セッションの確立と暗号化トラフィックの転送を防止します。リセット付きブロック ルールでは接続のリセットも行います。

ブロックされた暗号化トラフィックについては、設定された応答ページが表示されないので注意してください。その代わりに、ユーザの要求する禁止されたURLの接続は、リセットされるか、またはタイムアウトになります。

ヒント　パッシブまたはインライン（タップ モード）展開では、デバイスがトラフィックを直接検査しないので、[ブロック（Block）] と [リセットしてブロック（Block with reset）] アクションを使用できないことに注意してください。パッシブまたはインライン（タップモード）インターフェイスを含むセキュリティゾーン条件内で、[ブロック（Block）] と [リセットしてブロック（Block with reset）] アクションを使用したルールを作成すると、ポリシー エディタでルールの横に警告アイコン（⚠）が表示されます。

関連トピック

HTTP 応答ページについて，（825 ページ）

SSL ルール：復号アクション

[復号 - 既知のキー（Decrypt - Known Key）] および [復号 - 再署名（Decrypt - Resign）] アクションは、暗号化トラフィックを復号します。復号されたトラフィックは、アクセス制御を使用して検査されます。アクセスコントロールルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。ここではデータの確認に加えて、侵入、禁止ファイル、マルウェアを検出およびブロックできます。システムは、許可されたトラフィックを再暗号化してから宛先に渡します。

SSL ルールの復号メカニズムとガイドライン

[復号 - 既知のキー（Decrypt - Known Key）] アクションを設定した場合は、1 つまたは複数のサーバ証明書と秘密キー ペアをアクションに関連付けることができます。トラフィックがルールに一致して、トラフィックの暗号化に使用された証明書とアクションに関連付けられた証明書が一致した場合、システムは適切な秘密キーを使用してセッションの暗号化と復号キーを取得します。秘密キーへのアクセスが必要なため、このアクションが最も適しているのは、組織の管理下にあるサーバへの入力トラフィックを復号する場合です。

同様に [復号 - 再署名（Decrypt - Resign）] アクションには、1 つの認証局証明書と秘密キーを関連付けることができます。トラフィックがこのルールに一致した場合、システムは CA 証明書を使用してサーバ証明書を再署名してから、中間者（man-in-the-middle）として機能します。ここでは 2 つの SSL セッションが作成され、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間で使用されます。各セッションにはさまざまな暗号セッションの詳細が含まれており、システムはこれを使用することでトラフィックの復号化と再暗号化が行えます。このアクションは、証明書の秘密キーを各自の管理下にあるキーに置き換えてセッション キーを取得するため、発信トラフィックに適しています。

サーバ証明書の再署名では、証明書の公開キーを CA 証明書の公開キーに置き換えるか、あるいは証明書全体が置き換えられます。通常、サーバ証明書全体を置き換える場合は、SSL 接続が確立された時点で、証明書が信頼できる認証局によって署名されていないことがクライアント ブラウザで警告されます。ただし、その CA をクライアント ブラウザで信頼できることがポリシーに設定されている場合、ブラウザは証明書が信頼できないことについて警告しません。オリジナルのサーバ証明書が自己署名の場合、システムは証明書全体を置き換えて再署名する CA を信頼しますが、ユーザのブラウザは証明書が自己署名されていることを警告しません。この場合、サーバ証明書の公開キーを交換するだけで、クライアント ブラウザは証明書が自己署名であることを警告します。

[復号 - 再署名（Decrypt - Resign）] アクションをルールに設定すると、ルールによるトラフィックの照合は、設定されている他のルール条件に加えて、参照する内部 CA 証明書の署名アルゴリズム タイプに基づいて実施されます。各 [復号 - 再署名（Decrypt - Resign）] アクションにはそれぞれ 1 つの CA 証明書が関連付けられるので、異なる署名アルゴリズムで暗号化された複数のタイプの発信トラフィックを復号化する SSL ルールは作成できません。また、ルールに追加する暗号スイートと外部証明書のオブジェクトのすべては、関連する CA 証明書の暗号化アルゴリズム タイプに一致する必要があります。オプションで、証明書全体ではなく自己署名証明書キーのみを置き換えることができます。この場合、ユーザはブラウザで自己署名証明書キー通知を確認します。

たとえば、楕円曲線暗号（EC）アルゴリズムで暗号化された発信トラフィックが [復号 - 再署名（Decrypt - Resign）] ルールに一致するのは、アクションが EC ベースの CA 証明書を参照している場合だけです。証明書と暗号スイートのルール条件を作成する場合は、EC ベースの外部証明書と暗号スイートをルールに追加する必要があります。同様に、RSA ベースの CA 証明書を参照する [復号 - 再署名（Decrypt - Resign）] ルールは、RSA アルゴリズムで暗号化された発信トラフィックとのみ一致します。EC アルゴリズムで暗号化された発信トラフィックは、設定されている他のルール条件がすべて一致したとしても、このルールには一致しません。

次の点に注意してください。

- SSL 接続の確立に使用される暗号スイートが Diffie-Hellman Ephemeral（DHE）または楕円曲線 Diffie-Hellman Ephemeral（ECDHE）キー交換アルゴリズムを適用している場合、パッシブ展開では [復号 - 既知のキー（Decrypt - Known Key）] アクションを使用できません。SSL ポリシーのターゲット デバイスにパッシブまたはインライン（タップ モード）インターフェイスがあり、そこに含まれる [復号 - 既知のキー（Decrypt - Known Key）] ルールで DHE または ECDHE の暗号スイート条件が使われている場合、ルールの横に情報アイコン（[]）が表示されます。パッシブまたはインライン（タップ モード）インターフェイスを含む SSL ルールに後からゾーン条件を追加すると、警告アイコン（[]）が表示されます。
- デバイスはトラフィックを直接検査しないため、パッシブまたはインライン（タップ モード）展開では [復号 - 再署名（Decrypt - Resign）] アクションを使用できません。セキュリティ ゾーン内にパッシブまたはインライン（タップ モード）インターフェイスを含む [復号 - 再署名（Decrypt - Resign）] アクションを指定してルールを作成すると、ポリシー エディタでルールの横に警告アイコン（  ）が表示されます。SSL ポリシーのターゲット デバイスにパッシブまたはインライン（タップモード）インターフェイスがあり、[復号 - 再署名（Decrypt - Resign）] ルールが含まれる場合、ルールの横に情報アイコン（[]）が表示されます。パッシブまたはインライン（タップ モード）インターフェイスを含む SSL ルールに後からゾーン条件を追加すると、警告アイコン（[]）が表示されます。パッシブまたはインライン（タップ モード）インターフェイスを含むデバイスに、[復号 - 再署名（Decrypt - Resign）] ルールを含む SSL ポリシーを適用した場合、このルールに一致する SSL セッションはすべて失敗します。
- サーバ証明書の再署名に使用する CA をクライアントが信頼していない場合、証明書が信頼できないという警告がユーザに出されます。これを防ぐには、クライアントの信頼できる CA ストアに CA 証明書をインポートします。または、組織にプライベート PKI がある場合は、組織の全クライアントにより自動的に信頼されるルート CA が署名する中間 CA 証明書を発行して、その CA 証明書をデバイスにアップロードすることもできます。
- 匿名の暗号スイートで暗号化されたトラフィックは復号化できません。匿名の暗号スイートを [暗号スイート（Cipher Suite）] 条件に追加した場合、SSL ルールで [復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Decrypt - Known Key）] アクションを使用できません。
- クライアントと管理対象デバイスの間に HTTP プロキシがあって、クライアントとサーバが CONNECT HTTP メソッドを使用してトンネル SSL 接続を確立する場合、システムはトラフィックを復号化できません。システムによるこのトラフィックの処理法は、ハンドシェイク エラー（Handshake Errors）の復号できないアクションが決定します。
- システムは、管理対象デバイス上のキャプティブ ポータルのユーザの Web ブラウザとキャプティブ ポータルのデーモン間のキャプティブ ポータルの認証接続でトラフィックを復号化できません。
- [復号 - 既知のキー（Decrypt - Known Key）] アクションを指定して SSL ルールを作成した場合は、[識別名（Distinguished Name）] や [証明書（Certificate）] 条件による照合はできません。ここでの前提は、このルールがトラフィックと一致する場合、証明書、サブジェクト DN、および発行元 DN は、ルールに関連付けられた証明書とすでに一致済みであることです。

- 内部CAオブジェクトを作成して証明書署名要求（CSR）の生成を選択した場合は、オブジェクトに署名付き証明書をアップロードするまで、このCAを[復号 - 再署名（Decrypt - Resign）]アクションに使用できません。
- [復号 - 再署名（Decrypt - Resign）]アクションをルールに設定し、1つまたは複数の外部証明書オブジェクトまたは暗号スイートで署名アルゴリズムタイプの不一致が生じた場合、ポリシーエディタでルールの横に情報アイコン（）が表示されます。すべての外部証明書オブジェクトまたはすべての暗号スイートで署名アルゴリズムタイプの不一致が生じた場合、ポリシーのルールの横には警告アイコン（[]）が表示され、SSL ポリシーに関連付けたアクセス コントロール ポリシーは適用できなくなります。
- ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号できません。このトラフィックを許可するには、サーバ証明書の共通名または識別名と一致させるために、[復号しない（Do not decrypt）]アクションを使用して SSL ルールを設定します。
- [インタラクティブ ブロック（Interactive Block）]または[リセット付きインタラクティブ ブロック（Interactive Block with reset）]アクションのアクセス コントロール ルールと復号化トラフィックが一致する場合、システムは一致する接続をインタラクションなしでブロックし、応答ページを表示しません。
- インライン正規化プリプロセッサで[余剰ペイロードの正規化（Normalize Excess Payload）]オプションを有効にすると、プリプロセッサによる復号トラフィックの標準化時に、パケットがドロップされてトリミングされたパケットに置き換えられる場合があります。これにより SSL セッションは終了しません。トラフィックが許可された場合、トリミングされたパケットは SSL セッションの一部として暗号化されます。

関連トピック

PKI オブジェクト, （440 ページ）

SSL ルール アクションの設定

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

手順

ステップ 1 SSL ポリシー エディタには、次のオプションがあります。

- 新しいルールを追加するには、[ルールの追加（Add Rule）]をクリックします。

- 既存のルールを編集するには、編集アイコン（  ）をクリックします。

ステップ 2 [アクション（Action）] ドロップダウン リストからルール アクションを選択します。

- 暗号化トラフィックをブロックするには、[ブロック（Block）] を選択します。
- 暗号化トラフィックをブロックし、接続をリセットするには、[リセットでブロック（Block with reset）] を選択します。
- 着信トラフィックの復号の詳細については、復号 - 既知のキー アクションの設定, （911 ページ）を参照してください。
- 発信トラフィックの復号の詳細については、復号 - 再署名アクションの設定, （910 ページ）を参照してください。
- 暗号化トラフィックを記録するには、[モニタ（Monitor）] を選択します。
- 暗号化トラフィックを復号しない場合は、[復号化しない（Do Not Decrypt）] を選択します。

ステップ 3 [追加（Add）] をクリックします。

次の作業

- ネットワーク ベースの SSL ルールの条件, （918 ページ）、ユーザベースの SSL ルールの条件, （926 ページ）、レピュテーション ベースの SSL ルール条件, （927 ページ）、およびサーバ証明書ベースの SSL ルール条件, （936 ページ）の説明に従ってルール条件を設定します。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

復号 - 再署名アクションの設定

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

手順

ステップ 1 SSL ルール エディタで、[アクション（Action）] リストから [復号 - 再署名（Decrypt - Resign）] を選択します。

ステップ 2 リストから内部 CA 証明書のオブジェクトを選択します。

ステップ 3 証明書全体ではなく証明書公開キーのみを置き換えるには、 をオンにする必要があります。公開キーのみを置き換えようとしているため、自己署名証明書の通知がユーザのブラウザに表示されます。

ステップ 4 [追加（Add）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

復号 - 既知のキー アクションの設定

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

手順

ステップ 1 SSL ルール エディタで、[アクション（Action）] ドロップダウン リストから、[復号 - 既知のキー（Decrypt - Known Key）] を選択します。

ステップ 2 [クリックして復号証明書を選択（Click to select decryption certs）] フィールドをクリックします。

ステップ 3 [使用可能な証明書（Available Certificates）] リストの 1 つ以上の内部証明書のオブジェクトを選択し、[ルールに追加（Add to Rule）] をクリックします。

ステップ 4 [OK] をクリックします。

ステップ 5 [追加（Add）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

SSL ルールの管理

SSL ポリシー エディタの [ルール（Rules）] タブでは、ポリシー内の SSL ルールの追加、編集、検索、移動、有効化、無効化、削除、およびその他の管理を行うことができます。

SSL ルール検索

スペースおよび印刷可能な特殊文字を含む英数字文字列を使用して、SSL ルールのリストで一致する値を検索できます。この検索では、ルール名およびルールに追加したルール条件が検査されます。ルール条件の場合は、条件タイプ（ゾーン、ネットワーク、アプリケーションなど）ごとに追加できる任意の名前または値が検索照合されます。これには、個々のオブジェクト名または値、グループ オブジェクト名、グループ内の個々のオブジェクト名または値、およびリテラル値が含まれます。

検索文字列のすべてまたは一部を使用できます。照合ルールごとに、一致する値のカラムが強調表示されます。たとえば、`100Bao` という文字列のすべてまたは一部を基準に検索すると、少なくとも、100Bao アプリケーションが追加された各ルールの [アプリケーション（Applications）] 列が強調表示されます。`100Bao` という名前のルールもある場合は、[名前（Name）] 列と [アプリケーション（Applications）] 列の両方が強調表示されます。

1 つ前または次の照合ルールに移動することができます。ステータス メッセージには、現行の一致および合計一致数が表示されます。

複数ページのルール リストでは、どのページでも一致が検出される可能性があります。最初の一致が検出されたのが最初のページではない場合は、最初の一致が検出されたページが表示されます。最後の一致が現行の一致となっている場合、次の一致を選択すると、最初の一致が表示されます。また、最初の一致が現行の一致となっている場合、前の一致を選択すると、最後の一致が表示されます。

SSL ルールの検索

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

手順

ステップ 1 SSL ポリシー エディタで、[検索ルール（Search Rules）] プロンプトをクリックし、検索文字列を入力してから Enter キーを押します。

ヒント 一致する値を含むルールのカラムが強調表示されます。表示されている（最初の）一致は、他とは区別できるように強調表示されます。

ステップ 2 目的のルールを見つけます。

- 照合ルールの間を移動する場合は、次の一致アイコン（▼）または前の一致アイコン（▲）をクリックします。
- ページを更新し、検索文字列および強調表示をクリアするには、クリアアイコン（✖）をクリックします。

SSL ルールの有効化と無効化

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

作成した SSL ルールは、デフォルトで有効になっています。ルールを無効にすると、システムはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。SSL ポリシーのルール リストを表示すると、無効なルールはグレー表示されますが、変更は可能です。またはルール エディタを使用して SSL ルールを有効または無効にできることに注意してください。

手順

ステップ 1 SSL ポリシー エディタで、ルールを右クリックしてルール状態を選択します。

ステップ 2 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

SSL ルールの移動

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

手順

ステップ 1 SSL ポリシー エディタで、各ルールの空白部分をクリックしてルールを選択します。

ステップ 2 ルールを右クリックして、[切り取り（Cut）] を選択します。

ステップ 3 切り取ったルールを貼り付けたい位置に隣接するルールの空白部分を右クリックし、[上に貼り付け（Paste above）] または [下に貼り付け（Paste below）] を選択します。

ヒント 2 つの異なる SSL ポリシーの間では、SSL ルールのコピー アンド ペーストはできません。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

新しい SSL ルール カテゴリの追加

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

余計なポリシーを作成することなくルールをさらに整理するため、標準ルールとルート ルールのカテゴリの間にカスタム カテゴリを作成できます。追加したカテゴリは、名前変更と削除ができます。これらのカテゴリの移動はできませんが、ルールのカテゴリ間およびカテゴリ内外への移動は可能です。

手順

ステップ 1 SSL ポリシー エディタで、[カテゴリの追加（Add Category）] をクリックします。

ヒント ポリシーにルールがすでに含まれている場合は、既存のルールの行の空白部分をクリックして、新しいカテゴリを追加する前にその位置を設定できます。既存のルールを右クリックし、[新規カテゴリの挿入（Insert new category）] を選択することもできます。

ステップ 2 [名前（Name）] を入力します。

ステップ 3 次の選択肢があります。

- 最初の [挿入（Insert）] ドロップダウン リストから [カテゴリの上（above Category）] を選択した後、2 番目のドロップダウン リストからカテゴリを選択します。ここで選択したカテゴリの上にルールが配置されます。

- ドロップダウン リストから [ルールの下（below rule）] を選択し、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。
- ドロップダウン リストから [ルールの上（above rule）] を選択し、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

ステップ 4 [OK] をクリックします。

ヒント 削除するカテゴリに含まれるルールは、その上にあるカテゴリに追加されます。

ステップ 5 [保存（Save）] をクリックします。

SSL ルールのトラブルシューティング

SSL ルールを適切に設定するのは複雑なタスクですが、暗号化トラフィックを処理する有効な導入には不可欠のタスクです。ルールが互いをプリエンプトしたり、追加ライセンスが必要になったりすることがあります。また、ルールに無効な設定が含まれる可能性もあります。慎重に設定された SSL ルールは、ネットワーク トラフィックの処理に必要なリソースの軽減にも寄与します。あまりにも複雑なルールを作成したり、ルールの順番が不適切であったりすると、パフォーマンスに影響する可能性があります。詳細については、ルールのパフォーマンスに関するガイドライン，（371 ページ）を参照してください。

SSL ルールの無効な設定に対する警告

SSL ポリシーが依存する外部の設定は変更される可能性があるため、有効であった SSL ポリシー設定が無効になる場合があります。次の例について考えてみます。

- URL カテゴリ条件を含むルールで、それまで有効であったものが、URL フィルタリング ライセンスを持たないデバイスをターゲットにすることで無効になる場合があります。その時点で、ルールの横にエラーアイコンが表示され、ポリシーをそのデバイスに展開できなくなります。展開可能にするには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、または適切なライセンスを有効にする必要があります。
- [復号 - 再署名（Decrypt-Resign）] ルールを作成し、後でパッシブ インターフェイスでセキュリティ ゾーンを条件として追加した場合、ルールの横に警告アイコンが表示されます。パッシブ展開では証明書の再署名によるトラフィックの復号はできないので、パッシブ インターフェイスをルールから削除するか、またはルール アクションを変更するまで、このルールには効果がありません。
- ルールにレルムまたはユーザを追加した後、そのレルムまたはユーザを除外するようにレルムの設定を変更すると、ルールは適用されなくなります。

関連トピック

ルールとその他のポリシーの警告, （370 ページ）
ルールのパフォーマンスに関するガイドライン, （371 ページ）

第 44 章

SSL ルールを使用した復号の調整

次のトピックでは、SSL ルール条件を設定する方法の概要を示します。

SSL ルール条件の概要

デバイスで検査されるすべての暗号化トラフィックには、基本的な SSL ルールに基づいたアクションが適用されます。暗号化トラフィックをより詳細に復号および制御するには、特定タイプのトラフィックの処理およびログ記録を制御するルール条件を設定します。各 SSL ルールには 0 個、1 個、または複数の条件を設定できますが、トラフィックに SSL ルールが適用されるのは、そのルールのすべての条件にトラフィックが一致する場合のみです。

（注） トラフィックがルールに一致すると、デバイスは設定されたルール アクションをトラフィックに適用します。ログの記録が指定されている場合、接続が終了した時点でトラフィックに関するログが記録されます。

各ルール条件には、照合するトラフィックのプロパティを 1 つまたは複数指定できます。たとえば、以下のプロパティを指定できます。

- 通過するセキュリティ ゾーン、IP アドレスおよびポート、送信元または宛先の国、送信元または宛先の VLAN などのトラフィック フロー
- 検出された IP アドレスに関連付けられたユーザ
- トラフィックで検出されたアプリケーションなどのトラフィック ペイロード

- 接続の暗号化に使用された SSL/TLS プロトコル バージョン、暗号スイート、サーバ証明書などの接続暗号化
- サーバ証明書の識別名に指定された URL のカテゴリおよびレピュテーション

ネットワーク ベースの SSL ルールの条件

SSL ポリシーに追加する SSL ルールにより、暗号化トラフィックの処理やログ記録を詳細に制御できます。ネットワークベースの条件を使用して、ネットワークを通過する暗号化トラフィックを管理できます。以下の条件を使用できます。

- SSL ルールでゾーン条件を設定すると、暗号化トラフィックの送信元および宛先のセキュリティ ゾーンに応じてそのトラフィックを制御できます。セキュリティ ゾーンとは、1 つ以上のインターフェイスの論理グループを指します。ゾーン内のインターフェイスが複数のデバイス間に配置される場合もあります。検出モードと呼ばれる、デバイスの初期セットアップ時に選択するオプションによって、システムが最初にデバイスのインターフェイスをどのように設定するか、およびこれらのインターフェイスがセキュリティ ゾーンに属するかどうかが決定します。
- SSL ルールでネットワーク条件を設定すると、暗号化トラフィックの送信元および宛先の IP アドレスに応じてそのトラフィックを制御および復号できます。制御対象とする暗号化トラフィックの送信元と宛先の IP アドレスを明示的に指定するか、地理位置情報機能を使用することができます。地理位置情報機能では、IP アドレスを地理的位置に関連付けて、暗号化トラフィックをその送信元または宛先の国や大陸に基づいて制御できます。
- SSL ルールで VLAN 条件を設定すると、トラフィックの VLAN タグに応じてそのトラフィックを制御できます。システムは、最も内側の VLAN タグを使用して VLAN を基準にパケットを識別します。
- SSL ルールでポート条件を設定すると、暗号化トラフィックの送信元および宛先の TCP ポートに応じてそのトラフィックを制御できます。

ネットワークベースの複数の条件を組み合わせたり、他のタイプの条件と組み合わせたりして、SSL ルールを作成できます。これらの SSL ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）

ネットワーク ゾーン SSL ルールの条件

1 つのゾーン条件で [送信元ゾーン（Sources Zones）] および [宛先ゾーン（Destination Zones）] それぞれに対し、最大 50 のゾーンを追加できます。

- 特定のゾーンのインターフェイスからデバイスを離れる暗号化トラフィックを照合するには、そのゾーンを [宛先ゾーン（Destination Zones）] に追加します。

パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブなインターフェイスで構成されるゾーンを [宛先ゾーン（Destination Zones）] 条件で使用することはできません。

- 特定のゾーンのインターフェイスからデバイスに入る暗号化トラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。

送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

ゾーン内のすべてのインターフェイスが同じタイプ（インライン、パッシブ、スイッチド、またはルーテッド）である必要があるため、SSL ルールのゾーン条件で使用されているすべてのゾーンが同じタイプでなければならないことに注意してください。つまり、異なるタイプのゾーンを送信元/宛先とする暗号化トラフィックを照合する単一ルールを定義することはできません。

ゾーンにインターフェイスが含まれていないなど、無効な設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

ネットワーク ゾーンによる暗号化トラフィックの制御

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

手順

ステップ 1 SSL ルール エディタで、[ゾーン（Zones）] タブを選択します。

ステップ 2 [利用可能なゾーン（Available Zones）] から追加するゾーンを見つけます。追加するゾーンを検索するには、[利用可能なゾーン（Available Zones）] リストの上にある [名前で検索（Search by name）] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

ステップ 3 クリックすると、ゾーンを選択できます。すべてのゾーンを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ 4 [送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。

ヒント 選択したゾーンをドラッグ アンド ドロップすることもできます。

ステップ 5 ルールを保存するか、編集を続けます。

例

単純な例として、インライン検出モードを選択したデバイスでは、Firepower Management Centerにより内部と外部の 2 つのゾーンが作成され、そのデバイスの最初のインターフェイスのペアがそれらのゾーンに割り当てられます。内部側のネットワークに接続されたホストは、保護されている資産を表します。

このシナリオを拡張すると、同等に設定された追加デバイス（同じFirepower Management Centerによって管理されるもの）を展開して、複数の異なるロケーションで同様のリソースを保護できます。最初のデバイスと同様に、これらのデバイスも内部セキュリティ ゾーンのアセットを保護します。

（注） 内部（または外部）のすべてのインターフェイスを1つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティ ポリシーが意味をなすグループ化を選択します。

この展開では、これらのホストにインターネットへの無制限アクセスを提供できますが、着信する暗号化トラフィックを復号および検査してホストを保護しなければなりません。

これを実現するには、[宛先ゾーン（Destination Zone）] が [内部（Internal）] に設定されたゾーン条件を持つ SSL ルールを設定します。この単純な SSL ルールでは、内部ゾーンのいずれかのインターフェイスからデバイスを離れるトラフィックが照合されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

セキュリティ ゾーン, （392 ページ）

ネットワークまたは地理位置情報 SSL ルールの条件

ネットワークベースの SSL ルールの条件を作成する場合、IP アドレスと地理的位置を手動で指定できます。または、再利用可能で名前を 1 つ以上の IP アドレス、アドレス ブロック、国、大陸などに関連付けるネットワーク オブジェクトおよび位置情報オブジェクトを使用してネットワーク条件を設定できます。

（注） 地理的位置別にトラフィックを制御するルールを作成して、確実に最新の位置情報データを使用してトラフィックをフィルタ処理する場合は、シスコはFirepower Management Center の位置情報データベース（GeoDB）を定期的に更新することを**強く**推奨しています。

1 つのネットワーク条件で [送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] それぞれに対し、最大 50 の項目を追加でき、ネットワークベースの設定と位置情報ベースの設定を組み合わせることができます。

- 特定のIPアドレスまたは地理的位置からの暗号化トラフィックを照合するには、[送信元ネットワーク（Source Networks）] を設定します。
- 特定の IP アドレスまたは地理的位置への暗号化トラフィックを照合するには、[宛先ネットワーク（Destination Networks）] を設定します。

送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信され**かつ**宛先 IP アドレスに送信される暗号化トラフィックの照合を行う必要があります。

ネットワーク条件を作成する際、警告アイコンは無効な設定を示します。アイコンの上にポインタを置くと詳細が表示されます。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）

ネットワークまたは地理位置情報による暗号化トラフィックの制御

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

はじめる前に

- 地理位置情報データベースの更新, （169 ページ）の説明に従って、Firepower Management Center で地理位置情報データベース（GeoDB）を更新します。

手順

ステップ 1 SSL ルール エディタで、[ネットワーク（Networks）] タブを選択します。

ステップ 2 [利用可能なネットワーク（Available Networks）] から、次のように追加するネットワークを見つけます。

- 追加するネットワーク オブジェクトとグループを表示するには [ネットワーク（Networks）] タブをクリックします。位置情報オブジェクトを表示するには [位置情報（Geolocation）] タブをクリックします。
- ネットワーク オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[利用可能なネットワーク（Available Networks）] リストの上にある追加アイコン（  ）をクリックします。
- 追加するネットワーク オブジェクトまたは位置情報オブジェクトを検索するには、適切なタブを選択し、[利用可能なネットワーク（Available Networks）] リストの上にある [名前また

は値で検索（Search by name or value）] プロンプトをクリックして、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ 4 [送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。

ヒント 選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5 手動で指定する送信元または宛先 IP アドレスまたはアドレスブロックを追加します。[送信元ネットワーク（Source Networks）] リストまたは [宛先ネットワーク（Destination Networks）] リストの下にある [IP アドレスの入力（Enter an IP address）] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [追加（Add）] をクリックします。

ステップ 6 ルールを保存するか、編集を続けます。

例

次の図は、内部ネットワークから発信され、ケイマン諸島（Cayman Islands）または海外にある持ち株会社のサーバ（182.16.0.3）のリソースにアクセスしようとする暗号化接続をブロックする SSL ルールのネットワーク条件を示しています。

この例では、持ち株会社のサーバの IP アドレスを手動で指定し、ケイマン諸島の IP アドレスを表すシステム提供の地理位置情報オブジェクト Cayman Islands を使用しています。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

関連トピック

ネットワーク オブジェクト，（388 ページ）
Firepower システムの IP アドレス表記法，（16 ページ）

VLAN SSL ルールの条件

VLAN ベースの SSL ルール条件を作成するときは、1 ～ 4094 の VLAN タグを手動で指定できます。または、VLAN タグ オブジェクトを使用して VLAN 条件を設定することもできます。VLAN タグ オブジェクトとは、いくつかの VLAN タグに名前を付けて再利用可能にしたものを指します。

ヒント　VLAN タグ オブジェクトを作成しておくと、それを使用して SSL ルールを作成したり、Web インターフェイスのさまざまな場所で VLAN タグを表すオブジェクトとして使用したりできます。VLAN タグ オブジェクトはオブジェクト マネージャを使用して作成できます。また、アクセス コントロール ルールの設定時に作成することもできます。

1 つの VLAN タグ条件で、[選択済み VLAN タグ（Selected VLAN Tags）] に最大 50 の項目を追加できます。無効な VLAN タグ条件設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

暗号化された VLAN トラフィックの制御

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

手順

ステップ 1　SSL ルール エディタで、[VLAN タグ（VLAN Tags）] タブを選択します。

ステップ 2　[利用可能な VLAN タグ（Available VLAN Tags）] で、次のように追加する VLAN を見つけます。

- VLAN タグ オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[利用可能な VLAN タグ（Available VLAN Tags）] リストの上にある追加アイコン（  ）をクリックします。
- 追加する VLAN タグ オブジェクトおよびグループを検索するには、[利用可能な VLAN タグ（Available VLAN Tags）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクト名またはオブジェクトの VLAN タグの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3　オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ 4　[ルールに追加（Add to Rule）] をクリックします。

ヒント　選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5　手動で指定する VLAN タグを追加します。[選択した VLAN タグ（Selected VLAN Tags）] リストの下にある [VLAN タグの入力（Enter a VLAN Tag）] プロンプトをクリックし、VLAN タグまた

はその範囲を入力して、[追加（Add）] をクリックします。1 から 4094 までの任意の VLAN タグを指定できます。VLAN タグの範囲を指定するにはハイフンを使用します。

ステップ 6 ルールを保存するか、編集を続けます。

例

次の図は、特定の公開 VLAN（VLAN タグ オブジェクト グループで指定）および手動で追加した VLAN「42」上の暗号化トラフィックに一致する SSL ルールの VLAN タグ条件を示しています。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

VLAN タグ オブジェクト, （394 ページ）

ポート SSL ルールの条件

ポートベースの SSL ルールの条件を作成するときは、手動で TCP ポートを指定できます。または、再利用可能で名前を 1 つ以上のポートに関連付けるポート オブジェクトを使用してポート条件を設定できます。

1 つのネットワーク条件で [選択した送信元ポート（Selected Source Ports）] および [選択した宛先ポート（Selected Destination Ports）] それぞれに対し、最大 50 の項目を追加できます。

- 特定の TCP ポートからの暗号化トラフィックを照合するには、[選択した送信元ポート（Selected Source Ports）] を設定します。
- 特定の TCP ポートへの暗号化トラフィックを照合するには、[選択した宛先ポート（Selected Destination Ports）] を設定します。
- TCP [選択した送信元ポート（Selected Source Ports）] から送信された暗号化トラフィックと TCP [選択した宛先ポート（Selected Destination Ports）] に送信した暗号化トラフィックを双方とも照合するには、それぞれのポートを設定します。

[選択した送信元ポート（Selected Source Ports）] および [選択した宛先ポート（Selected Destination Ports）] リストで設定できるのは TCP ポートだけです。非 TCP ポートを含むポート オブジェクトは、[使用可能ポート（Available Ports）] リストではグレイで表示されます。

ポート条件を作成する際、警告アイコンは無効な設定を示します。たとえば、オブジェクト マネージャを使用して使用中のポート オブジェクトを編集し、それらのオブジェクト グループを使用するルールを無効にできます。アイコンの上にポインタを置くと詳細が表示されます。

ポートによる暗号化トラフィックの制御

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

手順

ステップ 1 SSL ルール エディタで、[ポート（Ports）] タブを選択します。

ステップ 2 [利用可能なポート（Available Ports）] から追加する TCP ポートを次のように探します。

- TCP ポート オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[利用可能なポート（Available Ports）] リストの上にある追加アイコン（  ）をクリックします。
- 追加する TCP ベースのポート オブジェクトおよびグループを検索するには、[利用可能なポート（Available Ports）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトのポートの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。たとえば、「443」と入力すると、システム提供の HTTPS ポート オブジェクトが Firepower Management Center に表示されます。

ステップ 3 TCP ベースのポート オブジェクトを 1 つ選択するには、クリックします。TCP ベースのポート オブジェクトをすべて選択するには、右クリックして [すべて選択（Select All）] を選択します。非 TCP ベースのポートを含んでいるオブジェクトは、ポート条件に追加できません。

ステップ 4 [送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。

ヒント 選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5 送信元または宛先のポートを手動で指定するには、[選択した送信元ポート（Selected Source Ports）] または [選択した宛先ポート（Selected Destination Ports）] リストの下にある [ポート（Port）] にポート番号を入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。

ステップ 6 [追加（Add）] をクリックします。

（注） Firepower Management Centerでは、無効なポート設定はルール条件に追加されません。

ステップ 7 ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

ポート オブジェクト, （390 ページ）

ユーザベースの SSL ルールの条件

レルム、グループ、またはユーザに基づいてトラフィックと照合するように SSL ルールを設定することができます。SSL ルールのレルム、グループ、およびユーザの条件では、ユーザ制御を実行して、権威のあるユーザを IP アドレスに関連付けることにより、ネットワークを通過できるトラフィックを管理することができます。

ユーザ条件を設定した SSL ルールとトラフィックを一致させるには、モニタ対象のセッションにおける送信元または宛先ホストの IP アドレスと、ログインする権威のあるユーザを関連付ける必要があります。レルム、個々のユーザ、またはユーザが属しているグループに基づいてトラフィックを制御できます。

ユーザ ベースの暗号化トラフィックの制御

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

はじめる前に

- ユーザ アイデンティティ ソース, （1531 ページ）の説明に従って、1 つ以上の権限のあるユーザ アイデンティティ ソースを設定します。
- レルムの作成, （1586 ページ）の説明に従って、レルムを設定します。

手順

ステップ 1 SSL ルール エディタで、[ユーザ（Users）] タブを選択します。

ステップ 2 [使用可能なレルム（Available Realms）] リストで名前または値で検索してレルムを選択します。

ステップ 3 [使用可能なユーザ（Available Users）] リストで名前または値で検索してレルムを選択します。

ステップ 4 [ルールに追加（Add to Rule）] をクリックします。

ヒント 選択したユーザおよびグループをドラッグ アンド ドロップすることもできます。

ステップ 5 ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

レピュテーション ベースの SSL ルール条件

SSL ルールでレピュテーション ベース条件を設定すると、ネットワーク トラフィックをコンテキスト化して状況に応じて制限することで、ネットワーク通過を許可する暗号化トラフィックを管理できます。SSL ルールでのレピュテーション ベースの制御には、以下のタイプがあります。

- アプリケーション条件によりアプリケーション制御を実行できます。このシステムが暗号化された IP トラフィックを分析するときに、ネットワーク上で一般的に使用されている暗号化アプリケーションを識別および分類してから暗号化セッションを復号します。このシステムでは、こうした検出ベースのアプリケーション認識機能を使用して、ネットワーク上の暗号化されたアプリケーション トラフィックを制御できます。

  1 つの SSL ルールにおいて、カスタム アプリケーションなどの個々のアプリケーションを選択できます。システムにより提供されたアプリケーション フィルタを使用できます。これは、アプリケーションの基本的な特性（タイプ、リスク、ビジネスとの関連性、およびカテゴリ）に応じて構成された名前付きのアプリケーション セットです。

- URL 条件では、Web サイトに割り当てられたカテゴリおよびレピュテーションに基づいて Web トラフィックを制御できます。

SSL ルールの選択されたアプリケーションとフィルタ

シスコは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にディテクタを更新し追加しています。独自のディテクタを作成し、そのディテクタが検出するアプリケーションに特性（リスク、関連性など）を割り当てることもできます。アプリケーションの特性に基づいたフィルタを使用することで、システムは最新のディテクタを使用してアプリケーション トラフィックをモニタします。

アプリケーション条件を設定したSSLルールとトラフィックを一致させるには、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加したいずれかのアプリケーションまたはフィルタにトラフィックが一致する必要があります。

（注） アクセス コントロール ルールを使用してアプリケーション トラフィックをフィルタ処理する場合、フィルタ条件としてアプリケーション タグを使用できます。ただし、暗号化トラフィックはアプリケーション タグでフィルタ処理できません。そのことには意味がないからです。暗号化トラフィックのすべてのアプリケーションを検出するにはタグ付きの SSL プロトコルである必要があり、このタグが付けられていないアプリケーションは、非暗号化トラフィックまたは復号化されたトラフィックでしか検出できません。

1 つのアプリケーション条件において、最大 50 の項目を [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加できます。以下はそれぞれ 1 つの項目としてカウントされます。

- 個別またはカスタムな組み合わせの、[アプリケーション フィルタ（Application Filters）] リストからの 1 つ以上のフィルタ。この項目は、特性によってグループ化されたアプリケーションのセットを表します。
- [使用可能なアプリケーション（Available Applications）] リストにあるアプリケーションの検索結果を保存することで作成されたフィルタ。この項目は、部分文字列の一致によってグループ化されたアプリケーションのセットを表します。
- [使用可能なアプリケーション（Available Applications）] リストからの個々のアプリケーション。

Web インターフェイスでは、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。

SSL ポリシーの展開時には、一致する固有のアプリケーションのリストが、アプリケーションの条件を設定したルールごとに生成されます。つまり、完全なカバレッジを確保するために、重複フィルタおよび個々に指定されたアプリケーションを使用できます。

SSL ルールのアプリケーション フィルタ

SSL ルールのアプリケーション条件を作成するには、[アプリケーション フィルタ（Application Filters）] リストを使用して、照合するトラフィックの特性を基にアプリケーションをグループ化します。

ユーザの利便性のため、各アプリケーションの特性がタイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグによって判別されます。これらの基準をフィルタとして使用したり、フィルタのカスタムな組み合わせを作成してアプリケーション制御を実行したりできます。

SSL ルールにおけるアプリケーション フィルタのメカニズムは、オブジェクト マネージャを使用して再利用可能なカスタム アプリケーション フィルタを作成する場合と同じです。また、オンザフライで作成した多数のフィルタを、アクセス コントロール ルールに新規の再利用可能なフィル

タとして保存できます。ユーザが作成したフィルタはネストすることができないため、別のユーザが作成したフィルタを含むフィルタは保存できません。

フィルタの組み合わせ方について

フィルタを単独または組み合わせて選択すると、[使用可能なアプリケーション（Available Applications）] リストが更新され、条件を満たすアプリケーションのみが表示されます。システムによって提供されるフィルタは組み合わせて選択できますが、カスタム フィルタはできません。

システムは、OR 演算を使用して同じフィルタ タイプの複数のフィルタをリンクします。たとえば、Risks（リスク）タイプの下の Medium（中）および High（高）フィルタを選択すると、結果として次のようなフィルタになります。

```
Risk: Medium OR High
```

[中（Medium）] フィルタに 110 個のアプリケーション、[高（High）] フィルタに 82 個のアプリケーションが該当する場合は、それら 192 個のアプリケーションすべてが [使用可能なアプリケーション（Available Applications）] リストに表示されます。

システムは、AND 演算を使用して異なるタイプのフィルタをリンクします。たとえば Risks（リスク）タイプで Medium（中）および High（高）フィルタを選択し、Business Relevance（ビジネスとの関連性）タイプで Medium（中）および High（高）フィルタを選択した場合、結果として次のようなフィルタになります。

```
Risk: Medium OR High
AND
Business Relevance: Medium OR High
```

この場合、システムは [中（Medium）] または [高（High）] の [リスク（Risk）] タイプと [中（Medium）] または [高（High）] の [ビジネスとの関連性（Business Relevance）] タイプの両方に含まれるアプリケーションだけを表示します。

フィルタの検索および選択

フィルタを選択するには、フィルタ タイプの横にある矢印をクリックしてそれを展開し、アプリケーションを表示/非表示にする各フィルタの横のチェック ボックスを選択/選択解除します。また、Cisco 提供のフィルタ タイプ（[リスク（Risks）]、[ビジネスとの関連性（Business Relevance）]、[タイプ（Types）]、または [カテゴリ（Categories）]）を右クリックして、[すべて選択（Check All）] または [すべて選択解除（Uncheck All）] を選択することもできます。

フィルタを検索するには、[使用可能なフィルタ（Available Filters）] リストの上にある [名前で検索（Search by name）] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するフィルタが表示されます。

フィルタを選択したら、[使用可能なアプリケーション（Available Applications）] リストを使用して、それらのフィルタをルールに追加します。

関連トピック

アプリケーション フィルタ, （393 ページ）

SSL ルールで使用可能なアプリケーション

SSL ルールのアプリケーション条件を作成するには、[使用可能なアプリケーション（Available Applications）] リストを使用して、照合するトラフィックのアプリケーションを選択します。

アプリケーションのリストの参照

条件の作成を初めて開始するときは、リストは制約されておらず、システムが検出するすべてのアプリケーションを一度に 100 個ずつ表示します。

- アプリケーションを確認していくには、リストの下にある矢印をクリックします。
- アプリケーションの特性に関する概要情報と参照可能なインターネット検索リンクを含むポップアップ ウィンドウを表示するには、アプリケーションの横にある情報アイコン（  ）をクリックします。

一致するアプリケーションの検索

照合するアプリケーションを見つけやすくするために、[使用可能なアプリケーション（Available Applications）] リストを次のように制約できます。

- アプリケーションを検索するには、リスト上部にある [名前で検索（Search by name）] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するアプリケーションが表示されます。
- フィルタを適用してアプリケーションを制約するには、[アプリケーション フィルタ（Application Filters）] リストを使用します。フィルタを適用すると、[使用可能なアプリケーション（Available Applications）] リストが更新されます。

制約されると、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] オプションが [使用可能なアプリケーション（Available Applications）] リストの上部に表示されます。

（注） [アプリケーション フィルタ（Application Filters）] リストで 1 つ以上のフィルタを選択し、さらに [使用可能なアプリケーション（Available Applications）] リストも検索すると、選択内容と検索フィルタ適用後の [使用可能なアプリケーション（Available Applications）] リストが AND 演算を使用して結合されます。つまり [フィルタに一致するすべてのアプリケーション（All apps matching the filter）] 条件には、[使用可能なアプリケーション（Available Applications）] リストに現在表示されている個々のすべての条件と、[使用可能なアプリケーション（Available Applications）] リストの上で入力された検索文字列が含まれます。

条件内で照合する単一アプリケーションの選択

照合するアプリケーションを検索したら、それをクリックして選択します。現在制約されているビューですべてのアプリケーションを選択するには、右クリックして [すべて選択（Select All）] を選択します。

1 つのアプリケーション条件において、アプリケーションの個別選択で追加できる最大数は 50 です。50 を超えるアプリケーションを追加するには、複数の SSL ルールを作成するか、フィルタを使用してアプリケーションをグループ化する必要があります。

条件のフィルタに一致するすべてのアプリケーションの選択

[アプリケーション フィルタ（Application Filters）] リストで検索またはフィルタを使用して制約されると、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] オプションが [使用可能なアプリケーション（Available Applications）] リストの上部に表示されます。

このオプションを使用して、制約された [使用可能なアプリケーション（Available Applications）] リスト内のアプリケーションのセット全体を [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに同時に追加できます。アプリケーションを個別に追加するのとは対照的に、このアプリケーションのセットを追加すると、そのセットを構成する個々のアプリケーションの数にかかわらず、最大 50 のアプリケーションに対してただ 1 つのアイテムとしてカウントされます。

このようにアプリケーション条件を作成するときは、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加するフィルタの名前は、フィルタに表されているフィルタ タイプ + 各タイプの最大 3 つのフィルタの名前を連結させたものとなります。同じタイプのフィルタが 3 個を超える場合は、その後に省略記号（...）が表示されます。たとえば次のフィルタ名には、Risks（リスク）タイプの 2 つのフィルタと Business Relevance（ビジネスとの関連性）タイプの 4 つのフィルタが含まれています。

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] で追加するフィルタに表されないフィルタ タイプは、追加するフィルタの名前に含まれません。[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リスト内のフィルタ名の上にポインタを置いたときに表示される説明テキストは、これらのフィルタ タイプが [任意（any）] に設定されていることを示します。つまり、これらのフィルタ タイプはフィルタを制約しないので、任意の値が許可されます。

[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] の複数のインスタンスをアプリケーション条件に追加でき、各インスタンスは [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストで個別の項目としてカウントされます。たとえば、リスクが高いすべてのアプリケーションを 1 つの項目として追加し、選択内容をクリアしてから、ビジネスとの関連性が低いすべてのアプリケーションを別の項目として追加できます。このアプリケーション条件は、リスクが高いアプリケーションまたはビジネスとの関連性が低いアプリケーションに一致します。

アプリケーション ベースの SSL ルール条件の要件

アプリケーション条件を設定した SSL ルールと暗号化トラフィックを一致させるには、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加したいずれかのアプリケーションまたはフィルタにトラフィックが一致する必要があります。

1 条件ごとに最大 50 の項目を追加でき、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。アプリケーション条件を作成する際、警告アイコンは無効な設定を示します。アイコンの上にポインタを置くと詳細が表示されます。

SSL ルールへのアプリケーション条件の追加

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

手順

ステップ 1 SSL ルール エディタで、[アプリケーション（Applications）] タブを選択します。

ステップ 2 [使用可能なアプリケーション（Available Applications）] リストに表示されるアプリケーションのリストをフィルタするには、[アプリケーション フィルタ（Application Filters）] リストにあるフィルタを 1 つまたは複数選択します。詳細については、SSL ルールのアプリケーション フィルタ, （928 ページ）を参照してください。

ステップ 3 [使用可能なアプリケーション（Available Applications）] リストから追加するアプリケーションを見つけて選択します。個々のアプリケーションを検索して選択するか、またはリストが制約されている場合は、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] を選択できます。詳細については、SSL ルールで使用可能なアプリケーション, （930 ページ）を参照してください。

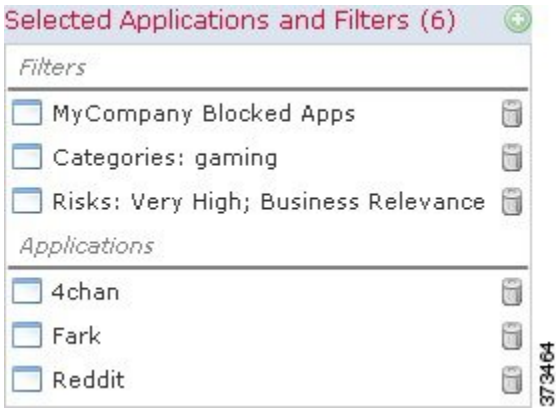
ステップ 4 [ルールに追加（Add to Rule）] をクリックします。

ヒント [すべてのフィルタをクリア（Clear All Filters）] をクリックして既存の選択をクリアします。選択したアプリケーションとフィルタをドラッグ アンド ドロップすることもできます。

ステップ 5 ルールを保存するか、編集を続けます。

例

次の図は、MyCompany のアプリケーション、リスクが高くビジネスとの関連性の低いすべてのアプリケーション、ゲーム アプリケーション、およびいくつかの指定アプリケーションからなるカスタム グループを復号する、SSL ルールのアプリケーション条件を示しています。



次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

暗号化されたアプリケーションの制御に対する制限

暗号化されたアプリケーションの識別

このシステムでは、StartTLS を使用して暗号化される非暗号化アプリケーションを識別できます。これには、SMTPS、POPS、FTPS、TelnetS、IMAPS などのアプリケーションが含まれます。また、TLS ClientHello メッセージ内の Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。

アプリケーション識別の速度

暗号化トラフィックのアプリケーション制御は、以下のすべての処理が完了するまで実行されません。

- 暗号化された接続がクライアントとサーバ間で確立される。
- 暗号化セッション内のアプリケーションがシステムにより識別される。

この識別が行われるのは、サーバ証明書が交換された後です。SSL ハンドシェイク中に交換されるトラフィックでアプリケーションの識別が完了する前に、アプリケーション条件を含んでいる SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。この動作により、ハンドシェイクが完了し、アプリケーションを識別できるようになります。便宜を図るため、影響を受けるルールは情報アイコン（ ）でマークされます。

システムによる識別が完了すると、アプリケーション条件に一致する残りのセッショントラフィックに SSL ルールのアクションが適用されます。

アプリケーション ディテクタの自動有効化

ポリシーのアプリケーション ルール条件ごとに、少なくとも 1 つのディテクタが有効にされている必要があります。有効になっているディテクタがないアプリケーションについては、システム

提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザ定義ディテクタが有効になります。

関連トピック

ディテクタのアクティブおよび非アクティブの設定, （1527 ページ）

暗号化トラフィックでのレピュテーションベースの URL ブロッキング

URL フィルタリング ライセンスでは、SSL ルールに設定した URL 条件により、要求された URL のカテゴリおよびレピュテーションに基づいて暗号化 Web サイトへのアクセスを制御できます。詳細については、URL 条件（URL フィルタリング）, （356 ページ）を参照してください。

ヒント　SSL ルールで使用する URL 条件は、手動による URL フィルタリングをサポートしていません。代わりに、サブジェクト共通名を照合する識別名条件を使用してください。

レピュテーション ベースの URL ブロッキングの実行

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
URL フィルタリング（URL Filtering）	URL フィルタリング（URL Filtering）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1　SSL ルール エディタで、[カテゴリ（Category）] タブを選択します。

ステップ 2　[カテゴリ（Categories）] リストで、追加する URL カテゴリを見つけます。カテゴリを指定せずにすべての暗号化 Web トラフィックと一致させるには、[任意（Any）] カテゴリを選択します。追加可能なカテゴリを検索するには、[カテゴリ（Categories）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、カテゴリ名を入力します。入力すると、リストが更新されて一致するカテゴリが表示されます。

ステップ 3　カテゴリを選択するには、そのカテゴリをクリックします。

ヒント　右クリックで表示される [すべて選択（Select All）] も利用できますが、この方法ですべてのカテゴリを追加すると、SSL ルールの最大項目数 50 を超えてしまいます。代わりに [任意（Any）] を使用してください。

ステップ 4　カテゴリの選択を限定する場合は、[レピュテーション（Reputations）] リストからレピュテーション レベルをクリックする必要があります。選択できるレピュテーション レベルは 1 つだけです。レピュテーション レベルを指定しない場合、システムはデフォルトとして [任意（Any）]（つまりすべてのレベル）を設定します。

- ルールで Web アクセスのブロックまたはトラフィックの復号を行う場合（ルール アクションが、[ブロック（Block）]、[リセットしてブロック（Block with reset）]、[復号 - 既知のキー（Decrypt - Known Key）]、[復号 - 再署名（Decrypt - Resign）]、または [モニタ（Monitor）] の場合）、選択したレピュテーション レベルよりも厳しいすべてのレピュテーションも自動的に選択されます。たとえば疑わしいサイト（Suspicious sites）（レベル 2）をブロックするようルールを設定した場合、高リスク（High Risk）（レベル 1）のサイトも自動的にブロックされます。
- ルールで Web アクセスを許可して、アクセス コントロールに従わせる場合（ルール アクションが [復号しない（Do not decrypt）] の場合）、選択したレピュテーション レベルよりも厳しくないすべてのレピュテーションも自動的に選択されます。たとえば無害なサイト（Benign sites）（レベル 4）を許可するようルールを設定した場合、有名（Well known）（レベル 5）サイトもまた自動的に許可されます。

（注） ルールのアクションを変更した場合、システムは、上記の点に従って URL 条件のレピュテーション レベルを自動的に変更します。

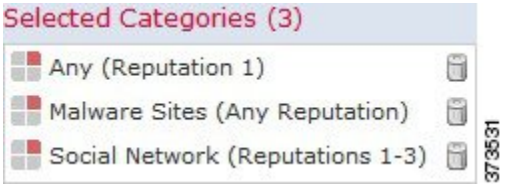
ステップ 5 [ルールに追加（Add to Rule）] をクリックして、選択した項目を [選択したカテゴリ（Selected Categories）] リストに追加します。

ヒント 選択した項目をドラッグ アンド ドロップすることもできます。

ステップ 6 ルールを保存するか、編集を続けます。

例

次の図は、すべてのマルウェア サイト、すべてのリスクの高いサイト、およびすべての安全でないソーシャル ネットワーキング サイトをブロックするアクセス コントロール ルール例の URL 条件を示しています。



次の表では、前の図で示した条件を作成する方法を要約します。

表 *73*：例：*URL* 条件の作成

ブロックする対象	選択するカテゴリまたは URL オブジェクト	選択するレピュテーション
マルウェア サイト（レピュテーションに関係なく）	マルウェア サイト（Malware Sites）	任意（Any）

ブロックする対象	選択するカテゴリまたは URL オブジェクト	選択するレピュテーション
高リスクの URL（レベル 1）	任意（Any）	1 - 高リスク（High Risk）
無害（benign）よりも大きいリスクがあるソーシャル ネットワーキング サイト（レベル 1 ～ 3）	ソーシャル ネットワーク（Social Network）	3 - セキュリティ リスクのある無害なサイト（Benign sites with security risks）

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

サーバ証明書ベースの SSL ルール条件

SSL ルールでは、サーバ証明書の特性に基づいて暗号化トラフックを処理および復号できます。SSL ルールは、以下のサーバ証明書属性に基づいて設定することができます。

- 識別名条件を設定すると、証明書所有者またはサーバ証明書の発行元 CA に応じて暗号化トラフィックを処理および検査できます。発行元の識別名を基準にすると、サイトのサーバ証明書を発行した CA に基づいてトラフィックを処理できます。
- SSL ルールで証明書条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書に応じて暗号化トラフィックを処理および検査できます。1 つの条件に 1 つまたは複数の証明書を設定でき、トラフィックの証明書がいずれかの条件の証明書と一致するとそのルールが適用されます。
- SSL ルールの証明書ステータス条件では、トラフィックの暗号化に使用されたサーバ証明書のステータスに基づいて暗号化されたトラフィックを処理して、証明書が有効か、失効しているか、期限切れか、まだ有効でないか、自己署名済みか、信頼できる CA によって署名済みか、証明書失効リスト（CRL）が有効かどうか、証明書のサーバ名指定（SNI）が要求内のサーバと一致するかどうかなどの検査を行うことができます。
- SSL ルールで暗号スイート条件を設定すると、暗号化セッションのネゴシエートに使用される暗号スイートに応じて暗号化トラフィックを処理および検査できます。
- SSL ルールでセッション条件を設定すると、トラフィックの暗号化に使用されている SSL または TLS のバージョンに応じて暗号化トラフィックを検査できます。

複数の暗号スイートを 1 つのルールで検出したり、証明書の発行元や証明書ホルダーを検出したりする場合は、再利用可能な暗号スイートのリストおよび識別名オブジェクトを作成してルールに追加できます。サーバ証明書および特定の証明書ステータスを検出するには、ルール用の外部証明書と外部 CA オブジェクトの作成が必要です。

証明書の識別名の SSL ルール条件

ルール条件を設定する場合は、手動でリテラル値を指定するか、識別名オブジェクトを参照するか、または複数のオブジェクトを含んでいる識別名グループを参照できます。

（注） [復号 - 既知のキー（Decrypt - Known Key）] アクションを選択した場合、識別名条件を設定することはできません。このアクションでは、トラフィック復号用のサーバ証明書の選択が必要であるため、トラフィックの照合はすでにこの証明書で行われています。

複数のサブジェクトおよび発行元の識別名との照合を単一の証明書ステータスのルール条件で行うことも可能ですが、ルールとの照合で一致する必要があるのは 1 つの共通名または識別名だけです。

識別名を手動で追加する場合、共通名属性（CN）を含めることができます。`CN=` なしで共通名を追加すると、オブジェクトを保存する前に `CN=` が追加されます。

また、以降の属性ごとに1つずつ識別名をカンマで区切って追加することができます。たとえば、C, CN, O, OU というようにします。

1 つの識別名条件で、[サブジェクト DN（Subject DNs）] リストおよび [発行元 DN（Issuer DNs）] リストにそれぞれ最大 50 のリテラル値および識別名オブジェクトを追加できます。

システム提供の識別名オブジェクト グループである Cisco-Undecryptable-Sites には、システムで復号できないトラフィックの Web サイトが含まれます。このグループを識別名条件に追加すると、該当する Web サイトとのトラフィックがブロックしたり復号を無効にしたりでき、これらのトラフィックの復号に使用されるシステム リソースの浪費を回避できます。グループ内の各エントリは変更できますが、このグループを削除することはできません。システムによる更新によってこのリストのエントリが変更されることがありますが、ユーザによる変更は保持されます。

証明書の識別名による暗号化トラフィックの制御

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

手順

ステップ 1 SSL ルール エディタで、[DN] タブを選択します。

ステップ 2 [使用可能な DN（Available DNs）] で、追加する識別名を探します。

- ここで識別名オブジェクトを作成してリストに追加するには（後で条件に追加できます）、[使用可能な DN（Available DNs）] リストの上にある追加アイコン（  ）をクリックします。
- 追加する識別名オブジェクトおよびグループを検索するには、[使用可能な DN（Available DNs）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ 4 [サブジェクトに追加（Add to Subject）] または [発行元に追加（Add to Issuer）] をクリックします。

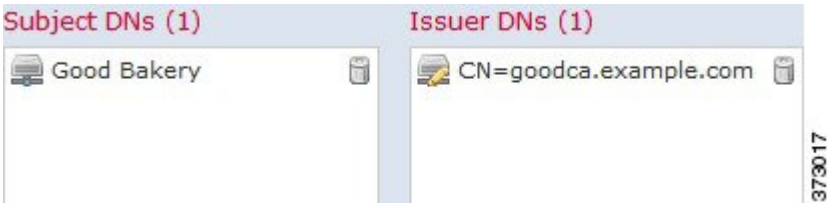
ヒント 選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5 手動で指定するリテラル共通名または識別名がある場合は、それらを追加します。[サブジェクト DN（Subject DNs）] または [発行元 DN（Issuer DNs）] リストの下にある [DN または CN の入力（Enter DN or CN）] プロンプトをクリックし、共通名または識別名を入力して [追加（Add）] をクリックします。

ステップ 6 ルールを追加するか、編集を続けます。

例

次の図は、goodbakery.example.com に対して発行された証明書および goodca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。これらの証明書で暗号化されたトラフィックは許可され、アクセス コントロールにより制御されます。



例

次の図は、badbakery.example.com および関連ドメインに対して発行された証明書および badca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。これらの証明書で暗号化されたトラフィックは、再署名された証明書を使用して復号されます。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

関連トピック

識別名オブジェクト，（438 ページ）

証明書の SSL ルール条件

証明書ベースの SSL ルール条件を作成するときにサーバ証明書をアップロードしたり、再利用可能な外部証明書オブジェクトとして保存してサーバ証明書の名前を関連付けたりできます。また、既存の外部証明書オブジェクトやオブジェクト グループを使用して証明書条件を設定することもできます。

ルール条件の [使用可能な証明書（Available Certificates）] フィールドでは、外部証明書オブジェクトやオブジェクト グループを証明書の識別名に関する以下の特性に基づいて検索できます。

- サブジェクトまたは発行元の共通名（CN）
- サブジェクトまたは発行元の組織（O）
- サブジェクトまたは発行元の組織単位（OU）

1 つの証明書のルール条件で複数の証明書を照合することもでき、トラフィックの暗号化に使用されている証明書がアップロードされた証明書のいずれかと一致した場合、その暗号化トラフィックはルールに一致したと判定されます。

1 つの証明書条件で、[選択した証明書（Selected Certificates）] リストに最大 50 の外部証明書オブジェクトおよび外部証明書オブジェクト グループを追加できます。

次の点に注意してください。

- [復号 - 既知のキー（Decrypt - Known Key）] アクションも選択すると、証明書条件を設定できなくなります。このアクションでは、トラフィック復号用のサーバ証明書の選択が必要であるため、トラフィックの照合はすでにこの証明書で行われていることになります。
- 証明書条件に外部証明書オブジェクトを設定する場合、暗号スイート条件に追加する暗号スイートまたは [復号 - 再署名（Decrypt - Resign）] アクションに関連付ける内部 CA オブジェクトのいずれかが、外部証明書の署名アルゴリズム タイプと一致する必要があります。たとえば、ルールの証明書条件で EC ベースのサーバ証明書を参照する場合は、追加する暗号スイート、または [復号 - 再署名（Decrypt - Resign）] アクションに関連付ける CA 証明書も EC ベースでなければなりません。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。

証明書による暗号化トラフィックの制御

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

手順

ステップ 1 SSL ルール エディタで、[証明書（Certificate）] タブを選択します。

ステップ 2 [使用可能な証明書（Available Certificates）] で、追加するサーバ証明書を探します。

- ここで外部証明書オブジェクトを作成してリストに追加するには（後で条件に追加できます）、[使用可能な証明書（Available Certificates）] リストの上にある追加アイコン（  ）をクリックします。
- 追加する証明書オブジェクトおよびグループを検索するには、[使用可能な証明書（Available Certificates）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ 4 [ルールに追加（Add to Rule）] をクリックします。

ヒント 選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5 ルールを追加するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

関連トピック

外部証明書オブジェクト，（450 ページ）

証明書ステータスの SSL ルール条件

証明書ステータスの SSL ルール条件では、各ステータスの有無を基準にしたトラフィックの照合ができます。1 つのルール条件で複数のステータスを選択でき、いずれかのステータスと証明書が一致すれば、ルールとトラフィックが一致したと判定されます。

複数の証明書ステータスの有無を単一の証明書ステータス ルール条件で照合するように選択できます（いずれか 1 つの基準に一致するだけで、その証明書はルールに一致します）。

次の表は、暗号化用のサーバ証明書のステータスを基準に、システムが暗号化トラフィックを評価する方法を示しています。

表 *74*：証明書ステータスのルール条件の基準

ステータスの確認	[はい（**Yes**）] を設定	[いいえ（**No**）] を設定
失効（Revoked）	ポリシーは、サーバ証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれています。	ポリシーは、サーバ証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれていません。
自己署名（Self-signed）	検出されたサーバ証明書が、同じサブジェクトと発行元の識別名を含んでいます。	検出されたサーバ証明書が、異なるサブジェクトと発行元の識別名を含んでいます。
有効（Valid）	以下のすべてを満たしています。 • 証明書を発行した CA をポリシーが信頼しています。 • 署名が有効です。 • 発行元が有効です。 • ポリシーの信頼できる CA のいずれも証明書を失効させていません。 • 現在の日付が証明書の有効期間の開始日と終了日の範囲内にあります。	以下の 1 つ以上を満たしています。 • 証明書を発行した CA をポリシーが信頼していません。 • 署名が無効です。 • 発行元が無効です。 • ポリシーの信頼できる CA の 1 つが証明書を失効させています。 • 現在の日付が証明書の有効期間の開始日より前です。 • 現在の日付が証明書の有効期限の終了日より後です。
署名が無効（Invalid signature）	証明書の内容に対して証明書の署名が適切に検証されません。	証明書の内容に対して証明書の署名が適切に検証されます。
発行元が無効（Invalid issuer）	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されていません。	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されています。
期限切れ	現在の日付が証明書の有効期限の終了日より後です。	現在の日付が証明書の有効期限の終了日であるかそれより前です。

ステータスの確認	[はい（Yes）] を設定	[いいえ（No）] を設定
まだ無効（Not yet valid）	現在の日付が証明書の有効期間の開始日より前です。	現在の日付が証明書の有効期間の開始日であるかそれより後です。

1 つの証明書が複数のステータスに一致する場合でも、ルールがトラフィックに行うアクションは一度に 1 つだけであることに注意してください。

CA が証明書を発行したか失効したかを確認するには、ルートおよび中間 CA 証明書とその関連 CRL をオブジェクトとしてアップロードする必要があります。その後で SSL ポリシーの信頼できる CA 証明書のリストに、これらの信頼できる CA のオブジェクトを追加します。

外部認証局の信頼

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

SSL ポリシーでルートおよび中間 CA 証明書を追加することで信頼できる CA が設定され、トラフィックの暗号化に使用されているサーバ証明書の検証に、これらの信頼できる CA を使用できるようになります。

信頼できる CA 証明書の中にアップロードされた証明書失効リスト（CRL）が含まれている場合は、信頼できる CA により、暗号化証明書が失効されているかどうかも確認できます。

手順

ステップ 1 SSL ルール エディタで、[信頼できる CA 証明書（Trusted CA Certificates）] タブを選択します。

ステップ 2 次のように、[使用可能な信頼できる CA（Available Trusted CAs）] で追加する信頼できる CA を見つけます。

- ここで信頼できる CA のオブジェクトを作成してリストに追加するには、[使用可能な信頼できる CA（Available Trusted CAs）] リストの上にある追加アイコン（  ）をクリックします。
- 追加する信頼できる CA オブジェクトおよびグループを検索するには、[使用可能な信頼できる CA（Available Trusted CAs）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ 4 [ルールに追加（Add to Rule）] をクリックします。

ヒント 選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5 ルールを追加するか、編集を続けます。

次の作業

- SSL ルールに証明書ステータスの SSL ルール条件を追加します。詳細については、証明書ステータスでのトラフィックの照合，（943 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

関連トピック

信頼できる認証局オブジェクト，（447 ページ）

信頼できる外部認証局の設定

検証されたサーバ証明書には、信頼できる CA によって署名された証明書が含まれます。SSL ポリシーに信頼できる CA 証明書を追加した後は、トラフィックと照合する証明書ステータス条件を SSL ルールに設定することができます。

ヒント 信頼できるルート CA の信頼チェーン内にあるすべての証明書を、信頼できる CA 証明書のリストにアップロードしますが、これにはルート CA 証明書およびすべての中間 CA 証明書が含まれます。これを行わないと、中間 CA から発行された信頼できる証明書の検出が困難になります。また、ルート発行者 CA に基づいてトラフィックを信頼するように証明書ステータス条件を設定する場合、信頼できる CA の信頼チェーン内のすべてのトラフィックは、復号する必要はなく、復号せずに許可することができます。

SSL ポリシーを作成すると、[信頼できる CA 証明書（Trusted CA Certificates）] タブにデフォルトの信頼できる CA オブジェクト グループ Cisco Trusted Authorities が入力されます。

このグループ内の各エントリは変更が可能で、SSL ポリシーにこのグループを含めるかどうかを選択できます。このグループを削除することはできません。システムによる更新によりこのリストのエントリが変更されることがありますが、ユーザによる変更は保持されます。

証明書ステータスでのトラフィックの照合

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

はじめる前に

- 信頼できる CA オブジェクトまたはグループを SSL ポリシーに追加します。詳細については、外部認証局の信頼, （942 ページ）を参照してください。

手順

ステップ 1 Firepower Management Center で、[ポリシー（Policies）]>[アクセス コントロール（Access Control）] > [SSL] を選択します。

ステップ 2 新しいポリシーを追加するか、既存のポリシーを編集します。

ステップ 3 新しい SSL ルールを追加するか、既存のルールを編集します。

ステップ 4 [ルールの追加（Add Rule）] または [ルールの編集（Editing Rule）] ダイアログボックスで [証明書ステータス（Cert Status）] タブを選択します。

ステップ 5 各証明書ステータスには次のオプションがあります。

- 該当する証明書ステータスが存在するときに照合する場合は、[はい（Yes）] を選択します。
- 該当する証明書ステータスが存在しないときに照合する場合は、[いいえ（No）] を選択します。
- ルールが一致する場合、[任意（Any）] を選択して条件をスキップします。つまり、[任意（Any）] を選択すると、証明書ステータスの有無に関わらずルールは一致します。

ステップ 6 ルールを追加するか、編集を続けます。

例

組織は Verified Authority という認証局を信頼しています。組織は Spammer Authority という認証局を信頼していません。システム管理者は、Verified Authority の証明書および、Verified Authority の発行した中間 CA 証明書をアップロードします。Verified Authority が以前に発行した証明書の 1 つを失効させたため、システム管理者は Verified Authority から提供された CRL をアップロードします。

次の図は、有効な証明書をチェックする証明書ステータスのルール条件を示しています。これにより、Verified Authority から発行されたが CRL には登録されておらず、現状で有効期間の開始日と終了日の範囲内にあるかどうかがチェックされます。この設定では、これらの証明書で暗号化されたトラフィックはアクセス コントロールにより復号および検査されません。

次の図は、ステータスが存在しないことをチェックする証明書ステータスのルール条件を示しています。この設定では、期限切れになっていない証明書を使用して暗号化されたトラフィックと照合し、そのトラフィックをモニタします。

次の図は、さまざまなステータスの有無に一致する証明書ステータスのルール条件を示しています。この設定でルールが一致するのは、着信トラフィックを暗号化した証明書が無効なユーザが発行元、自己署名、無効、または期限切れであった場合で、そうしたトラフィックを既知のキーで復号します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

暗号スイート SSL ルール条件

Cisco では、暗号スイートのルール条件に追加できる事前定義の暗号スイートを提供しています。複数の暗号スイートを含む、暗号スイートのリストのオブジェクトを追加することもできます。

（注） 新しい暗号スイートを追加することはできません。定義済みの暗号スイートは変更も削除もできません。

1 つの暗号スイート条件で、[選択した暗号スイート（Selected Cipher Suites）] リストに最大 50 の暗号スイートおよび暗号スイート リストを追加できます。暗号スイート条件に追加できる暗号スイートとして、次のものがサポートされています。

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA

- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

次の点に注意してください。

- 展開でサポートされていない暗号スイートを追加すると、設定を展開できません。たとえば、パッシブ展開では、一時 Diffie-Hellman（DHE）および一時的楕円曲線 Diffie-Hellman（ECDHE）暗号スイートを使用したトラフィックの復号がサポートされません。それらの暗号スイートを使用してルールを作成すると、アクセス コントロール ポリシーを展開できなくなります。
- 暗号スイート条件に暗号スイートを設定する場合は、証明書条件に追加する外部証明書オブジェクト、または [復号 - 再署名（Decrypt - Resign）] アクションに関連付ける内部 CA オブジェクトが、暗号スイートの署名アルゴリズム タイプと一致している必要があります。たとえば、ルールの暗号スイート条件でECベースの暗号スイートを参照する場合、追加するサーバ証明書または [復号 - 再署名（Decrypt - Resign）] アクションに関連付ける CA 証明書も EC ベースである必要があります。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。
- 匿名の暗号スイートで暗号化されたトラフィックは復号化できません。匿名の暗号スイートを [暗号スイート（Cipher Suite）] 条件に追加した場合、SSL ルールに [復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Decrypt - Known Key）] アクションは使用できません。

暗号スイートによる暗号化トラフィックの制御

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

手順

ステップ 1 SSL ルール エディタで、[暗号スイート（Cipher Suite）] タブを選択します。

ステップ 2 [使用可能な暗号スイート（Available Cipher Suites）] で、追加する暗号スイートを探します。

- ここで暗号スイートリストを作成してリストに追加するには（後で条件に追加できます）、[使用可能な暗号スイート（Available Cipher Suites）] リストの上にある追加アイコン（  ）をクリックします。
- 追加する暗号スイートおよびリストを検索するには、[使用可能な暗号スイート（Available Cipher Suites）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、暗号スイートの名前または暗号スイートの値を入力します。入力を開始するとリストが更新され、一致する暗号スイートが表示されます。

ステップ 3 暗号スイートをクリックして選択します。すべての暗号スイートを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ 4 [ルールに追加（Add to Rule）] をクリックします。

ヒント 選択した暗号スイートをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5 ルールを追加するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

暗号スイート リスト, （436 ページ）

暗号化プロトコル バージョンの SSL ルール条件

SSL バージョン 3.0 または TLS バージョン 1.0、1.1、1.2 のいずれかで暗号化されたトラフィックとの照合を選択できます。デフォルトでは、ルールの作成時にすべてのプロトコルのバージョンが選択されます。複数のバージョンが選択されている場合、いずれかのバージョンと一致する暗

号化トラフィックがルールに一致したと判定されます。ルール条件を保存するには、最低 1 つのプロトコル バージョンを選択する必要があります。

バージョンのルール条件で SSL バージョン 2.0 を選択することはできません。これは、SSL バージョン 2.0 で暗号化されたトラフィックの復号化がサポートされていないためです。復号できないアクションを設定すれば、それ以上のインスペクションなしで、これらのトラフィックを許可またはブロックできます。

暗号化プロトコルのバージョンによるトラフィックの制御

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

手順

ステップ 1 SSL ルール エディタで、[バージョン（Version）] タブを選択します。

ステップ 2 照合するプロトコル バージョンを選択します。

ステップ 3 ルールを追加するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 XIII 部

高度なマルウェア防御（AMP）とファイル制御

第 45 章

ファイル ポリシーと AMP for Firepower

次のトピックでは、ファイル制御、ファイル ポリシー、ファイル ルール、AMP クラウド接続、および動的分析接続の概要を示します。

ファイル ポリシーと AMP for Firepower について

悪意のあるソフトウェア、つまりマルウェアは、複数のルートで組織のネットワークに入る可能性があります。マルウェアの影響を特定して軽減しやすくするため、Firepower システムの *Advanced Malware Protection for Firepower*（AMP for Firepower）の機能によって、ネットワーク トラフィックでのマルウェアの伝送を検出、追跡、保存、分析、および必要に応じてブロックできます。

AMP for Firepower およびファイル制御（ファイルにマルウェアが含まれているかどうかにかかわらず、特定のタイプのすべてのファイルを制御できる）をアクセス制御設定全体の一部として設定します。作成してアクセス コントロール ルールに関連付けたファイル ポリシーは、ルールに一致するネットワーク トラフィックを処理します。そのトラフィックで検出されたファイルをダウンロードし、ローカル マルウェア分析を実行して、ファイルにマルウェアが含まれているかどうかを判断できます。また、ファイルを動的分析のために AMP Threat Grid クラウドに送信して、そのファイルがマルウェアを表しているかどうかを判断できます。

アクティブ ファイル ポリシーのファイル イベント、マルウェア イベント、および取得されたファイル ロギングが自動的に有効になります。また、ファイル ポリシーでファイル イベントまたはマルウェア イベントが生成されるか、ファイルがキャプチャされると、システムは関連する接続の終了を Firepower Management Center データベースに自動的に記録します。

（注） NetBIOS-ssn（SMB）トラフィックのインスペクションによって生成されるファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。システムはクライアントまたはサーバがセッションを終了した後に接続イベントを生成します。

分析のターゲットをさらに絞り込むために、マルウェア ファイルの [ネットワーク ファイル トラジェクトリ（network file trajectory）] ページを使用して、ホスト間での個々の脅威の広がりを時系列で追跡できます。これにより、最も効果的なアウトブレイク制御と防止対策に集中できます。

ヒント 組織で AMP for Endpoints を使用している場合は、システムで、AMP for Firepower によって収集されたデータとともにエンドポイントベースのデータをインポートして表示できます。このデータのインポートには、ライセンスは必要ありません。

組織で追加のセキュリティが必要であるか、外部接続を制限する場合は、Cisco AMP プライベート クラウド仮想アプライアンス（AMPv）を使用します。AMPv は個別に AMP for Endpoints イベントを収集し、Firepower Management Center に転送します。

ファイル制御および Cisco AMP の基本

AMP for Firepower

AMP for Firepower では、インライン展開された管理対象デバイスを使用して、ネットワーク上のマルウェアを検出、保存、トラッキング、分析、およびブロックできます。AMP for Firepower は、PDF、Microsoft Office ドキュメントを含め、多くのタイプのマルウェア ファイルをブロックできます。

ファイルの検出と保存

AMP for Firepower により、管理対象デバイスは、特定のファイル タイプの送信のネットワーク トラフィックをモニタします。

デバイスが対象のファイルを検出すると、ファイルの SHA-256 ハッシュ値を Firepower Management Center に送信します。Firepower Management Center は、マルウェア クラウド ルックアップを実行し、AMP クラウドでファイルの性質をクエリします。デバイスは、ファイル ストレージ機能を使用して、ハードドライブまたはマルウェアのストレージ パックに対象ファイルを保存できます。イベント ビューアのキャプチャ ファイル情報を表示したり、オフライン分析のためにコピーをダウンロードしたりできます。

ファイル分析

システムでは、ファイルにマルウェアが含まれるかどうかを判断するために、ファイル インスペクションと分析のいくつかの方法が適用されます。

（注） 設定に応じて、システムがファイルを初めて検出したときに、そのファイルを検査してクラウドルックアップの結果を待機するか、または、クラウドルックアップの結果を待機せずにファイルを通過させることができます。

ファイル ルールでオプションを有効にするかどうかに基づいて、システムは次の順序でファイルを検査します。

Spero 分析

ファイルが対象の実行可能ファイルの場合、デバイスはファイル構造を分析し、結果として得られた Spero シグネチャを AMP Threat Grid クラウドに送信できます。クラウドは、このシグネチャを使用して、ファイルにマルウェアが含まれるかを判断します。

ローカル マルウェア分析

ローカル マルウェア インスペクション エンジンを使用して、デバイスは対象ファイルを調べ、ファイルにマルウェアが含まれる場合、ファイル ルールでそのように設定されていればこのファイルをブロックし、マルウェア イベントを生成します。

また、デバイスにより、ファイル プロパティ、組み込みオブジェクト、および可能性のあるマルウェアの詳細情報を含むファイル構成レポートが生成されます。

動的分析

デバイスが、マルウェアの可能性があるとしてファイルを事前分類している場合、デバイスがファイルを保存するかどうかに関係なく、これらのファイルを AMP Threat Grid クラウドまたは AMP Threat Grid オンプレミス アプライアンスに動的分析のために送信します。

AMP Threat Grid クラウドまたはオンプレミスの AMP Threat Grid アプライアンスは、悪意のあるファイルかどうかを判断するためにサンドボックス環境でファイルを実行し、ファイルにマルウェアが含まれる可能性を示す脅威スコアを返します。脅威スコアから、クラウドが脅威スコアを割り当てた理由を詳細に説明する動的分析のサマリー レポートを表示できます。

ファイルとマルウェア イベント、およびキャプチャ ファイル

ファイル分析結果に基づいて、イベント ビューアからのキャプチャ ファイル、生成されたマルウェアとファイル イベントを確認できます。使用可能な場合は、ファイルの構成、性質、脅威スコア、動的分析のサマリー レポートを調べ、マルウェア分析をさらに詳細に把握できます。また、ファイルがネットワークをどのように通過するか（ホストを通過するか）を示すマップ、およびさまざまなファイル プロパティを表示する、ネットワーク ファイル トラジェクトリにアクセスできます。

アーカイブ ファイル

システムは、ファイルがアーカイブ（`.rar` または `.zip` アーカイブ ファイルなど）の場合、一番外側のアーカイブ ファイル（レベル 0）の下の最大 3 レベルのネストされたファイルを検査できます。ブロック アクションを含むファイル ルールにいずれかの個別ファイルが一致する場合は、

その個別ファイルだけでなくアーカイブ全体がブロックされます。また、指定したネストのレベルを超えるアーカイブ、またはそのコンテンツが暗号化されているか検査できないアーカイブも、ブロックされることがあります。

ファイル トラッキング

AMP クラウドにあるファイルの性質が不正確だとわかっている場合、次のようにして、ファイルの SHA-256 値をファイル リストに追加できます。

- AMP クラウドがクリーンの性質を割り当てた場合と同じ方法でファイルを扱うには、クリーン リストにファイルを追加します。
- AMP クラウドがマルウェアの性質を割り当てた場合と同じ方法でファイルを扱うには、カスタム検出リストにファイルを追加します。

これ以降に検出された場合、デバイスでは、ファイルの性質を再評価せずに許可またはブロックできます。ファイル ポリシーに応じてクリーン リストまたはカスタム検出リストを使用できます。

（注） ファイル ポリシーで、マルウェア クラウド ルックアップを実行するか、一致ファイルでマルウェアをブロックしてファイルの SHA-256 値を計算するルールを設定する必要があります。

関連トピック

ファイル リスト，（430 ページ）

マルウェアの性質

システムは、AMP クラウドから返される性質に基づいてファイルの性質を決定します。パフォーマンスを改善するために、SHA-256 値に基づいてファイルの性質がシステムですでにわかっている場合、Firepower Management Centerは AMP クラウドでクエリを行う代わりに、キャッシュ済みの性質を使用します。システムは、ファイルの性質に基づいてファイルをブロックすることもできます。アーカイブ ファイル内にネストされているファイルが 1 つでもブロックされる場合、システムはアーカイブ ファイル全体をブロックします。

ファイル リストへの追加操作の結果、または脅威スコアに応じて、ファイルの性質は次のいずれかになります。

- マルウェア（Malware）：ファイルが AMP クラウドでマルウェアと分類されていること、ローカル マルウェア分析でマルウェアとして識別されたこと、またはファイルの脅威スコアがファイル ポリシーに定義されたマルウェアのしきい値を超えたこと示します。
- [クリーン（Clean）]：AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。
- 不明（Unknown）：システムは AMP クラウドでファイルの性質をクエリしましたが、ファイルには性質が割り当てられていませんでした。言い換えると、AMP クラウドがファイルを分類できませんでした。

- カスタム検出（Custom Detection）：ユーザがカスタム検出リストにファイルを追加したことを示します。
- 利用不可（Unavailable）：システムがAMPクラウドでクエリを行えなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。

アーカイブ ファイルの性質は、アーカイブ内部のファイルに割り当てられた性質に基づきます。識別されたマルウェア ファイルを含んでいる**すべて**のアーカイブは、マルウェア（Malware）の性質になります。識別されたマルウェア ファイルを含んでいないアーカイブの場合、不明なファイルが1つでも含まれていれば不明（Unknown）の性質、クリーン ファイルのみが含まれていればクリーン（Clean）の性質になります。

表 *75*：内容に基づくアーカイブ ファイルの性質

アーカイブ ファイルの性質	不明なファイルの数	クリーン ファイルの数	マルウェア ファイルの数
不明	1 つ以上	任意（Any）	[0]
クリーン（Clean）	[0]	1 つ以上	[0]
マルウェア（Malware）	任意（Any）	任意（Any）	1 つ以上

他のファイルと同様に、アーカイブ ファイルにも、該当する性質に関する条件が適用される場合はカスタム検出（Custom Detection）または利用不可（Unavailable）の性質が割り当てられます。

ヒント 短時間で利用不可（Unavailable）マルウェア イベントが連続して発生した場合は、Firepower Management Center が AMP クラウドに接続できることを確認してください。

ファイルの性質は変更される可能性があることに注意してください。たとえば、AMPクラウドによる判定の結果、以前はクリーンであると考えられていたファイルが今はマルウェアとして識別されるようになったり、その逆、つまりマルウェアと識別されたファイルが実際にはクリーンであったりする可能性があります。前の週にクエリを行ったファイルの性質が変更された場合、AMPクラウドはシステムに通知して、システムが次回そのファイルの送信を検出した際に自動的にアクションをとれるようにします。変更された性質は、レトロスペクティブな性質と呼ばれます。

AMP クラウドのクエリから返された、脅威スコアに関連付けられた性質、およびローカル マルウェア分析によって割り当てられた性質には、存続可能時間（TTL）が設定されます。性質が更新されないまま、TTL 値で指定された期間にわたって保持された後は、キャッシュ情報が消去されます。性質および関連する脅威スコアには次の TTL 値が割り当てられます。

- クリーン：4 時間
- 不明：1 時間
- マルウェア：1 時間

このキャッシュに対するクエリで、キャッシュされた性質がタイムアウトになったことが識別された場合、システムは AMP クラウドに新しい性質を再びクエリします。

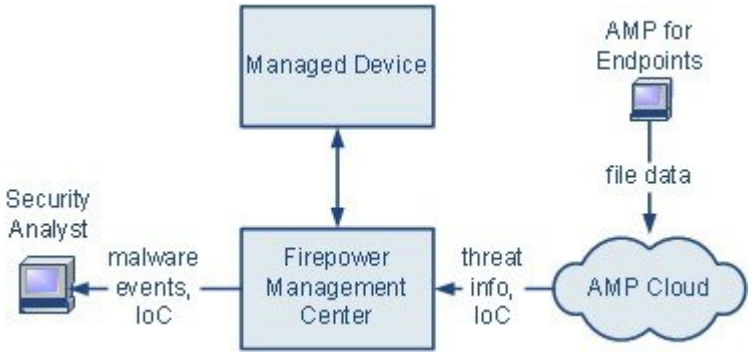
AMP for Firepower を使用しないファイル制御

マルウェア ファイル伝送のブロックに加えて、（マルウェアを含むかどうかにかかわらず）特定のタイプのすべてのファイルをブロックする必要がある場合は、ファイル制御機能により防御網を広げることができます。AMP for Firepower の場合と同様に、管理対象デバイスはネットワークトラフィック内で特定のファイル タイプの伝送をモニタし、そのファイルをブロックまたは許可します。

システムでマルウェアを検出できるすべてのファイル タイプだけでなく、さらに多数のファイル タイプに対するファイル制御がサポートされています。これらのファイル タイプは、マルチメディア（swf、mp3）、実行可能ファイル（exe、トレント）、PDF などの基本的なカテゴリにグループ分けされます。ファイル制御は AMP for Firepower とは異なり、AMP クラウドへの照会を必要としないことに注意してください。

エンドポイント向け AMP

エンドポイント向けAMPは、シスコのエンタープライズクラスの高度なマルウェア防御ソリューションです。高度なマルウェアの発生、高度で継続的な脅威、およびターゲット型攻撃を検出、分析、ブロックします。次の図に、エンドポイント向け AMP を使用した場合の一般的な情報フローを示します。



所属部門がエンドポイント向けAMPを使用している場合、個々のユーザはエンドポイント（つまり、コンピュータやモバイル デバイス）に軽量コネクタをインストールします。コネクタは、ファイルのアップロード、ダウンロード、実行、開く、コピー、移動などの操作を行う際にファイルを検査します。コネクタはAMPクラウドと通信して、検査対象のファイルにマルウェアが含まれるかどうかを判断します。

ファイルがマルウェアとして特定された場合、AMP クラウドは特定した脅威の情報を Firepower Management Centerに送ります。さらにAMPクラウドは、スキャン、検疫、実行のブロッキング、クラウド リコールなど、他の種類のデータを Firepower Management Center に送信することもできます。Firepower Management Center はこれらの情報をマルウェア イベントとしてログに記録します。

エンドポイント向けAMPは、ホストのセキュリティに感染の疑いがある場合、侵害の兆候（IOC）を生成することができます。Firepowerシステムでは、モニタ対象ホストのIOC情報が表示できます。シスコでは折にふれて、エンドポイントベースのマルウェア イベントに対応する新しいIOCタイプの開発を行っており、システムにより自動的にダウンロードされます。

エンドポイント向けAMPでは、マルウェア イベントに基づいてManagement Centerで開始される修復やアラートを設定できるだけでなく、エンドポイント向けAMP管理コンソールを使ってマルウェアの影響を軽減することもできます。管理コンソールの堅牢かつ柔軟なWebインターフェイスを使用すると、エンドポイント向けAMP展開のあらゆる側面を制御し、アウトブレイクのすべての段階を管理できます。次の操作を実行できます。

- 部門全体のためにカスタムマルウェア検出ポリシーとプロファイルを設定し、すべてのユーザのファイルに対してフラッシュ スキャンおよび完全スキャンを実行する
- マルウェア分析の実行：ヒートマップ、詳細なファイル情報、ネットワーク ファイル トラジェクトリ、脅威の根本原因の表示など
- アウトブレイク コントロールのさまざまな要素を設定する：自動検疫、検疫されていない実行可能ファイルの実行を停止するアプリケーション ブロッキング、除外リストなど
- カスタム保護の作成、グループ ポリシーに基づく特定のアプリケーションの実行ブロッキング、およびカスタム ホワイトリストの作成

ヒント エンドポイント向け AMP の詳細については『AMP for Endpoints management console』を参照してください。

AMP for Firepower とエンドポイント向け AMP の比較

Firepower システムは、AMP for Firepower およびエンドポイント向け AMP のどちらのデータも使用できます。

管理対象デバイスはネットワーク トラフィックのマルウェアを検出しますが、エンドポイント向けAMPのマルウェア検出はダウンロード時または実行時にエンドポイントで行われるため、この2種類のマルウェア イベントの情報は異なります。たとえば、エンドポイント ベースのマルウェア イベントには、ファイル パス、呼び出し元クライアント アプリケーションなどの情報が含まれるのに対して、ネットワーク トラフィックでのマルウェア検出には、ファイル伝送に使われた接続のポート、アプリケーション プロトコル、発信元 IP アドレス情報が含まれます。

別の例としては、ネットワークベースのマルウェア イベントの場合、ユーザ情報は、ネットワーク検出で判別された、マルウェアの送信先であるホストに最後にログインしたユーザを示すことが挙げられます。一方、エンドポイント向けAMPで報告されるユーザは、マルウェアが検出されたエンドポイントに現在ログインしているユーザを示します。

（注） 展開によっては、AMP for Endpoints がモニタするエンドポイントは、AMP for Firepower がモニタしているものと同じホストではない場合があります。このため、エンドポイントベースのマルウェア イベントは、ネットワーク マップにホストを追加しません。ただし、システムは IP アドレスおよび MAC アドレスのデータを使用して、AMP for Endpoints の展開から取得した侵害の兆候をモニタ対象のホストにタグ付けします。異なる AMP ソリューションによってモニタされる 2 つの異なるホストが同じ IP アドレスと MAC アドレスを持っている場合、システムは AMP for Endpoints の IOC をモニタ対象のホストに誤ってタグ付けする場合があります。

次の表に、2 つの戦略の違いをまとめます。

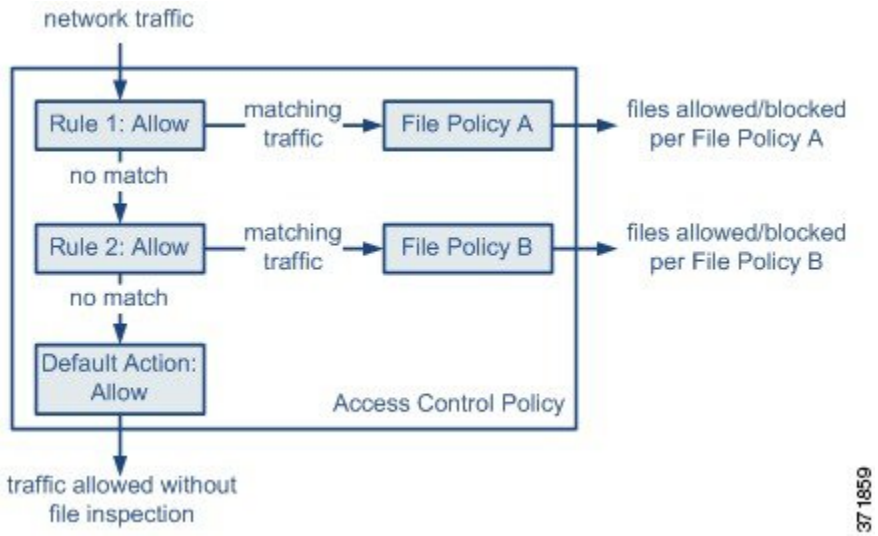
表 *76*：ネットワークベースとエンドポイントベースの高度なマルウェア防御戦略の比較

機能	AMP for Firepower	エンドポイント向け AMP
ファイル タイプの検出とブロッキングの方法（ファイル制御）	ネットワーク トラフィックで、アクセス コントロール ポリシーとファイル ポリシーを使用	未サポート
マルウェアの検出とブロッキングの方法	ネットワーク トラフィックで、アクセス コントロール ポリシーとファイル ポリシーを使用	個々のエンドポイントで、AMP クラウドとの通信を行うコネクタを使用
ネットワーク トラフィックを検査	管理対象デバイスを通過するトラフィック	なし（エンドポイントにインストールされたコネクタがファイルを直接検査する）
マルウェア検出の堅牢性	限定されたファイル タイプ	すべてのファイル タイプ
マルウェア分析の選択肢	Management Center ベース、および AMP クラウドでの分析	Management Center ベース、およびエンドポイント向け AMP 管理コンソールの追加オプション
マルウェアの影響軽減	ネットワーク トラフィックでのマルウェア ブロッキング、Management Center が開始する修復	エンドポイント向け AMP ベースの検疫およびアウトブレイク コントロール オプション、Management Center が開始する修復
生成されるイベント	ファイル イベント、キャプチャされたファイル、マルウェア イベント、およびレトロスペクティブ マルウェア イベント	マルウェア イベント
マルウェア イベントに含まれる情報	基本的なマルウェア イベント情報、および接続データ（IP アドレス、ポート、アプリケーション プロトコル）	詳細なマルウェア イベント情報（接続データなし）

機能	AMP for Firepower	エンドポイント向け AMP
ネットワーク ファイル トラジェクトリ	Management Center ベース	Management Center ベース、およびエンドポイント向け AMP 管理コンソールの追加オプション
必要なライセンスまたはサブスクリプション	ファイル制御および AMP for Firepower の実行に必要なライセンス	エンドポイント向け AMP サブスクリプション（ライセンスベースではありません）

ファイル ポリシー

ファイル ポリシーは、いくつかの設定からなるセットです。システムは全体的なアクセス制御設定の一部としてこれを使用して、AMP for Firepower とファイル制御を実行できます。この関連付けにより、アクセス コントロール ルールの条件と一致するトラフィック内のファイルを通過させる前に、システムは必ずファイルを検査するようになります。次の図のような、インライン展開での単純なアクセス コントロール ポリシーがあるとします。



このポリシーには 2 つのアクセス コントロール ルールがあり、両方とも許可アクションを使用し、ファイル ポリシーに関連付けられています。このポリシーのデフォルト アクションもまた「トラフィックの許可」ですが、ファイルポリシーインスペクションはありません。このシナリオでは、トラフィックは次のように処理されます。

- ルール 1 に一致するトラフィックはファイル ポリシー A で検査されます。
- ルール 1 に一致しないトラフィックはルール 2 に照らして評価されます。ルール 2 に一致するトラフィックはファイル ポリシー B で検査されます。
- どちらのルールにも一致しないトラフィックは許可されます。デフォルト アクションにファイル ポリシーを関連付けることはできません。

1 つのファイル ポリシーを、[許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションを含むアクセス コントロール ルールに関連付けることができます。その後、システムはそのファイル ポリシーを使用して、アクセス コントロール ルールの条件を満たすネットワーク トラフィックを検査します。

異なるファイル ポリシーを個々のアクセス コントロール ルールに関連付けることにより、ネットワークで伝送されるファイルを識別/ブロックする方法をきめ細かく制御できます。ただし、アクセス コントロールのデフォルト アクションによって処理されるトラフィックを検査するためにファイル ポリシーを使用**できない**ことに注意してください。

ファイル ポリシーの詳細設定

詳細なファイル インスペクションの設定に関する注意事項

ファイル ポリシーでは、詳細なオプションを設定して、カスタム検出リストのファイルのブロック、クリーン リストのファイルの許可、およびファイルがマルウェアと見なされる脅威スコアのしきい値の設定を行うことができます。

また、組織のニーズに合わせてアーカイブ ファイルを分析し、ブロックできるように、アーカイブ ファイルの内容を検査するようにファイル ポリシーを設定できます。圧縮解除されたファイルに適用できるすべての機能（動的分析やファイル ストレージなど）は、アーカイブ ファイル内のネストされたファイルに使用可能です。

アーカイブ ファイルのインスペクションに関する注意事項

一部のアーカイブ ファイルには、追加のアーカイブ ファイル（など）が含まれています。ファイルがネストされるレベルは、そのアーカイブ ファイルの深さです。トップレベルのアーカイブ ファイルは深さの数で考慮されないことに注意してください。深さは最初にネストされたファイルで 1 から始まります。

システムでは、ネストされたアーカイブ ファイルを最大 3 レベルまでしか検査できませんが、その深さ（または指定したそれより低い最大深さ）を超えるアーカイブ ファイルをブロックするようファイル ポリシーを設定できます。ネストされたアーカイブをさらに制限する場合は、2 または 1 のより低い最大ファイル深さを設定するオプションがあります。

最大アーカイブ ファイルの深さ 3 を超えるファイルをブロックしないよう選択した場合、抽出可能な内容と深さ 3 以上でネストされた内容を含むアーカイブ ファイルがモニタ対象のトラフィックに現れると、システムは検査可能だったファイルについてのみデータを検査して報告します。

（注） アーカイブ ファイルを含むトラフィックがセキュリティ インテリジェンスによってブラックリスト登録またはホワイトリスト登録された場合、またはトップレベルのアーカイブ ファイルの SHA-256 値がカスタム検出リストにある場合、システムはアーカイブ ファイルの内容を検査しません。ネストされたファイルがブラックリスト登録された場合、アーカイブ全体がブロックされます。しかし、ネストされたファイルがホワイトリスト登録された場合、アーカイブは自動的に渡されません（他のネストされたファイルおよび特性による）。

アーカイブ ファイルの内容を検査するようにファイル ポリシーが設定されている場合は、イベント ビューアのコンテキスト メニューおよびネットワーク ファイル トラジェクトリ ビューアを使用して、アーカイブ ファイルがファイル イベント、マルウェア イベントに現れた場合、またはキャプチャされたファイルとして現れた場合に、アーカイブ内のファイルに関する情報を表示できます。

アーカイブのすべてのファイル コンテンツは表形式でリストされます。そのリストには、名前、SHA-256 ハッシュ値、タイプ、カテゴリ、およびアーカイブの深さといった関連情報の概略が含まれています。ネットワーク ファイル トラジェクトリ アイコンはファイルごとに表示されます。そのアイコンをクリックすることで、特定のファイルに関する詳細な情報を表示することができます。

ファイル ポリシー設定に関する注意事項と制約事項

- 新しいポリシーの場合、ポリシーが使用中でないことが Web インターフェイスに示されます。使用中のファイル ポリシーを編集している場合は、そのファイル ポリシーを使用しているアクセス コントロール ポリシーの数が Web インターフェイスに示されます。どちらの場合も、テキストをクリックすると [アクセス コントロール ポリシー（Access Control Policies）] ページに移動できます。
- FTP に関する [マルウェア ブロック（Block Malware）] ルールを持つファイル ポリシーを使用するアクセス コントロール ポリシーでは、[インライン時にドロップ（Drop when Inline）] を無効にした侵入ポリシーをデフォルト アクションに設定した場合、システムはルールに一致するファイルやマルウェアの検出でイベントを生成しますが、ファイルをドロップしません。FTP ファイア転送をブロックし、ファイル ポリシーを選択するアクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを使用するには、[インライン時にドロップ（Drop when Inline）] を有効にした侵入ポリシーを選択する必要があります。

ファイル ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
Threat（ファイル制御） マルウェア（AMP for Firepower）	Protection（ファイル制御） マルウェア（AMP for Firepower）	任意（Any）	任意（Any）	Admin/Access Admin

[ファイル ポリシー（File Policies）] ページには、既存のファイル ポリシーが最終更新日とともに表示されます。このページは、ファイル ポリシーの管理に使用できます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

（注） 動的分析の対象になるファイル タイプのリストが更新されたかどうか検査するために、システムは AMP クラウドをチェックします（多くても 1 日に 1 回）。対象になるファイル タイプのリストが変更された場合、これはファイル ポリシーの変更を意味します。このファイル ポリシーを使用するアクセス コントロール ポリシーがいずれかのデバイスに展開されている場合、そのアクセス コントロール ポリシーには失効マークが付けられます。更新したファイル ポリシーがデバイスで有効になるには、まず、ポリシーを展開しておく必要があります。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [マルウェアとファイル（Malware & File）] を選択します。

ステップ 2 ファイル ポリシーを管理します。

- [比較（Compare）]：[ポリシーの比較（Compare Policies）] をクリックします（ポリシーの比較, （331 ページ） を参照）。
- 作成：ファイル ポリシーを作成するには、[新規ファイル ポリシー（New File Policy）] をクリックし、ファイル ポリシーの作成, （965 ページ） で説明する手順を実行します。
- コピー：ファイル ポリシーをコピーするには、コピー アイコン（  ）をクリックします。

  代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 削除：ファイルポリシーを削除するには、削除アイコン（  ）をクリックし、プロンプトが表示されたら [はい（Yes）] と [OK] をクリックします。

  コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 展開：[展開（Deploy）] をクリックします（設定変更の導入, （320 ページ） を参照）。
- 編集：既存のファイル ポリシーを変更するには、編集アイコン（  ）をクリックします。
- [レポート（Report）]：レポート アイコン（  ）をクリックします（現在のポリシー レポートの生成, （333 ページ） を参照）。

ファイル ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
Threat（ファイル制御） マルウェア（AMP for Firepower）	Protection（ファイル制御） マルウェア（AMP for Firepower）	任意（Any）	任意（Any）	Admin/Access Admin

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [マルウェアとファイル（Malware & File）] を選択します。

ヒント 既存のファイル ポリシーのコピーを作成するには、コピー アイコン（  ）をクリックして、表示されるダイアログ ボックスで新しいポリシーの固有名を入力します。その後、そのコピーを変更できます。

ステップ 2 [新しいファイル ポリシー（New File Policy）] をクリックします。

ステップ 3 新しいポリシーの [名前（Name）] とオプションの [説明（Description）] を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 ファイル ルールの作成，（973 ページ）の説明に従って、ファイル ポリシーに 1 つ以上のルールを追加します。

ステップ 6 必要に応じて、[詳細（Advanced）] タブを選択し、詳細オプションおよびアーカイブ ファイル検査オプション，（965 ページ）の説明に従って詳細オプションを設定します。

ステップ 7 ファイル ポリシーを保存します。

次の作業

- ファイル制御およびマルウェア保護のためのアクセス コントロール ルールの設定，（819 ページ）の説明に従って、アクセス コントロール ルールにファイル ポリシーを追加します。
- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

詳細オプションおよびアーカイブ ファイル検査オプション

ファイル ポリシー エディターの [詳細設定（Advanced）] タブには、次の一般オプションがあります。

- [初回ファイル分析（First Time File Analysis）]：システムで初めて検出するファイル分析のためのファイルを送信します。ファイルは、マルウェア クラウド ルックアップと Spero 分析、ローカル マルウェア分析、またはダイナミック分析を実行するように設定されているルール

に一致する必要があります。このオプションを無効にすると、初めて検出されたファイルの性質が「不明（Unknown）」になります。

- [カスタム検出リストを有効にする（Enable Custom Detection List）]：カスタム検出リストにあるファイルをブロックします。
- [クリーン リストを有効にする（Enable Clean List）]：クリーン リストにあるファイルを許可します。
- [ダイナミック分析の脅威スコアに基づいてマルウェアとしてファイルをマークする（Mark files as malware based on dynamic analysis threat score）]：しきい値の脅威スコアを設定します。スコアがしきい値以上のファイルはマルウェアと見なされます。

  しきい値に低い値を選択すると、マルウェアとして扱われるファイルの数が増えます。ファイル ポリシーで選択したアクションによっては、その結果、ブロックされるファイルの数が増える可能性があります。

ファイル ポリシー エディターの [詳細設定（Advanced）] タブには、次のアーカイブ ファイル検査オプションがあります。

- [アーカイブを検査する（Inspect Archives）]：アーカイブ ファイルの内容を検査します。

  注意 [アーカイブを検査する（Inspect Archives）] を有効化または無効化すると設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作，（326 ページ）を参照してください。

- [暗号化されているアーカイブをブロックする（Block Encrypted Archives）]：暗号化されている内容を含むアーカイブ ファイルをブロックします。
- [検査できないアーカイブをブロックする（Block Uninspectable Archives）]：暗号化以外の理由で検査できない内容を含むアーカイブ ファイルをブロックします。これは、通常、破損したファイル、または指定されているアーカイブの最大の深さを超えるファイルに適用されます。
- [アーカイブの最大の深さ（Max Archive Depth）]：指定されている深さを超えてネストされているアーカイブをブロックします。最上位のアーカイブ ファイルはこの数に含まれず、深さは最初のネスト ファイルを 1 として始まります。

関連トピック

Snort® の再起動シナリオ，（324 ページ）

ファイル ポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
Threat（ファイル制御） マルウェア（AMP for Firepower）	Protection（ファイル制御） マルウェア（AMP for Firepower）	任意（Any）	任意（Any）	Admin/Access Admin

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [マルウェアとファイル（Malware & File）] を選択します。

ステップ 2 編集するファイル ポリシーの横にある編集アイコン（）をクリックします。代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 次の選択肢があります。

- [ファイル ルールの追加（Add File Rule）] を選択して、ファイル ルールを追加します。詳細については、ファイル ルール，（967 ページ）を参照してください。
- 既存のファイル ルールを編集するには、そのルールの横にある編集アイコン（）をクリックします。
- 詳細オプションおよびアーカイブ ファイル検査オプション，（965 ページ）の説明に従って詳細オプションを設定します。

（注） ファイル ポリシー エディタに、現在編集中のファイル ポリシーを使用しているアクセス コントロール ポリシーの数が表示されます。この通知をクリックすると、親ポリシーのリストが表示され、オプションで [アクセス コントロール ポリシー（Access Control Policies）] ページに進むことができます。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

ファイル ルール

ファイルのポリシーには、その親であるアクセス コントロール ポリシーと同様に、各ルールの条件に一致したファイルをシステムがどのように処理するかを決定するルールが含まれています。

ファイルタイプ、アプリケーションプロトコル、転送方向の違いに応じて異なるアクションを実行する別個のファイル ルールを設定できます。

ファイルがルールに一致すると、ルールは以下を実行できます。

- 単純なファイル タイプ照合に基づいてファイルを許可またはブロックする
- 性質に基づいてファイルをブロックする
- キャプチャされたファイルをデバイスに保存する
- ローカル マルウェア分析、Spero 分析、または動的分析のために、キャプチャしたファイルを送信する。

さらに、ファイル ポリシーによって以下を実行できます。

- クリーン リストまたはカスタム検出リストのエントリに基づいて、ファイルがクリーンまたはマルウェアである場合と同じ方法で自動的にファイルを扱う
- ファイルの脅威スコアが、設定可能なしきい値を超えた場合、マルウェアと同じ方法でファイルを扱う
- アーカイブ ファイル（`.zip` や `.rar` など）の内容を検査する
- アーカイブ ファイルの内容が暗号化されている場合、アーカイブのネスト レベルが最大レベル指定値より深い場合、あるいはその反対で検査できない場合、アーカイブ ファイルをブロックする

ファイル ルールのコンポーネント

表 *77*：ファイル ルールのコンポーネント

ファイル ルールのコンポーネント	説明
アプリケーション プロトコル	システムは、FTP、HTTP、SMTP、IMAP、POP3、および NetBIOS-ssn（SMB）を介して伝送されるファイルを検出し、検査できます。デフォルトの [任意（Any）] は、HTTP、SMTP、IMAP、POP3、FTP、および NetBIOS-ssn（SMB）トラフィック内のファイルを検出します。パフォーマンスを向上させるには、ファイル ルールごとに、これらのアプリケーション プロトコルのうち 1 つだけでファイルを検出するよう限定できます。
転送の方向	ダウンロードされるファイルに対して、FTP、HTTP、IMAP、POP3、および NetBIOS-ssn（SMB）の着信トラフィックを検査できます。アップロードされるファイルに対しては、FTP、HTTP、SMTP、および NetBIOS-ssn（SMB）の発信トラフィックを検査できます。 **ヒント** [任意（Any）] を使用すると、ユーザが送信しているか受信しているかには関係なく、多数のアプリケーション プロトコルを介したファイルが検出されます。

ファイル ルールのコンポーネント	説明
ファイルのカテゴリとタイプ	システムは、さまざまなタイプのファイルを検出できます。これらのファイル タイプは、マルチメディア（swf、mp3）、実行可能ファイル（exe、トレント）、PDFなどの基本的なカテゴリにグループ分けされます。個々のファイルタイプを検出したり、ファイル タイプ カテゴリ全体を検出したりするよう、ファイル ルールを設定できます。 たとえば、すべてのマルチメディアファイルをブロックしたり、ShockWave Flash（swf）ファイルのみをブロックしたりできます。または、ユーザが BitTorrent（torrent）ファイルをダウンロードしたときにアラートを出すよう、システムを設定できます。 （注） 頻繁にトリガーされるファイルルールは、システムパフォーマンスに影響を与える可能性があります。たとえば、HTTP トラフィックでマルチメディアファイルを検出しようとすると（たとえば YouTube は多量の Flash コンテンツを伝送します）、膨大な数のイベントが生成される可能性があります。
ファイル ルール アクション	ファイル ルールのアクションによって、ルールの条件に一致したトラフィックをシステムが処理する方法が決定されます。 選択したアクションに応じて、システムでファイルを保存するか、ファイルに対してSpero分析、ローカルマルウェア分析、または動的分析を実行するかを設定できます。[ブロック（Block）]アクションを選択すると、システムでブロックされた接続をリセットするかどうかも設定できます。 （注） ファイルルールは数値上の順番ではなく、ルールアクションの順番で評価されます。

ファイル ルール アクションと評価順序

効果を発揮するには、ファイル ポリシーに 1 つ以上のルールが含まれている必要があります。ファイル ルールを使用すると、ロギング、ブロック、またはマルウェア スキャンの対象となるファイル タイプを詳細に制御できます。

各ファイル ルールには、ルールの条件に一致するトラフィックがシステムによってどのように処理されるかを決定する1つのアクションが関連付けられます。1つのファイルポリシー内に、ファイルタイプ、アプリケーションプロトコル、転送方向の違いに応じて異なるアクションを実行する別々のルールを設定できます。（優先度の高い順に）単純なブロッキング、次にマルウェア インスペクションとブロッキング、さらにその次に単純な検出とロギングとなります。

複数のファイル ルール アクションは、以下のようなルール アクション順になります。

- [ファイル ブロック（Block Files）] ルールを使用すると、特定のファイル タイプをブロックできます。ファイル転送がブロックされたときに接続をリセットするオプション、およびキャプチャされたファイルを管理対象デバイスに保存するオプションを設定できます。
- [マルウェア ブロック（Block Malware）] ルールを使用すると、特定のファイル タイプのSHA-256ハッシュ値を計算した後、AMPクラウドを照会して、ネットワークを通過するファ

イルにマルウェアが含まれているかどうかを判断し、脅威を示すファイルをブロックできます。

- [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] ルールを使用すると、ネットワークを通過するファイルの性質を取得して記録したうえでその伝送を許可できます。
- [ファイル検出（Detect Files）] ルールを使用すると、ファイルの伝送を許可しながら、特定のファイル タイプの検出をデータベースに記録できます。

注意 [ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] を選択、[ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] ルールで [ファイルの保存（Store files）] または無効化、または [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] または [マルウェア ブロック（Block Malware）] ファイル ルール アクションを分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[動的分析（Dynamic Analysis）]、または [ローカル マルウェア分析（Local Malware Analysis）]）またはファイルの保存オプション（[マルウェア（Malware）]、[不明（Unknown）]、[正常（Clean）]、または [カスタム（Custom）]）と結合する最初のファイル ルールを追加または最後のファイル ルールを削除すると、設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

ファイル ルール アクションに応じて、ファイル転送がブロックされたときに接続をリセットするオプション、管理対象デバイスに取得したファイルを保存するオプション、ファイルでマルウェアをローカルで分析するオプション、取得したファイルを動的分析および Spero 分析のために AMP クラウドに送信するオプション、および後で送信するためにクラウドに現在送信できないファイルを保存するオプションを設定できます。

表 *78*：ファイル ルール アクション

ファイル ルール アクションのオプション	ファイルのブロックが可能か	マルウェアのブロックが可能か	ファイルの検出が可能か	マルウェア クラウド ルックアップが可能か
MSEXE 用の Spero 分析（Spero Analysis for MSEXE）	No	はい：実行可能ファイルを送信できます	No	はい：実行可能ファイルを送信できます
動的分析（Dynamic Analysis）	No	はい：不明なファイルの性質の実行可能ファイルを送信できます	No	はい：不明なファイルの性質の実行可能ファイルを送信できます

ファイル ルール アクションのオプション	ファイルのブロックが可能か	マルウェアのブロックが可能か	ファイルの検出が可能か	マルウェア クラウド ルックアップが可能か
容量処理（Capacity Handling）	No	Yes	No	Yes
ローカル マルウェア分析（Local Malware Analysis）	No	Yes	No	Yes
接続のリセット（Reset Connection）	はい（推奨）	はい（推奨）	No	No
ファイルの保存（Store files）	はい：一致するすべてのファイルを保存できます	はい：選択したファイルの性質に一致するファイル タイプを保存できます	はい：一致するすべてのファイルを保存できます	はい：選択したファイルの性質に一致するファイル タイプを保存できます

ファイル ポリシーの注意事項と制約事項

ファイル ルール設定に関する注意事項と制約事項

- パッシブ展開でファイルをブロックするよう設定されたルールは、一致するファイルをブロックしません。接続ではファイル伝送が続行されるため、接続の開始をログに記録するルールを設定した場合、この接続に関して複数のイベントが記録されることがあります。
- [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] アクションまたは [マルウェア ブロック（Block Malware）] アクションを使ってファイル ルールが設定されている場合、Firepower Management Center が AMP クラウドとの接続を確立できないと、接続が復元されるまで、システムは設定済みルール アクション オプションを実行できません。
- シスコでは、[ファイル ブロック（Block Files）] アクションと [マルウェア ブロック（Block Malware）] アクションで [接続のリセット（Reset Connection）] を有効にすることを推奨しています。これにより、ブロックされたアプリケーション セッションが TCP 接続リセットまで開いたままになることを防止できます。接続をリセットしない場合、TCP 接続が自身をリセットするまで、クライアント セッションが開いたままになります。
- 大量のトラフィックをモニタしている場合、キャプチャしたすべてのファイルを保存したり、動的分析用に送信したり**しないでください**。そのようにすると、システム パフォーマンスに悪影響が及ぶことがあります。

- システムで検出されるすべてのファイル タイプに対してマルウェア分析を実行できるわけではありません。[アプリケーション プロトコル（Application Protocol）]、[転送の方向（Direction of Transfer）]、および [アクション（Action）] ドロップダウン リストで値を選択すると、システムはファイル タイプのリストを限定します。

ファイル検出に関する注意事項と制約事項

- ファイルがアプリケーション プロトコル条件を持つルールに一致する場合、ファイル イベントの生成は、システムがファイルのアプリケーション プロトコルを正常に識別した後に行われます。識別されていないファイルは、ファイル イベントを生成しません。
- FTP は、さまざまなチャネルを介してコマンドおよびデータを転送します。パッシブまたはインライン タップ モードの展開では、FTP データ セッションとその制御セッションからのトラフィックは同じ内部リソースに負荷分散されない場合があります。
- POP3、POP、SMTP、または IMAP セッションでのすべてのファイル名の合計バイト数が 1024 を超えると、セッションのファイル イベントでは、ファイル名バッファがいっぱいになった後で検出されたファイルの名前が正しく反映されないことがあります。
- SMTP 経由でテキストベースのファイルを送信すると、一部のメール クライアントは改行を CRLF 改行文字標準に変換します。MAC ベースのホストはキャリッジ リターン（CR）文字を使用し、UNIX/Linux ベースのホストはライン フィード（LF）文字を使用するので、メール クライアントによる改行変換によってファイルのサイズが変更される場合があります。一部のメール クライアントは、認識できないファイル タイプを処理する際に改行変換を行うようデフォルト設定されていることに注意してください。

ファイル ブロックに関する注意事項と制約事項

- ファイルの終わりを示す End of File マーカーが検出されない場合、転送プロトコルとは無関係に、そのファイルはマルウェア ブロック ルールでもカスタム検出リストでもブロックされません。システムは、End of File マーカーで示されるファイル全体の受信が完了するまでファイルのブロックを待機し、このマーカーが検出された後にファイルをブロックします。
- FTP ファイル転送で End of File マーカーが最終データ セグメントとは別に伝送される場合、マーカーがブロックされ、ファイル転送失敗が FTP クライアントに表示されますが、実際にはそのファイルは完全にディスクに転送されます。
- [ファイル ブロック（Block Files）] アクションおよび [マルウェア ブロック（Block Malware）] アクションを持つファイル ルールでは、最初のファイル転送試行後 24 時間で検出される、同じファイル、URL、サーバ、クライアント アプリケーションを使った新しいセッションをブロックすることにより、HTTP 経由のファイル ダウンロードの自動再開をブロックします。
- まれに、HTTP アップロード セッションからのトラフィックが不適切である場合、システムはトラフィックを正しく再構築できなくなり、トラフィックのブロックやファイル イベントの生成を行いません。

- [ファイル ブロック（Block Files）] ルールでブロックされる NetBIOS-ssn 経由ファイル転送（SMB ファイル転送など）の場合、宛先ホストでファイルが見つかることがあります。ただし、ダウンロード開始後にファイルがブロックされ、結果としてファイル転送が不完全になるため、そのファイルは使用できません。
- （SMB ファイル転送など）NetBIOS-ssn 経由で転送されるファイルを検出またはブロックするファイル ルールを作成した場合、ファイル ポリシーを呼び出すアクセス コントロール ポリシーの展開前に開始された、確立済み TCP または SMB セッションで転送されるファイルに対しては、検査が行われません。このため、これらのファイルは検出/ブロックされません。

ファイル ルールの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
Threat（ファイル制御） Malware（AMP for Firepower）	Protection（ファイル制御） Malware（AMP for Firepower）	任意（Any）	任意（Any）	Admin/Access Admin

注意 [ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] を選択、[ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] ルールで [ファイルの保存（Store files）] または無効化、または [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] または [マルウェア ブロック（Block Malware）] ファイル ルール アクションを分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[動的分析（Dynamic Analysis）]、または [ローカル マルウェア分析（Local Malware Analysis）]）またはファイルの保存オプション（[マルウェア（Malware）]、[不明（Unknown）]、[正常（Clean）]、または [カスタム（Custom）]）と結合する最初のファイル ルールを追加または最後のファイル ルールを削除すると、設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

手順

ステップ 1 ファイル ポリシー エディタで、[ファイル ルールの追加（Add File Rule）] をクリックします。

ステップ 2 ファイル ルールのコンポーネント, （968 ページ）の説明に従って、[アプリケーション プロトコル（Application Protocol）] および [転送の宛先（Direction of Transfer）] を選択します。

ステップ 3 [ファイル タイプ（File Types）] を 1 つ以上選択します。ファイル タイプのリストを、次のようにフィルタ処理できます。

- 1 つ以上の [ファイル タイプ カテゴリ（File Type Categories）] を選択し、[選択したカテゴリのすべてのタイプ（All types in selected Categories）] をクリックします。
- 名前または説明でファイル タイプを検索します。たとえば、Microsoft Windows 固有のファイルのリストを表示するには、[名前および説明の検索（Search name and description）] フィールドに Windows と入力します。

ヒント ファイル タイプの上にポインタを移動すると、説明が表示されます。

ステップ 4 ファイル ルール アクションと評価順序, （969 ページ）の説明に従って、ファイル ルールの [アクション（Action）] を選択します。

ステップ 5 選択したアクションに応じて、以下を実行するかどうかを設定します。

- ファイルのブロック後に接続をリセットする
- 一致するファイルを保存する
- Spero 分析を有効にする
- ローカル マルウェア分析を有効にする
- ダイナミック分析およびキャパシティの処理を有効にする

ファイル ルール アクションと評価順序, （969 ページ）の説明を参照してください。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

Snort® の再起動シナリオ , （324 ページ）

クラウド接続

Firepower システムでは Cisco Advanced Malware Protection（AMP）を実施するため、次のパブリック クラウドベースのサーバへの接続を行います。

- AMP クラウド：AMP for Firepower のマルウェア判定結果と更新、エンドポイント向け AMP のスキャン レコード、マルウェア検出、検疫、侵害の兆候（IOC）を取得できます。
- AMP Threat Grid クラウド：AMP for Firepower ダイナミック分析に利用可能なファイルの送信、脅威スコアやダイナミック分析レポートの取得ができます。

部門のプライバシー、セキュリティ保護のニーズに応じて、プライベートクラウドサーバを導入することもできます。

- AMP プライベート クラウド仮想アプライアンス（AMPv）は、圧縮型、オンプレミス AMP クラウドとして機能します。
- AMP Threat Grid アプライアンスはパブリック AMP Threat Grid クラウドとは連絡しないオンプレミス AMP Threat Grid クラウドとして機能します。

AMP クラウド接続

高度なマルウェア防御（AMP）クラウドは、ビッグデータ分析や連続分析によりネットワーク上のマルウェアを検出およびブロックするシスコ ホステッド サーバです。次の 2 つのシスコ AMP ソリューションはどちらも AMP クラウドを使用します。

- AMP for Firepower は、管理対象デバイスがネットワーク トラフィックから検出した潜在的なマルウェアの性質を取得し、ローカルマルウェア分析とファイルの事前分類の更新を取得するために AMP クラウドを使用します。
- エンドポイント向け AMP は、シスコのエンタープライズクラスの AMP ソリューションです。ユーザはそれぞれ、AMP クラウドと通信するコンピュータやモバイル デバイスに軽量コネクタをインストールします。次に Firepower Management Center がスキャン、マルウェア検出、隔離、および侵害の兆候（IOC）のレコードをインポートします。

展開によっては、AMP for Endpoints がモニタするエンドポイントは、AMP for Firepower がモニタしているものと同じホストではない場合があります。このため、エンドポイントベースのマルウェア イベントは、ネットワーク マップにホストを追加しません。ただし、システムは IP アドレスおよび MAC アドレスのデータを使用して、AMP for Endpoints の展開から取得した侵害の兆候をモニタ対象のホストにタグ付けします。異なる AMP ソリューションによってモニタされる 2 つの異なるホストが同じ IP アドレスと MAC アドレスを持っている場合、システムは AMP for Endpoints の IOC をモニタ対象のホストに誤ってタグ付けする場合があります。

[AMP 管理（AMP Management）] ページ（[AMP] > [AMP 管理（AMP Management）]）で AMP クラウドとの接続を管理します。AMP for Firepower では、デフォルトで米国 (US) AMP パブリック クラウドへの接続が設定され、有効になっています。AMP for Firepower クラウド接続の削除や無

効化はできませんが、欧州連合（EU）および米国（US）AMP クラウドの切り替え、またはプライベート クラウド（AMPv）の接続の設定が可能です。

エンドポイントに独自の FireAMP 接続を追加するには、FireAMP ポータルのアカウントが必要です。ポータルに登録されていないエンドポイント向け AMP 接続では、AMP for Firepower は無効になりません。

AMP クラウド接続要件

- AMP for Networks：パブリックまたはプライベートいずれの AMP クラウドを使用していても、ポート 443 を使って AMP for Networks のマルウェア クラウド ルックアップを行います。Firepower Management Center からの通信を行うため、このポートをアウトバウンドに開く必要があります。
- エンドポイント向け AMP：エンドポイントベースのマルウェア イベントを受信するために、システムはポート 443/HTTPS を使用してシスコ クラウド（パブリックまたはプライベート）に接続します。Firepower Management Center との通信を行うため、このポートをインバウンドとアウトバウンドの両方に開く必要があります。また、Firepower Management Center はインターネットに直接アクセスできる必要があります。デフォルトの正常性ポリシーに含まれる AMP ステータス モニタは、Firepower Management Center からクラウドへの最初の接続が成功した後で接続できなくなった場合、または AMP ポータルを使って接続が登録解除された場合に警告を出します。

AMP の通信にレガシー ポートを使用するには 集合型セキュリティ インテリジェンスの通信設定オプション，（984 ページ） を参照してください。

AMP クラウド接続とマルチテナンシー

マルチドメイン導入環境では、AMP for Firepower 接続はグローバル レベルでのみ設定します。各 Firepower Management Center で可能な AMP for Firepower 接続数は 1 接続のみです。エンドポイント向け AMP 接続は、どのドメイン レベルでも設定可能です。ただし、各接続にそれぞれ個別のエンドポイント向け AMP アカウントを使用する必要があります。たとえば、MSSP の各クライアントは、それぞれ独自のエンドポイント向け AMP を展開している場合があります。

注意 特にリーフ ドメインに重複する IP スペースがある場合、エンドポイント向け AMP 接続はリーフ レベルのみで設定することを**強く**推奨します。複数のサブドメインに同じ IP-MAC アドレス ペアを持つホストが存在する場合、誤ったリーフ ドメインにエンドポイントベースのマルウェア イベントを保存したり、誤ったホストに IOC を関連付けたりする可能性があります。

AMP for Endpoints クラウド接続の設定

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

組織で AMP for Endpoints が展開されると、脅威の識別、侵害の兆候（IOC）、およびその他のマルウェア関連の情報を AMP クラウドからシステムにインポートできます。AMP for Firepower 接続がすでに設定されている場合にも、AMP for Endpoints 接続を設定する必要があります。

注意 マルチドメイン展開では、特にリーフ ドメインに重複する IP スペースがある場合は、AMP for Endpoints 接続をリーフ レベルのみで設定することを**強く**お勧めします。複数のサブドメインに同じ IP-MAC アドレス ペアを持つホストがある場合、システムが誤ったリーフ ドメインにエンドポイントベースのマルウェア イベントを保存したり、誤ったホストに IOC を関連付けたりする可能性があります。

はじめる前に

- Firepower Management Center を工場出荷時の初期状態に復元した後、または以前のバージョンに戻した後に AMP クラウドに接続している場合は、AMP for Endpoints 管理コンソールを使用して以前の接続を削除します。

手順

ステップ 1 [AMP] > [AMP 管理（AMP Management）]を選択します。

ステップ 2 [AMP クラウド接続の作成（Create AMP Cloud Connection）] をクリックします。

ステップ 3 [クラウド名（Cloud Name）] ドロップダウン リストから、使用するクラウドを選択します。

- 欧州連合 AMP クラウドの場合、[EU クラウド（EU Cloud）] を選択します。
- 米国 AMP クラウドの場合、[US クラウド（US Cloud）] を選択します。
- AMPv の場合、[プライベート クラウド（Private Cloud）] を選択し、Cisco AMP プライベート クラウド, （978 ページ）の説明に従って続行します。

ステップ 4 このクラウドを AMP for Firepower と AMP for Endpoints に使用する場合は、[AMP for Firepower に使用（Use for AMP for Firepower）] チェックボックスをオンにします。
マルチドメイン展開では、このチェックボックスはグローバル ドメインにのみ表示されます。各 Firepower Management Center には、AMP for Firepower 接続を 1 つだけ設定できます。

ステップ 5 [登録（Register）] をクリックします。
回転状態のアイコンは、たとえば、Firepower Management Center で接続を設定した後、AMP for Endpoints 管理コンソールの使用を許可する前に、接続が保留中であることを示します。失敗または拒否を示すアイコン（）は、クラウドが接続を拒否したこと、または他の理由で接続が失敗したことを示します。

ステップ 6 AMP for Endpoints 管理コンソールを続行することを確認し、管理コンソールにログインします。

ステップ 7 管理コンソールを使用して、AMP for Endpoints データを Firepower Management Center に送信することを AMP クラウドに許可します。

ステップ 8 受信するデータを制限する場合は、情報を受け取る組織内の特定のグループを選択します。デフォルトでは、AMP クラウドはすべてのグループのデータを送信します。グループを管理するには、AMP for Endpoints 管理コンソールで [管理（Management）] > [グループ（Groups）] を選択します。詳細については、管理コンソールのオンライン ヘルプを参照してください。

ステップ 9 [許可（Allow）] をクリックして接続を有効にして、データの転送を開始します。[拒否（Deny）] をクリックすると Firepower Management Center に戻りますが、接続には拒否マークが付きます。接続を拒否/許可しないまま AMP for Endpoints 管理コンソールの [アプリケーション（Applications）] ページから別のページに移動した場合、Firepower Management Center の Web インターフェイスでは接続に保留中のマークが付きます。これらのいずれの状況でも、ヘルス モニタは失敗した接続のアラートを生成**しません**。後で AMP クラウドに接続するには、失敗した接続または保留中の接続を削除してから再作成します。

AMP for Endpoints 接続の登録が未完了であっても、AMP for Firepower 接続は無効になりません。

Cisco AMP プライベート クラウド

Cisco AMP プライベート クラウド仮想アプライアンス（AMPv）を構成することで、ネットワーク上の AMP エンドポイント データを収集することができます。AMPv は、AMP クラウドの圧縮型、オンプレミス バージョンとして機能する、シスコ独自の仮想マシンです。

エンドポイント向け AMP のすべてのコネクタが AMPv にデータを送信し、AMPv は Firepower Management Center にデータを転送します。AMPv は、エンドポイント データを外部接続では一切共有しません。Firepower Management Center は AMP クラウドに接続し、ネットワーク トラフィックで検出されたファイルの判定結果をクエリしたり、レトロスペクティブ マルウェア イベントを受信したりします。

各プライベート クラウドは、エンドポイント向け AMP コネクタを最大 10,000 までサポート可能で、複数のプライベート クラウドを設定できます。

[AMP 管理（AMP Management）] ページ（[AMP] > [AMP 管理（AMP Management）]）を使って、Firepower Management Center から AMPv との接続を制御します。

（注） AMP for Firepower のコンポーネントであるダイナミック分析では、管理対象デバイスがポート 443 から AMP Threat Grid クラウドまたはオンプレミス AMP Threat Grid アプライアンスに、直接あるいはプロキシを介してアクセスできる必要があります。AMPv はダイナミック分析をサポート**していません**。また、シスコ集合型セキュリティ インテリジェンス (CSI) に依存するその他の機能（URL フィルタリングやセキュリティ インテリジェンス フィルタリングなど）のための脅威インテリジェンスの匿名での取得もサポートしていません。

AMPv への接続

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
マルウェア（AMP for Firepower） 任意（AMP for Endpoints）	マルウェア（AMP for Firepower） 任意（AMP for Endpoints）	任意（Any）	任意（Any）	Admin

はじめる前に

- AMPv のマニュアルの指示に従って、Cisco AMP プライベート クラウドまたはクラウドを設定します。設定時に、プライベート クラウドのホスト名をメモしてください。このホスト名は、後で Firepower Management Center で接続を設定するときに必要になります。
- Firepower Management Center が AMPv と通信できることを確認し、AMPv がインターネットにアクセスでき、AMP クラウドと通信できることを確認します。

手順

ステップ 1 [AMP] > [AMP 管理（AMP Management）]を選択します。

ステップ 2 [AMP クラウド接続の作成（Create AMP Cloud Connection）] をクリックします。

ステップ 3 [クラウド名（Cloud Name] ドロップダウン リストから [プライベート クラウド（Private Cloud）] を選択します。

ステップ 4 名前を入力します。
この情報は、AMPv によって生成または送信されるマルウェア イベントに表示されます。

ステップ 5 [ホスト（Host）] フィールドに、AMPv の設定時に設定したプライベート クラウドのホスト名を入力します。

ステップ 6 [証明書アップロード パス（Certificate Upload Path）] フィールドの横にある [参照（Browse）] をクリックして、AMPv の有効な TLS または SSL 暗号化証明書の場所を参照します。詳細については、AMPv のマニュアルを参照してください。

ステップ 7 このプライベート クラウドを AMP for Firepower および AMP for Endpoints に使用する場合は、[AMP for Firepower に使用（Use for AMP for Firepower）] チェックボックスをオンにします。
AMP for Firepower 通信を処理する別のプライベート クラウドを設定した場合は、このチェックボックスをオフにすることができます。これが唯一の AMPv 接続の場合は、オフにできません。

マルチドメイン展開では、このチェックボックスはグローバル ドメインにのみ表示されます。各 Firepower Management Center には、AMP for Firepower 接続を 1 つだけ設定できます。

ステップ 8 プロキシを使用して AMPv と通信するには、[接続にプロキシを使用（Use Proxy for Connection）] チェックボックスをオンにします。

ステップ 9 [登録（Register）] をクリックし、AMP クラウドへの既存の直接接続を無効にすることを確認し、最後に AMPv 管理コンソールを続行して登録を完了することを確認します。

ステップ 10 管理コンソールにログインして登録プロセスを完了します。手順の詳細については、AMPv のマニュアルを参照してください。

AMP クラウドおよび AMPv 接続の管理

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

クラウドからマルウェア関連の情報を受信する必要がなくなったら、Firepower Management Center を使用して AMP クラウドまたは AMPv 接続を削除します。AMP for Endpoints または AMPv 管理コンソールを使用して接続の登録を解除しても、システムから接続を削除することにはならない点に注意してください。登録解除した接続は、Firepower Management Center の Web インターフェイスに障害発生状態で表されます。

また、接続は一時的に無効にすることもできます。クラウド接続を再度有効化すると、クラウドは、無効化されていた期間にキューに保持していたデータを含めて、システムへのデータ送信を再開します。

注意 無効化された接続に対して、AMP クラウドおよび AMPv は、接続を再有効化するまでマルウェア イベントや侵害の兆候などを保存できます。まれに、イベント レートが非常に高い場合や接続が長期間無効になっていた場合など、接続無効中に生成されたすべての情報をクラウドで保存できないことがあります。

マルチドメイン展開では、現在のドメインで作成された接続が表示されます。これは、管理が可能な接続です。また、先祖ドメインで作成した接続も表示されますが、この接続は管理できません。下位ドメインの接続を管理するには、そのドメインに切り替えます。各 Firepower Management Center は、グローバル ドメインに属する AMP for Firepower 接続を 1 つのみ保持できます。

手順

ステップ 1 [AMP] > [AMP 管理（AMP Management）] を選択します。

ステップ 2 AMP クラウド接続を管理します。

- 削除：削除アイコン（）をクリックして、選択内容を確認します。
- 有効化または無効化：スライダをクリックして、選択内容を確認します。

動的分析接続

AMP Threat Grid クラウドでは、ファイルがサンドボックス環境で実行されます。AMP for Firepower ではクラウドを使用して、動的分析送信ファイルの脅威スコアと動的分析レポートを取得します。適切なライセンスを使用して、システムが自動的にクラウドにアクセスします。

組織のセキュリティ ポリシーが Firepower システムによるネットワーク外部へのファイルの送信を許可しない場合は、オンプレミスの AMP Threat Grid アプライアンスを設定できます。詳細については、『*Cisco AMP Threat Grid Appliance Setup and Configuration Guide*』を参照してください。

Firepower Management Center の [ダイナミック分析接続（Dynamic Analysis Connections）] ページ（[AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）]）を使用して、AMP Threat Grid クラウドへのパブリック動的分析接続およびオンプレミスの AMP Threat Grid アプライアンスへのプライベート動的分析接続を管理します。

デフォルトの動的分析接続の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
マルウェア	マルウェア	任意（Any）	グローバルだけ	Admin/Access Admin/Network Admin

デフォルトで、Firepower Management Center は、ファイルを送信したり、レポートを取得したりするために、パブリック AMP Threat Grid クラウドに接続できます。この接続は、設定したり、削除したりすることはできません。

手順

ステップ 1 [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）]を選択します。

ステップ 2 編集アイコン（  ）をクリックします。

Threat Grid のオンプレミス アプライアンス

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

1 台のオンプレミス AMP Threat Grid アプライアンスを Firepower Management Center に接続できます。詳細については、『*Cisco AMP Threat Grid* アプライアンス セットアップおよび構成ガイド』を参照してください。

このオンプレミス アプライアンスへの動的分析接続を設定した場合、システムではパブリックの AMP クラウドを使用してマルウェア クラウド ルックアップを実行し、またファイルが以前に動的分析用に送信されていないことを確認します。

システムでは、パブリック レポートの取得に AMP クラウドへのデフォルトのパブリック動的分析接続も使用します。オンプレミス アプライアンスがファイル用の動的分析レポートを生成しなかった場合、システムはこの動的分析レポートについてパブリックの AMP クラウドに問い合わせます。組織がファイルを送信していない限り、表示できるのは、限られたデータが含まれた、スクラビング処理が実行されたレポートだけです。

オンプレミスの動的分析接続の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
マルウェア	マルウェア	任意（Any）	グローバルだけ	Admin/Access Admin/Network Admin

ネットワークでオンプレミスの AMP Threat Grid アプライアンスをインストールする場合は、動的分析接続を設定して、ファイルを送信し、アプライアンスからレポートを取得できます。オンプレミスのアプライアンスの動的分析接続を設定するには、オンプレミスのアプライアンスに Firepower Management Center を登録します。

はじめる前に

- オンプレミスの AMP Threat Grid アプライアンスを設定します。『*Cisco AMP Threat Grid Appliance Setup and Configuration Guide*』を参照してください。
- ログインに使用する公開キー証明書を AMP Threat Grid アプライアンスからオンプレミスのアプライアンスにダウンロードします。『*Cisco AMP Threat Grid Appliance Administrator's Guide*』を参照してください。
- プロキシを使用してオンプレミスのアプライアンスに接続する場合は、プロキシを設定します。Firepower Management Center 管理インターフェイスの設定, （569 ページ）を参照してください。

手順

ステップ 1 [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）]を選択します。

ステップ 2 [新しい接続を追加（Add New Connection）] をクリックします。

ステップ 3 名前を入力します。

ステップ 4 [ホスト URL（Host URL）] を入力します。

ステップ 5 [証明書のアップロード（Certificate Upload）] の横にある [参照（Browse）] をクリックして、オンプレミスのアプライアンスとの接続を確立するために使用する公開キー証明書をアップロードします。

ステップ 6 設定されているプロキシを使用して接続を確立する場合は、[可能な場合はプロキシを使用（Use Proxy When Available）] を選択します。

ステップ 7 [登録（Register）] をクリックします。

ステップ 8 [はい（Yes）] をクリックして、オンプレミスの AMP Threat Grid アプライアンスのログイン ページを表示します。

ステップ 9 オンプレミスの AMP Threat Grid アプライアンスにユーザ名とパスワードを入力します。

ステップ 10 [サインイン（Sign in）] をクリックします。

ステップ 11 次の選択肢があります。

- 以前にオンプレミスのアプライアンスに Firepower Management Center を登録した場合は、[戻る（Return）] をクリックします。
- Firepower Management Center を登録していない場合は、[アクティブ化（Activate）] をクリックします。

集合型セキュリティ インテリジェンス通信の設定

Firepowerシステムは、レピュテーション、リスク、脅威インテリジェンスに関して、シスコ集合型セキュリティ インテリジェンス（CSI）を使用します。適正なライセンスがあれば、URL フィルタリングおよび AMP for Firepower 機能の通信オプションを指定できます。

集合型セキュリティ インテリジェンスの通信設定オプション

Enable URL Filtering

Web サイトの一般的な分類、カテゴリ、リスク レベル、またはレピュテーションに基づくトラフィックのフィルタリングを可能にします。URLフィルタリングライセンスが自動的に追加されるようにして、[URL フィルタンリングを有効にする（Enable URL Filtering）] および [自動更新を有効にする（Enable Automatic Updates）] を有効にします。URL フィルタリングは、他の URL フィルタリング オプションを選択する前に有効にする必要があります。

URLフィルタリングを有効にする場合は、URLフィルタリングが最後に有効になってから経過した時間に応じて、またはURLフィルタリングを今回初めて有効にするかどうかに応じて、Firepower Management Center が Cisco CSI から URL データを取得します。

メモリの制約上、一部のモデルでは、小規模でそれほど細分化されていないカテゴリとレピュテーションによって URL フィルタリングが実行されます。たとえば、親 URL のサブサイトがそれぞれ異なるURLカテゴリとレピュテーションを持っている場合、一部のデバイスでは、すべてのサブサイトに対して親URLのデータが使用されます。具体的な例として、システムはgoogle.comカテゴリとレピュテーションを使用して mail.google.com を評価します。

メモリが少ないデバイスには、7100 ファミリと次の ASA モデルが含まれます：ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X。NGIPSv で、カテゴリおよびレピュテーション ベースの URL フィルタリングを実行するための正しいメモリ量を割り当てる方法ついて、詳しくは *Firepower System Virtual Installation Guide* を参照してください。

自動更新を有効にする（Enable Automatic Updates）

Firepower Management Center で展開環境の URL データが自動的に更新されるようにします。一般的に、URL データは 1 日 1 回更新されますが、自動更新を有効にすると、30 分ごとに Firepower Management Centerが確認するようになります。通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

システムが外部リソースと通信するタイミングを厳格に制御する必要がある場合は、自動更新を無効にし、代わりにスケジューラを使用します。

（注） Cisco では、自動更新を有効にするか、またはスケジューラを使用して更新をスケジュールすることを推奨しています。[今すぐ更新する（Update Now）] をクリックして手動でオンデマンド更新を実行できますが、プロセスを自動化すると、最新の関連データを使用できるようになります。更新がすでに進行中である場合は、オンデマンド更新を開始できません。

不明 URL を Cisco CSI に問い合わせる（Query Cisco CSI for Unknown URL）

カテゴリとレピュテーションがローカルデータセットにない Web サイトをユーザが閲覧するときに URL が脅威インテリジェンス評価のために送信されるようにします。プライバシー上の理由などで未分類の URL を送信したくない場合は、このオプションを無効にしてください。

未分類の URL への接続は、カテゴリまたはレピュテーションベースの URL 条件を含むルールに一致**しません**。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

ローカル マルウェア検出の自動更新を有効にする（Enable Automatic Local Malware Detection Updates）

ローカル マルウェア検出エンジンは、Cisco が提供する署名を使用して統計的にファイルを分析し、事前に分類します。このオプションを有効にすると、Firepower Management Center が 30 分ごとに署名の更新を確認します。

マルウェア イベントの URL を Cisco と共有する（Share URI from Malware Events with Cisco）

ネットワーク トラフィックで検出されたファイルに関する情報を AMP クラウドに送信することができます。この情報には、検出されたファイルに関連する URI 情報と SHA-256 ハッシュ値が含まれます。共有はオプトインですが、この情報を Cisco に送信すると、マルウェアを識別して追跡する今後の取り組みに役立ちます。

レガシー ポート 32137 を AMP for Firepower に使用する（Use Legacy Port 32137 for AMP for Firepower）

デフォルトでは、AMP for Firepower はポート 443/HTTPS を使用して AMP クラウド（または AMPv）と通信します。このオプションは、AMP for Firepower によるポート 32137 の使用を許可します。システムを以前のバージョンから更新する場合は、このオプションを有効にすることができます。

関連トピック

通信ポートの要件, （2189 ページ）

集合型セキュリティ インテリジェンスとの通信の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
URLフィルタリング（URLフィルタリング） マルウェア（AMP for Firepower）	URLフィルタリング（URLフィルタリング） マルウェア（AMP for Firepower）	任意（Any）	任意（Any）	Admin

手順

ステップ 1 [システム（System）] > [統合（Integration）]を選択します。

ステップ 2 [Cisco CSI] タブをクリックします。

ステップ 3 集合型セキュリティインテリジェンスの通信設定オプション，（984 ページ）の説明に従ってCisco CSI 通信を設定します。

ステップ 4 [保存（Save）] をクリックします。

第 46 章

ファイルとマルウェアのインスペクション パフォーマンスとストレージの調整

次のトピックでは、ファイルとマルウェアのインスペクション パフォーマンスとストレージを設定する方法について説明します。

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

ファイル制御を実行するか、AMP for Firepower を使用する場合は、次の詳細設定ファイルとマルウェア インスペクション機能のオプションを設定できます。

- ファイル タイプを検出したときに検査されるバイト数を制限する。
- マルウェア ブロック ルールがキャッシュされた性質のないファイルと一致し、性質を取得せずに経過した時間が長すぎる場合は、ファイルの通過を許可する。
- 特定のサイズよりも大きい場合は、ファイルの保存、ファイルでのマルウェア クラウドルックアップの実行、またはカスタム検出リストでのファイルのブロックを回避する。
- 保存する最小ファイル サイズと最大ファイル サイズを指定する。
- 動的分析に送信する最小ファイル サイズと最大ファイル サイズを指定する。

これらのオプションはシステムパフォーマンスおよびファイルストレージに影響を与える可能性があります。

ファイルおよびマルウェアのインスペクションパフォーマンスとストレージのオプション

ファイル サイズを増やすと、システムのパフォーマンスに影響を与える可能性があります。

注意 [ファイルおよびマルウェアの設定（File and Malware Settings）] でデフォルト以外の値を設定します 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作,（326 ページ）を参照してください。

表 *79*：アクセス コントロール ファイルおよび *AMP for Firepower* の詳細オプション

フィールド	説明	使用可能な値	注記（**Notes**）
ファイルタイプを検知する前に検閲するバイト数制限（Limit the number of bytes inspected when doing file type detection）	ファイル タイプを検出するときに検査するバイト数を指定します。	0 ～ 4294967295（4GB）	制限を取り除くには、0 を入力します。 デフォルト値は、TCP パケットの最大セグメント サイズです。ほとんどの場合、システムは最初のパケットによって、一般的なファイル タイプを特定できます。
ファイルを許可するのにかかるマルウェア ブロックのクラウド ルックアップの制限時間（秒）（Allow file if cloud lookup for Block Malware takes longer than (seconds)）	マルウェア クラウド ルックアップの実行中に、システムが [マルウェア ブロック（Block Malware）] ルールに一致し、性質がキャッシュに入っていないファイルの最後のバイトを保持する期間を指定します。システムが性質を取得する前にこの期間が満了すると、ファイルが渡されます。「使用不可」の性質はキャッシュに入れられません。	0 ～ 30 秒	シスコは、接続の障害によってトラフィックのブロックを防ぐために、デフォルト値を使用することをお勧めします。サポートに連絡することなくこのオプションを 0 に設定**しない**でください。

フィールド	説明	使用可能な値	注記（**Notes**）
SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA--256 hash values for files larger than (in bytes)）	システムが特定のサイズを超えるファイルを保管すること、ファイルでマルウェア クラウド ルックアップを実行すること、またはカスタム検出リストに追加されたファイルをブロックすることを防止します。	`0` ～ `4294967295`（4GB）	制限を取り除くには、`0` を入力します。 この値は、[保存する最大ファイルサイズ（バイト）（Maximum file size to store (bytes)）] および [動的分析テストの最大ファイルサイズ (バイト)（Maximum file size for dynamic analysis testing (bytes)）] の値以上に設定する必要があります。
保存する最小ファイル サイズ(バイト)（Minimum file size to store (bytes)）	システムがファイル ルールを使用して保管できるファイルの最小サイズを指定します。	`0` ～ `10485760`（10MB）	ファイル ストレージを無効にするには、`0` を入力します。 このフィールドは、[保存する最大ファイルサイズ（バイト）（Maximum file size to store (bytes)）] および [SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Maximum file size to store (bytes)）] の値以下に設定する必要があります。
保存する最大ファイルサイズ(バイト)（Maximum file size to store (bytes)）	システムがファイル ルールを使用して保管できるファイルの最大サイズを指定します。	`0` ～ `10485760`（10MB）	ファイル ストレージを無効にするには、`0` を入力します。 このフィールドは、[保存する最小ファイル サイズ(バイト)（Minimum file size to store (bytes)）] の値以上、および [SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。

フィールド	説明	使用可能な値	注記（**Notes**）
ダイナミック分析の最小ファイルサイズ（バイト）（Minimum file size for dynamic analysis testing (bytes)）	システムがAMPクラウドに動的分析対象として送信できるファイルの最小サイズを指定します。	`0` 〜 `104857600`（100 MB）	このフィールドは、[動的分析テストの最大ファイルサイズ(バイト)（Maximum file size for dynamic analysis testing (bytes)）] および [SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。 バージョン 5.x の Firepower システムを実行するデバイスにアクセス コントロール ポリシーを展開した場合、システムは`15360`より小さい値をすべて`15360`に変更します。 システムはAMPクラウドをチェックして、送信可能なファイルの最小サイズが更新されているかどうかを調べます（最大で1日1回）。新しい最小サイズが現在の値より大きい場合、現在の値が新しい最小サイズに更新され、ポリシーは古いポリシーとしてマークされます。

フィールド	説明	使用可能な値	注記（**Notes**）
ダイナミック分析の最大ファイルサイズ(バイト)（Maximum file size for dynamic analysis testing (bytes)）	システムがAMPクラウドに動的分析対象として送信できるファイルの最大サイズを指定します。	`0` ～ `104857600`（100 MB）	このフィールドは、[Mダイナミック分析の最小ファイルサイズ（バイト）（Minimum file size for dynamic analysis testing (bytes)）] の値以上、[SHA-256ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。 バージョン5.xのFirepowerシステムを実行するデバイスにアクセス コントロール ポリシーを展開した場合、システムは`2097152`より大きい値をすべて`2097152`に変更します。 システムはAMPクラウドをチェックして、送信可能なファイルの最大サイズが更新されているかどうかを調べます（最大で1日1回）。新しい最大サイズが現在の値より小さい場合、現在の値が新しい最大サイズに更新され、ポリシーは古いポリシーとしてマークされます。

ファイルおよびマルウェアのインスペクションパフォーマンスおよびストレージの調整

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（ファイル制御） マルウェア（AMP）	保護（ファイル制御） マルウェア（AMP）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

注意 [ファイルおよびマルウェアの設定（Files and Malware Settings）] にデフォルト以外の値を設定することによって、設定の変更を展開するとSnortプロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作，（326 ページ）を参照してください。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [ファイルおよびマルウェアの設定（Files and Malware Settings）] の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 3 ファイルおよびマルウェアのインスペクション パフォーマンスとストレージのオプション，（988 ページ）で説明されている任意のオプションを設定します。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

第 XIV 部

侵入検知と防御

第 47 章

ネットワーク分析ポリシーと侵入ポリシーの概要

以下のトピックでは、ネットワーク分析ポリシーと侵入ポリシーの概要を示します。

ネットワーク分析ポリシーと侵入ポリシーの基本

ネットワーク分析ポリシーと侵入ポリシーは、Firepower システムの侵入検知および防御機能の一部として連携して動作します。侵入検知という用語は、一般に、ネットワーク トラフィックへの侵入の可能性を受動的に分析し、セキュリティ分析用に攻撃データを保存するプロセスを指します。侵入防御という用語には、侵入検知の概念が含まれますが、さらにネットワークを通過中の悪意のあるトラフィックをブロックしたり変更したりする機能も追加されます。

侵入防御の展開では、システムがパケットを検査するときに次のことが行われます。

- **ネットワーク分析ポリシー**は、トラフィックのデコードと前処理の方法を管理し、特に、侵入を試みている兆候がある異常なトラフィックについて、さらに評価できるようにします。
- **侵入ポリシー**では侵入およびプリプロセッサ ルール（総称的に「侵入ルール」とも呼ばれる）を使用し、パターンに基づき、デコードされたパケットを検査して攻撃の可能性を調べます。侵入ポリシーは変数セットとペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映することができます。

ネットワーク分析ポリシーと侵入ポリシーは、どちらも親のアクセス コントロール ポリシーによって呼び出されますが、呼び出されるタイミングが異なります。システムでトラフィックが分

析される際には、侵入防御（追加の前処理と侵入ルール）フェーズよりも前に、別途ネットワーク分析（デコードと前処理）フェーズが実行されます。ネットワーク分析ポリシーと侵入ポリシーを一緒に使用すると、広範囲で詳細なパケット インスペクションを行うことができます。このポリシーは、ホストとそのデータの可用性、整合性、機密性を脅かす可能性のあるネットワーク トラフィックの検知、通知および防御に役立ちます。

Firepower システムには、同様の名前（Balanced Security and Connectivity など）が付いた複数のネットワーク分析ポリシーと侵入ポリシーが付属しており、それらは相互に補完して連携します。システム付属のポリシーを使用することで、Cisco Talos Security Intelligence and Research Group（Talos）の経験を活用できます。これらのポリシーでは、Talos は侵入ルールおよびプリプロセッサ ルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。

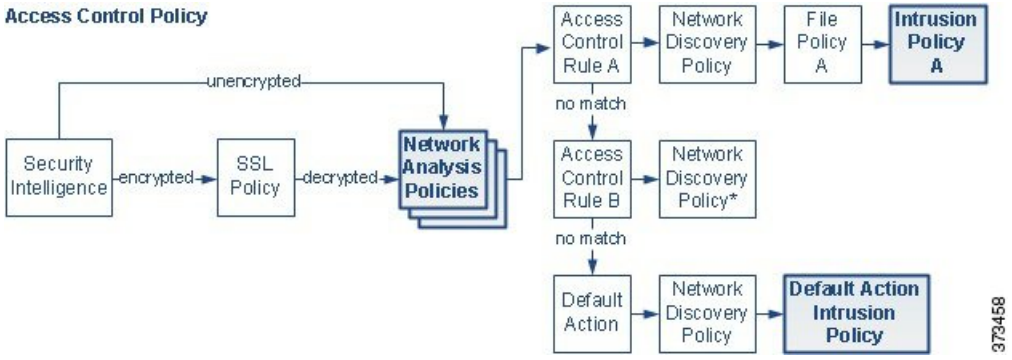
また、カスタムのネットワーク分析ポリシーや侵入ポリシーも作成できます。カスタム ポリシーの設定を調整することで、各自にもっとも役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

Web インターフェイスで同様のポリシーエディタを使用し、ネットワーク分析ポリシーや侵入ポリシーを作成、編集、保存、管理します。いずれかのタイプのポリシーを編集するときには、Web インターフェイスの左側にナビゲーション パネルが表示され、右側にさまざまな設定ページが表示されます。

ポリシーが侵入についてトラフィックを検査する仕組み

アクセス コントロールの展開の一部としてシステムがトラフィックを分析すると、ネットワーク分析（復号化と前処理）フェーズが侵入防御（侵入ルールおよび詳細設定）フェーズとは別にその前に実行されます。

次の図は、インラインの侵入防御および AMP for Firepower 展開におけるトラフィック分析の順序を簡略化して示しています。アクセス コントロール ポリシーが他のポリシーを呼び出してトラフィックを検査するしくみ、およびそれらのポリシーが呼び出される順序が示されています。ネットワーク分析ポリシーおよび侵入ポリシーの選択フェーズが強調表示されています。



インライン展開（つまり、ルーテッド、スイッチド、トランスペアレント インターフェイスまたはインライン インターフェイスのペアを使用して関連設定がデバイスに展開される展開）では、システムは上図のプロセスのほぼすべての段階において、追加のインスペクションなしでトラ

フィックをブロックすることができます。セキュリティ インテリジェンス、SSL ポリシー、ネットワーク分析ポリシー、ファイル ポリシー、および侵入ポリシーのすべてで、トラフィックをドロップまたは変更できます。唯一の例外として、パケットをパッシブに検査するネットワーク検出ポリシーは、トラフィック フローに影響を与えることができません。

同様に、プロセスの各ステップで、パケットによってシステムがイベントを生成する場合があります。侵入イベントおよびプリプロセッサ イベント（まとめて侵入イベントと呼ばれることもあります）は、パケットまたはその内容がセキュリティ リスクを表す可能性があることを示すものです。

ヒント この図では、SSLインスペクションの設定で暗号化トラフィックの通過が許可されている場合や、SSL インスペクションが設定されていない場合については、アクセス コントロール ルールによる暗号化トラフィックの処理を反映していません。デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイル インスペクションは無効になっています。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

単一の接続の場合は、図に示すように、アクセスコントロールルールよりも前にネットワーク分析ポリシーが選択されますが、一部の前処理（特にアプリケーション層の前処理）はアクセス コントロールルールの選択後に実行されます。これは、カスタムネットワーク分析ポリシーでの前処理の設定には影響**しません**。

復号化、正規化、前処理：ネットワーク分析ポリシー

デコードと前処理を実行しないと、プロトコルの相違によりパターン マッチングを行えなくなるので、侵入についてトラフィックを適切に評価できません。これらのトラフィック処理タスクは、以下のタイミングでネットワーク分析ポリシーによる処理の対象となります。

- 暗号化トラフィックがセキュリティ インテリジェンスによってフィルタリングされた**後**
- 暗号化トラフィックがオプションの SSL ポリシーによって復号化された**後**
- ファイルポリシーまたは侵入ポリシーによってトラフィックを検査できるようになる**前**

ネットワーク分析ポリシーは、フェーズでのパケット処理を制御します。最初に、システムは最初の 3 つの TCP/IP 層を通ったパケットを復号化し、次にプロトコル異常の正規化、前処理、および検出に進みます。

- パケットデコーダは、パケットヘッダーとペイロードを、プリプロセッサや以降の侵入ルールで簡単に使用できる形式に変換します。TCP/IP スタックの各レイヤのデコードは、データリンク層から開始され、ネットワーク層、トランスポート層へと順番に行われます。パケット デコーダは、パケット ヘッダーのさまざまな異常動作も検出します。
- インライン展開では、インライン正規化プリプロセッサは、攻撃者が検出を免れる可能性を最小限にするために、トラフィックを再フォーマット（正規化）します。その他のプリプロセッサや侵入ルールによる検査用にパケットを準備し、システムで処理されるパケットがネットワーク上のホストで受信されるパケットと同じものになるようにします。

（注） パッシブな展開の場合、シスコでは、ネットワーク分析レベルでインライン正規化を行うのではなく、アクセス コントロール ポリシー レベルでアダプティブプロファイルを設定しことを推奨しています。

- ネットワーク層とトランスポート層のさまざまなプリプロセッサは、IPフラグメントを悪用する攻撃を検出したり、チェックサム検証を実行したり、TCP および UDP セッションの前処理を実行したりします。

  トランスポートおよびネットワーク プリプロセッサの一部の詳細設定は、アクセス コントロール ポリシーのターゲット デバイスで処理されるすべてのトラフィックにグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。

- 各種のアプリケーション層プロトコルデコーダは、特定タイプのパケットデータを侵入ルールエンジンで分析可能な形式に正規化します。アプリケーション層プロトコルのエンコードを正規化することにより、システムはデータ表現が異なるパケットに同じコンテンツ関連の侵入ルールを効果的に適用し、大きな結果を得ることができます。

- Modbus と DNP3 SCADA のプリプロセッサは、トラフィックの異常を検出し、データを侵入ルールに提供します。Supervisory Control and Data Acquisition（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャプロセス、および設備プロセスからのデータをモニタ、制御、取得します。

- 一部のプリプロセッサでは、Back Orifice、ポートスキャン、SYN フラッドおよび他のレートベース攻撃など、特定の脅威を検出できます。

  侵入ポリシーで、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出する機密データ プリプロセッサを設定することに注意してください。

新たに作成されたアクセス コントロール ポリシーでは、1 つのデフォルト ネットワーク分析ポリシーが、同じ親アクセスコントロールポリシーによって呼び出されるすべての侵入ポリシー向けのすべてのトラフィックの前処理を制御します。初期段階では、デフォルトで[バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] ネットワーク分析ポリシーが使用されますが、別のシステム付属ポリシーやカスタム ネットワーク分析ポリシーに変更できます。より複雑な展開では、上級ユーザは、一致するトラフィックの前処理にさまざまなカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN に合わせてトラフィックの前処理オプションを調整できます。

アクセス コントロール ルール：侵入ポリシーの選択

最初の前処理の後、トラフィックはアクセスコントロールルール（設定されている場合）によって評価されます。ほとんどの場合、パケットが一致する最初のアクセスコントロールルールがそのトラフィックを処理するルールとなります。一致するトラフィックをモニタ、信頼、ブロック、または許可できます。

アクセス コントロール ルールでトラフィックを許可すると、ディスカバリ データ、マルウェア、禁止ファイル、侵入について、この順序でトラフィックを検査できます。アクセス コントロール ルールに一致しないトラフィックは、アクセス コントロール ポリシーのデフォルト アクションによって処理されます。デフォルト アクションでは、ディスカバリ データと侵入についても検査できます。

（注） どのネットワーク分析ポリシーによって前処理されるかに**関わらず**、すべてのパケットは、設定されているアクセス コントロール ルールと上から順に照合されます（したがって、侵入ポリシーによる検査の対象となります）。

ポリシーが侵入についてトラフィックを検査する仕組み，（996 ページ） の図では、インラインの侵入防御と AMP for Firepower の展開における、デバイスを経由したトラフィック フローを示しています。

- アクセス コントロール ルール A により、一致したトラフィックの通過が許可されます。次にトラフィックは、ネットワーク検出ポリシーによるディスカバリ データの検査、ファイル ポリシー A による禁止ファイルおよびマルウェアの検査、侵入ポリシー A による侵入の検査を受けます。
- アクセス コントロール ルール B も一致したトラフィックを許可します。ただし、このシナリオでは、トラフィックは侵入（あるいはファイルまたはマルウェア）について検査されないので、ルールに関連付けられている侵入ポリシーやファイル ポリシーはありません。通過を許可されたトラフィックは、デフォルトでネットワーク検出ポリシーによって検査されます。したがって、この設定を行う必要はありません。
- このシナリオでは、アクセス コントロール ポリシーのデフォルト アクションで、一致したトラフィックを許可しています。次に、トラフィックはネットワーク検出ポリシー、さらにその後侵入ポリシーによって検査されます。アクセス コントロール ルールまたはデフォルトのアクションに侵入ポリシーを関連付けるときは、異なる侵入ポリシーを使用できます（ただし必須ではありません）。

ブロックされたトラフィックや信頼済みトラフィックは検査されないので、図の例には、ブロック ルールや信頼ルールは含まれていません。

侵入インスペクション：侵入ポリシー、ルール、変数セット

トラフィックが宛先に向かうことを許可する前に、システムの最終防御ラインとして侵入防御を使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーの主な機能は、どの侵入ルールおよびプリプロセッサ ルールを有効にしてどのように設定するかを管理することです。

侵入ルールおよびプリプロセッサ ルール

侵入ルールはキーワードと引数のセットとして指定され、ネットワーク上の脆弱性を悪用する試みを検出します。システムは侵入ルールを使用してネットワーク トラフィックを分析し、トラ

フィックがルールの条件に合致しているかどうかをチェックします。システムは各ルールで指定された条件をパケットに照らし合わせます。ルールで指定されたすべての条件にパケット データが一致する場合、ルールがトリガーされます。

システムには、Cisco Talos Security Intelligence and Research Group（Talos） によって作成された次のタイプのルールが含まれています。

- 共有オブジェクト侵入ルール：コンパイルされており、変更できません（ただし、送信元と宛先のポートや IP アドレスなどのルール ヘッダー情報を除く）
- 標準テキスト侵入ルール：ルールの新しいカスタムインスタンスとして保存および変更できます。
- プリプロセッサルール：ネットワーク分析ポリシーのプリプロセッサおよびパケットデコーダ検出オプションに関連付けられています。プリプロセッサ ルールはコピーまたは編集できません。ほとんどのプリプロセッサ ルールはデフォルトで無効になっています。プリプロセッサを使用して イベントを生成し、インライン展開では、違反パケットをドロップします。 するにはそれらを有効にする必要があります。

システムで侵入ポリシーに従ってパケットを処理する際には、最初にルール オプティマイザが、基準（トランスポート層、アプリケーション プロトコル、保護されたネットワークへの入出力方向など）に基づいて、サブセット内のすべてのアクティブなルールを分類します。次に、侵入ルール エンジンが、各パケットに適用する適切なルールのサブセットを選択します。最後に、マルチルール検索エンジンが 3 種類の検索を実行して、トラフィックがルールに一致するかどうかを検査します。

- プロトコル フィールド検索は、アプリケーション プロトコル内の特定のフィールドでの一致を検索します。
- 汎用コンテンツ検索は、パケット ペイロードの ASCII またはバイナリ バイトでの一致を検索します。
- パケット異常検索では、特定のコンテンツが含まれているかどうかではなく、確立されたプロトコルに違反しているパケット ヘッダーやペイロードが検索されます。

カスタム侵入ポリシーでは、ルールを有効化および無効化し、独自の標準テキスト ルールを記述および追加することで、検出を調整できます。Firepower 推奨機能を使用して、ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます。

変数セット

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セット使用します。セット内の大部分の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスとポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

システムには、定義済みのデフォルト変数から構成される 1 つのデフォルト変数セットが含まれています。システム提供の共有オブジェクト ルールと標準テキスト ルールは、これらの定義済みのデフォルト変数を使用してネットワークおよびポート番号を定義します。たとえば、ルールの

大半は、保護されたネットワークを指定するために変数 $HOME_NET を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 $EXTERNAL_NET を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Web サーバに対するエクスプロイトを検出するルールは、$HTTP_SERVERS 変数および $HTTP_PORTS 変数を使用します。

ヒント システム提供の侵入ポリシーを使用する場合でも、シスコでは、デフォルト セットの主要なデフォルト変数を変更すること**強く**推奨します。ネットワーク環境を正確に反映する変数を使用すると、処理が最適化され、システムによって疑わしいアクティビティに関連するシステムをモニタできます。高度なユーザは、1 つ以上のカスタム侵入ポリシーとペアリングするために、カスタム変数セットを作成して使用できます。

関連トピック

定義済みデフォルト変数, （400 ページ）

侵入イベントの生成

侵入されている可能性を特定すると、システムは侵入イベントまたはプリプロセッサ イベント（まとめて侵入イベントと呼ばれることもあります）を生成します。管理対象デバイスは、Firepower Management Center にイベントを送信します。ここで、集約データを確認し、ネットワーク アセットに対する攻撃を的確に把握できます。インライン展開では、管理対象デバイスは、有害であると判明しているパケットをドロップまたは置き換えることがきます。

データベース内の各侵入イベントにはイベント ヘッダーがあり、イベント名と分類、送信元と宛先の IP アドレス、ポート、イベントを生成したプロセス、およびイベントの日時に関する情報、さらに攻撃の送信元とそのターゲットに関するコンテキスト情報が含まれています。パケット ベースのイベントの場合、システムは復号化されたパケット ヘッダーとイベントをトリガーしたパケット（複数の場合あり）のペイロードのコピーもログに記録します。

パケットデコーダ、プリプロセッサ、および侵入ルールエンジンはすべて、システムによるイベントの生成を引き起こします。次に例を示します。

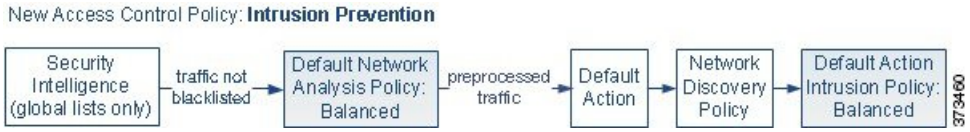
- （ネットワーク分析ポリシーで設定された）パケット デコーダが 20 バイト（オプションやペイロードのない IP データグラムのサイズ）未満の IP パケットを受け取った場合、デコーダはこれを異常なトラフィックと解釈します。パケットを検査する侵入ポリシー内の付随するデコーダ ルールが有効な場合、システムは後でプリプロセッサ イベントを生成します。
- IP 最適化プリプロセッサが重複する一連の IP フラグメントを検出した場合、プリプロセッサはこれを潜在的な攻撃と解釈して、付随するプリプロセッサ ルールが有効な場合、システムはプリプロセッサ イベントを生成します。
- 侵入ルール エンジン内では、ほとんどの標準テキスト ルールおよび共有オブジェクト ルールはパケットによってトリガーされた場合に侵入イベントを生成するように記述されます。

データベースに侵入イベントが蓄積されると、ユーザは攻撃の可能性について分析を開始できます。システムは、ユーザが侵入イベントを確認し、ネットワーク環境とセキュリティ ポリシーのコンテキストでそのイベントが重要であるかどうかを評価するために必要なツールを提供します。

システム提供およびカスタムのネットワーク分析ポリシーと侵入ポリシー

Firepowerシステムを使用してトラフィック フローを管理する最初のステップの1つは、新しいアクセス コントロール ポリシーを作成することです。デフォルトでは、新しく作成されたアクセス コントロール ポリシーは、システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーを呼び出してトラフィックを検査します。

次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理および侵入防御のフェーズが強調表示されています。



以下の点に注意してください。

- デフォルトのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が制御されます。初期段階では、システムによって提供される *Balanced Security and Connectivity* ネットワーク分析ポリシーがデフォルトです。
- アクセス コントロール ポリシーのデフォルト アクションがシステムによって提供される *Balanced Security and Connectivity* 侵入ポリシーで指定された通りに悪意のないすべてのトラフィックを許可する。デフォルトアクションはトラフィックの通過を許可するので、侵入ポリシーが悪意のあるトラフィックを検査して潜在的にブロックする前に、検出機能によって、ホスト、アプリケーション、ユーザ データについてトラフィックを検査できます。
- ポリシーは、デフォルトのセキュリティ インテリジェンス オプション（グローバルなホワイトリストとブラックリストのみ）を使用し、SSL ポリシーによる暗号化トラフィックの復号や、アクセス コントロール ルールによるネットワーク トラフィックの特別な処理や検査を実行しません。

侵入防御展開を調整するために実行できるシンプルなステップは、システム付属のネットワーク分析ポリシーと侵入ポリシーの別のセットをデフォルトとして使用することです。Firepowerシステムには、これらのポリシーの複数のペアが提供されています。

または、カスタム ポリシーを作成して使用することで、侵入防御展開を調整できます。それらのポリシーに設定されているプリプロセッサ オプション、侵入ルール、およびその他の詳細設定が、ネットワークのセキュリティ ニーズに適合しない場合があります。設定できるネットワーク分析ポリシーおよび侵入ポリシーを調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

システム提供のネットワーク分析ポリシーと侵入ポリシー

Firepowerシステムには、ネットワーク分析ポリシーと侵入ポリシーのペアがいくつか付属しています。システム提供のネットワーク分析ポリシーおよび侵入ポリシーを使用して、Cisco Talos Security Intelligence and Research Group（Talos） のエクスペリエンスを活用することができます。これらのポリシーでは、Talos が侵入ルールおよびプリプロセッサ ルールの状態、ならびにプリプロセッサおよび他の詳細設定の初期設定も指定しています。

システム提供のポリシーはいずれも、あらゆるネットワーク プロファイル、トラフィックの混合、防御ポスチャを網羅しているわけではありません。それぞれのポリシーは、十分に調整した防御ポリシーを作成するための出発点となるように、共通のケースとネットワーク設定をカバーしています。システム提供のポリシーをそのまま使用することもできますが、カスタム ポリシーのベースとして使用して、ネットワークに応じて調整することを強くお勧めします。

ヒント システム付属のネットワーク分析ポリシーと侵入ポリシーを使用する場合でも、ネットワーク環境が正確に反映されるように、システムの侵入変数を設定する必要があります。少なくとも、デフォルトのセットにある主要なデフォルトの変数を変更します。

新たな脆弱性が発見されると、Talosは侵入ルールの更新をリリースします。これらのルール更新により、システム付属のネットワーク分析ポリシーや侵入ポリシーが変更され、侵入ルールやプリプロセッサ ルールの新規作成または更新、既存ルールのステータスの変更、デフォルトのポリシー設定の変更が実施されます。ルールの更新では、システムによって提供されるポリシーからのルールが削除されたり、新しいルール カテゴリの提供やデフォルトの変数セットの変更が行われることがあります。

ルール更新によって展開が影響を受けると、Web インターフェイスは影響を受けた侵入ポリシーやネットワーク分析ポリシー、およびそれらの親のアクセスコントロールポリシーを失効したものとして扱います。変更を有効にするには、更新されたポリシーを再展開する必要があります。

必要に応じて、影響を受けた侵入ポリシーを（単独で、または影響を受けたアクセス コントロール ポリシーと組み合わせて）自動的に再展開するように、ルールの更新を設定できます。これにより、新たに検出されたエクスプロイトおよび侵入から保護するために展開環境を容易に自動的に最新に維持することができます。

前処理の設定を最新の状態に保つには、アクセスコントロールポリシーを再展開する**必要があります**。これにより、現在実行されているものとは異なる、関連する SSL ポリシー、ネットワーク分析ポリシー、ファイル ポリシーが再展開され、前処理とパフォーマンスの詳細設定オプションのデフォルト値も更新できるようになります。

Firepowerシステムに付属しているネットワーク分析ポリシーと侵入ポリシーのペアは以下のとおりです。

Balanced Security and Connectivity ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、速度と検出の両方を目的として作成されています。一緒に使用すると、ほとんどの組織および展開タイプにとって最適な出発点となります。ほとんどの場合、システムはBalanced Security and Connectivityのポリシーおよび設定をデフォルトとして使用します。

Connectivity Over Security ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、（すべてのリソースに到達可能な）接続がネットワーク インフラストラクチャのセキュリティよりも優先される組織向けに作成されています。この侵入ポリシーは、Security over Connectivity ポリシー内で有効になっているルールよりもはるかに少ないルールを有効にします。トラフィックをブロックする最も重要なルールだけが有効にされます。

Security over Connectivity ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、ネットワーク インフラストラクチャのセキュリティがユーザの利便性よりも優先される組織向けに作られています。この侵入ポリシーは、正式なトラフィックに対して警告またはドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。

Maximum Detection ネットワーク分析ポリシーおよび侵入ポリシー

このポリシーは、Security over Connectivity ポリシー以上にネットワーク インフラストラクチャのセキュリティを重視する組織のために作成されています。動作への影響がさらに高くなる可能性があります。たとえば、この侵入ポリシーでは、マルウェア、エクスプロイトキット、古い脆弱性や一般的な脆弱性、および既知の流行中のエクスプロイトを含め、多数の脅威カテゴリのルールを有効にします。

No Rules Active 侵入ポリシー

No Rules Active 侵入ポリシーでは、すべての侵入ルールと詳細設定が無効化されます。このポリシーは、他のシステムによって提供されるポリシーのいずれかで有効になっているルールをベースにするのではなく、独自の侵入ポリシーを作成する場合の出発点を提供します。

カスタム ネットワーク分析とカスタム侵入ポリシーの利点

システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーに設定されたプリプロセッサオプション、侵入ルール、およびその他の詳細設定は、組織のセキュリティニーズに十分に対応しない場合があります。

カスタム侵入ポリシーを作成すると、環境内のシステムのパフォーマンスを向上させ、ネットワークで発生する悪意のあるトラフィックやポリシー違反を重点的に観察できるようになります。設定できるカスタム ポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

すべてのカスタム ポリシーには基本ポリシー（別名「基本レイヤ」）があり、それによって、ポリシー内のすべてのコンフィギュレーションのデフォルト設定が定義されます。レイヤは、複数のネットワーク分析ポリシーまたは侵入ポリシーを効率的に管理するために使用できる構成要素です。

ほとんどの場合、カスタムポリシーはシステム付属のポリシーに基づきますが、別のカスタムポリシーを使用することもできます。ただし、すべてのカスタムポリシーには、ポリシーチェーンの根本的な基礎としてシステム付属ポリシーが含まれています。システム付属のポリシーはルールの更新によって変更される可能性があるので、カスタム ポリシーを基本として使用している場

合でも、ルールの更新をインポートするとポリシーに影響が及びます。ルール更新によって展開が影響を受けると、Web インターフェイスは影響を受けたポリシーを失効として扱います。

ユーザが作成するカスタム ポリシーに加えて、システムには、初期インライン ポリシーと初期パッシブ ポリシーという 2 つのカスタム侵入ポリシーと 2 つのネットワーク分析ポリシーが用意されています。これらのポリシーは、該当する [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] ポリシーを基本ポリシーとして使用します。両者の唯一の相違点はドロップ動作です。インライン ポリシーではトラフィックのブロックと変更が有効化され、パッシブポリシーでは無効化されます。これらのシステム提供のカスタムポリシーは編集して使用できます。

カスタム ネットワーク分析ポリシーの利点

デフォルトでは、1 つのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべての暗号化されていないトラフィックが前処理されます。これは、後でパケットを検査する侵入ポリシー（および侵入ルール セット）に関係なく、すべてのパケットが同じ設定に基づいて復号化および前処理されることを意味します。

初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。前処理を調整する簡単な方法は、カスタム ネットワーク分析ポリシーを作成し、それをデフォルトとして使用することです。

使用可能な調整オプションはプリプロセッサによって異なりますが、プリプロセッサおよびデコーダを調整できる方法には次のものがあります。

- モニタしているトラフィックに適用されないプリプロセッサを無効にできます。たとえば、HTTP Inspect プリプロセッサは HTTP トラフィックを正規化します。ネットワークに Microsoft インターネット インフォメーション サービス（IIS）を使用する Web サーバが含まれていないことが確実な場合は、IIS 特有のトラフィックを検出するプリプロセッサ オプションを無効にすることで、システム処理のオーバーヘッドを軽減できます。

（注） カスタム ネットワーク分析ポリシーでプリプロセッサが無効化されているときに、パケットを有効な侵入ルールまたはプリプロセッサ ルールと照合して評価するために、プリプロセッサを使用する必要がある場合、システムはプリプロセッサを有効化して使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効なままになります。

- 必要に応じて、特定のプリプロセッサのアクティビティを集中させるポートを指定します。たとえば、DNS サーバの応答や暗号化 SSL セッションをモニタするための追加ポートや、Telnet、HTTP、RPC トラフィックを復号化するポートを特定できます。

複雑な環境での高度なユーザの場合は、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを別々に前処理するように調整することができます。さらに、トラフィックのセキュリティ ゾーン、ネットワーク、または VLAN に応じて前処理が制御されるようにこれらのポリシーを設定できます（ASA FirePOWER モジュールでは、VLAN に応じて前処理を制限することはできません）。

（注） カスタム ネットワーク分析ポリシー（特に複数のネットワーク分析ポリシー）を使用して前処理を調整することは、高度なタスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一のパケットを検査するネットワーク分析ポリシーと侵入ポリシーが相互補完することを許可する場合は、注意する**必要があります**。

カスタム侵入ポリシーの利点

侵入防御を実行するように初期設定して、新規にアクセス コントロール ポリシーを作成した場合、そのポリシーでは、デフォルト アクションはすべてのトラフィックを許可しますが、最初にシステム付属の Balanced Security and Connectivity 侵入ポリシーでトラフィックをチェックします。アクセス コントロール ルールを追加するか、またはデフォルト アクションを変更しない限り、すべてのトラフィックがその侵入ポリシーによって検査されます。

侵入防御展開をカスタマイズするために、複数の侵入ポリシーを作成し、それぞれがトラフィックを異なる方法で検査するように調整できます。次に、どのポリシーがどのトラフィックを検査するかを指定するルールを、アクセス コントロール ポリシーに設定します。アクセス コントロール ルールは単純でも複雑でもかまいません。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、またはユーザなど、複数の基準を使用してトラフィックを照合および検査します。

侵入ポリシーの主な機能は、次のように、どの侵入ルールおよびプリプロセッサ ルールを有効にしてどのように設定するかを管理することです。

- 各侵入ポリシーで、環境に適用されるすべてのルールが有効になっていることを確認し、環境に適用されないルールを無効化することによって、パフォーマンスを向上させます。インライン展開では、どのルールによって悪質なパケットをドロップまたは変更するかを指定できます。
- Firepower 推奨機能を使用すると、ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます。
- 必要に応じて、既存のルールの変更や、新しい標準テキスト ルールの作成により、新たなエクスプロイトの検出やセキュリティ ポリシーの適用が可能です。

侵入ポリシーに対して行えるその他のカスタマイズは次のとおりです。

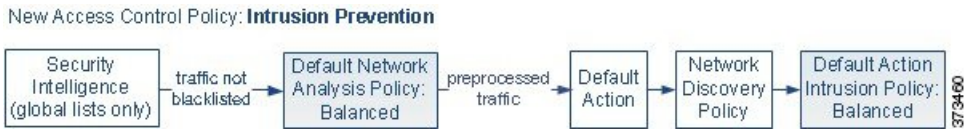
- 機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。特定の脅威（Back Orifice 攻撃、数種類のポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃）を検出するプリプロセッサは、ネットワーク分析ポリシーで設定します。
- グローバルしきい値を設定すると、侵入ルールに一致するトラフィックが、指定期間内に特定のアドレスまたはアドレス範囲で送受信される回数に基づいて、イベントが生成されます。これにより、大量のイベントによってシステムに過剰な負荷がかかることを回避できます。

- また、個々のルールまたは侵入ポリシー全体に対して、侵入イベント通知を抑制し、しきい値を設定することで、大量のイベントによってシステムに過剰な負荷がかかることを回避することもできます。
- Webインターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、syslogファシリティへのロギングを有効にしたり、イベント データを SNMP トラップ サーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギングファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。これらのポリシー単位のアラート設定に加えて、各ルールまたはルール グループの侵入イベントを通知する電子メール アラートをグローバルに有効化/無効化できます。どの侵入ポリシーがパケットを処理するかに関わらず、ユーザの電子メール アラート設定が使用されます。

カスタム ポリシーの制限

前処理および侵入インスペクションは密接に関連しているため、単一パケットを処理して検査するネットワーク分析ポリシーと侵入ポリシーが互いに補完することを許可する設定を行う場合は慎重になる**必要があります**。

デフォルトでは、システムは、管理対象デバイスでアクセス コントロール ポリシーにより処理されるすべてのトラフィックを、1 つのネットワーク分析ポリシーを使用して前処理します。次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理および侵入防御のフェーズが強調表示されています。



アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が、デフォルトのネットワーク分析ポリシーによってどのように制御されるのか注意してください。初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。

前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。ただし、カスタム ネットワーク分析ポリシーでプリプロセッサが無効化されているときに、前処理されたパケットを有効な侵入ルールまたはプリプロセッサ ルールと照合して評価する必要がある場合、システムはプリプロセッサを有効化して使用します。ただし、ネットワーク分析ポリシーの Web ユーザ インターフェイスではプリプロセッサは無効なままになります。

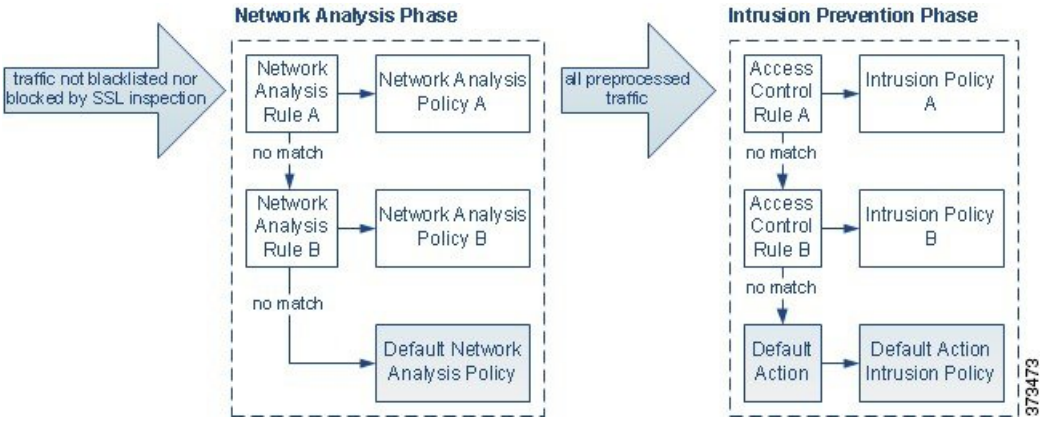
（注） プリプロセッサを無効にするパフォーマンス上の利点を得るには、侵入ポリシーでそのプリプロセッサを必要とするルールが有効になっていないことを確認する**必要があります**。

複数のカスタム ネットワーク分析ポリシーを使用する場合は、さらに課題があります。複雑な展開内の上級ユーザの場合は、一致したトラフィックの前処理にカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN に合わせて前処理を調整できます。（ただし、ASA FirePOWER VLAN による前処理を制限できません）。これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。各ルールにはネットワーク分析ポリシーが関連付けられており、ルールに一致するトラフィックの前処理を制御します。

ヒント アクセス コントロール ポリシーの詳細設定としてネットワーク分析ルールを設定します。Firepower システムの他のタイプのルールとは異なり、ネットワーク分析ルールは、ネットワーク分析ポリシーに含まれるのではなく、ネットワーク分析ポリシーを呼び出します。

システムは、ルール番号の昇順で、設定済みネットワーク分析ルールとパケットを照合します。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。これにより非常に柔軟にトラフィックを前処理できます。ただし、留意すべき点として、パケットがどのネットワーク分析ポリシーによって前処理されるかに**関係なく**、すべてのパケットは、それら独自のプロセスにおいて引き続きアクセス コントロール ルールと照合されます（つまり、侵入ポリシーにより検査される可能性があります）。つまり、特定のネットワーク分析ポリシーでパケットを前処理しても、そのパケットが確実に特定の侵入ポリシーで検査されるわけでは**ありません**。アクセス コントロール ポリシーを設定するときは、そのポリシーが正しいネットワーク分析ポリシーおよび侵入ポリシーを呼び出して特定のパケットを評価するように、慎重に行う**必要があります**。

次の図は、侵入防御（ルール）フェーズよりも前に、別にネットワーク分析ポリシー（前処理）の選択フェーズが発生するしくみを詳細に示しています。簡略化するために、図では検出フェーズとファイル/マルウェア インスペクション フェーズが省かれています。また、デフォルトのネットワーク分析ポリシーおよびデフォルト アクションの侵入ポリシーを強調表示しています。



このシナリオでは、アクセス コントロール ポリシーは、2 つのネットワーク分析ルールとデフォルトのネットワーク分析ポリシーで設定されています。

- Network Analysis Rule A は、一致するトラフィックを Network Analysis Policy A で前処理します。その後、このトラフィックを Intrusion Policy A で検査されるようにすることができます。

- Network Analysis Rule B は、一致するトラフィックを Network Analysis Policy B で前処理します。その後、このトラフィックを Intrusion Policy B で検査されるようにすることができます。
- 残りのトラフィックはすべて、デフォルトのネットワーク分析ポリシーにより前処理されます。その後、このトラフィックをアクセス コントロール ポリシーのデフォルト アクションに関連付けられた侵入ポリシーによって検査されるようにすることができます。

システムはトラフィックを前処理した後、侵入についてトラフィックを検査できます。図では、2 つのアクセス コントロール ルールとデフォルト アクションが含まれるアクセス コントロール ポリシーを示しています。

- アクセス コントロール ルール A は、一致したトラフィックを許可します。トラフィックはその後、Intrusion Policy A によって検査されます。
- アクセス コントロール ルール B は、一致したトラフィックを許可します。トラフィックはその後、Intrusion Policy B によって検査されます。
- アクセス コントロール ポリシーのデフォルト アクションは一致したトラフィックを許可します。トラフィックはその後、デフォルト アクションの侵入ポリシーによって検査されます。

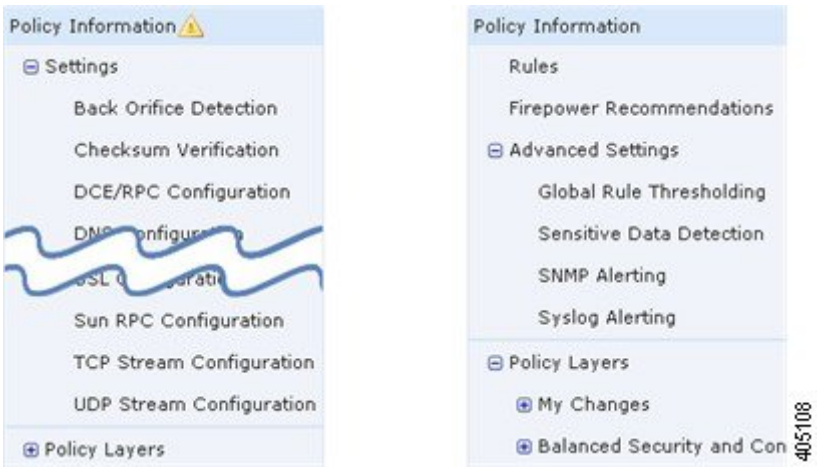
各パケットの処理は、ネットワーク分析ポリシーと侵入ポリシーのペアにより制御されますが、このペアはユーザに合わせて調整**されません**。アクセス コントロール ポリシーが誤って設定されているため、ネットワーク分析ルール A とアクセス コントロール ルール A が同じトラフィックを処理しない場合を想定してください。たとえば、特定のセキュリティ ゾーンのトラフィックの処理をポリシー ペアによって制御することを意図している場合に、誤まって、異なるゾーンを使用するように 2 つのルールの条件を設定したとします。この誤設定により、トラフィックが誤って前処理される可能性があります。したがって、ネットワーク分析ルールおよびカスタム ポリシーを使用した前処理の調整は、**高度な**タスクです。

単一の接続の場合は、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、一部の前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定には影響**しません**。

ナビゲーション ウィンドウ: ネットワーク分析と侵入ポリシー

ネットワーク分析ポリシーと侵入ポリシーは同様の Web インターフェイスを使用して、設定への変更を編集して保存します。

いずれかのタイプのポリシーを編集するときに、Web インターフェイスの左側にナビゲーション パネルが表示されます。次の図は、ネットワーク分析ポリシー（左）および侵入ポリシー（右）のナビゲーション パネルを示しています。



ナビゲーション パネルは境界線によって複数のポリシー設定項目リンクに分割されており、ポリシー層との直接対話により（下側）または直接対話なしで（上側）ポリシー設定項目を設定できます。いずれかの設定ページに移動するには、ナビゲーション パネル内の名前をクリックします。ナビゲーション パネルで影付きで強調表示されている項目は、現在の設定ページを示しています。たとえば、上の図では、[ポリシー情報（Policy Information）] ページがナビゲーション パネルの右側に表示されます。

[ポリシー情報（Policy Information）]

[ポリシー情報（Policy Information）]ページには、一般的に使用される設定の設定オプションが示されます。上記のネットワーク分析ポリシー パネルの図に示すように、ポリシーに未保存の変更がある場合は、ナビゲーション パネルの [ポリシー情報（Policy Information）] の横にポリシー変更アイコン（⚠）が表示されます。アイコンは、変更を保存すると消えます。

[ルール（Rules）]（侵入ポリシーのみ）

侵入ポリシーの [ルール（Rules）]ページでは、共有オブジェクト ルール、標準テキスト ルール、およびプリプロセッサ ルールのルール ステータスとその他の設定項目を設定できます。

[Firepower の推奨事項（Firepower Recommendations）]（侵入ポリシーのみ）

侵入ポリシーの [Firepower の推奨事項（Firepower Recommendations）] ページでは、ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。

[Settings]（ネットワーク分析ポリシー）および [Advanced Settings]（侵入ポリシー）

ネットワーク分析ポリシーの [設定（Settings）]ページでは、プリプロセッサを有効または無効にしたり、プリプロセッサの設定ページにアクセスしたりできます。[設定（Settings）] リンクを展開すると、ポリシー内で有効になっているすべてのプリプロセッサの個々の設定ページへのサブリンクが表示されます。

侵入ポリシーの [詳細設定（Advanced Settings）] ページでは、詳細設定を有効または無効にしたり、詳細設定の設定ページにアクセスしたりできます。[詳細設定（Advanced Settings）] リンクを展開すると、ポリシー内で有効になっているすべての詳細設定を個々に設定する設定ページへのサブリンクが表示されます。

[Policy Layers]

[ポリシー層（Policy Layers）] ページには、ネットワーク分析ポリシーまたは侵入ポリシーを構成する階層の要約が表示されます。[ポリシー層（Policy Layers）] リンクを展開すると、ポリシー内の階層に関する概要ページへのサブリンクが表示されます。各階層のサブリンクを展開すると、その階層で有効になっているすべてのルール、プリプロセッサ、または詳細設定の設定ページへのサブリンクがさらに表示されます。

競合と変更：ネットワーク分析ポリシーと侵入ポリシー

ネットワーク分析ポリシーや侵入ポリシーを編集するときに、ポリシーに未保存の変更がある場合は、そのことを示すために、ナビゲーション パネルの [ポリシー情報（Policy Information）] の横にポリシー変更アイコン（⚠）が表示されます。変更をシステムに認識させるには、変更を保存（確定）する必要があります。

（注） 保存後は、変更を反映させるためにネットワーク分析ポリシーまたは侵入ポリシーを展開する必要があります。保存しないでポリシーを展開すると、最後に保存された設定が使用されます。

編集競合の解決

[ネットワーク分析ポリシー（Network Analysis Policy）] ページ（[ポリシー（Policies）] > [アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。）および [侵入ポリシー（Intrusion Policy）] ページ（[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]）には、各ポリシーの未保存の変更の有無、および現在ポリシーを編集中のユーザ情報が表示されます。シスコでは、同時に 1 人だけがポリシーを編集することを推奨します。同時編集を実行すると、次のようになります。

- ネットワーク分析ポリシーまたは侵入ポリシーを編集しているときに、同時に他のユーザが同じポリシーを編集し、ポリシーへの変更を保存した場合、ポリシーを確定すると、他のユーザの変更が上書きされることを警告するメッセージが表示されます。
- 同じユーザとして複数の Web インターフェイス インスタンス経由で同じネットワーク分析ポリシーまたは侵入ポリシーを編集中に、1 つのインスタンスの変更を保存すると、他のインスタンスの変更は保存できません。

設定の依存関係の解決

特定の分析を実行する場合、多くのプリプロセッサルールとセキュリティルールでは、最初に特定の方法でトラフィックをデコードまたは前処理するか、他の依存関係を割り当てる必要があります。ネットワーク分析ポリシーまたは侵入ポリシーを保存すると、システムが必要な設定を自動的に有効にするか、または次のように無効な設定はトラフィックに影響しないことが警告されます。

- SNMP ルール アラートを追加しても、SNMP アラートを設定しなかった場合は、侵入ポリシーを保存できません。SNMPアラートを設定するか、またはルールアラートを無効にしてから、再度保存します。
- 侵入ポリシーに有効なセンシティブデータ ルールが含まれているときに、センシティブデータプリプロセッサが有効になっていない場合は、侵入ポリシーを保存できません。システムがプリプロセッサを有効にしてポリシーを保存するように許可するか、またはルールを無効にしてから、再度保存します。
- ネットワーク分析ポリシーで必要なプリプロセッサを無効にしても、ポリシーを引き続き保存できます。ただし、ネットワーク分析ポリシーのWebインターフェイスでプリプロセッサは無効になっていても、システムは無効になっているプリプロセッサを自動的に現在の設定で使用します。
- ネットワーク分析ポリシーでインラインモードを無効にしても、インライン正規化プリプロセッサが有効になっている場合は、ポリシーを引き続き保存できます。ただし、正規化設定が無視されることが警告されます。インライン モードを無効化すると他の設定が無視されるので、プリプロセッサは、チェックサム検証やレートベース攻撃の防御を含めて、トラフィックを変更またはブロックできます。

ポリシー変更のコミット、破棄、およびキャッシュ

ネットワーク分析ポリシーまたは侵入ポリシーの編集時に、変更を保存しないでポリシー エディタを終了した場合、それらの変更はシステムによってキャッシュされます。システムからログアウトした場合や、システム クラッシュが発生した場合でも、変更はキャッシュされます。システム キャッシュには、ユーザごとに 1 つのネットワーク分析ポリシーと 1 つの侵入ポリシーの未保存の変更しか格納されないため、同じタイプの別のポリシーを編集する場合は、その前に、行った変更を確定または破棄する必要があります。システムは、ユーザが最初のポリシーへの変更を保存せずに別のポリシーを編集したり、侵入ルールの更新をインポートした場合に、キャッシュされた変更内容を破棄します。

ネットワーク分析ポリシー エディタまたは侵入ポリシー エディタの [ポリシー情報（Policy Information）] ページでポリシーの変更内容をコミットまたは破棄できます。

Firepower Management Center 設定では、以下を制御できます。

- ネットワーク分析ポリシーまたは侵入ポリシーへの変更を確定するときに、それに関するコメントの入力を求めるか（または、コメントの入力を必須とするか）
- 変更内容とコメントを監査ログに記録するか

関連トピック

ネットワーク解析ポリシーの設定の構成
侵入ポリシー設定の構成

ネットワーク分析または侵入ポリシーの終了

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

手順

ネットワーク分析、または侵入ポリシーの拡張エディタを終了するには、以下の方法があります。

- キャッシュ：ポリシーを終了し、変更をキャッシュするには、いずれかのメニューを選択するか、別のページへのほかのパスを選択します。終了時に表示される [ページを移動（Leave page）] をクリックするか、[ページを移動しない（Stay on page）] をクリックして拡張エディタに残ります。
- 破棄：保存されていない変更を破棄するには、[ポリシー情報（Policy Information）] ページの [変更の破棄（Discard Changes）] をクリックし、[OK] をクリックします。
- 保存：ポリシーの変更を保存するには、[ポリシー情報（Policy Information）] ページの [変更の確定（ommit Changes）] をクリックします。プロンプトが表示される場合、コメントを入力し、[OK] をクリックします。

第 48 章

侵入ポリシーおよびネットワーク分析ポリシーのレイヤ

以下のトピックでは、侵入ポリシーおよびネットワーク分析ポリシーでレイヤ（層）を使用する方法について説明します。

レイヤの基本

多数の管理対象デバイスが存在する大規模な組織では、さまざまな部署や事業部門、場合によってはさまざまな企業の固有のニーズをサポートするために、多数の侵入ポリシーやネットワーク分析ポリシーが存在することがあります。両方のポリシー タイプでの設定はレイヤと呼ばれる構成要素に含まれており、それを使用することで効率的に複数のポリシーを管理することができます。

侵入ポリシーおよびネットワーク分析ポリシーのレイヤは、原則的に同じ方法で動作します。ポリシー タイプの作成および編集は、レイヤを意識せずに行えます。ポリシー設定を変更でき、ポリシーにユーザ レイヤを追加していない場合は、システムによって自動的に変更内容が単一の設定可能なレイヤ（最初は*My Changes* という名前が付けられています）に含められます。また、最大 200 までレイヤを追加して、それらのレイヤで設定を任意に組み合わせて構成することもできます。ユーザ レイヤのコピー、マージ、移動、削除を実行できます。最も重要なこととして、個々のユーザ レイヤを同じタイプの他のポリシーと共有できます。

レイヤ スタック

レイヤ スタックは、次の各レイヤから構成されています。

ユーザ レイヤ

ユーザ設定可能なレイヤです。ユーザ設定可能なレイヤは、コピー、マージ、移動、または削除を行うことができます。また、任意のユーザ設定可能なレイヤが同じタイプの他のポリシーと共有されるように設定することもできます。このレイヤには、最初に My Changes という名前が付けられた自動生成されたレイヤが含まれています。

組み込み型レイヤ

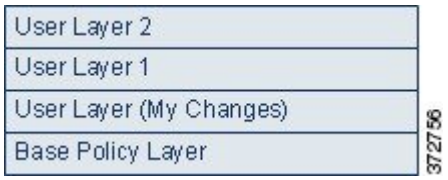
読み取り専用の基本ポリシー レイヤです。このレイヤ内のポリシーは、システムによって提供されるポリシー、または自分で作成したカスタム ポリシーにできます。

ネットワーク分析ポリシーまたは侵入ポリシーには、デフォルトでは基本ポリシー レイヤと My Changes レイヤが含まれています。ユーザ レイヤは必要に応じて追加できます。

各ポリシー レイヤには、ネットワーク分析ポリシー内のすべてのプリプロセッサまたは侵入ポリシー内のすべての侵入ルールと詳細設定の完全な設定が含まれます。最下部の基本ポリシー レイヤには、ポリシーの作成時に選択した基本ポリシーのすべての設定が含まれます。上位レイヤの設定は、下位レイヤの同じ設定よりも優先されます。レイヤで明示的に設定されていない機能は、明示的に設定されている次の高いレイヤから設定を継承します。システムはレイヤをフラット化します。つまり、ネットワーク トラフィックの処理時にすべての設定の蓄積効果のみを適用します。

ヒント 侵入またはネットワークの分析ポリシーは、基本ポリシーのデフォルト設定のみに基づいて作成できます。侵入ポリシーの場合に、モニタ対象ネットワークの特定のニーズに合わせて侵入ポリシーを調整したいときは、Firepower のルール状態の推奨を使用することもできます。

次の図は、基本ポリシー レイヤと初期設定の My Changes レイヤの他に、2 つの追加のユーザ設定可能なレイヤ *User Layer 1* と *User Layer 2* も含まれているレイヤ スタックの例を示しています。この図では、ユーザが追加したユーザ設定可能なレイヤそれぞれがスタックの最上位レイヤとして最初に配置されるため、図内の User Layer 2 が最後に追加されたもので、このスタックの最上位になっていることに注目してください。



ルール更新にポリシーの変更を許可しているかどうかに関わらず、ルール更新での変更は、レイヤで行った変更を上書きしません。これは、ルール更新での変更が、基本ポリシー レイヤのデフォルト設定を決定する基本ポリシーで行われるためです。変更は常により上位のレイヤに加えられ、その変更によって、ルール更新が基本ポリシーに加えた変更が上書きされます。

基本レイヤ

侵入ポリシーまたはネットワーク分析ポリシーの基本レイヤ（基本ポリシーとも呼ばれる）は、ポリシーのすべての設定のデフォルト設定を定義し、ポリシーの最下位に位置します。新しいポリシーを作成し、新しいレイヤを追加しないで設定を変更すると、その変更はMy Changesレイヤに保存され、基本ポリシーの設定を上書きしますが変更はしません。

システム提供の基本ポリシー

Firepowerシステムには、ネットワーク分析ポリシーと侵入ポリシーのペアがいくつか提供されています。システム提供のネットワーク分析ポリシーおよび侵入ポリシーを使用して、Cisco Talos Security Intelligence and Research Group（Talos） のエクスペリエンスを活用することができます。これらのポリシーでは、Talosは侵入ルールおよびプリプロセッサ ルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。これらのシステムによって提供されるポリシーをそのまま使用したり、カスタム ポリシーのベースとして使用することができます。

システムによって提供されるポリシーをベースとして使用する場合、ルール更新をインポートすると、基本ポリシー内の設定が変更される場合があります。ただし、カスタム ポリシーを設定して、これらの変更内容がシステム提供の基本ポリシーに自動的に反映されないようにすることもできます。これにより、ルール更新とは関係ないスケジュールで、システム提供の基本ポリシーを手動で更新できます。いずれの場合も、ルール更新が基本ポリシーに加えた変更によってMy Changesまたは他のレイヤの設定が変更または上書きされることはありません。

システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。

カスタム基本ポリシー

カスタムポリシーを基本（ベース）として使用することができます。カスタムポリシーの設定を調整することで、最も役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

別のポリシーのベースとして使用するカスタム ポリシー変更すると、変更内容はこのベースを使用するポリシーのデフォルト設定として自動的に使用されます。

また、ポリシーはすべて、システムが提供するポリシーをポリシー チェーンにおける最終的なベースとしているため、たとえカスタム基本ポリシーを使っていても、ルールが更新されればポリシーに影響する可能性があります。チェーン内の最初のカスタム ポリシー（システムによって提供されるポリシーをベースとして使用するポリシー）によってルール更新がその基本ポリシーを変更することが許可されている場合は、ポリシーが影響を受ける可能性があります。

基本ポリシーがどのように変更されたかに関わらず（ルール更新による変更でも、基本ポリシーとして使用するカスタムポリシーを変更でも）、ユーザの基本ポリシーに対する変更によってMy Changesやその他のレイヤの設定が変更または上書きされることはありません。

基本ポリシーに対するルール更新の影響

ルール更新をインポートすると、システム提供の侵入ポリシー、アクセス コントロール ポリシー、ネットワーク分析ポリシーが変更されます。ルール更新には次の要素が含まれる場合があります。

- 変更されたネットワーク分析プリプロセッサの設定
- 変更された侵入ポリシーおよびアクセス コントロール ポリシーの詳細設定
- 新規または更新された侵入ルール
- 既存のルールの変更された状態
- 新しいルール カテゴリとデフォルト変数

ルール更新により、既存のルールがシステム提供のポリシーから削除される場合もあります。

デフォルト変数とルール カテゴリに対する変更はシステム レベルで処理されます。

システム提供のポリシーを侵入またはネットワーク分析の基本ポリシーとして使用するときは、ルール更新が基本ポリシー（この場合はシステムによって提供されるポリシーのコピー）を変更することを許可することができます。ルール更新で基本ポリシーの更新を許可する場合は、新しいルール更新によって、基本ポリシーとして使用するシステム提供のポリシーに対する変更と同じ変更が基本ポリシーにも加えられます。対応する設定を変更しなかった場合は、基本ポリシー内の設定によって、ポリシー内の設定が決定されます。ただし、ルール更新では、ポリシー内で行った変更は上書きされません。

ルール更新による基本ポリシーの変更を許可しない場合は、1 つ以上のルール更新のインポート後に、基本ポリシーを手動で更新できます。

ルール更新では、侵入ポリシー内のルール状態またはルール更新による基本の侵入ポリシーの変更が許可されているかどうかに関係なく、Talos が削除する侵入ルールが常に削除されます。

ネットワーク トラフィックに変更を再展開するまで、現在展開されている侵入ポリシー ルールは次のように動作します。

- 無効になっている侵入ルールは無効のままになります。
- [イベントを生成する（Generate Events）] に設定されたルールでは、トリガーされたときのイベントの生成が継続されます。
- [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールでは、トリガーされたときのイベントの生成と違反パケットのドロップが継続されます。

次の両方の条件が満たされていない限り、ルール更新でカスタム基本ポリシーは変更されません。

- ルール更新が親ポリシーのシステムによって提供される基本ポリシー（つまり、カスタム基本ポリシーの起源となるポリシー）を変更することを許可している。
- 親の基本ポリシー内の対応する設定が上書きされる親ポリシー内の変更を実施していない。

両方の条件が満たされている場合は、親ポリシーを保存したときに、ルール更新内の変更が子ポリシー（つまり、カスタム基本ポリシーを使用したポリシー）に渡されます。

たとえば、ルール更新で以前に無効になっていた侵入ルールを有効にして、親の侵入ポリシー内のルール状態を変更していない場合は、親ポリシーを保存したときに、変更されたルール状態が基本ポリシーに渡されます。

同様に、ルール更新でデフォルトのプリプロセッサ設定を変更し、親のネットワーク分析ポリシーの設定を変更していない場合は、変更された設定は親ポリシーを保存したときに基本ポリシーに渡されます。

ベースポリシーの変更

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

別のシステム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

最大 5 つのカスタム ポリシーをチェーンすることができます。5 つのうちの 4 つのポリシーで事前に作成されたポリシーが基本ポリシーとして使用され、5 つ目のポリシーでシステムによって提供されたポリシーをベースとして使用する必要があります。

手順

ステップ 1 ポリシーの編集中に、ナビゲーション パネルで [ポリシー情報（Policy Information）] をクリックします。

ステップ 2 次の選択肢を設定できます。

- 基本ポリシーを選択する：[基本ポリシー（Base Policy）] ドロップダウンリストから選択します。
- ベースポリシーを変更するルール更新を許可する：[ベースポリシーの管理（Manage Base Policy）] をクリックし、[新しいルール更新のインストールでポリシーを更新する（Update when a new Rule Update is installed）] チェックボックスをオンにします。

  ヒント このチェックボックスをオフにしてポリシーを保存してから、ルール更新をインポートすると、[基本ポリシー（Base Policy）] 概要ページに [今すぐ更新（Update Now）] ボタンが表示され、そのページ上のステータス メッセージが更新されて、ポリシーが期限切れであることが示されます。最近インポートしたルール更新内の変更で基本ポリシーを更新するには、[今すぐ更新（Update Now）] をクリックします。

ステップ 3 最後のコミットからポリシーに加えられた変更を保存するには、[ポリシー情報（Policy information）] をクリックし、次に [変更をコミット（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

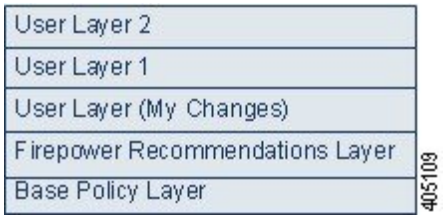
関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

Firepower 推奨レイヤ

侵入ポリシーでルール状態の推奨を生成する場合は、その推奨に基づいてルール状態を自動的に変更するかどうかを選択できます。

下記の図に示すように、推奨されたルール状態を使用すると、侵入ポリシーの基本レイヤのすぐ上に読み取り専用の組み込み Firepower 推奨レイヤが挿入されます。



このレイヤは侵入ポリシー固有のものです。

それ以後、推奨されたルール状態を使用しないことを選択すると、Firepower 推奨レイヤは削除されます。このレイヤは手動で削除できませんが、推奨されるルール状態を使用するかどうかを選択することで、サービスを追加したり削除することができます。

Firepower 推奨レイヤを追加すると、ナビゲーション パネルの [ポリシー階層（Policy Layers）] の下に Firepower 推奨リンクが追加されます。このリンクから Firepower 推奨レイヤ ページの読み取り専用ビューにアクセスして、[ルール（Rules）] ページの推奨でフィルタリングされたビューを読み取り専用モードで表示できます。

推奨されたルール状態を使用すると、ナビゲーション パネルの Firepower 推奨リンクの下に [ルール（Rules）] サブリンクも追加されます。[ルール（Rules）] サブリンクから、Firepower 推奨レイヤの [ルール（Rules）] ページの読み取り専用画面にアクセスできます。このビューでは次の点に注意してください。

- 状態列にルール状態のアイコンがない場合、状態は基本ポリシーから継承されます。
- このビューまたは他の [ルール（Rules）] ページ ビューの Firepower 推奨列にルール状態のアイコンがない場合、このルールに対する推奨は存在しません。

関連トピック

ネットワーク資産に応じた侵入防御の調整, （1077 ページ）

レイヤ管理

[ポリシー層（Policy Layers）]ページには、ネットワーク分析ポリシーまたは侵入ポリシーの完全なレイヤ スタックの単一ページの概要が示されます。このページでは、共有レイヤおよび非共有レイヤの追加、レイヤのコピー、マージ、移動、および削除、各レイヤの概要ページへのアクセス、各レイヤ内の有効、無効、および上書きされている設定の設定ページへのアクセスを行うことができます。

各レイヤについて、次の情報が表示されます。

- レイヤが組み込み型レイヤ、共有ユーザ レイヤ、または非共有ユーザ レイヤであるかどうか
- どのレイヤに最上位の（つまり効果的な）プリプロセッサまたは詳細設定が含まれているか（機能名別に）
- 侵入ポリシーで、状態がレイヤで設定されている侵入ルールの数、および各ルール状態に設定されているルールの数

[ポリシー層（Policy Layers）]ページには、有効なすべてのプリプロセッサ（ネットワーク分析）または詳細設定（侵入）、また侵入ポリシーの場合は侵入ルールの最終的な効果の概要も示されます。

各レイヤのサマリーにある機能名は、以下のように、設定がレイヤで有効、無効、上書き、または継承されているかを示します。

機能の状態	機能名
レイヤで有効	プレーン テキストで表示
レイヤで無効	取り消し線が引かれる
上位レイヤの設定によって上書きされる	イタリック テキストで表示
下位レイヤから継承される	表示されない

最大 200 のレイヤをネットワーク分析ポリシーまたは侵入ポリシーに追加できます。レイヤを追加すると、ポリシーで最上位レイヤとして表示されます。初期状態はすべての機能に対して[継承（Inherit）] で、侵入ポリシーでは、イベントのフィルタリング、動的状態、またはルール アクションのアラートは設定されません。

レイヤをポリシーに追加する際は、ユーザが設定可能なレイヤに一意の名前を指定します。その名前は後で変更できます。また、必要に応じて、レイヤを編集する際に表示される説明を追加あるいは変更することもできます。

レイヤはコピーすることも、[ユーザ レイヤ（User Layers）] ページ内での表示位置を上下に移動することもできます。また、初期の My Changes レイヤを含め、ユーザ レイヤを削除することも可能です。次の考慮事項に注意してください。

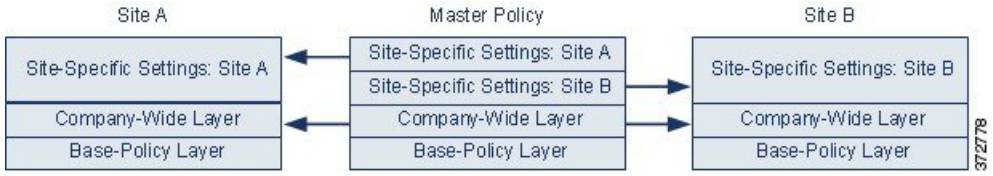
- レイヤをコピーすると、そのコピーが最上位レイヤとして表示されます。
- 共有レイヤをコピーすると、初期状態ではそのレイヤは共有されませんが、必要に応じて、後から共有できます。
- 共有レイヤは削除できません。共有が有効になっているレイヤで別のポリシーと共有していないものは、共有レイヤではありません。

ユーザ設定可能なレイヤの直下に、別のユーザ設定可能なレイヤをマージできます。マージされたレイヤは、どちらかのレイヤに固有だったすべての設定を保持します。また、両方のレイヤに同じプリプロセッサ、侵入ルール、または詳細設定が含まれていた場合、上位のレイヤの設定を受け入れます。マージされたレイヤでは、下位レイヤの名前が保持されます。他のポリシーに追加できる共有可能なレイヤを作成するポリシーでは、共有可能なレイヤのすぐ上に非共有レイヤのある共有可能なレイヤをマージできますが、共有可能なレイヤの直下には非共有レイヤのある共有可能なレイヤをマージすることはできません。別のポリシーに作成した共有レイヤを追加するポリシーでは、共有レイヤをそのすぐ下の非共有レイヤとマージできますが、作成されたレイヤは共有されなくなります。非共有レイヤをその下の共有レイヤとマージすることはできません。

共有レイヤ

共有レイヤとは、あるポリシー内で作成して共有を許可し、別のポリシーに追加されたレイヤのことです。共有可能レイヤとは、共有が許可されているレイヤのことです。

以下の図に示すマスター ポリシーの例では、全社的レイヤと、サイト A およびサイト B に固有のレイヤを作成し、これらのサイト固有のレイヤの共有を許可しています。その上で、これらのサイト固有のレイヤを共有レイヤとしてサイト A とサイト B のポリシーに追加しています。



マスター ポリシーの全社的なレイヤには、サイト A とサイト B に適用される設定が含まれる一方、サイト固有のレイヤには各サイトに固有の設定が含まれています。たとえば、ネットワーク分析ポリシーの場合、サイト A にはモニタ対象ネットワークに Web サーバがないため、保護したり、HTTP インスペクション プリプロセッサのオーバーヘッドを処理したりする必要はありませんが、両方のサイトで TCP ストリームの前処理が必要になる場合があります。両方のサイトで共有する全社的レイヤで TCP ストリーム処理を有効にし、サイト A で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを無効にして、サイト B で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを有効にできます。サイト固有のポリシーで上位レイヤの設定を編集することで、必要に応じて、設定の調整によって各サイトのポリシーをさらに調整することもできます。

この例のマスター ポリシーでフラット化された設定値そのものがトラフィックをモニタするのに役立つわけではありませんが、サイト固有のポリシーを設定および更新する際に時間が節約されるため、ポリシー階層で活用することができます。

その他にも多くのレイヤ設定が可能です。たとえば、企業、部門、ネットワーク、さらにはユーザごとにポリシー階層を定義できます。侵入ポリシーの場合は、一方のレイヤに詳細設定を含め、もう一方にルール設定を含めることもできます。

ユーザ設定可能なレイヤを同じタイプの他のポリシー（侵入またはネットワーク分析）と共有できるように設定できます。共有可能レイヤ内の設定を変更し、変更をコミットすると、そのレイヤを共有するすべてのポリシーが更新され、影響を受けたすべてのポリシーのリストが提供されます。レイヤを作成したポリシーの機能設定のみを変更できます。

別のポリシーに追加しているレイヤの共有を無効にすることはできません。まずレイヤを他のポリシーから削除するか、他のポリシーを削除する必要があります。

基本ポリシーが共有するレイヤが作成されたカスタム ポリシーである場合、ポリシーに共有レイヤを追加することはできません。追加した場合、ポリシーで依存関係が循環することになります。

マルチドメイン展開では、先祖ポリシーの共有レイヤを子孫ドメインのポリシーに追加できます。

レイヤの管理

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

手順

ステップ 1 ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。

ステップ 2 [ポリシー層（Policy Layers）] ページでは、次に示す管理アクションを実行できます。

- 別のポリシーからの共有レイヤの追加：[ユーザ レイヤ（User Layers）] の横にある共有レイヤの追加アイコン（  ）をクリックし、[共有レイヤの追加（Add Shared Layer）] ドロップダウンリストからレイヤを選択して、[OK] をクリックします。
- 非共有レイヤの追加：[ユーザ レイヤ（User Layers）] の横にあるレイヤの追加アイコン（  ）をクリックし、[名前（Name）] を入力して、[OK] をクリックします。
- レイヤの説明の追加または変更：レイヤの横にある編集アイコン（  ）をクリックして、[説明（Description）] を追加または変更します。
- 別のポリシーとのレイヤの共有の許可：レイヤの横にある編集アイコン（  ）をクリックして、[共有（Sharing）] チェックボックスをオフにします。
- レイヤの名前の変更：レイヤの横にある編集アイコン（  ）をクリックして、[名前（Name）] を変更します。
- レイヤのコピー：レイヤのコピー アイコン（）をクリックします。

- レイヤの削除：レイヤの削除アイコン（）をクリックして、[OK] をクリックします。
- 2 つのレイヤのマージ：2 つのレイヤの上部のマージ アイコン（）をクリックして、[OK] をクリックします。
- レイヤの移動：レイヤ サマリ内の任意の空いている場所をクリックし、位置矢印（）が移動するレイヤの上または下の行を指すまでドラッグします。

ステップ 3 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

レイヤ間のナビゲーション

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

手順

ステップ 1 ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。

ステップ 2 レイヤの移動は、次のいずれかのアクションで実行できます。

- プリプロセッサ ページまたは詳細設定ページにアクセスする：レイヤ レベルのプリプロセッサまたは詳細設定の設定ページにアクセスするには、そのレイヤに対応する行の機能名をクリックします。基本ポリシーおよび共有レイヤでは、設定ページは読み取り専用です。
- ルール ページにアクセスする：ルールの状態タイプでフィルタ処理されたレイヤ レベルのルール設定ページにアクセスする場合は、レイヤの概要でイベントのドロップおよび生成アイコン（）、イベントの生成アイコン（）、または無効化アイコン（）をクリックします。選択したルール状態に設定されているルールがレイヤに含まれていない場合、ルールは表示されません。

- [ポリシー情報ページ（Policy Information）]ページを表示する：[ポリシー情報ページ（Policy Information）]ページを表示するには、ナビゲーション ウィンドウで[ポリシーの概要（Policy Summary）]をクリックします。
- レイヤの概要ページを表示する：レイヤの概要ページを表示するには、レイヤに対応する行のレイヤ名をクリックするか、ユーザ レイヤの横にある編集アイコン（  ）をクリックします。表示アイコン（  ）をクリックして、共有レイヤの読み取り専用のサマリ ページにアクセスすることもできます。

ステップ 3 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、[ポリシー情報（Policy Information）]をクリックして、[変更を確定（Commit Changes）]をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

レイヤでの侵入ルール

レイヤの[ルール（Rules）]ページで個々のレイヤ設定を表示することも、[ルール（Rules）]ページのポリシー ビューですべての設定の最終的な効果を表示することもできます。[ルール（Rules）]ページのポリシー ビューのルール設定を変更する場合、ポリシーの最上位のユーザ設定可能なレイヤを変更します。[ルール（Rules）]ページにあるレイヤ ドロップダウンリストを使用して、別のレイヤに切り替えることができます。

次の表では、複数のレイヤで同じ種類の設定を構成した場合の結果について説明しています。

表 *80*：レイヤ ルールの設定

設定可能なレイヤ数	設定の種類	目的
1	ルール状態	下位レイヤのルールに対して設定されたルール状態を上書きします。また、下位レイヤで設定されたそのルールのすべてのしきい値、抑制、レートベースのルール状態、およびアラートを無視します。 基本ポリシーまたは下位レイヤからルールのルール状態を継承したい場合は、ルール状態を[継承（Inherit）]に設定します。侵入ポリシーの[ルール（Rules）]ページは、すべてのルール設定の最終的な効果を示す複合ビューであるため、このページでの作業中にルールの状態を[継承（Inherit）]に設定することはできないことに注意してください。

設定可能なレイヤ数	設定の種類	目的
1	しきい値 SNMP アラート	下位レイヤのルールの同じ種類の設定を上書きします。しきい値を設定すると、レイヤのルールの既存のしきい値が上書きされることに注意してください。
1 つ以上	抑制 レートベースのルール状態	選択した各ルールの同じ種類の設定を、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせます。ルール状態が設定されているレイヤより下の設定は無視されます。
1 つ以上	コメント	ルールにコメントを追加します。コメントは、ポリシー固有またはレイヤ固有ではなく、ルール固有です。任意のレイヤの 1 つのルールに 1 つ以上のコメントを追加できます。

たとえば、あるレイヤでルール状態を [ドロップしてイベントを生成する（Drop and Generate Events）]に設定し、それよりも上位のレイヤで[無効（Disabled）]に設定した場合、侵入ポリシーの [ルール（Rules）] ページには、ルールが無効であることが示されます。

別の例として、あるレイヤでルールの送信元ベースの抑制を 192.168.1.1 に設定し、別のレイヤでそのルールの宛先ベースの抑制を 192.168.1.2 に設定した場合、[ルール（Rules）]ページには、送信元アドレス 192.168.1.1 と宛先アドレス 192.168.1.2 に関するイベントを抑制する累積的な結果が示されます。抑制およびレート ベースのルール状態の設定では、選択した各ルールの同じ種類の設定が、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせられることに注意してください。ルール状態が設定されているレイヤより下の設定は無視されます。

特定のレイヤの各 [ルール（Rules）]ページの色分けでは、有効状態が上位レイヤ、下位レイヤ、現在のレイヤのどれに該当するのかが次の色で示されます。

- 赤：上位レイヤでの有効状態
- 黄色：下位レイヤでの有効状態
- 陰影なし：現在のレイヤでの有効状態

侵入ポリシーの [ルール（Rules）]ページはすべてのルール設定の最終的な効果の複合ビューであるため、ルール状態はこのページでは色分けされません。

レイヤでの侵入ルールの設定

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

侵入ポリシーでは、すべてのユーザ設定可能なレイヤのルールに対して、ルール状態、イベントフィルタリング、動的状態、アラート、およびルール コメントを設定できます。変更を加えるレイヤにアクセスした後、そのレイヤの [ルール（Rules）] ページの設定を、侵入ポリシーの [ルール（Rules）] ページの設定と同じように追加します。

手順

ステップ 1 侵入ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] を展開します。

ステップ 2 変更するポリシー階層を展開します。

ステップ 3 変更するポリシー レイヤのすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 ルールを使用した侵入ポリシーの調整, （1043 ページ）に示されている任意の設定を変更します。

ヒント 編集可能なレイヤから個々の設定を削除するには、そのレイヤの [ルール（Rules）] ページでルール メッセージをダブルクリックして、ルールの詳細を表示します。削除する設定の横にある [削除（Delete）] をクリックして [OK] を 2 回クリックします。

ステップ 5 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

複数のレイヤからのルール設定の削除

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

侵入ポリシーの複数のレイヤから、特定のタイプのイベント フィルタ、動的状態、またはアラートを同時に削除できます。システムは選択された設定を削除し、ルールの残りの設定をポリシーの最上位の編集可能なレイヤにコピーします。

システムは、すべての設定を削除するか、ルール状態がルールに対して設定されているレイヤに遭遇するまで、下位方向にある各レイヤの同じ種類の設定を削除します。後者の場合、そのレイヤから設定が削除され、設定タイプの削除が停止されます。

共有レイヤまたは基本ポリシーで同じタイプの設定に遭遇したときに、ポリシーの最上位のレイヤが編集可能である場合、システムはそのルールの残りの設定およびルール状態をその編集可能なレイヤにコピーします。そうではない場合、ポリシーの最上位のレイヤが共有レイヤであれば、システムは新しい編集可能なレイヤをその共有レイヤの上に作成し、そのルールの残りの設定およびルール状態をその編集可能なレイヤにコピーします。

（注） 共有レイヤまたは基本ポリシーから派生したルール設定を削除すると、下位レイヤまたは基本ポリシーからこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーからの変更を無視しないようにするには、最上位のレイヤのサマリー ページでルール状態を [継承（Inherit）] に設定します。

手順

ステップ 1 侵入ポリシーの編集中に、ナビゲーション ウィンドウで [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ヒント また、任意のレイヤの [ルール（Rules）] ページでレイヤのドロップダウンリストから [ポリシー（Policy）] を選択するか、[ポリシー情報（Policy Information）] ページの [ルールの管理（Manage Rules）] をクリックすることもできます。

ステップ 2 複数の設定を削除するルールを選択します。

- 特定の選択（Choose specific）：特定のルールを選択するには、各ルールの横にあるチェックボックスをオンにします。
- すべて選択（Choose all）：現在のリストのルールをすべて選択するには、列の上部にあるチェックボックスをオンにします。

ステップ 3 次のいずれかのオプションを選択します。

- [イベントのフィルタリング（Event Filtering）] > [しきい値の削除（Rmove Thresholds）]
- [イベントのフィルタリング（Event Filtering）] > [抑制の削除（Remove Suppressions）]
- [動的状態（Dynamic State）] > [レート ベースのルール状態の削除（Remove Rate-Based Rule States）]
- [アラート（Alerting）] > [SNMP アラートの削除（Remove SNMP Alerts）]

（注） 共有レイヤまたは基本ポリシーから派生したルール設定を削除すると、下位レイヤまたは基本ポリシーからこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーからの変更を無視しないようにするには、最上位のレイヤのサマリー ページでルール状態を [継承（Inherit）] に設定します。

ステップ 4 [OK] をクリックします。

ステップ 5 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

カスタム基本ポリシーからのルール変更の受け入れ

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

レイヤを追加していないカスタム ネットワーク分析ポリシーまたは侵入ポリシーが別のカスタム ポリシーを基本ポリシーとして使用するとき、以下を行う場合は、そのルール状態を継承するようにルールを設定する必要があります。

- 基本ポリシーのルールに設定されたイベント フィルタ、動的状態、またはSNMP アラートを削除する場合
- 基本ポリシーとして使用する他のカスタム ポリシー内のルールに行った後続の変更をルールが受け入れるようにする場合

手順

ステップ 1 侵入ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] を展開します。

ステップ 2 [個人用の変更（My Changes）] を展開します。

ステップ 3 [個人用の変更（My Changes）] のすぐ下にある [ルール（Rules）] リンクをクリックします。

ステップ 4 設定を受け入れるルールを選択します。次の選択肢があります。

- [特定ルールの選択（Choose specific rules）]：特定のルールを選択するには、各ルールの横にあるチェックボックスをチェックします。

- [すべてのルールを選択（Choose all rules）]：現在のリストのすべてのルールを選択する場合は、列の最上部にあるチェックボックスをチェックします。

ステップ 5 [ルール状態（Rule State）] ドロップダウンリストから、[継承（Inherit）] を選択します。

ステップ 6 最後のコミットからポリシーに加えられた変更を保存するには、[ポリシー情報（Policy information）] をクリックし、次に [変更をコミット（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

レイヤでのプリプロセッサと詳細設定

ネットワーク分析ポリシーでプリプロセッサを設定するときと、侵入ポリシーで詳細詳細を設定するときのメカニズムは同様です。プリプロセッサの有効化および無効化はネットワーク分析の [設定（Settings）] ページで行うことができ、侵入ポリシーの詳細設定の有効化および無効化は侵入ポリシーの [詳細設定（Advanced Settings）] ページで行うことができます。これらのページでは、すべての関連機能の有効な状態の概要も示されます。たとえば、ネットワーク分析 SSL プリプロセッサが、あるレイヤでは無効になっていて上位レイヤでは有効になっている場合、[設定（Settings）]ページにはプリプロセッサが有効であるとして表示されます。これらのページで行った変更は、ポリシーの最上位レイヤに表示されます。Back Orifice プリプロセッサにはユーザ設定可能なオプションがないことに注意してください。

また、プリプロセッサまたは詳細設定を有効化または無効化したり、ユーザ設定可能なレイヤのサマリ ページの設定ページにアクセスしたりできます。このページで、レイヤの名前および説明を変更し、レイヤを同じタイプの他のポリシーと共有するかどうかを設定できます。ナビゲーション パネルの [ポリシー層（Policy Layers）] の下のレイヤの名前を選択することによって、別のレイヤのサマリー ページに切り替えることができます。

プリプロセッサまたは詳細設定を有効にすると、その機能の設定ページへのサブリンクがナビゲーション パネルのレイヤの名前の下に表示され、編集アイコン（  ）がそのレイヤのサマリー ページの機能の横に表示されます。レイヤで機能を無効にしたり、[継承（Inherit）] に設定した場合はこれらは表示されません。

プリプロセッサまたは詳細設定の状態（有効または無効）を設定すると、下位レイヤでのその機能の状態と構成設定が上書きされます。プリプロセッサまたは詳細設定についてその状態と設定を基本ポリシーまたは下位レイヤから継承する場合、状態を [継承（Inherit）] に設定します。[設定（Settings）] または [詳細設定（Advanced Settings）] ページで操作するときには、[継承（Inherit）] の選択項目は使用できないことに注意してください。また、現在有効にされている機能を継承す

ると、ナビゲーション パネルではその機能のサブリンクが表示されなくなり、設定ページではその機能の編集アイコンが表示されなくなることにも注意してください。

システムは、機能が有効にされている最上位レイヤの設定を使用します。設定を明示的に変更しなかった場合は、デフォルト設定が使用されます。たとえば、あるレイヤでネットワーク分析DCE/RPCプリプロセッサを有効にして変更し、それより上位のレイヤでプリプロセッサを有効にするが変更はしない場合、システムは上位レイヤのデフォルト設定を使用します。

各レイヤのサマリ ページは次のようにカラーコード化されており、有効な設定が上位レイヤ、下位レイヤ、または現在のレイヤのいずれにあるかが示されます。

- 赤色：有効な設定は上位レイヤにあります
- 黄色：有効な設定は下位レイヤにあります
- 陰影なし：有効な設定は現在のレイヤにあります

[設定（Settings）] および [詳細設定（Advanced Settings）] ページは、関連するすべての設定の複合ビューであるため、これらのページは有効な設定の位置を示すためにカラー コーディングを使用しません。

層のプリプロセッサと詳細の設定

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

手順

ステップ 1 ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] を展開し、変更するレイヤの名前をクリックします。

ステップ 2 次の選択肢があります。

- 層の名前を変更します。
- 説明を追加または変更します。
- [共有（Sharing）] チェックボックスをオンまたはオフにして、層を別のポリシーと共有できるようにするかどうかを指定します。
- 有効にしたプリプロセッサ/詳細設定の設定ページにアクセスするには、編集アイコン（）または機能のサブリンクをクリックします。
- 現在の層のプリプロセッサ/詳細設定を無効にするには、機能の横にある [無効化（Disabled）] をクリックします。

- 現在の層のプリプロセッサ/詳細設定を有効にするには、機能の横にある [有効化（Enabled）] をクリックします。
- 現在の層の下にある最上位レイヤの設定からプリプロセッサ/詳細設定の状態および構成を継承するには、[継承（Inherit）] をクリックします。

ステップ 3 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

第 49 章

侵入ポリシーの使用を開始するには

ここでは、侵入ポリシーの使用を開始する方法について説明します。

侵入ポリシーの基本

侵入ポリシーは定義済みの侵入検知のセットであり、セキュリティ違反についてトラフィックを検査し、インライン展開の場合は、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーは、アクセスコントロールポリシーによって呼び出され、システムの最終防御ラインとして、トラフィックが宛先に到達することを許可するかどうかを判定します。

各侵入ポリシーの中核となるのは、侵入ルールです。ルールを有効にすると、ルールに一致するトラフィックに対して侵入イベントが生成されます（さらに、必要に応じてトラフィックがブロックされます）。ルールを無効にすると、ルールの処理が停止されます。

Firepower システムが提供するいくつかの基本的な侵入ポリシーにより、Cisco Talos Security Intelligence and Research Group（Talos）の経験を活用できます。これらのポリシーに対して、Talos は侵入およびプリプロセッサ ルールの状態（有効または無効）を設定し、他の詳細設定の初期設定も行います。

ヒント　システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。

カスタム侵入ポリシーを作成すると、以下を実行できます。

- ルールを有効化/無効化することに加え、独自のルールを作成して追加し、検出を調整する。
- ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコルをそれらの資産を保護するために明確に書き込まれたルールに関連付けるには、Firepower の推奨事項を使用します。
- 外部アラート、センシティブ データの前処理、グローバル ルールのしきい値設定など、さまざまな詳細設定を設定する。
- レイヤを構成要素として使用し、複数の侵入ポリシーを効率的に管理する。

インライン展開では、侵入ポリシーによってトラフィックを変更したりブロックすることができます。

- 廃棄ルールを使用すると、一致したパケットをドロップして、侵入イベントを生成できます。侵入またはプリプロセッサの廃棄ルールを設定するには、そのステータスを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定します。
- 侵入ルールでは、`replace` キーワードを使用して悪意のあるコンテンツを置き換えることができます。

侵入ルールがトラフィックに影響を与えるようにするには、廃棄ルールおよびコンテンツを置き換えるルールを適切に設定し、さらに管理対象デバイスを適切にインライン展開する（つまり、インライン インターフェイス セットを設定する）必要があります。最後に、侵入ポリシーのドロップ動作（[インライン時にドロップ（Drop when Inline）] 設定）を有効にします。

留意事項として、侵入ポリシーを調整する場合（特にルールを有効化して追加する場合）、一部の侵入ルールでは、最初に特定の方法でトラフィックをデコードまたは前処理する必要があります。侵入ポリシーによって検査される前に、パケットはネットワーク分析ポリシーの設定に従って前処理されます。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

注意　前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。

カスタム侵入ポリシーを設定した後、それを1つ以上のアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに関連付けることによって、カスタム侵入ポリシーをアクセス コントロール設定の一部として使用できます。これによって、システムは、最終宛先に渡す前に、特定の許可されたトラフィックを侵入ポリシーによって検査します。変数セットを侵入ポリシーと組み合わて使用することにより、ホーム ネットワークと外部ネットワークに加えて、必要に応じてネットワーク上のサーバを正確に反映させることができます。

デフォルトでは、暗号化ペイロードの侵入インスペクションは無効化されます。これにより、侵入インスペクションが設定されているアクセスコントロールルールと暗号化された接続を照合する際の誤検出が減少し、パフォーマンスが向上します。

侵入ポリシーの管理

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

[侵入ポリシー（Intrusion Policy）]ページ（[ポリシー（Policies）]>[アクセス コントロール（Access Control）] > [侵入（Intrusion）]）では、次に示す情報とともに、現在のカスタム侵入ポリシーを表示できます。

- ポリシーが最後に変更された日時（ローカル時間）とそれを変更したユーザ
- [インライン時にドロップ（Drop when Inline）] 設定が有効になっているかどうか。この設定が有効な場合、インライン展開でトラフィックをドロップしたり変更することができます。
- トラフィックの検査に侵入ポリシーを使用しているアクセス コントロール ポリシーとデバイス
- ポリシーに保存されていない変更があるかどうか、およびポリシーを現在編集している人（いれば）に関する情報
- マルチドメイン展開では、ポリシーが作成されたドメイン

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 侵入ポリシーを管理します。

- [比較（Compare）]：[ポリシーの比較（Compare Policies）]をクリックします（ポリシーの比較, （331 ページ） を参照）。
- 作成：[ポリシーの作成（Create Policy）] をクリックします。カスタム侵入ポリシーの作成, （1037 ページ）を参照してください。
- 削除：削除するポリシーの横にある削除アイコン（）をクリックします。別のユーザが保存していないポリシーの変更がある場合は、システムによって確認と通知のプロンプトが表示されます。[OK] をクリックして確認します。

  コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 編集：編集するポリシーの横にある編集アイコン（）をクリックします。侵入ポリシーの編集, （1038 ページ）を参照してください。

  代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- エクスポート：別の Firepower Management Center にインポートするために、侵入ポリシーをエクスポートするには、エクスポートアイコン（）をクリックします。設定のエクスポート, （189 ページ）を参照してください。
- 展開：[展開（Deploy）] をクリックします（設定変更の導入, （320 ページ） を参照）。
- [レポート（Report）]：レポートアイコン（）をクリックします（現在のポリシー レポートの生成, （333 ページ） を参照）。

カスタム侵入ポリシーの作成

新しい侵入ポリシーを作成する場合は、一意の名前を付けて基本ポリシーを指定し、ドロップ動作を指定する必要があります。

基本ポリシーは侵入ポリシーのデフォルト設定を定義します。新しいポリシーの設定の変更は、基本ポリシーの設定を変更するのではなく、オーバーライドします。システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

侵入ポリシーのドロップ動作、または [インライン時にドロップ（Drop when Inline）] の設定によって、廃棄ルール（ルール状態が [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されている侵入ルールまたはプリプロセッサ ルール）、およびトラフィックに影響を与えるその他の侵入ポリシー設定のシステムにおける処理方法が決まります。悪意のあるパケットをドロップまたは置き換える場合は、インライン展開でドロップ動作を有効にする必要があります。パッシブ展開では、ドロップ動作に関わらず、システムはトラフィック フローに影響を与えることはできません。

カスタム侵入ポリシーの作成

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

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。別のポリシー内に未保存の変更が存在する場合は、[侵入ポリシー（Intrusion Policy）] ページに戻るかどうか尋ねられたときに [キャンセル（Cancel）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力し、オプションで [説明（Description）] を入力します。

ステップ 4 [基本ポリシー（Base Policy）] で最初の基本ポリシーを指定します。
システム提供のポリシーまたは別のカスタム ポリシーを基本ポリシーとして使用できます。

ステップ 5 インライン展開でのドロップ動作の設定，（1040 ページ）の説明に従って、インライン導入でのシステムのドロップ動作を設定します。

ステップ 6 ポリシーを作成します。

- 新しいポリシーを作成して、[侵入ポリシー（Intrusion Policy）]ページに戻るには、[ポリシーの作成（Create Policy）] をクリックします。新しいポリシーには基本ポリシーと同じ設定項目が含まれています。
- ポリシーを作成し、高度な侵入ポリシー エディタでそれを開いて編集するには、[ポリシーの作成と編集（Create and Edit Policy）] をクリックします（侵入ポリシーの変更，（1039 ページ）を参照）。

関連トピック

レイヤでの侵入ルール，（1025 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー，（1011 ページ）

侵入ポリシーの編集

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

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 設定する侵入ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ポリシーを編集します。

- 基本ポリシーの変更：[基本ポリシー（Base Policy）] ドロップダウン リストから基本ポリシーを選択します。ベースポリシーの変更，（1019 ページ）を参照してください。
- 詳細設定の構成：ナビゲーション パネルで [詳細設定（Advanced Settings）] をクリックします。侵入ポリシーの詳細設定，（1041 ページ）を参照してください。
- Firepower 推奨ルールの設定：ナビゲーション パネルで [Firepower 推奨ルール（Firepower Recommended Rules）] をクリックします。Firepower の推奨事項の生成と適用，（1081 ページ）を参照してください。
- インライン展開でのドロップ動作：[インライン時にドロップ（Drop when Inline）] をオンまたはオフにします。インライン展開でのドロップ動作の設定，（1040 ページ）を参照してください。
- 推奨ルール状態によるルールのフィルタ：推奨を生成した後、各推奨タイプの横にある [表示（View）] をクリックします。すべての推奨を表示するには、[推奨される変更の表示（View Recommended Changes）] をクリックします。
- 現在のルール状態によるルールのフィルタ：ルール状態タイプ（イベントを生成する、ドロップしてイベントを生成する）の横にある [表示（View）] をクリックします。侵入ポリシー内の侵入ルール フィルタ，（1053 ページ）を参照してください。
- ポリシー階層の管理：ナビゲーション パネルで、[ポリシー層（Policy Layers）] をクリックします。レイヤ管理，（1021 ページ）を参照してください。
- 侵入ルールの管理：[ポリシー情報（Policy Information）] をクリックします。侵入ポリシー内の侵入ルールの表示，（1045 ページ）を参照してください。

- 基本ポリシーの設定の表示：[基本ポリシーの管理（Manage Base Policy）] をクリックします。基本レイヤ，（1017 ページ）を参照してください。

ステップ 4 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] を選択して、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

関連トピック

Firepower の推奨事項の生成と適用，（1081 ページ）
レイヤでの侵入ルールの設定，（1026 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー，（1011 ページ）

侵入ポリシーの変更

新しい侵入ポリシーを作成すると、そのポリシーには基本ポリシーと同じ侵入ルールと詳細設定が付与されます。

システムは、ユーザごとに 1 つのセキュリティ ポリシーをキャッシュします。侵入ポリシーの編集中に、メニューまたは別のページへのパスを選択すると、そのページから移動しても、変更内容はシステム キャッシュに残ります。

インライン展開でのドロップ動作

実際にトラフィックを変更せず、使用している設定がインライン展開（つまり、ルーテッド、スイッチド、またはトランスペアレントインターフェイス、あるいはインラインインターフェイスペアを使用して、関連する設定がデバイスに展開されている）でどのように機能するかを評価する場合は、ドロップ動作を無効にすることができます。その場合、システムは侵入イベントを生成しますが、廃棄ルールをトリガーしたパケットをドロップしません。結果を確認したら、ドロップ動作を有効化できます。

パッシブ展開またはタップ モードでのインライン展開では、ドロップ動作に関わらず、システムはトラフィックに影響を与えることはできません。つまり、パッシブ展開では、[ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールは [イベントを生成する（Generate Events）] に設定されたルールと同様に動作します。システムは侵入イベントを生成しますが、パケットをドロップできません。

（注） FTP を介してマルウェアの転送をブロックするには、Firepower の AMP を正しく設定するだけでなく、アクセス コントロール ポリシーのデフォルトの侵入ポリシーで [インライン時にドロップ（Drop when Inline）] を有効にする必要があります。

侵入イベントを表示する際に、ワークフローにインライン結果を含めることができます。インライン結果は、トラフィックが実際にドロップされたのか、あるいはドロップが想定に過ぎなかったのかを示します。

インライン展開でのドロップ動作の設定

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

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。
代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ポリシーのドロップ動作を設定します。

- [インライン時にドロップ（Drop when Inline）] チェックボックスをオンにして、侵入ルールのトラフィックへの適用とイベントの生成を許可します。
- [インライン時にドロップ（Drop when Inline）] チェックボックスをオフにすると、侵入ルールのトラフィックへの適用が禁止されますが、イベントは生成されます。

ステップ 4 [変更を確定（Commit Changes）] をクリックして、最後のポリシーの確定以降に、このポリシーに加えた変更を保存します。
ポリシーの変更を確定しない場合、最後の確定以降の変更は、別のポリシーを編集するときに破棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

侵入ポリシーの詳細設定

侵入ポリシーの詳細設定を設定するには、特定の専門知識が必要です。デフォルトで有効になる詳細設定や、詳細設定ごとのデフォルトは、侵入ポリシーの基本ポリシーに応じて決まります。

侵入ポリシーのナビゲーション パネルで [詳細設定（Advanced Settings）] を選択すると、ポリシーの詳細設定がタイプ別に一覧表示されます。[詳細設定（Advanced Settings）] ページでは、侵入ポリシーの詳細設定を有効または無効にしたり、詳細設定の設定ページにアクセスすることができます。詳細設定を行うには、それを有効にする必要があります。

詳細設定を無効にすると、サブリンクと [編集（Edit）] リンクは表示されなくなりますが、設定は保持されます。侵入ポリシーの一部の設定（センシティブ データ ルール、侵入ルールの SNMP アラート）では、詳細設定を有効化して適切に設定する必要があります。このように誤って設定された侵入ポリシーは保存できません。

詳細設定を変更する場合、変更する設定と、その変更がネットワークに及ぼす可能性のある影響について理解していることが必要です。

特定の脅威の検出（Specific Threat Detection）

機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。

特定の脅威（Back Orifice 攻撃、何種類かのポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレート ベース攻撃）を検出するプリプロセッサは、ネットワーク分析ポリシーで設定します。

侵入ルールしきい値（Intrusion Rule Thresholds）

グローバル ルールのしきい値を設定すると、しきい値を使用して、システムが侵入イベントを記録したり表示したりする回数を制限できるので、多数のイベントでシステムが圧迫されないようにすることができます。

外部レスポンス（External Responses）

Web インターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、システム ログ（syslog）ファシリティへのロギングを有効にしたり、イベント データを SNMP トラップ サーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。

これらのポリシー単位のアラート設定に加えて、各ルールまたはルール グループの侵入イベントを通知する電子メール アラートをグローバルに有効化/無効化できます。どの侵入ポリシーがパケットを処理するかに関わらず、ユーザの電子メール アラート設定が使用されます。

関連トピック

機密データ検出の基本, （1083 ページ）
グローバル ルールのしきい値の基本, （1099 ページ）

侵入検知および防御のパフォーマンスの最適化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin (access control); Admin/Discovery Admin (network discovery)

Firepowerシステムを使用して侵入検知および防御を実行するものの検出データを利用する必要がない場合は、以下の説明に従って新しい検出を無効にしてパフォーマンスを最適化できます。

手順

ステップ1 ターゲットデバイスに導入したアクセス コントロール ポリシーと関連付けられたルールを変更または削除します。そのデバイスに関連付けられたアクセス制御ルールはいずれも、ユーザ、アプリケーション、またはURLの条件を指定できません（アクセス コントロール ルールの作成および編集，（807 ページ）を参照）。

ステップ2 ターゲットデバイスのネットワーク検出ポリシーからすべてのルールを削除します（ネットワーク検出ルールの設定，（1553 ページ）を参照）。

ステップ3 変更された設定をターゲットデバイスに導入します（設定変更の導入，（320ページ）を参照）。

第 50 章

ルールを使用した侵入ポリシーの調整

ここでは、ルールを使用して侵入ポリシーを調整する方法について説明します。

侵入ルールの調整の基本

侵入ポリシーの [ルール（Rules）] ページを使用して、共有オブジェクト ルール、標準テキスト ルール、プリプロセッサ ルールに関するルール状態とその他の設定を構成できます。

ルールは、ルール状態を [イベントを生成する（Generate Events）] または [ドロップしてイベントを生成する（Drop and Generate Events）] に設定することによって有効にします。ルールを有効にすると、システムがそのルールと一致するトラフィックに対するイベントを生成します。ルールを無効にすると、ルールの処理が停止されます。また、インライン展開で [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールによって、一致するトラフィックに対するイベントが生成され、そのトラフィックが破棄されるように、侵入ポリシーを設定できます。パッシブ展開では、[ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールによって、一致するトラフィックに対するイベントが生成されるだけです。

ルールのサブセットを表示するようにルールをフィルタ処理することによって、ルール状態やルール設定を変更するルールのセットを正確に選択できます。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。

侵入ルールのタイプ

侵入ルールとは、ネットワーク内の脆弱性を不正利用する試みを検出するためにシステムが使用する、指定されたキーワードと引数のセットのことです。システムはネットワーク トラフィックを分析する際に、パケットを各ルールに指定された条件に照らし合わせ、データ パケットがルールに指定されたすべての条件を満たす場合、そのルールをトリガーします。

侵入ポリシーには以下の構成要素があります。

- 侵入ルール。共有オブジェクト ルールと標準テキスト ルールに分割されます。
- プリプロセッサ ルール。パケット デコーダの検出オプション、または Firepower システムに付属のプリプロセッサの 1 つに関連付けられます。

次の表に、以上のルール タイプの属性を要約します。

表 *81*：侵入ルールのタイプ

タイプ（Type）	ジェネレータ ID（GID）	Snort ID（SID）	ソース（Source）	コピーの可否	編集の可否
共有オブジェクト ルール	3	1000000 未満	Cisco Talos Security Intelligence and Research Group（Talos）	Yes	制限付き
標準テキスト ルール	1	1000000 未満	Talos	Yes	制限付き
		1000000 以上	ユーザが作成またはインポート	Yes	Yes
プリプロセッサ ルール	デコーダまたはプリプロセッサに固有	1000000 未満	Talos	No	No
		1000000 以上	オプション設定時にシステムにより生成	No	No

Talosによって作成されたルールを変更して保存することはできませんが、ルールをコピーして変更し、それをカスタム ルールとして保存することはできます。ルールで使用される変数またはルールヘッダー情報情報（送信元と宛先のポートやIPアドレスなど）を変更できます。マルチドメイン展開では、Talos によって作成されるルールはグローバル ドメインに属します。子孫ドメインの管理者は、ルールのローカル コピーを保存してから、ルールを編集できます。

Talosによって作成されるルールには、各デフォルト侵入ポリシー内でデフォルトのルール状態が割り当てられます。ほとんどのプリプロセッサ ルールがデフォルトで無効になっているため、シ

ステムにプリプロセッサ ルールに対するイベントの生成とインライン展開での違反パケットの破棄を行わせる場合は、これらのルールを有効にする必要があります。

マルチドメイン展開では、子孫ドメインで作成されたか、または子孫ドメインにインポートされたカスタム ルールの SID の先頭にドメイン番号が追加されます。たとえば、グローバル ドメインに追加されたルールに 1000000 以上の SID があり、子孫ドメインに追加されたルールには [ドメイン番号]000000 以上の SID があります。

侵入ポリシー内の侵入ルールの表示

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

侵入ポリシーでのルールの表示方法を調整でき、複数の条件によってルールをソートできます。特定のルールの詳細を表示して、ルール設定、ルール ドキュメント、およびその他のルール仕様を確認することもできます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルの [ポリシー情報（Policy Information）] の下にある [ルール（Rules）] をクリックします。

ステップ 4 ルールを表示している間、以下を実行できます。

- 侵入ポリシー内のルール フィルタの設定, （1060 ページ）の説明に従ってルールをフィルタリングします。
- ソートの基準とするカラムの一番上のタイトルまたはアイコンをクリックすることによって、ルールをソートします。
- 侵入ルール詳細の表示, （1048 ページ）の説明に従って、侵入ルールの詳細を表示します。
- [ポリシー（Policy）] ドロップダウン リストから階層を選択することによって、異なるポリシー階層のルールを表示します。

[侵入ルール（Intrusion Rules）] ページの列

[侵入ルール（Intrusion Rules）] ページでは、メニュー バーおよび列ヘッダーに同じアイコンが使用されます。たとえば、[ルール状態（Rule State）] メニューでは、ルール リストの [ルール状態（Rule State）] 列と同じアイコン（  ）が使用されます。

表 *82*：*[ルール（Rules）]* ページの列

見出し	説明
GID	ルールのジェネレータ ID（GID）を表す整数。
SID	ルールの固有識別子として機能する Snort ID（SID）を表す整数。 カスタム ルールの場合、SID は 1000000 以上です。 マルチドメイン展開では、子孫ドメインで作成されたか、または子孫ドメインにインポートされたカスタム ルールの SID の先頭にドメイン番号が追加されます。たとえば、グローバル ドメインに追加されたルールに 1000000 以上の SID があり、子孫ドメインに追加されたルールには [ドメイン番号]000000 以上の SID があります。
メッセージ	このルールによって生成されるイベントに含まれるメッセージ。ルールの名前としても機能します。
	ルールのルール状態。 • ドロップしてイベントを生成する（） • イベントを生成する（） • 無効（） 無効なルールのアイコンは、トラフィックをドロップせずにイベントを生成するように設定されたルールのアイコンのグレー表示されたバージョンです。また、ルールのルール状態アイコンをクリックすると、ルール状態を変更できます。
	ルールの Firepower 推奨ルール状態。
	ルールに適用されるイベントしきい値やイベント抑制などのイベント フィルタ。
	ルールの動的ルール状態。指定されたレート異常が発生した場合に有効になります。
	ルールに対して設定されたアラート（現在は SNMP アラートのみ）。
	ルールに追加されたコメント。

レイヤのドロップダウンリストを使用して、ポリシー内の他のレイヤの[ルール（Rules）]ページに切り替えることもできます。ポリシーにレイヤを追加しなかった場合にドロップダウンリストに表示される編集可能なビューはポリシーの[ルール（Rules）]ページと、元は`My Changes`という名前だったポリシー階層の[ルール（Rules）]ページだけであることに注意してください。これらのビューの一方を変更すると、もう一方も同じように変更されることにも注意してください。ドロップダウンリストには、読み取り専用の基本ポリシーの[ルール（Rules）]ページも表示されます。

侵入ルールの詳細

[ルールの詳細（Rule Detail）]ビューで、ルール ドキュメント、Firepowerの推奨事項、およびルール オーバーヘッドを表示できます。また、ルール固有の機能を表示および追加できます。

表 *83*：ルールの詳細

項目	説明
要約	ルールの概要。ルール ベースのイベントでは、ルール ドキュメントに概要情報が含まれている場合にこの行が表示されます。
ルール状態（Rule State）	ルールの現在のルール状態。ルール状態が設定された階層も示します。
Firepowerの推奨事項（Firepower Recommendation）	Firepowerの推奨事項が生成されている場合は、推奨されるルール状態を表すアイコン。[侵入ルール（Intrusion Rules）]ページの列, （1046ページ）を参照してください。ルールを有効にすることが推奨されている場合、システムは推奨事項をトリガーしたネットワーク アセットまたは設定も示します。
ルールのオーバーヘッド（Rule Overhead）	システム パフォーマンスに対するルールの潜在的影響とルールが誤検出を引き起こす確率。脆弱性にマップされていないローカル ルールにはオーバーヘッドが割り当てられていません。
しきい値	このルールに現在設定されているしきい値と、ルールのしきい値を追加するための機能。
抑制（Suppressions）	このルールに現在設定されている抑制設定と、ルールの抑制を追加するための機能。
動的状態（Dynamic State）	このルールに現在設定されているレート ベースのルール状態と、ルールの動的ルール状態を追加するための機能。
アラート（Alerts）	このルールに設定されているSNMPアラートと、ルールのアラートを追加するための機能。
説明	このルールに追加されたコメントと、ルールのコメントを追加するための機能。
資料	Cisco Talos Security Intelligence and Research Group（Talos） によって提供される現在のルールのルール ドキュメント。

侵入ルール詳細の表示

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

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ペインで [ルール（Rules）] をクリックします。

ステップ 4 ルールの詳細を表示したいルールをクリックし、ページの下部にある [詳細の表示（Show Details）] をクリックします。

侵入ルールの詳細, （1047 ページ）で説明されているように、ルールの詳細が表示されます。

ステップ 5 ルールの詳細から、以下を設定できます。

- アラート：侵入ルールの SNMP アラートの設定, （1052 ページ）を参照してください。
- コメント：侵入ルールへのコメントの追加, （1052 ページ）を参照してください。
- ダイナミック ルールの状態：[ルール詳細（Rule Details）] ページからの動的ルール状態の設定, （1050 ページ）を参照してください。
- しきい値：侵入ルールのしきい値の設定, （1048 ページ）を参照してください。
- 抑制：侵入ルールの抑制の設定, （1049 ページ）を参照してください。

侵入ルールのしきい値の設定

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

[ルールの詳細（Rule Detail）]ページで、ルールの単一のしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

無効な値を入力するとフィールドに復元アイコン（）が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

手順

ステップ 1 侵入ルールの詳細で、[しきい値（Thresholds）] の横にある [追加（Add）] をクリックします。

ステップ 2 [タイプ（Type）] ドロップダウンリストから、設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベントインスタンス数に通知を制限する場合は、[制限（Limit）] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[しきい値（Threshold）] を選択します。
- 指定されたイベントインスタンス数に達した後で、期間あたり 1 回ずつ通知を提供する場合は、[両方（Both）] を選択します。

ステップ 3 [追跡対象（Track By）] ドロップダウンリストから、[送信元（Source）] または [宛先（Destination）] を選択し、イベント インスタンスが送信元 IP アドレスまたは宛先 IP アドレスのどちらによって追跡されるかを指定します。

ステップ 4 [カウント（Count）]フィールドに、しきい値として使用するイベントインスタンスの数を入力します。

ステップ 5 [秒数（Seconds）]フィールドに、イベントインスタンスを追跡する期間（秒数）を指定する数値を入力します。

ステップ 6 [OK] をクリックします。

ヒント [イベント フィルタリング（Event Filtering）] 列のルールの横にイベント フィルタ アイコン（  ）が表示されます。ルールに複数のイベント フィルタを追加すると、アイコン上にイベント フィルタの数が表示されます。

侵入ルールの抑制の設定

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

侵入ポリシーのルールに対して 1 つ以上の抑制を設定できます。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

手順

ステップ 1 侵入ルールの詳細で、[抑制（Suppressions）] の横にある [追加（Add）] をクリックします。

ステップ 2 [抑制タイプ（Suppression Type）] ドロップダウンリストから、次のいずれかのオプションを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[ルール（Rule）] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元（Source）] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先（Destination）] を選択します。

ステップ 3 抑制タイプとして [送信元（Source）] または [宛先（Destination）] を選択した場合は、[ネットワーク（Network）] フィールドに IP アドレス、アドレス ブロック、またはそれらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。
侵入ポリシーがアクセス コントロール ポリシーのデフォルト アクションに関連付けられている場合は、デフォルト アクション変数セットでネットワーク変数を指定または列挙することもできます。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 4 [OK] をクリックします。

ヒント 抑制するルールの横にある [イベント フィルタリング（Event Filtering）] 列のルールの横にあるイベント フィルタ アイコン（）が表示されます。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

[ルール詳細（Rule Details）] ページからの動的ルール状態の設定

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

1 つのルールに対して 1 つ以上の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2 つの動的ルール状態が競合している場合は、最初のアクションが実行されます。

動的ルール状態はポリシー固有です。

無効な値を入力するとフィールドに復元アイコン（）が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

手順

ステップ 1 侵入ルールの詳細で、[動的状態（Dynamic State）] の横にある [追加（Add）] をクリックします。

ステップ 2 [追跡対象（Track By）] ドロップダウンリストから、ルール一致の追跡方法を指定するオプションを選択します。

- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[送信元（Source）] を選択します。
- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[宛先（Destination）] を選択します。
- そのルールのすべての一致を追跡する場合は、[ルール（Rule）] を選択します。

ステップ 3 [追跡対象（Track By）] を [送信元（Source）] または [宛先（Destination）] に設定した場合は、[ネットワーク（Network）] フィールドに追跡する各ホストのアドレスを入力します。
システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 4 [レート（Rate）] の横で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [カウント（Count）] フィールドで、しきい値として使用するルール一致の数を指定します。
- [秒（Seconds）] フィールドで、攻撃を追跡する期間を表す秒数を指定します。

ステップ 5 [新しい状態（New State）] ドロップダウンリストから、条件が満たされたときに実行する新しいアクションを選択します。

ステップ 6 [タイムアウト（Timeout）] フィールドに値を入力します。
タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションがタイムアウトしないようにする場合は、0 を入力します。

ステップ 7 [OK] をクリックします。

ヒント [動的状態（Dynamic State）] 列のルールの横に動的状態アイコン（  ）が表示されます。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

侵入ルールの SNMP アラートの設定

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

[ルールの詳細（Rule Detail）] ページで、ルールの SNMP アラートを設定できます。

手順

侵入ルールの詳細で、[アラート（Alerts）] の横にある [SNMP アラートの追加（Add SNMP Alert）] をクリックします。

ヒント [アラート（Alerting）] 列のルールの横にアラートアイコン（）が表示されます。ルールに複数のアラートを追加した場合は、アイコン上にアラートの数が表示されます。

侵入ルールへのコメントの追加

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

手順

ステップ 1 侵入ルールの詳細で、[コメント（Comments）] の横の [追加（Add）] をクリックします。

ステップ 2 [コメント（Comments）] フィールドに、ルール コメントを入力します。

ステップ 3 [OK] をクリックします。

ヒント システムは [コメント（Comments）] カラムのルールの横にコメントアイコン（）を表示します。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

ステップ 4 ルール コメントを削除するには、ルール コメント セクションで [削除（Delete）] をクリックします。侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけコメントを削除できます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

侵入ポリシー内の侵入ルール フィルタ

[ルール（Rules）] ページに表示するルールは、1 つの基準または 1 つ以上の基準の組み合わせに基づいてフィルタ処理できます。

ルール フィルタ キーワードは、ルール状態やイベント フィルタなどのルール設定を適用するルールを見つけやすくします。[ルール（Rules）] ページのフィルタ パネルで必要な引数を選択することによって、キーワードでフィルタ処理すると同時に、キーワードの引数を選択することができます。

侵入ルール フィルタの注意事項

作成したフィルタが [フィルタ（Filter）] テキストボックスに表示されます。フィルタ パネルでキーワードとキーワード引数をクリックしてフィルタを作成できます。複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[カテゴリ（Category）] で [プリプロセッサ（preprocessor）] を選択してから、[ルール コンテンツ（Rule Content）] > [GID] の順に選択して、「116」と入力すると、プリプロセッサ ルールで、**かつ**、GID が 116 のすべてのルールを取得する「`Category: "preprocessor" GID:"116"`」というフィルタが返されます。

[カテゴリ（Category）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[プラットフォーム特有（Platform Specific）]、[プリプロセッサ（Preprocessor）]、および [優先度（Priority）] の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、[カテゴリ（Category）] から [os-linux] と [os-windows] を選択すると、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,os-linux"`」というフィルタを作成できます。

フィルタ パネルを表示するには、表示アイコン（  ）をクリックします。

フィルタ パネルを非表示にするには、非表示アイコン（  ）をクリックします。

侵入ポリシー ルール フィルタ構築のガイドライン

ほとんどの場合、フィルタを作成するときに、侵入ポリシー内の [ルール（Rules）] ページの左側にあるフィルタ パネルを使用して必要なキーワード/引数を選択できます。

フィルタ パネルでは、ルール フィルタがルール フィルタ グループに分類されます。多くのルール フィルタ グループにサブ基準が含まれているため、探している特定のルールを簡単に見つけることができます。一部のルール フィルタには、展開して個別のルールにドリルダウンするための複数のレベルが設定されています。

フィルタ パネル内の項目は、場合によって、フィルタ タイプ グループを表したり、キーワードを表したり、キーワードの引数を表したりします。次の点に注意してください。

- キーワード（[ルール設定（Rule Configuration）]、[ルール コンテンツ（Rule Content）]、[プラットフォーム特有（Platform Specific）]、および [優先度（Priority）]）以外のフィルタ タ

イプ グループ見出しを選択すると、そのグループが展開されて使用可能なキーワードが一覧表示されます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定するためのポップアップ ウィンドウが表示されます。

そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [ルール設定（Rule Configuration）] > [推奨（Recommendation）] で [ドロップしてイベントを生成する（Drop and Generate Events）] をクリックすると、「`Recommendation:"Drop and Generate Events"`」がフィルタ テキスト ボックスに追加されます。その後で、[ルール設定（Rule Configuration）] > [推奨（Recommendation）] で [イベントを生成する（Generate Events）] をクリックすると、フィルタが「`Recommendation:"Generate Events"`」に変更されます。

- キーワード（[カテゴリ（Category）]、[分類（Classifications）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[優先度（Priority）]、および [ルール アップデート（Rule Update）]）になっているフィルタ タイプ グループ見出しを選択すると、使用可能な引数が一覧表示されます。

  このタイプのグループから項目を選択すると、適用される引数とキーワードがすぐにフィルタに追加されます。キーワードがすでにフィルタ内に存在していた場合は、そのグループに対応するキーワードの既存の引数が置き換えられます。

  たとえば、フィルタ パネルの [カテゴリ（Category）] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキストボックスに追加されます。その後で、[カテゴリ（Category）] で [os-windows] をクリックすると、フィルタが「`Category:"os-windows"`」に変更されます。

- [ルール コンテンツ（Rule Content）] の下の [参照（Reference）] はキーワードであり、その下に特定の参照 ID タイプが列挙されます。参照キーワードのいずれかを選択すると、引数を指定するためのポップアップ ウィンドウが表示され、キーワードが既存のフィルタに追加されます。キーワードがすでにフィルタ内で使用されていた場合は、既存の引数が指定した新しい引数に置き換えられます。

  たとえば、フィルタ パネルで [ルール コンテンツ（Rule Content）] > [参照（Reference）] > [CVE ID] の順にクリックすると、ポップアップ ウィンドウが開いて CVE ID を指定するよう求められます。「`2007`」と入力すると、「`CVE:"2007"`」がフィルタ テキストボックスに追加されます。別の例では、フィルタ パネルで [ルール コンテンツ（Rule Content）] > [参照（Reference）] の順にクリックすると、ポップアップ ウィンドウが開いて、参照を指定するよう求められます。「`2007`」と入力すると、「`Reference:"2007"`」がフィルタ テキストボックスに追加されます。

- 複数のグループからルール フィルタ キーワードを選択した場合は、各フィルタ キーワードがフィルタに追加され、既存のキーワードが維持されます（同じキーワードの新しい値で上書きされなかった場合）。

  たとえば、フィルタ パネルの [カテゴリ（Category）] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキストボックスに追加されます。その後で、[Microsoft

脆弱性（Microsoft Vulnerabilities）] で [MS00-006] をクリックすると、フィルタが「`Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`」に変更されます。

- 複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[カテゴリ（Category）] で [プリプロセッサ（preprocessor）] を選択してから、[ルール コンテンツ（Rule Content）] > [GID] の順に選択して、「`116`」と入力すると、プリプロセッサ ルールで、**かつ**、GID が 116 のすべてのルールを取得する「`Category: "preprocessor" GID:"116"`」というフィルタが返されます。
- [カテゴリ（Category）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[プラットフォーム特有（Platform Specific）]、および [優先度（Priority）] の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、[カテゴリ（Category）] から [os-linux] と [os-windows] を選択すると、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,app-detect"`」というフィルタを作成できます。

複数のフィルタ キーワード/引数のペアで同じルールが取得される場合があります。たとえば、ルールが dos カテゴリでフィルタ処理された場合と High 優先度でフィルタ処理された場合はともに、DOS Cisco attempt rule（SID 1545）が表示されます。

（注） Cisco Talos Security Intelligence and Research Group（Talos） がルール更新メカニズムを使用してルール フィルタを追加または削除する場合があります。

[ルール（Rules）] ページのルールは、共有オブジェクト ルール（ジェネレータ ID 3）または標準テキスト ルール（ジェネレータ ID 1）のいずれかになります。次の表に、さまざまなルール フィルタの説明を示します。

表 *84*：ルール フィルタ グループ

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
ルール設定（Rule Configuration）	ルールの設定に基づいてルールを検索します。	なし	グループ	キーワード
ルール コンテンツ（Rule Content）	ルールの内容に基づいてルールを検索します。	なし	グループ	キーワード
カテゴリ（Category）	ルール エディタで使用されるルール カテゴリに基づいてルールを検索します。ローカル ルールはローカル サブグループに表示されることに注意してください。	○	キーワード	引数

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
分類（Classifications）	ルールによって生成されるイベントのパケット画面内に表示される攻撃分類に基づいてルールを検索します。	なし	キーワード	引数
Microsoft 脆弱性（Microsoft Vulnerabilities）	Microsoft セキュリティ情報番号に従ってルールを検索します。	○	キーワード	引数
Microsoft ワーム（Microsoft Worms）	Microsoft Windows ホストに影響する特定のワームに基づいてルールを検索します。	○	キーワード	引数
プラットフォーム特有（Platform Specific）	オペレーティング システムの特定のバージョンとの関連性に基づいてルールを検索します。 ルールが複数のオペレーティング システムまたは 1 つのオペレーティング システムの複数のバージョンに影響する場合があることに注意してください。たとえば、SID 2260 を有効にすると、Mac OS X、IBM AIX、およびその他のオペレーティング システムの複数のバージョンに影響します。	○	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
プリプロセッサ（Preprocessors）	個別のプリプロセッサのルールを検索します。 プリプロセッサが有効になっている場合にプリプロセッサ オプションに対するイベントを生成し、インライン展開では、違反パケットをドロップします。するためには、そのオプションに関連付けられたプリプロセッサ ルールを有効にする必要があることに注意してください。	○	グループ	サブグループ
[プライオリティ（Priority）]	高、中、および低の優先度に基づいてルールを検索します。 ルールに割り当てられた分類によってその優先度が決定されます。これらのグループは、さらにルール カテゴリに分類されます。ローカル ルール（つまり、ユーザがインポートまたは作成したルール）は優先度グループに表示されないことに注意してください。	○	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
ルール アップデート（Rule Update）	特定のルール更新を通して追加または変更されたルールを検索します。ルール更新ごとに、更新内のすべてのルール、更新でインポートされた唯一の新しいルール、または更新によって変更された唯一の既存のルールを表示します。	なし	キーワード	引数

侵入ルール構成フィルタ

[ルール（Rules）] ページに表示されたルールをいくつかのルール構成設定でフィルタ処理できます。たとえば、ルール状態が推奨ルール状態と一致しない一連のルールを表示する場合は、[推奨と一致しない（Does not match recommendation）] を選択することによってルール状態をフィルタ処理できます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定できます。そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [ルール設定（Rule Configuration）] > [推奨（Recommendation）] で [ドロップしてイベントを生成する（Drop and Generate Events）] をクリックすると、「`Recommendation:"Drop and Generate Events"`」がフィルタ テキスト ボックスに追加されます。その後で、[ルール設定（Rule Configuration）] > [推奨（Recommendation）] で [イベントを生成する（Generate Events）] をクリックすると、フィルタが「`Recommendation:"Generate Events"`」に変更されます。

侵入ルール コンテンツ フィルタ

[ルール（Rules）]ページに表示されたルールをいくつかのルール コンテンツ項目でフィルタ処理できます。たとえば、ルールの SID を検索することによって、ルールをすばやく取得できます。特定の宛先ポートに送信されるトラフィックを検査するすべてのルールを検索することもできます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定できます。そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [ルール コンテンツ（Rule Content）] で [SID] をクリックすると、ポップアップ ウィンドウが開いてSIDの入力が促されます。「`1045`」と入力すると、「`SID:"1045"`」がフィルタ テキストボックスに追加されます。その後で、再度 [SID] をクリックして、SID フィルタを「`1044`」に変更すると、フィルタが「`SID:"1044"`」に変更されます。

表 *85*：ルール コンテンツ フィルタ

フィルタ	検索するルールの内容
メッセージ	メッセージ フィールドで指定された文字列を含む。
SID	指定された SID がある。
GID	指定された GID がある。
参照	参照フィールドで指定された文字列を含む。また、特定のタイプの参照および指定された文字列でフィルタリングすることもできます。
操作	`alert` または `pass` から開始する。
プロトコル	選択されたプロトコルを含む。
方向（Direction）	ルールに、指定された方向設定が含まれているかどうかに基づく。
ソース IP	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用する。有効な IP アドレス、CIDR ブロック/プレフィックス長、または `$HOME_NET` や `$EXTERNAL_NET` などの変数を使用してフィルタ処理できます。
宛先 IP（Destination IP）	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用する。有効な IP アドレス、CIDR ブロック/プレフィックス長、または `$HOME_NET` や `$EXTERNAL_NET` などの変数を使用してフィルタ処理できます。
ソース ポート	指定された送信元ポートを含む。ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。
接続先ポート（Destination port）	指定された宛先ポートを含む。ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。
ルールのオーバーヘッド	選択されたルールのオーバーヘッドがある。
メタデータ	一致するキーと値のペアを含むメタデータがある。たとえば、HTTP アプリケーション プロトコルに関連するメタデータを使用したルールを検索するには、「`metadata:"service http"`」と入力します。

侵入ルール カテゴリ

Firepower システムは、ルールが検出するトラフィックのタイプに基づいてカテゴリにルールを配置します。[ルール（Rules）]ページで、ルール カテゴリでフィルタ処理することによって、カテゴリ内のすべてのルールにルール属性を設定できます。たとえば、ネットワーク上に Linux ホス

トが存在しない場合は、os-linux カテゴリでフィルタ処理してから、表示されたすべてのルールを無効にすることによって、os-linux カテゴリ全体を無効にすることができます。

カテゴリ名の上にポインタを移動すると、そのカテゴリ内のルールの数を表示できます。

（注） Cisco Talos Security Intelligence and Research Group（Talos）がルール更新メカニズムを使用してルール カテゴリを追加または削除する場合があります。

侵入ルールのフィルタ コンポーネント

フィルタ パネルでフィルタをクリックしたときに入力される特殊なキーワードとその引数を変更するようにフィルタを編集できます。[ルール（Rules）] ページのカスタム フィルタはルール エディタで使用されるものと同様に機能しますが、フィルタ パネルを通してフィルタを選択したときに表示される構文を使用して、[ルール（Rules）] ページのフィルタに入力されたキーワードのいずれかを使用することもできます。今後使用するキーワードを決定するには、右側のフィルタ パネルで該当する引数をクリックします。フィルタ キーワードと引数構文がフィルタ テキスト ボックスに表示されます。キーワードのカンマ区切りの複数の引数は [カテゴリ（Category）] と [優先度（Priority）] のフィルタ タイプでしかサポートされないことに注意してください。

引用符内のキーワードと引数、文字列、およびリテラル文字列と一緒に、複数のフィルタ条件を区切るスペースを使用できます。ただし、正規表現、ワイルドカード文字、および除外文字（!）、「大なり」記号（>）、「小なり」記号（<）などの特殊な演算子をフィルタに含めることはできません。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[カテゴリ（Category）]、[メッセージ（Message）]、および [SID] の各フィールドで指定された単語が検索されます。

`gid` キーワードと `sid` キーワードを除くすべての引数と文字列が部分文字列として扱われます。`gid` と `sid` の引数は、完全一致のみを返します。

各ルール フィルタに、次の形式で 1 つ以上のキーワードを含めることができます。

keyword:*"argument"*

ここで、Keyword は侵入ルール フィルタ グループ内のキーワードのいずれかで、argument は二重引用符で囲まれ、キーワードに関連した特定のフィールド内で検索される単一の大文字と小文字が区別されない英数字文字列です。キーワードは先頭文字を大文字にして入力する必要があることに注意してください。

`gid` と `sid` を除くすべてのキーワードの引数が部分文字列として扱われます。たとえば、引数 `123` によって `"12345"`、`"41235"`、`"45123"` などが返されます。`gid` と `sid` の引数は完全一致のみを返します。たとえば、`sid:3080` は `SID 3080` のみを返します。

各ルール フィルタに、1 つ以上の英数字文字列を含めることもできます。文字列はルールの [メッセージ（Message）] フィールド、Snort ID（SID）、およびジェネレータ ID（GID）を検索します。たとえば、文字列 `123` は、ルール メッセージ内の文字列 `"Lotus123"` や `"123mania"` などを返し、`SID 6123` や `SID 12375` なども返します。部分的な SID を検索するには、1 つ以上の文字列を使ってフィルタ処理できます。

すべての文字列では大文字と小文字が区別されず、部分的な文字列として扱われます。たとえば、文字列 `ADMIN`、`admin`、または `Admin` はすべて、`"admin"`、`"CFADMIN"`、`"Administrator"` などを返します。

文字列を引用符で囲むと、完全一致を返すことができます。たとえば、引用符付きのリテラル文字列 `"overflow attempt"` は完全一致のみを返しますが、引用符なしの 2 つの文字列 `overflow` と `attempt` で構成されるフィルタは `"overflow attempt"`、`"overflow multipacket attempt"`、`"overflow with evasion attempt"` などを返します。

複数のキーワード、文字列、またはその両方をスペースで区切って任意に組み合わせて入力することで、フィルタリングの結果を絞り込むことができます。結果には、すべてのフィルタ条件に一致するルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のフィルタはそれぞれ同じルールを返します。

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

侵入ルール フィルタの使用

侵入ポリシー内の [ルール（Rules）] ページの左側にあるフィルタ パネルから事前定義のフィルタ キーワードを選択できます。フィルタを選択すると、ページに、すべての一致するルールが表示されるか、どのルールも一致しなかったことが表示されます。

フィルタにキーワードを追加してさらに絞り込むことができます。入力されたフィルタは、ルール データベース全体を検索して、一致するすべてのルールを返します。前回のフィルタ結果がページに表示されている状態でフィルタを入力すると、そのページの内容が消去され、代わりに新しいフィルタの結果が返されます。

また、フィルタを選択したとき、または、フィルタを選択後にその中の引数値を変更したときに指定したものと同じキーワードと引数の構文を使用してフィルタを入力することもできます。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[カテゴリ（Category）]、[メッセージ（Message）]、および [SID] の各フィールドで指定された単語が検索されます。

侵入ポリシー内のルール フィルタの設定

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

[ルール（Rules）] ページで、ルールのサブセットを表示するようにルールをフィルタ処理できます。その後で、いずれかのページ機能を使用できます。これには、コンテキスト メニューで使用可能な機能の選択も含まれます。これは、特定のカテゴリのすべてのルールのしきい値を設定する場合などに便利です。フィルタ処理されている場合もされていない場合も、リスト内のルールで同じ機能を使用できます。たとえば、新しいルール状態を、フィルタ処理されたリスト内のルールまたはフィルタ処理されていないリスト内のルールに適用できます。

すべてのフィルタのキーワード、キーワード引数、および文字列では大文字と小文字が区別されません。フィルタ内に存在するキーワードの引数をクリックすると、既存の引数が置き換えられます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルール（Rules）] をクリックします。

ステップ 4 次に示す方法を個別に使用したり、組み合わせて使用することでフィルタを作成します。

- [フィルタ（Filter）] テキスト ボックスに値を入力して、Enter キーを押します。
- 事前定義されたキーワードのいずれかを展開します。たとえば、[ルール設定（Rule Configuration）] をクリックします。
- キーワードをクリックして、プロンプトが表示されたら引数の値を指定します。次に例を示します。
  - [ルール設定（Rule Configuration）] の下で、[ルール状態（Rule State）] をクリックし、ドロップダウンリストから [イベントの生成（`Generate Events`）] を選択して、[OK] をクリックします。
  - [ルール設定（Rule Configuration）] の下で、[コメント（Comment）] をクリックし、フィルタ条件として使用するコメント テキストの文字列を入力して、[OK] をクリックします。
  - [カテゴリ（Category）] の下で、[アプリ検出（app-detect）] をクリックします。システムは、これを引数の値として使用します。
- キーワードを展開して、引数の値をクリックします。たとえば、[ルール状態（Rule State）] を展開して、[イベントの生成（Generate Events）] をクリックします。

侵入ルールの状態

侵入ルールの状態により、個々の侵入ポリシー内のルールを有効または無効にできるだけでなく、モニタ対象の条件によってルールがトリガーされたときにシステムが実行するアクションを指定できます。

各デフォルト ポリシーの侵入ルールとプリプロセッサ ルールのデフォルト状態は、Cisco Talos Security Intelligence and Research Group（Talos）が設定します。たとえば、ルールを Security over Connectivity デフォルト ポリシーでは有効にして、Connectivity over Security デフォルト ポリシーでは無効にすることができます。Talos がルール更新を使用してデフォルト ポリシー内の 1 つ以上のルールのデフォルト状態を変更する場合もあります。ルール更新での基本ポリシーの更新を許可すると、ポリシーの作成時に使用されたデフォルト ポリシー（または基礎となるデフォルト ポリシー）のデフォルト状態が変更されたときの、そのポリシー内のルールのデフォルト状態の変更も許可することになります。ただし、ルール状態を変更している場合は、ルール更新でその変更が上書きされないことに注意してください。

侵入ルールを作成すると、そのルールは、ポリシーの作成時に使用されたデフォルト ポリシー内のルールのデフォルト状態を継承します。

侵入ルールの状態オプション

侵入ポリシーでは、ルールの状態を次の値に設定できます。

イベントを生成する（Generate Events）

システムで特定の侵入試行を検出して、一致したトラフィックが見つかった時点で侵入イベントを生成する場合。悪意のあるパケットがネットワークを通過してルールをトリガーすると、そのパケットが宛先に送信され、システムが侵入イベントを生成します。悪意のあるパケットはその対象に到達しますが、イベント ロギングによって通知されます。

ドロップおよびイベントの生成（Drop and Generate Events）

システムで特定の侵入試行を検出して、その攻撃を含むパケットをドロップし、一致したトラフィックが見つかった時点で侵入イベントを生成する場合。悪意のあるパケットはその対象に到達せず、イベント ロギングによって通知されます。

このルール状態に設定されたルールはイベントを生成しますが、7000 または 8000 シリーズ デバイスのインライン インターフェイス セットがタップ モードの場合の展開を含むパッシブ展開ではパケットをドロップしないことに注意してください。システムがパケットをドロップするには、侵入ポリシーで [インライン時にドロップ（Drop when Inline）] を有効にして、デバイス インラインを展開する必要もあります。

Disable

システムで一致するトラフィックを評価しない場合。

（注） [イベントを生成する（Generate Events）] または [ドロップおよびイベントの生成（Drop and Generate Events）] オプションのいずれかを選択すると、ルールが有効になります。[無効（Disable）] を選択すると、ルールが無効になります。

シスコでは、侵入ポリシー内のすべての侵入ルールを有効に**しない**ことを**強く**推奨しています。すべてのルールが有効になっている場合は、管理対象デバイスのパフォーマンスが低下する可能性があります。代わりに、できるだけネットワーク環境に合わせてルール セットを調整してください。

侵入ルール状態の設定

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

侵入ルール状態は、ポリシー固有です。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ヒント このページには、有効なルールの総数、[イベントを生成する（Generate Events）] に設定された有効なルールの総数、および [ドロップしてイベントを生成する（Drop and Generate Events）] に設定された有効なルールの総数が表示されます。また、パッシブ展開では、[ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールで行われるのはイベントの生成のみであることにも注意してください。

ステップ 3 ナビゲーション ウィンドウで、[ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 ルール状態を設定する 1 つ以上のルールを選択します。

ステップ 5 次のいずれかを実行します。

- [ルール状態（Rule State）] > [イベントの生成（Generate Events）]
- [ルール状態（Rule State）] > [ドロップしてイベントを生成する（Drop and Generate Events）]

- [ルール状態（Rule State）] > [無効化（Disable）]

ステップ 6 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、ナビゲーション ウィンドウで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

侵入ポリシーの侵入イベント通知のフィルタ

侵入イベントの重要度は、発生頻度、送信元 IP アドレス、または宛先 IP アドレスに基づいて設定できます。イベントが特定の回数発生するまで注意が必要ない場合もあります。たとえば、何者かがサーバにログインしようとしても、特定の回数失敗するまで、気にする必要はありません。一方、ほんの少数の発生を見れば、広範な問題があることを理解できる場合もあります。たとえば、Web サーバに対して DoS 攻撃が行われた場合は、少数の侵入イベントの発生を確認しただけで、その状況に対処しなければならないことが分かります。同じイベントが何百回も確認されれば、システムの機能が麻痺します。

侵入イベントのしきい値

指定された期間内にイベントが生成された回数に基づいて、システムが侵入イベントを記録して表示する回数を制限するための個別のルールのしきい値を侵入ポリシー単位で設定できます。これにより、大量の同じイベントが原因で機能が麻痺するのを避けることができます。共有オブジェクトのルール、標準テキストルール、またはプリプロセッサルールごとにしきい値を設定できます。

侵入イベントしきい値の設定

しきい値を設定するには、最初にしきい値のタイプを指定します。

表 *86*：しきい値設定オプション

オプション	説明
制限（Limit）	指定された数のパケット（count引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [制限（Limit）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。

オプション	説明
しきい値（Threshold）	指定された数のパケット（count引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [しきい値（Threshold）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[秒（Seconds）] と [カウント（Count）] のカウンタを 0 にリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。
両方	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [両方（Both）] に、[カウント（Count）] を 2 に、[秒（Seconds）] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される）。

次に、トラッキングを指定します。これにより、イベントしきい値が送信元 IP アドレス単位と宛先 IP アドレス単位のどちらで計算されるかが決まります。

表 *87*：*IP* しきい値設定オプション

オプション	説明
ソース（Source）	送信元 IP アドレス単位でイベント インスタンス カウントを計算します。
[接続先（Destination）]	宛先 IP アドレス単位でイベント インスタンス カウントを計算します。

最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 *88*：インスタンス/時間のしきい値設定オプション

オプション	説明
メンバー数（Count）	しきい値を満たすために必要な、追跡する IP アドレス単位で指定された期間単位のイベント インスタンスの数。

オプション	説明
秒（Seconds）	カウントがリセットされるまでの秒数。しきい値タイプを [制限（limit）] に、トラッキングを [送信元 IP（Source IP）] に、[カウント（count）] を 10 に、[秒（seconds）] を 10 に設定した場合は、システムが指定された送信元ポートから 10 秒間に発生した最初の 10 のイベントを記録して表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。

侵入イベントのしきい値設定は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベント抑制のいずれかと組み合わせて使用することもできます。

ヒント 侵入イベントのパケット ビューでしきい値を追加することもできます。

関連トピック

detection_filter キーワード, （1223 ページ）
パケット ビュー内でのしきい値オプションの設定, （1991 ページ）

侵入イベントのしきい値の変更と追加

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

侵入ポリシーの 1 つ以上の特定のルールにしきい値を設定できます。既存のしきい値設定を個別にまたは同時に変更することもできます。それぞれに 1 つずつのしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

また、侵入ポリシーに関係したすべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。

無効な値を入力するとフィールドに復元アイコン（）が表示されます。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ヒント 複数の CPU を搭載した管理対象デバイスでグローバルしきい値または個別のしきい値を設定すると、予想より多くのイベントが生成される場合があります。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。
代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ナビゲーション（navigation）] ペインの [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 しきい値を設定するルールを選択します。

ステップ 5 [イベントのフィルタリング（Event Filtering）] > [しきい値（Threshold）] を選択します。 >

ステップ 6 [タイプ（Type）] ドロップダウン リストからしきい値のタイプを選択します。

ステップ 7 [追跡対象（Track By）] ドロップダウンリストから、イベント インスタンスが [送信元（Source）] IP アドレスまたは [宛先（Destination）] IP アドレスのどちらによって追跡されるかを選択します。

ステップ 8 [数（Count）] フィールドに値を入力します。

ステップ 9 [秒数（Seconds）] フィールドに値を入力します。

ステップ 10 [OK] をクリックします。

ヒント [イベント フィルタリング（Event Filtering）] カラムのルールの横にイベント フィルタ アイコン（  ）が表示されます。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がイベント フィルタの数を示します。

ステップ 11 最後のコミットからポリシーに加えられた変更を保存するには、[ポリシー情報（Policy information）] をクリックし、次に [変更をコミット（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

グローバル ルールのしきい値の基本, （1099 ページ）

侵入イベントしきい値の表示と削除

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

ルールに関する既存のしきい値設定を表示または削除することができます。[ルールの詳細（Rules Details）] ビューを使用してしきい値の既存の設定を表示することによって、それらがシステムに適切かどうかを確認できます。そうでない場合は、新しいしきい値を追加して既存の値を上書きすることができます。

侵入ポリシーによって記録されるすべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウの [ポリシー情報（Policy Information）] の直下にある [ルール（Rules）] をクリックします。

ステップ 4 表示または削除する、しきい値が設定された 1 つまたは複数のルールを選択します。

ステップ 5 選択した各ルールのしきい値を削除するには、[イベント フィルタリング（Event Filtering）] > [しきい値の削除（Remove Thresholds）] の順に選択します。

ステップ 6 [OK] をクリックします。

ステップ 7 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

グローバル ルールのしきい値の基本, （1099 ページ）

侵入ポリシーの抑制の設定

特定の IP アドレスまたは IP アドレスの範囲が特定のルールまたはプリプロセッサをトリガーしたときの侵入イベント通知を抑制できます。これは、誤検出を回避するのに役立ちます。たとえば、特定のエクスプロイトのように見えるパケットを伝送しているメール サーバが存在する場合は、そのメール サーバによってトリガーとして使用されたイベントに関するイベント通知を抑制

できます。ルールはすべてのパケットに対してトリガーとして使用されますが、本物の攻撃に対するイベントだけが表示されます。

侵入ポリシー抑制タイプ

侵入イベント抑制は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベントしきい値構成のいずれかと組み合わせて使用することもできることに注意してください。

ヒント 侵入イベントのパケット ビュー内から抑制を追加できます。また、侵入ルール エディタ ページ（[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]）や任意の侵入イベント ページ（イベントが侵入ルールによってトリガーされた場合）で右クリック コンテキスト メニューを使用して、抑制設定にアクセスすることもできます。

関連トピック

detection_filter キーワード, （1223 ページ）
パケット ビュー内でのしきい値オプションの設定, （1991 ページ）

特定のルールの侵入イベントの抑制

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

侵入ポリシーのルールに関連する侵入イベント通知を抑制できます。ルールに関する通知が抑制されると、ルールはトリガーとして使用されますが、イベントは生成されません。ルールの 1 つまたは複数の抑制を設定できます。リスト内の最初の抑制に最も高いプライオリティが割り当てられます。2 つの抑制が競合している場合は、最初の抑制のアクションが実行されます。

無効な値を入力するとフィールドに復元アイコン（）が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルの [ポリシー情報（Policy Information）] の直下にある [ルール（Rules）] をクリックします。

ステップ 4 抑制条件を設定する 1 つまたは複数のルールを選択します。

ステップ 5 [イベント フィルタリング（Event Filtering）] > [抑制（Suppression）] を選択します。

ステップ 6 [抑制タイプ（Suppression Type）] を選択します。

ステップ 7 抑制タイプとして [送信元（Source）] または [宛先（Destination）] を選択した場合は、[ネットワーク（Network）] フィールドに、IP アドレス、アドレス ブロック、または送信元 IP アドレスまたは宛先 IP アドレスとして指定する変数、あるいは、これらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。
システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 8 [OK] をクリックします。

ヒント 抑制するルールの横にある [イベント フィルタリング（Event Filtering）] カラムのルールの横にイベント フィルタ アイコン（）が表示されます。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がイベント フィルタの数を示します。

ステップ 9 最後のコミットからポリシーに加えられた変更を保存するには、[ポリシー情報（Policy information）] をクリックし、次に [変更をコミット（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

抑制条件の表示と削除

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

既存の抑制条件を表示または削除することもできます。たとえば、メール サーバがエクスプロイトのように見えるパケットを普段から送信しているという理由で、そのメール サーバの IP アドレスから送信されたパケットに関するイベント通知を抑制できます。その後、そのメール サーバが使用停止になり、その IP アドレスが別のホストに再割り当てされたら、その送信元 IP アドレスの抑制条件を削除する必要があります。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルの [ポリシー情報（Policy Information）] の直下にある [ルール（Rules）] をクリックします。

ステップ 4 抑制を表示または削除する 1 つまたは複数のルールを選択します。

ステップ 5 次の選択肢があります。

- ルールのすべての抑制を削除するには、[イベント フィルタリング（Event Filtering）] > [抑制の削除（Remove Suppressions）] を選択します。
- 特定の抑制設定を削除するには、ルールをクリックして、[詳細の表示（Show Details）] をクリックします。抑制設定を展開して、削除する抑制設定の横にある [削除（Delete）] をクリックします。

ステップ 6 [OK] をクリックします。

ステップ 7 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

動的侵入ルール状態

レート ベースの攻撃は、ネットワークまたはホストに過剰なトラフィックを送信することによって、低速化または正規の要求の拒否を引き起こし、ネットワークまたはホストを混乱させようとします。レートベースの防御を使用して、特定のルールの過剰なルール一致に対応してルール アクションを変更することができます。

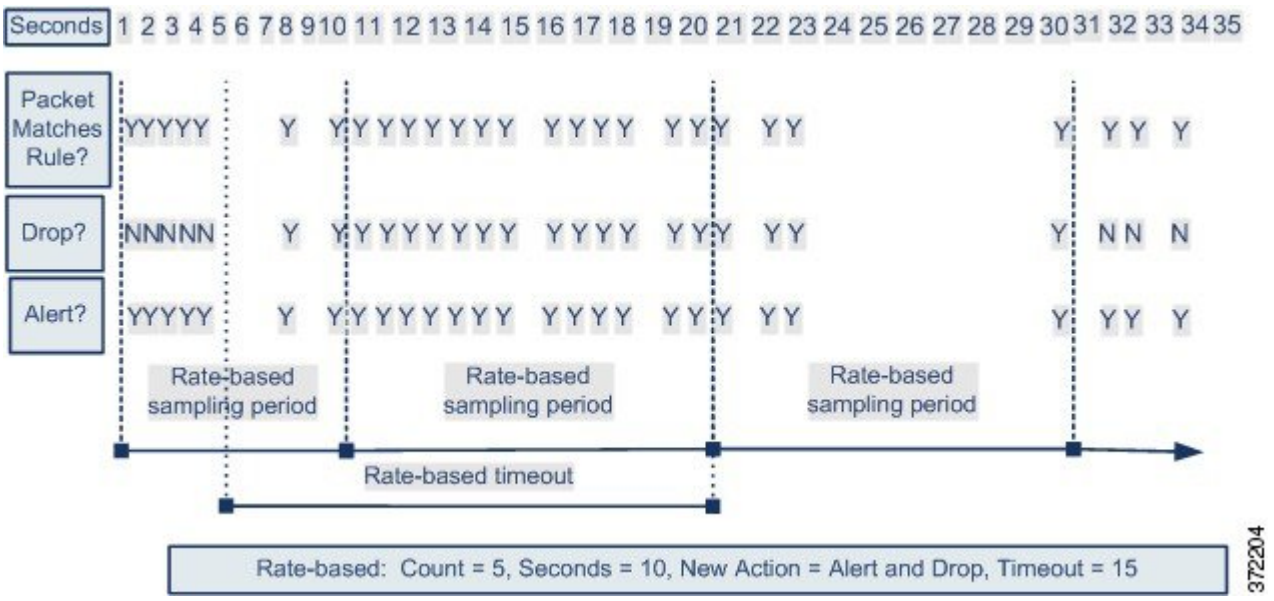
侵入ポリシーにレートベースのフィルタを含めることにより、一定期間においてルールの一致が過剰に発生した時点を検出できます。インライン展開された管理対象デバイス上でこの機能を使用して、指定された時刻のレートベースの攻撃をブロックしてから、ルール一致がイベントを生成するだけでトラフィックをドロップしないルール状態に戻すことができます。

レートベースの攻撃防止は、異常なトラフィック パターンを識別し、正規の要求に対するそのトラフィックの影響を最小限に抑えようとします。特定の宛先 IP アドレスに送信されるトラフィックまたは特定の送信元 IP アドレスから送信されるトラフィックの過剰なルール一致を識別できます。また、検出されたすべてのトラフィックを通して特定のルールの過剰な一致に対処することもできます。

ルールと一致したすべてのパケットをドロップするのではなく、指定された期間に特定の一致率に達した場合にルールと一致したパケットをドロップするために、ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] 状態に設定しない場合があります。動的ルール状態を使用すれば、ルールのアクションの変更をトリガーするレート、あるレートに達したときに変更すべきアクション、および新しいアクションの継続時間を設定できます。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。繰り返しパスワードを特定しようとする試みが、レートベースの攻撃防止が設定されたルールをトリガーします。レートベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [ドロップしてイベントを生成する（Drop and Generate Events）] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または過去のサンプリング期間のしきい値を上回っている場合は、新しいアクションが継続されます。新しいアクションは、サンプリング レートがしきい値レートを下回るサンプリング期間の終了後にのみ、[イベントを生成する（Generate Events）] に戻ります。



ダイナミックな侵入ルール状態の設定

侵入ポリシーでは、侵入ルールまたはプリプロセッサルールのレートベースのフィルタを設定できます。レート ベースのフィルタは次の 3 つの要素で構成されます。

- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率
- レートを超えた時点で実行される新しいアクション（[イベントを生成する（Generate Events）]、[ドロップしてイベントを生成する（Drop and Generate Events）]、および [無効（Disable）] の 3 種類がある）
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウトに達すると、レートがしきい値を下回っていれば、ルールのアクションがルールの初期設定に戻ります。

インライン展開のレート ベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レート ベースの設定を使用しない場合、[イベントを生成する（Generate Events）] に設定されたルールはイベントを生成しますが、システムはそのようなルールに関するパケットをドロップしません。ただし、攻撃トラフィックが、レート ベースの基準が設定されているルールに一致した場合、それらのルールが当初 [イベントのドロップおよび生成（Drop and Generate Events）]に設定されていないとしても、レート アクションがアクティブである期間は、パケットがドロップされる場合があります。

（注） レート ベース アクションでは、無効にされたルールを有効にすることも、無効にされたルールに一致するトラフィックをドロップすることもできません。

同じルールに複数のレート ベース フィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレート ベースのフィルタ アクションが競合している場合は、最初のレート ベースのフィルタのアクションが実行されることに注意してください。

[ルール（Rule）] ページからの動的ルール状態の設定

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

1 つのルールに対して 1 つ以上の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2 つの動的ルール状態が競合している場合は、最初のアクションが実行されます。

動的ルール状態はポリシー固有です。

無効な値を入力するとフィールドに復元アイコン（）が表示されます。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

（注） 動的ルール状態は、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで、[ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 動的ルール状態を追加する 1 つまたは複数のルールを選択します。

ステップ 5 [動的状態（Dynamic State）] > [レート ベースのルール状態の追加（Add Rate-Based Rule State）] を選択します。

ステップ 6 [追跡対象（Track By）] ドロップダウンリストから値を選択します。

ステップ 7 [追跡対象（Track By）] を [送信元（Source）] または [宛先（Destination）] に設定した場合は、[ネットワーク（Network）] フィールドに追跡する各ホストのアドレスを入力します。単一の IP アドレス、アドレス ブロック、変数、またはこれらの任意の組み合わせで構成されたカンマ区切りのリストを指定できます。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 8 [レート（Rate）] の横で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [カウント（Count）] フィールドに値を入力します。
- [秒数（Seconds）] フィールドに値を入力します。

ステップ 9 [新しい状態（New State）] ドロップダウンリストから、条件が満たされたときに実行する新しいアクションを指定します。

ステップ 10 [タイムアウト（Timeout）] フィールドに値を入力します。

タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションのタイムアウトを阻止する場合は、[0] を指定するか、[タイムアウト（Timeout）] フィールドを空白のままにします。

ステップ 11 [OK] をクリックします。

ヒント [動的状態（Dynamic State）] 列のルールの横に動的状態アイコン（）が表示されます。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

ヒント ルールのセットに対する動的ルール設定を削除するには、[ルール（Rules）] ページでルールを選択して、[動的状態（Dynamic State）]>[レート ベースの状態の削除（Remove Rate-Based States）] を選択します。また、ルールのルール詳細から個別のレート ベースのルール状態フィルタを削除するには、ルールを選択して、[詳細の表示（Show Details）] をクリックしてから、削除するレート ベースのフィルタのそばにある [削除（Delete）] をクリックします。

ステップ 12 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

侵入ルールのコメントの追加

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

侵入ポリシーのルールにコメントを追加できます。このようにして追加されたコメントはポリシー専用のコメントとなります。よって、ある侵入ポリシーのルールに追加したコメントは、他の侵入ポリシーでは表示されません。追加したコメントは、侵入ポリシーの [ルール（Rules）] ページ上の [ルールの詳細（Rule Details）] ビューで確認できます。

コメントを含む侵入ポリシーの変更をコミットしてから、ルールの [編集（Edit）] ページで [ルール コメント（Rule Comment）] をクリックしてコメントを表示することもできます。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）] を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。
代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ナビゲーション（navigation）] パネルの [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 コメントを追加する 1 つまたは複数のルールを選択します。

ステップ 5 [コメント（Comments）] > [ルール コメントの追加（Add Rule Comment）] の順に選択します。 >

ステップ 6 [コメント（Comments）] フィールドに、ルール コメントを入力します。

ステップ 7 [OK] をクリックします。

ヒント システムは [コメント（Comments）] カラムのルールの横にコメント アイコン（）を表示します。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

ステップ 8 必要に応じて、コメントの横にある [削除（Delete）] をクリックし、ルールのコメントを削除します。
侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけコメントを削除できます。侵入ポリシーの変更がコミットされた後は、ルール コメントを削除できなくなります。

ステップ 9 最後のコミットからポリシーに加えられた変更を保存するには、[ポリシー情報（Policy information）] をクリックし、次に [変更をコミット（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 51 章

ネットワーク資産に応じた侵入防御の調整

以下のトピックでは、Firepower 推奨ルールの使用方法について説明します。

Firepower 推奨ルールについて

Firepowerの侵入ルールの推奨事項を使用して、ネットワーク上で検出されたオペレーティングシステム、サーバ、およびクライアントアプリケーションプロトコルを、それらのアセットを保護するために作成されたルールに関連付けることができます。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。

システムは、侵入ポリシーごとに個別の推奨事項のセットを作成します。これにより、通常、標準テキストルールと共有オブジェクトルールのルール状態の変更が推奨されます。ただし、プリプロセッサおよびデコーダのルールの変更も推奨されます。

ルール状態の推奨事項を生成する場合は、デフォルト設定を使用するか、詳細設定を指定できます。詳細設定では次の操作が可能です。

- システムが脆弱性をモニタするネットワーク上のホストを再定義する。
- ルール オーバーヘッドに基づき、システムが推奨するルールに影響を与える。
- ルールを無効にする推奨事項を生成するかどうかを指定する。

推奨事項をすぐに使用するか、推奨事項（および影響を受けるルール）を確認してから受け入れることができます。

推奨ルール状態を使用することを選択すると、読み取り専用の Firepower 推奨レイヤが侵入ポリシーに追加されますが、後で、推奨ルール状態を使用しないことを選択すると、そのレイヤが削除されます。

侵入ポリシーに最近保存された構成設定に基づいて自動的に推奨を生成するためのタスクをスケジュールできます。

システムは、手動で設定されたルール状態を変更しません。

- 推奨を生成する前に指定したルールの状態を手動で設定すると、その後、システムはそのルールの状態を変更できなくなる。
- 推奨の生成後に指定したルールの状態を手動で設定すると、そのルールの推奨状態が上書きされる。

ヒント　侵入ポリシー レポートには、推奨状態と異なるルール状態を持つルールのリストを含めることができます。

推奨が絞り込まれた[ルール（Rules）]ページを表示している最中に、あるいは、ナビゲーションパネルまたは [ポリシー情報（Policy Information）] ページから [ルール（Rules）] ページに直接アクセスした後に、手動で、ルール状態を設定したり、ルールをソートしたり、[ルール（Rules）] ページで可能なその他の操作（ルールの抑制やルールしきい値の設定など）を実行することができます。

（注）　Cisco Talos Security Intelligence and Research Group（Talos）は、システム提供のポリシーでの各ルールの適切な状態を決定します。システム提供のポリシーを基本ポリシーとして使用し、システムがルールを Firepower の推奨ルール状態に設定できるようにする場合、侵入ポリシーのルールは、シスコが推奨するネットワーク アセットの設定と一致します。

推奨ルールおよびマルチテナンシー

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、先祖ドメインの侵入ポリシーでこの機能を有効にすると、システムはすべての子孫のリーフ ドメインからのデータを使用して、推奨事項を生成します。これにより、侵入ルールをすべてのリーフ ドメインに存在しない可能性があるアセットに調整することができ、パフォーマンスに影響を与えることができます。

Firepower 推奨のデフォルト設定

Firepower推奨を生成すると、システムがネットワーク資産に関連付けられた脆弱性から保護するルールの基本ポリシーを検索して、その基本ポリシー内のルールの現在の状態を特定します。システムによってルールの状態が推奨されますが、自身で設定する場合はルールを推奨される状態に設定します。

システムによって次の基本的な分析が実行され、推奨が生成されます。

表 *89*：脆弱性に基づく *Firepower* ルール状態推奨

基本ポリシー ルール状態	ルールは検出された資産を保護するか	推奨ルール状態
イベントの生成または無効化	Yes	イベントを生成する（Generate Events）
ドロップおよびイベントの生成	Yes	ドロップおよびイベントの生成（Drop and Generate Events）
任意	No	無効（Disable）

Firepower 推奨ルールの詳細設定を変更せずに推奨を生成する場合は、システムが検出対象のネットワーク全体のすべてのホストのルール状態の変更を推奨します。

デフォルトで、システムは、オーバーヘッドが低または中のルールに対してのみ推奨を生成し、ルールを無効にする推奨を生成します。

システムは、Impact Qualification 機能を使用して無効にされた脆弱性に基づく侵入ルールのルール状態を推奨しません。

システムは、常に、ホストにマップされたサードパーティの脆弱性に関連付けられたローカル ルールを有効にするように推奨します。

マップされていないローカル ルールに対する状態推奨は生成されません。

関連トピック

個々の脆弱性の非アクティブ化，（2088 ページ）
サードパーティ製品のマッピング，（1467 ページ）

Firepower 推奨の詳細設定

推奨とルール状態とのすべての差をポリシー レポートに含める（Include all differences between recommendations and rule states in policy reports）

デフォルトで、侵入ポリシー レポートには、ポリシーで有効になっているルール、つまり、[イベントを生成する（Generate Events）] と [ドロップしてイベントを生成する（Drop and Generate Events）] のいずれかに設定されているルールが表示されます。また、[すべての差を含める（Include all differences）] オプションを有効にすると、推奨されている状態が保存されている状態と異なるルールが一覧表示されます。ポリシー レポートの詳細については、ポリシー レポート，（332 ページ）を参照してください。

検査対象のネットワーク（Networks to Examine）

モニタ対象のネットワークまたは推奨について検査する個々のホストを指定します。1つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。

指定したホスト内のアドレスのリストは、否定以外の OR 演算でリンクされ、すべての OR 演算の実行後に AND 演算でリンクされます。

ホスト情報に基づいて特定のパケットのアクティブルール処理を動的に適応させる場合は、アダプティブ プロファイル を有効にすることもできます。

推奨しきい値（ルール オーバーヘッドの指定）（Recommendation Threshold (By Rule Overhead)）

選択したしきい値をオーバーヘッドが超える侵入ルールが推奨または自動的に有効にされないようにします。

オーバーヘッドは、システム パフォーマンスに対するルールの潜在的影響とルールが誤検出を引き起こす確率に基づいています。オーバーヘッドが高いルールを許可すると、通常、より多くの推奨が生成されるようになりますが、システム パフォーマンスに影響を及ぼす可能性があります。[侵入ルール（Intrusion Rules）] ページのルール詳細ビューでルールのオーバーヘッドの評価を確認できます。

ただし、ルールを無効にする推奨ではルール オーバーヘッドが考慮されません。また、ローカル ルールは、サードパーティの脆弱性にマップされていない限り、オーバーヘッドがないものと見なされます。

特定の設定のオーバーヘッド評価のルールについて推奨を生成した場合でも、別のオーバーヘッドの推奨を生成してから、再び元のオーバーヘッド設定の推奨を生成することができます。推奨を生成する回数や生成時に使用する異なるオーバーヘッド設定の数に関係なく、同じルール セットについては、推奨を生成するたびに、オーバーヘッド設定ごとに同じルール状態の推奨が生成されます。たとえば、オーバーヘッドを「中」に設定して推奨を生成し、次に「高」にして推奨を生成してから、再び「中」にして推奨を生成することができます。ネットワーク上のホストとアプリケーションが変更されていなければ、オーバーヘッドが「中」の推奨は、どちらも、そのルール セットに対して同じになります。

ルールを無効にする推奨を受け入れる（Accept Recommendations to Disable Rules）

Firepower の推奨に基づいて侵入ルールを無効にするかどうかを指定します。

ルールを無効にする推奨を受け入れると、ルールの適用範囲が制限されます。ルールを無効にする推奨を無視すると、ルールの適用範囲が拡大されます。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）
アダプティブプロファイルおよび Firepower 推奨ルール, （1430 ページ）

Firepower の推奨事項の生成と適用

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

Firepowerの推奨事項の使用を開始または停止する場合、ネットワークのサイズと侵入ルールセットに応じて、数分かかる場合があります。

システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、先祖ドメインの侵入ポリシーでこの機能を有効にすると、システムはすべての子孫のリーフ ドメインからのデータを使用して、推奨事項を生成します。これにより、侵入ルールをすべてのリーフ ドメインに存在しない可能性があるアセットに調整することができ、パフォーマンスに影響を与えることができます。

手順

ステップ 1 侵入ポリシー エディタのナビゲーション ウィンドウで、[Firepower の推奨事項（Firepower Recommendations）] をクリックします。

ステップ 2 （オプション）詳細設定を設定します。Firepower推奨の詳細設定, （1079ページ）を参照してください。

ステップ 3 推奨事項を生成して適用します。

- 推奨事項の生成および使用（Generate and Use Recommendations）：推奨事項を生成して、一致するようにルール状態を変更します。これまでに推奨事項を生成したことがない場合にのみ使用できます。
- 推奨事項の生成（Generate Recommendations）：推奨事項を使用しているかどうかに関係なく、新しい推奨事項を生成しますが、一致するようにルールの状態を変更しません。
- 推奨事項の更新（Update Recommendations）：推奨事項を使用している場合は、推奨事項を生成してルールの状態を一致するように変更します。それ以外の場合は、ルールの状態を変更することなく、新しい推奨事項を生成します。
- 推奨事項の使用（Use Recommendations）：ルールの状態を未実装の推奨事項に一致するように変更します。
- 推奨事項を使用しない（Do Not Use Recommendations）：推奨事項の使用を停止します。推奨事項の適用前にルールの状態を手動で変更した場合、ルールの状態は指定した値に戻ります。それ以外の場合、ルールの状態はデフォルト値に戻ります。

推奨事項の生成時に、システムは推奨される変更の概要を表示します。システムによって状態の変更が推奨されるルールのリストを表示するには、新しく提案されたルール状態の横にある [表示（View）] をクリックします。

ステップ 4 実装した推奨事項を評価して調整します。
ほとんどの Firepower の推奨事項を承認する場合でも、ルールの状態を手動で設定することで、個別の推奨事項を上書きできます。侵入ルール状態の設定, （1063 ページ）を参照してください。

ステップ 5 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

Firepower の推奨ルールの自動化, （205 ページ）

第 52 章

機密データの検出

ここでは、機密データ検出とその設定方法について説明します。

機密データ検出の基本

社会保障番号、クレジットカード番号、運転免許証番号などのセンシティブデータは、インターネットに意図的に、または誤って漏洩される可能性があります。システムには、ASCII テキストのセンシティブ データに関するイベントを検出し、生成できるセンシティブ データ プロセッサが用意されています。このプロセッサは、特に誤って漏洩されたデータの検出に役立ちます。

グローバル センシティブ データ プリプロセッサ オプションは、プリプロセッサの動作を制御します。以下のことを指定するグローバル オプションを変更できます。

- プリプロセッサが、ルールをトリガーしたパケットで、クレジットカード番号または社会保障番号の下位 4 桁を除くすべての桁を置換するかどうか
- センシティブ データをモニタする、ネットワーク上の宛先ホスト
- イベントの生成基準となる、単一のセッションでの全データ タイプの合計オカレンス数

個別のデータ タイプによって、指定した宛先ネットワーク トラフィックで検出しイベントを生成できるセンシティブ データを特定します。以下のことを指定するデータ タイプ オプションのデフォルト設定を変更できます。

- 検出されたデータ タイプに対して単一のセッションごとのイベントを生成する基準とするしきい値
- 各データ タイプをモニタする宛先ポート
- 各データ タイプをモニタするアプリケーション プロトコル

指定するデータ パターンを検出するためのカスタム データ タイプを作成および変更することができます。たとえば、病院で患者番号を保護するためのデータ タイプを作成したり、大学で固有の番号パターンを持つ学生番号を検出するためのデータ タイプを作成したりすることが考えられます。

システムはトラフィックに対して個別のデータ タイプを照合することによって、TCP セッションごとにセンシティブデータを検出します。侵入ポリシーの、各データ タイプのデフォルト設定およびすべてのデータ タイプに適用されるグローバル オプションのデフォルト設定は変更できます。Firepower システムには、一般的に使用されているデータ タイプがすでに定義されています。カスタム データ タイプを作成することも可能です。

センシティブ データのプリプロセッサ ルールは、各データ タイプに関連付けられます。各データ タイプのセンシティブ データ検出とイベント生成を有効にするには、そのデータ タイプに対応するプリプロセッサ ルールを有効にします。設定ページのリンクを使用すると、センシティブ データ ルールにフィルタリングされたビューが [ルール（Rules）] ページに表示されます。このビューで、ルールを有効または無効にしたり、その他のルール属性を設定したりできます。

変更を侵入ポリシーに保存する際に提示されるオプションによって、データ タイプに関連付けられたルールが有効になっていてセンシティブ データ検出が無効になっている場合には、自動的にセンシティブ データ プリプロセッサを有効にすることができます。

ヒント 機密データ プリプロセッサでは、FTP または HTTP を使用してアップロードおよびダウンロードされる暗号化されていない Microsoft Word ファイル内の機密データを検出できます。これが可能である理由は、Word ファイルが ASCII テキストとフォーマット設定コマンドを分けてグループ化する方式だからです。

このシステムは、暗号化または難読化された機密データ、あるいは圧縮または符号化された形式の機密データ（たとえば、Base64 でエンコードされた電子メールの添付ファイルなど）の検出は行いません。たとえば、システムは電話番号 (555)123-4567 を検出しますが、(5 5 5) 1 2 3 - 4 5 6 7 のようにスペースで難読化されたバージョン、あるいは (555)-123--4567 のように HTML コードが介在するバージョンは検出しません。ただし、(555)-123-4567 のように、HTML にコーディングされた番号のパターンの途中にコードが入っていなければ検出されます。

グローバル センシティブ データ検出オプション

グローバル センシティブ データ オプションはポリシーに固有であり、すべてのデータ タイプに適用されます。

マスク

ルールをトリガーしたパケットで、クレジット カード番号および社会保障番号の下位 4 桁を除くすべての桁を「X」に置換します。Web インターフェイスの侵入イベント パケット ビューおよびダウンロードされたパケットでは、マスクされた番号が表示されます。

ネットワーク

センシティブ データをモニタする 1 つ以上の宛先ホストを指定します。単一の IP アドレス、アドレス ブロック、あるいはこのいずれかまたは両方のカンマ区切りリストを指定できます。空白のフィールドは、`any` として解釈されます。これは、任意の宛先 IP アドレスを意味します。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

グローバルしきい値（Global Threshold）

グローバルしきい値イベントの生成基準となる、単一セッションでの全データ タイプの合計オカレンス数を指定します。データ タイプの組み合わせを問わず、プリプロセッサは指定された数のデータ タイプを検出すると、グローバルしきい値イベントを生成します。1 ～ 65535 の値を指定できます。

シスコでは、このオプションに、ポリシーで有効にする個々のデータ タイプに対するしきい値のどれよりも大きい値を設定することを推奨しています。

グローバルしきい値については、以下の点に注意してください。

- 複数のデータ タイプを合わせたオカレンス数を検出して イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、プリプロセッサ ルールの 139:1 を有効にする必要があります。
- プリプロセッサが生成するグローバルしきい値イベントは、セッションあたり最大 1 件です。
- グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立しています。つまり、グローバルしきい値に達すると、個別データ タイプに対するイベントしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も当てはまります。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）

個別のセンシティブ データ タイプのオプション

最低でも、カスタム データ タイプごとにイベントしきい値を指定し、モニタする少なくとも 1 つのポートまたはアプリケーション プロトコルを指定する必要があります。

各システム定義済みデータ タイプでは、デフォルト値が変更されない限り、アクセス不能な `sd_pattern` キーワードを使用して、トラフィックで検出する組み込みデータ パターンを定義します。カスタム データ タイプを作成して、そのデータ タイプに対し、単純な正規表現を使用して独自のデータ パターンを指定することもできます。

センシティブ データ タイプは、センシティブ データ検出が有効になっているすべての侵入ポリシーに表示されます。システム提供のデータ タイプは読み取り専用として表示されます。カスタム データ タイプの場合、名前とパターン フィールドは読み取り専用として表示されますが、他のオプションはポリシー固有の値に設定できます。

マルチドメイン展開では、現在のドメインで作成されたセンシティブデータ タイプが表示されます。これは編集できます。また、先祖ドメインで作成されたデータ タイプも表示されますが、これらは限定的に編集できます。先祖データ タイプの場合、名前とパターンフィールドは読み取り専用として表示されますが、他のオプションはポリシー固有の値に設定できます。

表 *90*：個別のデータ タイプのオプション

オプション	説明
データ タイプ	データ タイプの一意の名前を指定します。
しきい値（Threshold）	イベント生成の基準とする、データ タイプのオカレンス数を指定します。1 ～ 255 の値を指定できます。 プリプロセッサが検出したデータ タイプに対して生成するイベント数は、セッションごとに 1 つであることに注意してください。グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立していることにも注意してください。つまり、データ タイプ イベントしきい値に達すると、グローバル イベントしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も同様です。
宛先ポート（Destination Ports）	データ タイプでモニタする宛先ポートを指定します。単一のポート、複数のポートをカンマで区切ったリスト、または任意の宛先ポートを意味する `any` を指定できます。
アプリケーションプロトコル（Application Protocols）	データ タイプでモニタする最大 8 つのアプリケーション プロトコルを指定します。モニタするアプリケーションプロトコルを識別するには、アプリケーションディテクタをアクティブにする必要があります。 従来のデバイスの場合、この機能には制御ライセンスが必要であることに注意してください。
パターン	検出するパターンを指定します。このフィールドは、カスタムデータ タイプの場合にのみ存在します。

関連トピック

ディテクタのアクティブおよび非アクティブの設定, （1527 ページ）

システム提供のセンシティブ データのタイプ

それぞれの侵入ポリシーには、よく使用されるデータ パターンを検出するためのシステム提供のデータ タイプが含まれています。これらのデータ パターンには、クレジット カード番号、電子メールアドレス、米国の電話番号、および米国の社会保障番号などがあります（番号にはハイフン付きのパターン、ハイフン抜きのパターンがあります）。

それぞれのシステム提供のデータ タイプは、ジェネレータ ID（GID）が 138 に設定された単一のセンシティブデータのプリプロセッサルールに関連付けられます。侵入ポリシーで関連する機密データ ルールを有効にして、ポリシーで使用する各データ タイプに対して イベントを生成し、インライン展開では、違反パケットをドロップします。 する必要があります。

次の表に、各データ タイプの説明と対応するプリプロセッサ ルールの一覧を示します。

表 *91*：システム提供のセンシティブ データのタイプ

データ タイプ	説明	プリプロセッサ ルール GID:SID
クレジット カード番号	Visa®、MasterCard®、Discover®、および American Express® の 15 桁または 16 桁のクレジット カード番号（通常の区切り文字として使用されるハイフンまたはスペースが含まれるパターンと含まれないパターン）に一致します。また、Luhn アルゴリズムを使用してクレジット カード番号の検査数字を確認します。	138:2
電子メール アドレス	電子メール アドレスに一致します。	138:5
米国の電話番号	米国の電話番号（`(\d\{3\}) ?\d\{3\}-\d\{4\}` のパターンに準拠）に一致します。	138:6
米国の社会保障番号（ハイフンなし）	米国の 9 桁の社会保障番号（有効な 3 桁のエリア番号と有効な 2 桁のグループ番号が含まれ、ハイフンを使用していない番号）に一致します。	138:4
米国の社会保障番号（ハイフンあり）	米国の 9 桁の社会保障番号（有効な 3 桁のエリア番号と有効な 2 桁のグループ番号が含まれ、ハイフンを使用している番号）に一致します。	138:3

社会保障番号以外の 9 桁の番号からの誤検出を軽減するために、プリプロセッサでは、各社会保障番号の 4 桁のシリアル番号の前にある 3 桁のエリア番号と 2 桁のグループ番号を検証するアル

ゴリズムを使用します。プリプロセッサは 2009 年 11 月末までの社会保障グループ番号を検証します。

センシティブ データ検出の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	保護またはコントロール	任意（Any）	任意（Any）	Admin/Intrusion Admin

センシティブデータ検出は、Firepowerシステムのパフォーマンスに非常に大きな影響を与える可能性があるため、以下のガイドラインに従うことをお勧めします。

- 基本侵入ポリシーとして [アクティブなルールなし（No Rules Active）] デフォルト ポリシーを選択します。
- 次の設定が対応するネットワーク分析ポリシーで有効になっていることを確認します。
  - [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [FTP と Telnet の構成（FTP and Telnet Configuration）]
  - [トランスポートまたはネットワーク レイヤ プロセッサ（Transport/Network Layer Preprocessors）] の下の [IP 最適化（IP Defragmentation）] および [TCP ストリームの構成（TCP Stream Configuration）]

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）] を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [センシティブ データ検出（Sensitive Data Detection）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 次の選択肢があります。

- グローバル センシティブ データ検出オプション, （1085 ページ）の説明に従って、グローバル設定を変更します。
- [ターゲット（Targets）] セクションでデータ タイプを選択し、個別のセンシティブ データ タイプのオプション, （1086 ページ）の説明に従って、データ タイプ構成を変更します。
- カスタム センシティブ データを検査するには、カスタム 機密データ タイプ, （1092 ページ）を参照してください。

ステップ 7 データ タイプでモニタするアプリケーション プロトコルを追加または削除します。監視対象のアプリケーション プロトコルおよび機密データ, （1090 ページ）を参照してください。

（注） FTP トラフィックでセンシティブ データを検出するには、`Ftp data` アプリケーション プロトコルを追加します。

ステップ 8 オプションで、センシティブ データ プリプロセッサ ルールを表示するには、[センシティブ データ検出のルールの設定（Configure Rules for Sensitive Data Detection）] をクリックします。
リストされているルールを有効または無効にすることができます。[ルール（Rules）] ページで使用可能なその他の操作（ルールの抑制、レートベース攻撃防止など）のセンシティブデータ ルールも設定できます。詳細については、侵入ルールのタイプ, （1044 ページ）を参照してください。

ステップ 9 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーション パネルで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
ポリシーでセンシティブ データ プリプロセッサ ルールを有効にして、センシティブ データ検出を有効にしていなければ、変更をポリシーに保存する際に、センシティブ データ検出を有効にするよう求めるプロンプトが出されます。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次の作業

- 侵入イベントを生成する場合は、センシティブ データ検出ルール（138:2、138:3、138:4、138:5、138:6、138:>999999、または 139:1）を有効にします。詳細については、侵入ルールの状態, （1062 ページ）、グローバル センシティブ データ検出オプション, （1085 ページ）、システム提供のセンシティブ データのタイプ, （1087 ページ）、およびカスタム 機密データ タイプ, （1092 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

特別なケース：FTP トラフィックでのセンシティブ データの検出, （1092 ページ）

監視対象のアプリケーション プロトコルおよび機密データ

各データ タイプでモニタするアプリケーション プロトコルを最大 8 つ指定できます。選択するアプリケーション プロトコルごとに、少なくとも 1 つのディテクタを有効にする必要があります。デフォルトでは、すべてのディテクタがアクティブになっています。有効になっているディテクタがないアプリケーション プロトコルについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザ定義ディテクタが有効になります。

各データ タイプをモニタするアプリケーション プロトコルまたはポートを少なくとも 1 つ指定する必要があります。ただし、FTP トラフィックでセンシティブ データを検出する場合を除き、シスコでは最も包括的なカバレッジにするために、アプリケーション プロトコルを指定する際には対応するポートを指定することを推奨しています。たとえば、HTTP を指定するとしたら、既知の HTTP ポート 80 を設定することお勧めします。このように設定すると、ネットワークの新しいホストが HTTP を実装する場合には、システムは新しい HTTP アプリケーション プロトコルを検出する間、ポート 80 をモニタします。

FTP トラフィックでセンシティブ データを検出する場合は、`FTP data` アプリケーション プロトコルを指定する必要があります。この場合、ポート番号を指定する利点はありません。

関連トピック

ディテクタのアクティブおよび非アクティブの設定, （1527 ページ）
特別なケース：FTP トラフィックでのセンシティブ データの検出, （1092 ページ）

モニタ対象のアプリケーション プロトコルの選択

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

モニタ対象のアプリケーション プロトコルは、システムが提供するセンシティブ データ タイプとカスタムのセンシティブ データ タイプの両方で指定できます。選択するアプリケーション プロトコルはポリシー固有になります。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [センシティブ データの検出（Sensitive Data Detection）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 [データ タイプ（Data Types）] の下でデータ タイプの名前をクリックします。

ステップ 7 [アプリケーションプロトコル（Application Protocols）] フィールドの横にある編集アイコン（  ）をクリックします。

ステップ 8 次の選択肢があります。

- モニタするアプリケーション プロトコルを追加するには、[使用可能（Available）] リストからアプリケーション プロトコルを 1 つ以上選択して、右矢印（[>]）ボタンをクリックします。モニタするアプリケーション プロトコルは、8 つまで追加できます。
- モニタ対象からアプリケーションプロトコルを削除するには、[有効（Enabled）] リストから削除するプロトコルを選択して、左矢印（[<]）ボタンをクリックします。

ステップ 9 [OK] をクリックします。

ステップ 10 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、ナビゲーション ウィンドウで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

ポリシーの変更を確定しない場合、最後の確定以降の変更は、別のポリシーを編集するときに破棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

特別なケース：FTP トラフィックでのセンシティブ データの検出, （1092 ページ）

特別なケース：FTP トラフィックでのセンシティブ データの検出

一般に、センシティブ データをモニタするトラフィックを決めるには、導入でのモニタ対象のポートを指定するか、アプリケーション プロトコルを指定します。

ただし、FTP トラフィックでセンシティブ データを検出するには、ポートまたはアプリケーション プロトコルを指定するだけでは不十分です。FTP トラフィックのセンシティブ データは、FTP アプリケーションプロトコルのトラフィックで検出されますが、FTP アプリケーションプロトコルは断続的に発生し、一時的なポート番号を使用するため、センシティブ データを検出するのが困難です。FTP トラフィックでセンシティブ データを検出するには、以下の設定を含めることが**必須**となります。

- `FTP data` アプリケーション プロトコルを指定すると、FTP トラフィックでのセンシティブ データの検出が可能になります。

  FTP トラフィックでセンシティブ データを検出するという特殊な場合では、`FTP data` アプリケーションプロトコルを指定すると、検出が呼び出される代わりに、FTP トラフィックでセンシティブ データを検出するために FTP/Telnet プロセッサの高速処理が呼び出されます。

- FTP データ ディテクタが有効であることを確認します（デフォルトで有効にされています）。
- 設定に、センシティブ データをモニタするポートが少なくとも 1 つ含まれていることを確認します。

FTP トラフィックでセンシティブ データを検出することだけが目的の場合を除き（そのような場合はほとんどありません）、FTP ポートを指定する必要はありません。通常のセンシティブ データ設定には、HTTP ポートや電子メール ポートなどの他のポートが含まれることになります。モニタ対象の FTP ポートを 1 つだけ指定し、他のポートを指定しない場合、シスコでは FTP コマンド ポート `23` を指定することを推奨しています。

関連トピック

FTP/Telnet デコーダ, （1295 ページ）
ディテクタのアクティブおよび非アクティブの設定, （1527 ページ）
センシティブ データ検出の設定, （1088 ページ）

カスタム 機密データ タイプ

作成するカスタム データ タイプごとに、単一の機密データ プリプロセッサ ルールも作成します。このルールのジェネレータ ID（GID）は 138 で、Snort ID（SID）は 1000000 以上（これは、ローカル ルールの SID）です。 マルチドメイン展開では、子孫ドメインで作成されたか、または子孫ドメインにインポートされたカスタム ルールの SID の先頭にドメイン番号が追加されます。たとえば、グローバル ドメインに追加されたルールに 1000000 以上の SID があり、子孫ドメインに追加されたルールには [ドメイン番号]000000 以上の SID があります。

ポリシーで使用する各カスタム データ タイプに対し、関連付けられた機密データ ルールを有効にして検出を有効にし、イベントを生成し、インライン展開では、違反パケットをドロップします。 する必要があります。

機密データ ルールを有効にするには、設定ページに表示されるリンクを利用できます。このリンクを使用すると、すべてのシステム定義済み機密データ ルールおよびカスタム機密データ ルールを表示するフィルタリングされたビューの侵入ポリシーの [ルール（Rules）] ページが表示されます。また、侵入ポリシーの [ルール（Rules）] ページでローカル フィルタリング カテゴリを選択することで、カスタム機密データ ルールをカスタム ローカル ルールとともに表示できます。カスタム機密データ ルールは、侵入ルール エディタ ページ（[オブジェクト（Objects）]>[侵入ルール（Intrusion Rules）]）には表示されないことに注意してください。

カスタムデータ タイプを作成すると、システム内の任意の侵入ポリシーで、マルチドメイン展開の場合は現在のドメイン内の侵入ポリシーでそれを有効にすることができます。カスタム データ タイプを有効にするには、そのカスタムデータ タイプの検出に使用するポリシーで、関連する機密データ ルールを有効にする必要があります。

カスタム機密データ タイプのデータ パターン

カスタム データ タイプのデータ パターンを定義するには、以下の要素からなる単純な正規表現のセットを使用します。

- 3 つのメタ文字
- メタ文字をリテラル文字として使用するためのエスケープ文字
- 6 文字クラス

メタ文字は正規表現内で特別な意味を持つリテラル文字です。

表 *92*：機密データ パターンのメタ文字

メタ文字	説明	例
?	先行する文字またはエスケープ シーケンスのゼロまたは1つのオカレンスに一致します。つまり、先行する文字またはエスケープ シーケンスはオプションです。	`colou?r` は、`color` または `colour` に一致します。
{n}	先行する文字またはエスケープ シーケンスの n 回の繰り返しに一致します。	たとえば、`\d{2}` は `55`、`12` などに一致し、`\l{3}` は `AbC`、`www` などに、`\w{3}` は `a1B`、25C などに、`x{5}` は `xxxxx` に一致します。
\	メタ文字を実際の文字として使用できます。また、事前定義された文字クラスを指定するためにも使われます。	その他、`\?` は疑問符に、`\\` はバックスラッシュに、`\d` は数字に一致します

特定の文字をリテラル文字として機密データ プリプロセッサに正しく解釈させるには、バックスラッシュで文字をエスケープする必要があります。

表 *93*：機密データ パターンのエスケープ文字

使用するエスケープ文字	表現されるリテラル文字
\?	?
\{	{
\}	}
\\	\

カスタム機密データ パターンを定義するときは、文字クラスを使用できます。

表 *94*：機密データ パターンの文字クラス

文字クラス	説明	文字クラスの定義
\d	ASCII 文字の数字 0 ～ 9 に一致します。	0 ～ 9
\D	ASCII 文字の数字ではないバイトに一致します。	0 ～ 9 以外
\l（小文字の「エル」）	任意の ASCII 文字に一致します。	a ～ z および A ～ Z
\L	ASCII 文字ではないバイトに一致します。	a ～ z および A ～ Z 以外
\w	任意の ASCII 英数字に一致します。 PCRE 正規表現とは異なり、アンダースコア（_）は含まれないことに注意してください。	a ～ z、A ～ Z、および 0 ～ 9
\W	ASCII 英数字でないバイトに一致します。	a-zA-Z0-9 以外

プリプロセッサは、そのまま入力された文字を、正規表現の一部ではなく、リテラル文字として扱います。たとえば、データ パターン 1234 は `1234` に一致します。

以下に、システム定義済み機密データ ルール 138:4 で使用するデータ パターンの例を示します。このパターンでは、エスケープされた数値の文字クラス、複数個を示すメタ文字およびオプション指定子のメタ文字、リテラル ハイフン（-）文字、および左右の括弧 () 文字を使用して、米国の電話番号を検出します。

```
(\d{3}) ?\d{3}-\d{4}
```

カスタムデータ パターンを作成する際には注意が必要です。以下に、電話番号を検出するための別のデータ パターンを示します。このパターンでは有効な構文を使用しているものの、多数の誤検出が発生する可能性があります。

```
(?\d{3})? ?\d{3}-?\d{4}
```

上記の 2 番目の例では、オプションの括弧、オプションのスペース、オプションのハイフンを組み合わせているため、目的とする以下のパターンの電話番号が検出されます。

- `(555)123-4567`
- `555123-4567`
- `5551234567`

ただし、2 番目の例のパターンでは、以下の潜在的に無効なパターンも検出されて、結果的に誤検出となります。

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

最後に、説明目的の極端な例として、小規模な企業ネットワーク上のすべての宛先トラフィックで小さいイベントしきい値を使用して、小文字の a を検出するデータ パターンを作成するとします。このようなデータ パターンは、わずか数分で文字通り数百万ものイベントを生成することになり、システムを過負荷に陥らせる可能性があります。

カスタム センシティブ データ タイプの設定

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

マルチドメイン展開では、現在のドメインで作成されたセンシティブ データ タイプが表示されます。これは編集できます。また、先祖ドメインで作成されたデータ タイプも表示されますが、これらは限定的に編集できます。先祖のデータ タイプについては、名前およびパターン フィールドは読み取り専用として表示されますが、その他のオプションはポリシー固有の値に設定できます。

データ タイプのセンシティブ データ ルールがいずれかの侵入ポリシーで有効にされている場合、そのデータ タイプを削除することはできません。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）] を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [センシティブ データ検出（Sensitive Data Detection）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 [データ タイプ（Data Types）] の横にある追加アイコン（  ）をクリックします。

ステップ 7 データ タイプの名前を入力します。

ステップ 8 このデータ タイプで検出するパターンを入力します。カスタム機密データ タイプのデータ パターン，（1093 ページ）を参照してください。

ステップ 9 [OK] をクリックします。

ステップ 10 必要に応じて、データ タイプ名をクリックし、個別のセンシティブ データ タイプのオプション，（1086 ページ）で説明されているオプションを変更します。

ステップ 11 必要に応じて、削除アイコン（  ）をクリックしてカスタム データ タイプを削除し、[OK] をクリックして確認します。

（注） いずれかの侵入ポリシーでデータ タイプのセンシティブ データ ルールが有効になっている場合は、そのデータ タイプを削除できないことが警告されます。再度削除を試みる前に、影響を受けるポリシーでセンシティブ データ ルールを無効にする必要があります。侵入ルール状態の設定，（1063 ページ）を参照してください。

ステップ 12 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーション パネルで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次の作業

- データ型を使用する各ポリシーで、関連付けられたカスタム センシティブ データの前処理ルールを有効にします。侵入ルール状態の設定，（1063 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

関連トピック

カスタムセンシティブ データ タイプの編集, （1097 ページ）

カスタムセンシティブ データ タイプの編集

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

カスタム センシティブ データ タイプのすべてのフィールドを編集できます。ただし、名前またはパターン フィールドを変更すると、システム内のすべての侵入ポリシーのこれらの設定が変更されることに注意してください。その他のオプションは、ポリシー固有の値に設定できます。

マルチドメイン展開では、現在のドメインで作成されたセンシティブデータ タイプが表示されます。これは編集できます。また、先祖ドメインで作成されたデータ タイプも表示されますが、これらは限定的に編集できます。先祖のデータ タイプについては、名前およびパターン フィールドは読み取り専用として表示されますが、その他のオプションはポリシー固有の値に設定できます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）] を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 5 [センシティブ データ検出（Sensitive Data Detection）] の横にある [編集（Edit）] をクリックします。

ステップ 6 [ターゲット（Targets）] セクションで、カスタム データ タイプの名前をクリックします。

ステップ 7 [データ タイプの名前およびパターンの編集（Edit Data Type Name and Pattern）] をクリックします。

ステップ 8 データ タイプの名前およびパターンを変更します。カスタム機密データ タイプのデータ パターン, （1093 ページ）を参照してください。

ステップ 9 [OK] をクリックします。

ステップ 10 残りのオプションをポリシー固有の値に設定します。個別のセンシティブ データ タイプのオプション, （1086 ページ）を参照してください。

ステップ 11 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーション パネルで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 53 章

侵入イベント ロギングのグローバル制限

次のトピックでは、侵入イベント ロギングをグローバルに制限する方法について説明します。

グローバル ルールのしきい値の基本

グローバルルールのしきい値は、侵入ポリシーによってイベントロギングの限界を設定します。すべてのトラフィックに対するグローバル ルールのしきい値を設定して、指定された期間に特定の送信元または宛先からのイベントがポリシーで記録および表示される頻度を制限できます。ポリシー内で共有オブジェクトのルール、標準テキストルール、またはプリプロセッサルールごとにしきい値を設定できます。グローバルしきい値を設定すると、上書きする特定のしきい値を指定していないポリシー内の各ルールでそのしきい値が適用されます。しきい値により、多数のイベントでいっぱいになることを回避できます。

すべての侵入ポリシーにはデフォルトのグローバル ルールしきい値が含まれていて、デフォルトですべての侵入ルールとプリプロセッサ ルールに適用されます。このデフォルトのしきい値は、宛先へのトラフィックでのイベントの数を 60 秒あたり 1 個のイベントに制限しています。

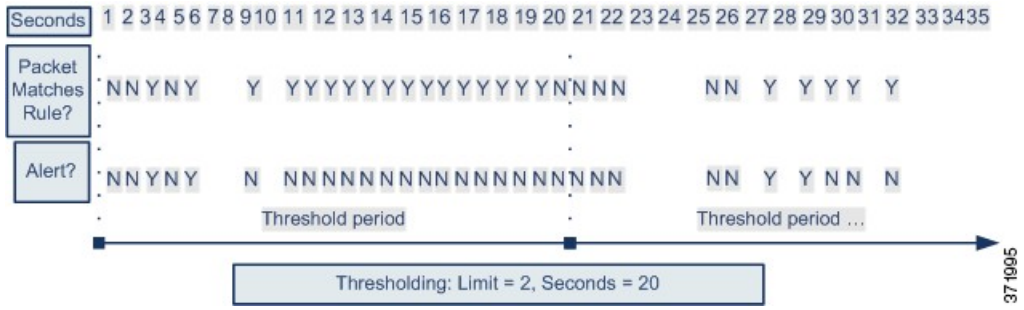
次の操作を実行できます。

- グローバルしきい値の変更。
- グローバルしきい値の無効化。
- 特定のルールに個別のしきい値を設定して、グローバルしきい値の上書き。

  たとえば、グローバル制限しきい値を 60 秒ごとに 5 個のイベントに設定してから、SID 1315 について特定のしきい値として 60 秒ごとに 10 個のイベントに設定できます。他のすべてのルールでは 60 秒ごとに 6 個以上のイベントは生成されませんが、SID 1315 では 60 秒ごとに最大 10 個のイベントが生成されます。

ヒント　複数の CPU を搭載した管理対象デバイスでグローバルしきい値または個別のしきい値を設定すると、予想より多くのイベントが生成される場合があります。

次の図で、グローバル ルールのしきい値がどのように機能するかを示します。この例では、特定のルールに対して攻撃が進行中です。グローバル制限しきい値は、各ルールのイベント生成が 20 秒あたり 2 つのイベントに制限されるように設定されています。期間は 1 秒で始まり 21 秒で終わることに注意してください。期間が終了すると、サイクルが再び開始され、次の 2 つのルール一致によってイベントが生成されます。その後、その期間にさらにイベントが生成されることはありません。



グローバル ルールしきい値オプション

デフォルトのしきい値では、各ルールのイベント生成が、同じ宛先に送られるトラフィックで 60 秒あたり 1 つのイベントに制限されます。グローバル ルールしきい値オプションのデフォルト値は次のとおりです。

- タイプ（Type）：制限（Limit）
- 追跡対象（Track By）：宛先（Destination）
- カウント（Count）：1
- 秒（Seconds）：60

これらのデフォルト値は次のように変更することができます。

表 *95*：しきい値のタイプ

オプション	説明
制限（Limit）	指定された数のパケット（count 引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。 たとえば、タイプを [制限（Limit）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。
しきい値（Threshold）	指定された数のパケット（count 引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。 たとえば、タイプを [しきい値（Threshold）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[秒（Seconds）] と [カウント（Count）] のカウンタを 0 にリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。
両方	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。 たとえば、タイプを [両方（Both）] に、[カウント（Count）] を 2 に、[秒（Seconds）] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される）。

[追跡対象（Track By）] オプションにより、イベント インスタンスの数が送信元 IP アドレスと宛先 IP アドレスのどちらに基づいて計算されるかが決まります。

また、しきい値を定義するインスタンスの数と期間を次のように指定できます。

表 *96*：インスタンス/時間のしきい値設定オプション

オプション	説明
メンバー数（Count）	[制限（Limit）] しきい値の場合は、しきい値を満たすために必要な、追跡する IP アドレスまたはアドレス範囲単位で指定された期間単位のイベント インスタンスの数。 [しきい値（Threshold）] しきい値の場合は、しきい値として使用するルールの一致回数。
秒（Seconds）	[制限（Limit）] しきい値の場合は、攻撃を追跡する期間の秒数。 [しきい値（Threshold）] しきい値の場合は、カウントをリセットするまでの経過時間（秒数）。しきい値タイプを [制限（Limit）] に、トラッキングを [送信元（Source）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 10 に設定した場合、特定の送信元ポートで 10 秒間に発生した最初の 10 のイベントを記録し表示します。最初の 10 秒で7個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。

関連トピック

グローバルなしきい値の設定, （1102 ページ）
侵入イベントのしきい値, （1064 ページ）

グローバルなしきい値の設定

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

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [侵入ルールしきい値（Intrusion Rule Thresholds）] で [グローバル ルールしきい値（Global Rule Thresholding）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [グローバル ルールしきい値（Global Rule Thresholding）] の横にある編集アイコン（）をクリックします。

ステップ 6 [タイプ（Type）] オプション ボタンを使用して、[秒（Seconds）] フィールドで指定された時間内に適用するしきい値のタイプを指定します。

ステップ 7 [追跡対象（Track By）] オプション ボタンを使用して、追跡方法を指定します。

ステップ 8 [カウント（Count）] フィールドに値を入力します。

ステップ 9 [秒（Seconds）] フィールドに値を入力します。

ステップ 10 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

グローバル ルールしきい値オプション, （1100 ページ）
レイヤでの侵入ルールの設定, （1026 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

グローバルしきい値の無効化

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

デフォルトですべてのルールにしきい値を適用するのではなく、特定のルールに関するイベントにしきい値を適用する場合は、最高位のポリシー階層でグローバルしきい値を無効にできます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）] を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [侵入ルールしきい値（Intrusion Rule Thresholds）] で、[グローバル ルールしきい値（Global Rule Thresholding）] の隣にある [無効（Disabled）] をクリックします。

ステップ 5 最後のポリシーの確定以降にこのポリシーに加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）
レイヤでの侵入ルールの設定, （1026 ページ）

第 54 章

侵入ルール エディタ

以下のトピックでは、侵入ルール エディタの使用方法について説明します。

侵入ルールの編集について

侵入ルールは、ネットワークの脆弱性を不正利用する試みを検出するために使用するキーワードや引数です。ネットワーク トラフィックの分析では、パケットを各ルールで指定した条件と比較します。パケットのデータがルールで指定したすべての条件に一致すると、そのルールがトリガーされます。アラート ルールであれば、侵入イベントが生成されます。通過ルールであれば、トラフィックを無視します。インライン展開の廃棄ルールでは、システムがパケットを破棄してイベントを生成します。侵入イベントは、Firepower Management Center の Web インターフェイスから表示して評価できます。

Firepower システムの侵入ルールには、共有オブジェクト ルールと標準テキスト ルールの 2 種類があります。Cisco Talos Security Intelligence and Research Group（Talos） では、共有オブジェクト ルールを使うことにより、従来の標準テキスト ルールではできなかった方法で脆弱性に対する攻撃を検出できます。共有オブジェクト ルールを作成することはできません。独自の侵入ルールを作成する場合は、標準テキスト ルールを作成します。

発生する可能性のあるイベントのタイプを調整するために、カスタム標準テキスト ルールを作成することができます。このマニュアルでは特定のエクスプロイトの検出を目的とするルールについて説明することもありますが、優秀なルールのほとんどは、特定の既知のエクスプロイトではなく既知の脆弱性を悪用しようとするトラフィックをターゲットとすることに注意してください。

ルールを作成してルールのイベント メッセージを指定することにより、攻撃とポリシー回避を示唆するトラフィックをより簡単に識別できます。

カスタム侵入ポリシーでカスタム標準テキストルールを有効にすると、一部のルールキーワードと引数では、トラフィックを特定の方法で最初に復号化または前処理する必要があることに留意してください。この章では、前処理を制御するネットワーク分析ポリシーで設定する必要があるオプションについて説明します。注意点として、必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーのWeb インターフェイスではプリプロセッサは無効のままになります。

注意 作成した侵入ルールを実稼働環境で使用する前に、制御されたネットワーク環境で必ずテストしてください。不適切に作成された侵入ルールは、システムのパフォーマンスに重大な影響を与える可能性があります。

マルチドメイン展開では、現在のドメインで作成されたルールが表示されます。これは編集できます。先祖ドメインで作成されたルールも表示されますが、これは編集できません。下位のドメインで作成されたルールを表示および編集するには、そのドメインに切り替えます。 システム提供の侵入ルールはグローバル ドメインに属します。子孫ドメインの管理者は、これらのシステムルールをローカルにコピーして編集できます。

ルールの詳細

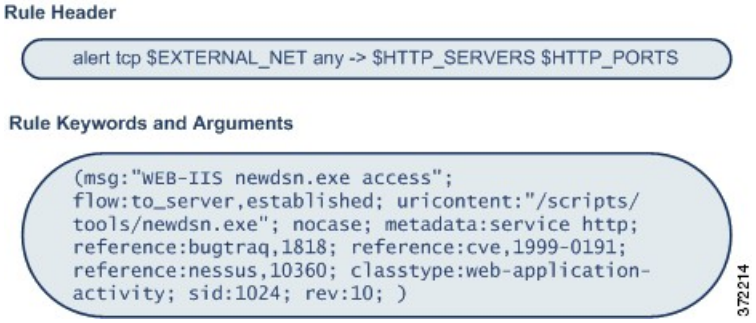
すべての標準テキスト ルールには、ルール ヘッダーとルール オプションという 2 つの論理セクションが含まれています。ルール ヘッダーの内容は次のとおりです。

- ルールのアクションまたはタイプ
- プロトコル
- 送信元および宛先の IP アドレスとネットマスク
- 送信元から宛先へのトラフィック フローを示す方向インジケータ
- 送信元ポートと宛先ポート

ルール オプション セクションの内容は次のとおりです。

- イベント メッセージ
- キーワードとそのパラメータおよび引数
- ルールをトリガーとして使用するためにパケットのペイロードが一致しなければならないパターン
- パケットのどの部分をルール エンジンで検査するかの指定

次の図に、ルールの構成要素を示します。



ルールのオプション セクションは、カッコで囲まれたセクションであることに注意してください。侵入ルールエディタは、標準テキストルールの作成を支援する使いやすいインターフェイスを備えています。

侵入ルール ヘッダー

すべての標準テキストルールおよび共有オブジェクトルールに、パラメータと引数を含むルールヘッダーがあります。ルール ヘッダーの構成要素を以下に示します。

次の表では、上記のルール ヘッダーの各部分について説明します。

表 *97*：ルール ヘッダーの値

ルールヘッダーのコンポーネント	値の例	機能
操作	`alert`	トリガー時に侵入イベントを生成します。
プロトコル	`tcp`	TCP トラフィックのみをテストします。
送信元 IP アドレス	`$EXTERNAL_NET`	内部ネットワーク上に存在しないホストから送られてきたトラフィックをテストします。
送信元ポート	任意	発信元ホスト上の任意のポートから送られてきたトラフィックをテストします。
演算子	`->`	（このネットワーク上の Web サーバに向かう）外部トラフィックをテストします。

ルールヘッダーのコンポーネント	値の例	機能
宛先 IP アドレス	`$HTTP_SERVERS`	この内部ネットワーク上の Web サーバとして指定された任意のホストに送られるトラフィックをテストします。
宛先ポート	`$HTTP_PORTS`	この内部ネットワーク上の HTTP ポートに送られるトラフィックをテストします。

（注） 前述の例では、ほとんどの侵入ルールの場合と同様に、デフォルト変数が使用されています。

関連トピック

変数セット，（397 ページ）

侵入ルール ヘッダー アクション

各ルール ヘッダーには、パケットがルールをトリガーとして使用したときにシステムで行われるアクションを指定するパラメータが 1 つ含まれています。アクションが [アラート（alert）] に設定されたルールは、それをトリガーとして使用したパケットに関する侵入イベントを生成し、そのパケットの詳細をログに記録します。アクションが *pass* に設定されたルールは、それをトリガーとして使用したパケットに関するイベントを生成せず、そのパケットの詳細も記録しません。

（注） インライン展開において、ルール状態が [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールは、それをトリガーとして使用したパケットに関する侵入イベントを生成します。また、パッシブ展開で廃棄ルールを適用した場合は、ルールがアラートルールとして機能します。

デフォルトでは、パス ルールがアラート ルールをオーバーライドします。パス ルールを作成することで、アラート ルールを無効にする代わりに、パス ルールで定義された基準を満たすパケットが特定の状況でアラート ルールをトリガーとして使用しないことを指定できます。たとえば、ユーザ "anonymous" として FTP サーバにログインする試行を検索するルールをアクティブのままにする必要があるとします。ただし、1 つ以上の正式な匿名 FTP サーバがネットワークに存在する場合、そのような特定のサーバで匿名ユーザにより最初のルールがトリガーとして使用されないことを指定するパス ルールを作成し、アクティブにすることができます。

侵入ルール エディタで、[アクション（Action）] リストからルール タイプを選択します。

侵入ルール ヘッダー プロトコル

各ルール ヘッダーで、ルールにより検査されるトラフィックのプロトコルを指定する必要があります。次のネットワーク プロトコルを分析対象として指定できます。

- ICMP（Internet Control Message Protocol）
- インターネット プロトコル（IP）

（注） プロトコルが `ip` に設定されている場合、システムは侵入ルール ヘッダー内のポート定義を無視します。

- 伝送制御プロトコル（TCP）
- ユーザ データグラム プロトコル（UDP）

TCP、UDP、ICMP、IGMP など、IANA によって割り当てられたすべてのプロトコルを検査するには、プロトコル タイプとして IP を使用します。

（注） 現在のところ、IP ペイロード内の次のヘッダー（TCP ヘッダーなど）でパターンを照合するルールを作成することはできません。代わりに、最後にデコードされたプロトコルからコンテンツ照合が始まります。次善策として、ルール オプションを使用して TCP ヘッダー内のパターンを照合できます。

侵入ルール エディタで、[プロトコル（Protocol）] リストからプロトコル タイプを選択します。

関連トピック

侵入ルール ヘッダー プロトコル, （1109 ページ）

侵入ルール ヘッダーの方向

ルールによる検査対象となるパケットが進むべき方向を、ルール ヘッダー内で指定できます。以下の表は、それらのオプションを示しています。

表 *98*：ルール ヘッダー内の方向オプション

使用するフィルタ	テスト対象
指向性	指定された送信元 IP アドレスから指定された宛先 IP アドレスに向かうトラフィックのみ
双方向	指定された送信元 IP アドレスと宛先 IP アドレスの間を移動するすべてのトラフィック

侵入ルール ヘッダーの送信元と宛先の IP アドレス

パケット検査の対象を、特定の IP アドレスから発信されたパケットまたは特定の IP アドレスに向かうパケットに制限すると、システムが実行しなければならないパケット検査の量が減ります。さらに、ルールをより具体化し、送信元および宛先 IP アドレスが疑わしい動作を示していないパケットに対してルールがトリガーとして使用される可能性をなくすと、誤検出も減ります。

ヒント システムは IP アドレスのみを認識し、送信元/宛先 IP アドレスのホスト名を受け入れません。

侵入ルール エディタの [送信元 IP（Source IPs）] フィールドと [宛先 IP（Destination IPs）] フィールドで、送信元および宛先の IP アドレスを指定します。

標準テキスト ルールの作成時には、必要に応じて、さまざまな方法で IPv4 アドレスと IPv6 アドレスを指定できます。単一の IP アドレス、`any`、IP アドレス リスト、CIDR 表記、プレフィクス長、ネットワーク変数、ネットワーク オブジェクトあるいはネットワーク オブジェクト グループを指定できます。加えて、1 つの特定の IP アドレスまたは IP アドレスのセットを除外するよう指定できます。IPv6 アドレスを指定するときには、RFC 4291 で定義された任意のアドレス指定規則を使用できます。

マルチドメイン展開では、この設定でリテラル IP アドレスを使用すると、予期しない結果になる可能性があります。たとえば、グローバル ドメイン内にリテラル送信元 IP アドレス（192.0.2.2）の侵入ルールを作成し、子孫ドメインで使用する侵入ポリシーでそのルールを有効にするとします。この場合、発生したイベントは子孫ドメイン A（192.0.2.2 が DeviceA を表すドメイン）と子孫ドメイン B（192.0.2.2 が DeviceB を表すドメイン）の両方で確認されることになりますが、侵入に対する脆弱性を確実に示すのは、いずれか一方のイベントのセットだけです。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

侵入ルールの *IP* アドレスの構文

次の表では、送信元と宛先の IP アドレスを指定するさまざまな方法を要約します。

表 *99*：送信元/宛先 *IP* アドレスの構文

指定する項目	使用するフィルタ	例
任意の IP アドレス	任意	任意
1 つの特定の IP アドレス	IP アドレス 同じルール内に IPv4 と IPv6 の送信元アドレスと宛先アドレスを混在させないでください。	`192.168.1.1` `2001:db8::abcd`
IP アドレスのリスト	複数の IP アドレスをカンマで区切り、それを大カッコ（`[]`）で囲む	`[192.168.1.1,192.168.1.15]` `[2001:db8::b3ff, 2001:db8::0202]`

指定する項目	使用するフィルタ	例
IPアドレスのブロック	IPv4 CIDR ブロックまたは IPv6 アドレス プレフィクス表記	`192.168.1.0/24` `2001:db8::/32`
特定の 1 つの IP アドレスまたはアドレス セットを除くすべて	拒否する IP アドレスの前に付ける「`!`」記号	`!192.168.1.15` `!2001:db8::0202:b3ff:fe1e`
特定の 1 つ以上の IP アドレスを除く、IPアドレスブロック内のすべて	アドレス ブロックの後に、除外アドレスのリストまたはブロック	`[10.0.0/8, !10.2.3.4, !10.1.0.0/16]` `[2001:db8::/32, !2001:db8::8329, !2001:db8::0202]`
ネットワーク変数で定義された IP アドレス	`$` で始まる大文字の変数名 プリプロセッサルールは、侵入ルールで使われているネットワーク変数で定義されたホストとは無関係に、イベントをトリガーできることに注意してください。	`$HOME_NET`
IPアドレス変数で定義されたアドレスを除く、すべての IP アドレス	大文字の変数名の前に `!$` を付ける	`!$HOME_NET`
ネットワーク オブジェクトまたはネットワーク オブジェクト グループで定義されたIP アドレス	`!{object_name}` という形式でオブジェクト名またはグループ名。	`${192.168sub16}`
ネットワーク オブジェクトまたはネットワーク オブジェクト グループで定義されたアドレスを除く、すべての IP アドレス	オブジェクト名またはグループ名を中カッコ（`{}`）で囲み、その前に `!$` を付ける。	`!${192.168sub16}`

以下の説明では、いくつかの IP アドレス入力方法に関する追加情報を提供します。

任意の IP アドレス

任意の IPv4 または IPv6 アドレスを示す「`any`」という単語を、ルールの送信元 IP アドレスまたは宛先 IP アドレスとして指定できます。

たとえば、次のルールでは [Source IPs] フィールドと [Destination IPs] フィールドで引数 any を使用して、任意の IPv4 または IPv6 の送信元または宛先アドレスを持つパケットを評価します。

```
alert tcp any any -> any any
```

また、任意の IPv6 アドレスを示すために :: を指定することもできます。

複数の IP アドレス

次の例に示すように、カンマを使って複数の IP アドレスを区切り、オプションで、非拒否リストを大カッコで囲むことにより、個別の IP アドレスを列挙できます。

```
[192.168.1.100,192.168.1.103,192.168.1.105]
```

IPv4 アドレスと IPv6 アドレスのいずれかだけを列挙することも、任意に組み合わせて列挙することもできます（次の例を参照）。

```
[192.168.1.100,2001:db8::1234,192.168.1.105]
```

以前のソフトウェア リリースでは IP アドレス リストを大カッコで囲む必要がありましたが、現在ではこれが必須でないことに注意してください。また、オプションで、リストを入力するときに各カンマの前または後にスペースを含めることができます。

（注） 否定リストは、大カッコで囲む必要があります。

また、IPv4 クラスレス ドメイン間ルーティング（CIDR）表記または IPv6 プレフィクス長を使用してアドレス ブロックを指定することもできます。次に例を示します。

- 192.168.1.0/24 は、サブネット マスク 255.255.255.0 の 192.168.1.0 ネットワーク内の IPv4 アドレス、つまり 192.168.1.0 ～ 192.168.1.255 を指定します。
- 2001:db8::/32 は、プレフィクス長 32 ビットの 2001:db8:: ネットワーク内の IPv6 アドレス、つまり 2001:db8:: ～ 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff を指定します。

ヒント IP アドレスのブロックを指定する必要があるが、CIDR またはプレフィクス長表記を単独で使ってそれを表現できない場合は、1 つの IP アドレス リスト内でいくつかの CIDR ブロックとプレフィクス長を使用できます。

ネットワーク オブジェクト

次の構文を使用して、ネットワーク オブジェクトまたはネットワーク オブジェクト グループを指定できます。

```
${object_name | group_name}
```

引数の説明

- object_name はネットワーク オブジェクトの名前です
- group_name はネットワーク オブジェクト グループの名前です

192.168sub16 という名前のネットワーク オブジェクトと all_subnets という名前のネットワーク オブジェクト グループをすでに作成済みであるとします。ネットワーク オブジェクトを使用して IP アドレスを特定するには、たとえば次のように指定できます。

```
${192.168sub16}
```

ネットワーク オブジェクト グループを使用するには、次のように指定できます。

```
${all_subnets}
```

さらに、ネットワーク オブジェクトとネットワーク オブジェクト グループで否定を使用することもできます。次に例を示します。

```
!${192.168sub16}
```

IP アドレスの否定

特定の IP アドレスを否定するために感嘆符（!）を使用できます。つまり、1 つ以上の特定の IP アドレスを除く、すべての IP アドレスに一致させることができます。たとえば、!192.168.1.1 は 192.168.1.1 以外の任意の IP アドレスを、!2001:db8:ca2e::fa4c は 2001:db8:ca2e::fa4c 以外の任意の IP アドレスを指定します。

一連の IP アドレスを拒否するには、大かっこで囲んだ IP アドレスのリストの前に「!」記号を付けます。たとえば、![192.168.1.1,192.168.1.5] は 192.168.1.1 と 192.168.1.5 を除くすべての IP アドレスを定義します。

（注） IP アドレスのリストを否定するには、大カッコを使用する必要があります。

否定文字と一緒に IP アドレス リストを使用する場合は注意が必要です。たとえば、192.168.1.1 と 192.168.1.5 を除くすべてのアドレスと一致させるために [!192.168.1.1,!192.168.1.5] を使用した場合、システムはこの構文を「192.168.1.1 以外のすべて、**または** 192.168.1.5 以外のすべて」と解釈します。

192.168.1.5 は 192.168.1.1 ではなく、192.168.1.1 は 192.168.1.5 ではないため、この両方の IP アドレスが [!192.168.1.1,!192.168.1.5] という IP アドレス値に一致します。つまり、実質的に「any」を使用するのと同じです。

代わりに ![192.168.1.1,192.168.1.5] を使用してください。システムはこの構文を「**192.168.1.1** でなく、**しかも** 192.168.1.5 でない」と解釈し、大カッコ内に列挙されたものを除くすべての IP アドレスに一致します。

論理的に言って、any を除外（negation）と同時に使用できないことに注意してください。any を除外すると「アドレスなし」を意味することになります。

関連トピック

変数セット，（397 ページ）

侵入ルール ヘッダーの送信元および宛先ポート

侵入ルール エディタの [送信元ポート（Source Port）] フィールドと [宛先ポート（Destination Port）] フィールドで、送信元および宛先ポートを指定します。

侵入ルールのポート構文

Firepower System では、特定のタイプの構文を使用して、ルール ヘッダーで使用されるポート番号を定義できます。

（注） プロトコルが `ip` に設定されている場合、システムは侵入ルール ヘッダー内のポート定義を無視します。

次の例に示すように、カンマでポートを区切ることによって、ポートのリストを指定できます。

```
80, 8080, 8138, 8600-9000, !8650-8675
```

任意により、次の例は、ポート リストを括弧で囲む方法を示します。この方法は旧バージョンのソフトウェアでは必要でしたが、今後は括弧で囲む必要ありません。

```
[80, 8080, 8138, 8600-9000, !8650-8675]
```

次の例に示すように、否定されたポート リストは括弧で示す必要がある点にご注意ください：

```
![20, 22, 23]
```

次の表に、使用可能な構文を要約します。

表 *100*：送信元/宛先ポート構文

指定する項目	用途	例
任意のポート	任意	任意
1 つの特定のポート	ポート番号	`80`
ポートの範囲	範囲内の最初のポート番号と最後のポート番号をダッシュでつなぐ	`80-443`

指定する項目	用途	例
1 つの特定のポートに等しい、またはより小さいすべてのポート	ポート番号の前にダッシュを付ける	`-21`
1 つの特定のポートに等しい、またはより大きいすべてのポート	ポート番号の後ろにダッシュを付ける	`80-`
1 つの特定のポートまたはポート範囲を除く、すべてのポート	否定する場合には、ポート、ポート リスト、ポート範囲の前に文字 ! を付けます。 否定が「ポートなし」を示す場合を除いて、すべてのポート宛先に論理上、否定を使用できる点にご注意ください。	`!20`
ポート変数で定義されるすべてのポート	$ の後ろに英大文字の変数名	`$HTTP_PORTS`
ポート変数で定義されるポートを除く、すべてのポート	!$ の後ろに英大文字の変数名	`!$HTTP_PORTS`

侵入イベント詳細

標準のテキスト ルールを作成するときには、ルールでエクスプロイト試行を検出する対象となる脆弱性についてのコンテキスト情報を含めることができます。また、脆弱性データベースへの外部参照を含めたり、組織内でイベントに設定するプライオリティを定義したりすることもできます。アナリストがイベントを認識すると、そのプライオリティ、エクスプロイト、および既知の対策についての情報をすぐに入手できます。

メッセージ

ルールのトリガー時にメッセージとして表示される、意味のあるテキストを指定できます。メッセージを読むと、ルールで攻撃試行を検出する対象となった脆弱性の特性をすぐに理解できます。中カッコ（{}）を除く、印字可能な任意の標準ASCII文字を使用できます。システムは、メッセージ全体を囲んでいる引用符を取り除きます。

ヒント ルール メッセージの指定は必須です。また、空白文字のみ、1 つ以上の引用符のみ、1 つ以上のアポストロフィのみ、あるいは空白文字/引用符/アポストロフィだけの組み合わせでメッセージを構成することはできません。

侵入ルール エディタでイベント メッセージを定義するには、[メッセージ（Message）] フィールドにイベント メッセージを入力します。

分類（Classification）

ルールごとに、イベントのパケット表示に含める攻撃分類を指定できます。次の表に、それぞれの分類の名前と番号を示します。

表 *101*：ルールの分類

番号（Number）	分類名	説明
1	not-suspicious	不審ではないトラフィック
2	unknown	不明なトラフィック
3	bad-unknown	有害な可能性のあるトラフィック
4	attempted-recon	情報漏えいが試行された
5	successful-recon-limited	情報漏えいが発生
[6]	successful-recon-largescale	大規模な情報漏えい
7	attempted-dos	サービス妨害が試行された
8	successful-dos	サービス妨害（DoS）
9	attempted-user	ユーザ特権の獲得が試行された
10	unsuccessful-user	ユーザ特権の獲得が失敗した
11	successful-user	ユーザ特権の獲得に成功
12	attempted-admin	管理者特権の獲得が試行された
13	successful-admin	管理者特権の獲得に成功
18	rpc-portmap-decode	RPC クエリのデコード
15	shellcode-detect	実行可能コードが検出された
16	string-detect	疑わしい文字列が検出された
17	suspicious-filename-detect	疑わしいファイル名が検出された
18	suspicious-login	疑わしいユーザ名を使用したログイン試行が検出された
19	system-call-detect	システム コールが検出された

番号（Number）	分類名	説明
20	tcp-connection	TCP 接続が検出された
21	trojan-activity	ネットワーク トロイの木馬が検出された
22	unusual-client-port-connection	通常とは異なるポートをクライアントが使用していた
23	network-scan	ネットワーク スキャンの検出
24	denial-of-service	サービス妨害攻撃の検出
25	non-standard-protocol	非標準プロトコルまたはイベントの検出
26	protocol-command-decode	一般的なプロトコル コマンド デコード
27	web-application-activity	脆弱な可能性のある Web アプリケーションへのアクセス
36	web-application-attack	Web アプリケーション攻撃
29	misc-activity	その他のアクティビティ
30	misc-attack	その他の攻撃
31	icmp-event	一般的な ICMP イベント
32	inappropriate-content	不適切な内容が検出された
33	policy-violation	企業プライバシー侵害の可能性
34	default-login-attempt	デフォルトのユーザ名とパスワードによるログイン試行
35	sdf	機密データ
36	malware-cnc	既知のマルウェア コマンドと制御トラフィック
37	client-side-exploit	既知のクライアント側エクスプロイト試行
38	file-format	既知の悪意のあるファイルまたはファイルベースのエクスプロイト

カスタム分類

定義したルールによって生成されるイベントのパケット表示記述の内容をもっとカスタマイズする必要がある場合には、カスタム分類を作成できます。

引数	説明
分類名	分類の名前。40 文字を超える文字を使用すると、ページが読みにくくなります。<>()\'"&$; 文字および空白文字はサポートされていません。
分類の説明	分類の説明。英数字とスペースを使用できます。<>()\'"&$; 文字はサポートされていません。
[プライオリティ（Priority）]	[高（High）]、[中（medium）]、または [低（low）]。

カスタム プライオリティ

デフォルトでは、ルールのイベント分類からルールのプライオリティが派生します。ただし、`priority` キーワードをルールに追加し、高、中、または低のプライオリティを選択することで、ルールの分類優先度を上書きすることができます。たとえば、Web アプリケーション攻撃を検出するルールに高プライオリティを割り当てるには、`priority` キーワードをルールに追加して、プライオリティとして [高（high）] を選択します。

カスタム参照

`reference` キーワードを使用すると、イベントに関する外部 Web サイトや追加情報への参照を追加できます。参照を追加すると、アナリストは参照情報をすぐに利用できるため、パケットがルールをトリガーとして使用した理由を特定するのに役立ちます。次の表に、既知のエクスプロイトや攻撃についてのデータを提供する外部システムをいくつか示します。

表 *102*：外部攻撃識別システム

システム ID（System ID）	説明	ID の例
bugtraq	[Bugtraq] ページ	8550
cve	[Common Vulnerabilities and Exposure] ページ	CAN-2003-0702
mcafee	[McAfee] ページ	98574
url	Web サイト参照	www.example.com?exploit=14
msb	Microsoft セキュリティ情報	MS11-082
nessus	[Nessus] ページ	10039
secure-url	セキュア Web サイト参照（https://...）	intranet/exploits/exploit=14 任意のセキュア Web サイトで secure-url を使用できることに注意してください。

次のように、参照値を入力して参照を指定します。

id_system,id
ここで、id_system はプレフィックスとして使用されるシステム、id は Bugtraq ID、CVE 番号、Arachnids ID、または URL（http://なし）です。

たとえば、Bugtraq ID 17134 に記載されている Microsoft Commerce Server 2002 サーバ上の認証バイパス脆弱性を指定するには、次の値を入力します。

bugtraq,17134
参照をルールに追加するときには、次の点に注意してください。

- カンマの後ろにスペースを入力しないでください。
- システム ID に大文字を使用しないでください。

関連トピック

カスタム分類の追加，（1120 ページ）
イベント優先順位の定義，（1120 ページ）
イベント参照の定義，（1121 ページ）

カスタム分類の追加

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

マルチドメイン展開では、現在のドメインで作成されたカスタム分類がシステムで表示されます。これらの分類には、優先度を設定できます。先祖ドメインで作成されたカスタム分類も表示されますが、これらの分類には優先度は設定できません。下位のドメインで作成されたカスタム分類を表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 ルールの作成または編集時に、[分類（Classification）] ドロップダウン リストから [分類の編集（Edit Classifications）] を選択します。
代わりに [分類の表示（View Classifications）] が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 侵入イベント詳細, （1115 ページ） の説明に従い、[分類名（Classification Name）] と [分類の説明（Classification Description）] を入力します。

ステップ 3 [優先度（Priority）] ドロップダウン リストから分類の優先度を選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [完了（Done）] をクリックします。

次の作業

- ルールの作成または編集を続けます。詳細については、新規ルールの作成, （1123 ページ） または 既存のルールの変更, （1124 ページ） を参照してください。

関連トピック

カスタム ルールの作成, （1122 ページ）

イベント優先順位の定義

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

手順

ステップ 1 ルールの作成または編集時に、[検出オプション（Detection Options）] ドロップダウン リストから [優先順位（priority）] を選択します。

ステップ 2 [Add Option] をクリックします。

ステップ 3 [優先順位（priority）] ドロップダウン リストから値を選択します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- ルールの作成または編集を続けます。詳細については、新規ルールの作成, （1123 ページ） または 既存のルールの変更, （1124 ページ） を参照してください。

関連トピック

カスタム ルールの作成, （1122 ページ）

イベント参照の定義

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

手順

ステップ 1 ルールの作成または編集時に、[検出オプション（Detection Options）] ドロップダウン リストから [参照（reference）] を選択します。

ステップ 2 [Add Option] をクリックします。

ステップ 3 侵入イベント詳細, （1115 ページ） の説明に従って、[参照（reference）] フィールドに値を入力します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- ルールの作成または編集を続けます。詳細については、新規ルールの作成, （1123 ページ） または 既存のルールの変更, （1124 ページ） を参照してください。

関連トピック

カスタム ルールの作成, （1122 ページ）

カスタム ルールの作成

カスタム侵入ルールは以下の方法で作成できます。

- 独自の標準テキスト ルールを作成する
- 既存の標準テキスト ルールを新規ルールとして保存する
- システムが提供する共有オブジェクト ルールを新規ルールとして保存する
- 先祖ルールを子孫ドメインにおける新規ルールとして保存する（マルチドメイン展開の場合）
- ローカル ルール ファイルをインポートする

作成方法に関わらず、システムはカスタム ルールをローカル ルールに分類して保存します。

カスタム侵入ルールを作成すると、システムは一意のルール番号（番号の形式は`GID:SID:Rev`）を割り当てます。この番号には次の要素が含まれます。

GID

ジェネレータ ID。標準テキスト ルールでは、値は 1 です。すべての共有オブジェクト ルールを新規ルールとして保存する場合、値は 3 です。

SID

Snort ID。ルールがシステム ルールのローカル ルールであるかどうかを示します。新しいルールを作成すると、システムは次に使用可能なローカル ルール SID 番号を割り当てます。

ローカル ルールの SID 番号は 1000000 から始まり、新しいローカル ルールにつき番号が 1 ずつ増えます。 マルチドメイン展開では、子孫ドメインで作成されたか、または子孫ドメインにインポートされたカスタム ルールの SID の先頭にドメイン番号が追加されます。たとえば、グローバル ドメインに追加されたルールに 1000000 以上の SID があり、子孫ドメインに追加されたルールには [ドメイン番号]000000 以上の SID があります。

Rev

改訂番号。新しいルールのリビジョン番号は 1 です。カスタム ルールを変更するたびに、リビジョン番号が 1 ずつ増えます。

カスタム標準テキスト ルールでは、ルール ヘッダー設定、ルール キーワード、およびルール引数を設定できます。特定のプロトコルを使用する、特定の IP アドレスまたはポートを行き来するトラフィックだけをルールで照合するよう、ルール ヘッダーを設定できます。

システムが提供する標準テキスト ルールまたは共有オブジェクト ルールのカスタム ルールで変更できるルール ヘッダー情報は、送信元と宛先ポートと IP アドレスなどの情報に限られます。ルール キーワードやルール引数は変更できません。

共有オブジェクト ルールのヘッダー情報を変更して変更内容を保存すると、ルールの新しいインスタンスが作成され、ジェネレータ ID（GID）3 、およびカスタム ルールとして次に使用可能な SID が割り当てられます。システムは、共有オブジェクト ルールの新しいインスタンスを予約済み `soid` キーワードにリンクします。これにより、新しく作成したルールが Cisco Talos Security Intelligence and Research Group（Talos） 作成のルールにマップされます。ユーザが作成した共有オブジェクト ルールのインスタンスは削除できますが、Talos が作成した共有オブジェクト ルールは削除できません。

新規ルールの作成

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

手順

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）] を選択し、[侵入ルール（Intrusion Rules）] をクリックします。
- [オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]を選択します。

ステップ 2 [Create Rule] をクリックします。

ステップ 3 [メッセージ（Message）] フィールドに値を入力します。

ステップ 4 次の各ドロップダウン リストから値を選択します。

- [分類（Classification）]
- 操作
- プロトコル
- 方向（Direction）

ステップ 5 次のフィールドに値を入力します。

- [送信元 IP（Source IPs）]
- [宛先 IP（Destination IPs）]
- 送信元ポート（Source Port）
- 宛先ポート（Destination Port）

これらのフィールドに値を指定しない場合、システムは値 [すべて（any）] を使用します。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 6 [検出オプション（Detection Options）] ドロップダウン リストから値を選択します。

ステップ 7 [Add Option] をクリックします。

ステップ 8 追加したキーワードの引数を入力します。

ステップ 9 必要に応じて、手順 6 ～ 8 を繰り返します。

ステップ 10 複数のキーワードを追加した場合、以下を実行できます。

- キーワードの並べ替え：移動するキーワードの横にある上矢印または下矢印をクリックします。
- キーワードの削除：そのキーワードの横にある [X] をクリックします。

ステップ 11 [新規として保存（Save As New）] をクリックします。

次の作業

- 該当する侵入ポリシー内の新規または変更されたルールを有効にします（侵入ポリシー内の侵入ルールの表示, （1045 ページ）を参照）。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

既存のルールの変更

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

カスタム侵入ルールは変更できます。マルチドメイン展開では、現在のドメインに属しているカスタム侵入ルールのみを変更できます。

システム提供のルールと先祖ドメインに属しているルールは、新しいカスタム ルールとしてローカル ルール カテゴリに保存してから変更できます。

手順

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）] を選択し、[侵入ルール（Intrusion Rules）] をクリックします。
- [オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]を選択します。

ステップ 2 変更するルールを見つけます。次の選択肢があります。

- フォルダからルールに移動します。
- ルールを検索します。ルールの検索, （1128 ページ）を参照してください。
- ルールが属しているグループにフィルタを適用します。フィルタリング ルール, （1133 ページ）を参照してください。

ステップ 3 ルールの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ルール タイプに応じて、ルールを変更します。

（注） 共有オブジェクト ルールのプロトコルは変更しないでください。これを変更すると、ルールの効果がなくなる可能性があります。

ステップ 5 次の選択肢があります。

- カスタム ルールを編集していて、そのルールの現在のバージョンを上書きする場合は、[保存（Save）] をクリックします。
- システム提供のルールまたは先祖ドメインに属しているルールを編集している場合や、カスタム ルールを編集しているときに変更を新しいルールとして保存する場合は、[新規に保存（Save As New）] をクリックします。

次の作業

- システム提供のルールの代わりにローカルで変更したルールを使用するには、侵入ルールの状態, （1062 ページ）の手順に従ってシステム提供のルールを非アクティブ化してから、ローカル ルールをアクティブ化します。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

ルールの検索, （1128 ページ）
侵入ルール エディタ ページでのルールのフィルタリング, （1130 ページ）

侵入ルールへのコメントの追加

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

任意の侵入ルールにコメントを追加できます。コメントにより、環境や条件の説明と、ルールやルールが検出する悪意あるプログラム、スクリプト（エクスプロイト）やポリシー違反の詳細を示すことができます。

マルチドメイン展開では、現在のドメインで作成されたコメントが表示されます。これは削除できます。先祖ドメインで作成されたコメントも表示されますが、これは削除できません。下位のドメインで作成されたコメントを表示するには、そのドメインに切り替えます。

手順

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）] を選択し、[侵入ルール（Intrusion Rules）] をクリックします。
- [オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]を選択します。

ステップ 2 注釈を付けるルールを探します。次の選択肢があります。

- フォルダからルールに移動します。
- ルールを探します。ルールの検索, （1128 ページ） を参照してください。
- ルールが属するグループをフィルタします。フィルタリング ルール, （1133 ページ） を参照してください。

ステップ 3 ルールの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ 4 [Rule Comment] をクリックします。

ステップ 5 テキスト ボックスにコメントを入力します。

ステップ 6 [コメントを追加（Add a Comment）] をクリックします。

ヒント また、侵入イベントのパケット ビューで、ルール コメントを追加して表示することもできます。

次の作業

- ルールの作成または編集を続けます。詳細については、新規ルールの作成, （1123 ページ） または 既存のルールの変更, （1124 ページ） を参照してください。

関連トピック

ルールの検索, （1128 ページ）
イベント情報のフィールド, （1985 ページ）

カスタム ルールの削除

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

侵入ポリシーで現在有効になっていないカスタム ルールを削除することができます。システムにより提供されている標準テキスト ルールおよび共有オブジェクト ルールは削除できません。マルチドメイン導入では、現在のドメインで作成されたローカル ルールのみを削除できます。

削除されたルールは削除済みカテゴリに保存されます。削除済みのルールを、新しいルールの基準として使用することができます。侵入ポリシーの [Rules] ページには削除済みカテゴリが表示されないため、削除したカスタム ルールを有効にすることはできません。

ヒント カスタム ルールには、変更されたヘッダー情報で保存する共有オブジェクト ルールが含まれます。また、これらはローカル ルール カテゴリに保存され、3の GID を使用してリストされます。変更した共有オブジェクト ルールは削除できますが、元の共有オブジェクト ルールは削除できません。

手順

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）] を選択し、[侵入ルール（Intrusion Rules）] をクリックします。
- [オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]を選択します。

ステップ 2 次の 2 つの選択肢があります。

- すべてのローカル ルールを削除します：[ローカル ルールの削除（Delete Local Rules）] をクリックし、[OK] をクリックします。

- 1 つのルールを削除します：[ルールのグループ化基準（Group Rules By）] ドロップダウンから [ローカル ルール（Local Rules）] を選択し、削除するルールの隣にある削除アイコン（）をクリックし、[OK] をクリックして削除を確認します。

関連トピック

侵入ルールの状態, （1062 ページ）

ルールの検索

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

Firepower システムには、数千もの標準テキスト ルールが用意されています。また、Cisco Talos Security Intelligence and Research Group（Talos） は新しい脆弱性およびエクスプロイトが見つかったときのルールを追加を継続します。特定のルールを簡単に検索して、そのルールをアクティブ化、非アクティブ化、または編集することができます。

手順

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）] を選択し、[侵入ルール（Intrusion Rules）] をクリックします。
- [オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]を選択します。

ステップ 2 ツールバーで [検索（Search）] をクリックします。

ステップ 3 検索条件を追加します。

ステップ 4 [検索（Search）] をクリックします。

次の作業

- 見つかったルール（システム ルールの場合はルールのコピー）を表示または編集する場合は、ハイパーリンクが付いたルール メッセージをクリックします。詳細については、新規ルールの作成, （1123 ページ） または既存のルールの変更, （1124 ページ） を参照してください。

侵入ルールの検索条件

次の表には、利用可能な検索オプションについて説明しています。

表 *103*：ルール検索規則

オプション	説明
署名 ID	Snort ID（SID）に基づいて 1 つのルールを検索するには、SID 番号を入力します。複数のルールを検索するには、SID 番号リストをコンマで区切って入力します。このフィールドは、80 文字以内です。
ジェネレータ ID	標準テキスト ルールを検索するには、[1] を選択します。共有オブジェクトのルールを検索するには、[3] を選択します。
メッセージ	特定のメッセージのあるルールを検索するには、[メッセージ（Message）] フィールドのルール メッセージから単語を 1 つ入力します。たとえば、DNS エクスプロイトを検索するには、`DNS` を入力します。バッファ オーバーフロー エクスプロイトを検索するには、`overflow` と入力します。
プロトコル	特定のプロトコルのトラフィックを評価するルールを検索するには、そのプロトコルを選択します。プロトコルを選択しない場合、検索結果に、すべてのプロトコルのフールが表示されます。
送信元ポート	指定ポートから発信されるパケットを調べるルールを検索するには、送信元ポート番号またはポート関連変数を入力します。
接続先ポート	特定ポートを宛先にしたパケットを調べるルールを検索するには、宛先ポート番号かポート関連変数を入力します。
ソース IP	特定の IP アドレスから発信されるパケットを調べるルールを検索するには、送信元 IP アドレスまたは IP アドレス関連変数を入力します。
宛先 IP（Destination IP）	特定の IP アドレスに送信するパケットを調べるルールを検索するには、宛先 IP アドレスまたは IP アドレス関連変数を入力します。
キーワード	特定のキーワードを検索するには、キーワード検索オプションを使用できます。キーワードを選択して、検索するキーワード値を入力します。特定値以外の任意の値に一致させるには、キーワードの前に疑問符（!）を入力します。
カテゴリ（Category）	特定カテゴリのルールを検索するには、カテゴリ リストからカテゴリを選択します。
分類	特定の分類のあるルールを検索するには、分類リストから分類名を選択します。

オプション	説明
ルール状態（Rule State）	特定のポリシー内のルールや特定のルール状態を検索するには、最初のルール状態リストからポリシーを選択し、第2のリストから状態を選択して、イベントの作成、イベントのドロップ、作成、無効に設定されたルールを検索します。

侵入ルール エディタ ページでのルールのフィルタリング

侵入ルールエディタページ上でルールをフィルタリングして、ルールのサブセットを表示することができます。たとえば、あるルールまたはその状態を変更したいが、数千ものルールの中からそれを見つけるのが困難な場合に、この機能が役立つことがあります。

フィルタを入力すると、1 つ以上の一致するルールを含むフォルダがページに表示され、一致するルールがない場合はメッセージが表示されます。

フィルタリング ガイドライン

フィルタには、特殊なキーワードとその引数、文字列、引用符で囲んだリテラル文字列、さらに複数のフィルタ条件を区切るスペースを含めることができます。ただし、正規表現、ワイルドカード文字、および否定文字（!）、「大なり」記号（>）、「小なり」記号（<）などの特殊な演算子をフィルタに含めることはできません。

すべてのキーワード、キーワード引数、および文字列では大文字と小文字が区別されません。`gid` キーワードと `sid` キーワードを除くすべての引数と文字列が部分文字列として扱われます。`gid` と `sid` の引数は、完全一致のみを返します。

フィルタ処理前の元のページで 1 つのフォルダを展開すると、その後のフィルタ処理でそのフォルダ内の一致が返されるときにフォルダが展開したままになります。探しているルールが多数のルールを含むフォルダ内に存在する場合には、これが役立つことがあります。

1つのフィルタを後続の別のフィルタで制約することはできません。入力されたフィルタは、ルール データベース全体を検索して、一致するすべてのルールを返します。前回のフィルタ結果がページに表示されている状態でフィルタを入力すると、そのページの内容が消去され、代わりに新しいフィルタの結果が返されます。

フィルタ処理されている場合もされていない場合も、リスト内のルールで同じ機能を使用できます。たとえば、侵入ルールエディタページでは、リストがフィルタ処理されているかどうかに関わらず、リスト内のルールを編集できます。また、ページのコンテキスト メニューの任意のオプションを使用することもできます。

ヒント すべてのサブグループ内のルールの合計数が多い場合は、フィルタリングに長い時間がかかることがあります。これは、個別のルールの数がかなり少なくても、1 つのルールが複数のカテゴリに出現することがあるためです。

キーワード フィルタリング

各ルール フィルタに、次の形式で 1 つ以上のキーワードを含めることができます。

`keyword:argument`

ここで、keyword は次の表のいずれかのキーワード、argument はキーワードに関連する特定のフィールドで検索される単一の、大文字/小文字を区別しない英数字文字列です。

`gid` と `sid` を除くすべてのキーワードの引数が部分文字列として扱われます。たとえば、引数 `123` によって `"12345"`、`"41235"`、`"45123"` などが返されます。`gid` と `sid` の引数は完全一致のみを返します。たとえば、`sid:3080` は SID 3080 のみを返します。

ヒント 部分的な SID を検索するには、1 つ以上の文字列を使ってフィルタ処理できます。

次の表に、ルールのフィルタ処理に使用できる特定のフィルタリング キーワードと引数を示します。

表 *104*：ルール フィルタ キーワード

キーワード	説明	例
`arachnids`	ルール参照内の Arachnids ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。	`arachnids:181`
`bugtraq`	ルール参照内の Bugtraq ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。	`bugtraq:2120`
`cve`	ルール参照内の CVE 番号全体またはその一部分に基づいて 1 つ以上のルールを返します。	`cve:2003-0109`
`gid`	引数 `1` は標準のテキスト ルールを返します。引数 `3` は共有オブジェクト ルールを返します。	`gid:3`
`mcafee`	ルール参照内の McAfee ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。	`mcafee:10566`
`msg`	ルールの [メッセージ（Message）] フィールド（イベント メッセージとも呼ばれる）の全体またはその一部分に基づいて 1 つ以上のルールを返します。	`msg:chat`
`nessus`	ルール参照内の Nessus ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。	`nessus:10737`
`ref`	ルール参照内またはルールの [メッセージ（Message）] フィールド内の単一の英数字文字列の全体または一部分に基づいて、1 つ以上のルールを返します。	`ref:MS03-039`
`sid`	正確な Snort ID を持つルールを返します。	`sid:235`
`url`	ルール参照内の URL 全体またはその一部分に基づいて 1 つ以上のルールを返します。	`url:faqs.org`

関連トピック

イベント参照の定義, （1121 ページ）
侵入イベント詳細, （1115 ページ）
プリプロセッサのジェネレータ ID, （1976 ページ）

文字列フィルタリング

各ルール フィルタに 1 つ以上の英数字文字列を含めることができます。文字列により、ルールの [メッセージ（Message）] フィールド、Snort ID ID（SID）、およびジェネレータ ID が検索されま

す。たとえば、文字列 123 を指定すると、ルール メッセージ内の文字列「Lotus123」や「123mania」などが返され、さらに、SID 6123、SID 12375 なども返されます。

すべての文字列では大文字と小文字が区別されず、部分的な文字列として扱われます。たとえば、文字列 ADMIN、admin、または Admin はすべて、"admin"、"CFADMIN"、"Administrator" などを返します。

文字列を引用符で囲むと、完全一致を返すことができます。たとえば、引用符付きのリテラル文字列 "overflow attempt" は完全一致のみを返しますが、引用符なしの 2 つの文字列 overflow と attempt で構成されるフィルタは "overflow attempt"、"overflow multipacket attempt"、"overflow with evasion attempt" などを返します。

関連トピック

侵入イベント詳細, （1115 ページ）
プリプロセッサのジェネレータ ID, （1976 ページ）

キーワードと文字列の組み合わせによるフィルタリング

複数のキーワード、文字列、またはその両方をスペースで区切って任意に組み合わせて入力することで、フィルタリングの結果を絞り込むことができます。結果には、すべてのフィルタ条件に一致するルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のフィルタはそれぞれ同じルールを返します。

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

フィルタリング ルール

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

[侵入ルール（Intrusion Rules）] ページで、ルールをサブセットにフィルタ処理すると、より簡単に特定のルールを見つけることができます。その後で、いずれかのページ機能を使用できます。これには、コンテキスト メニューで使用可能な機能の選択も含まれます。

編集する特定のルールを見つけるのに、規則のフィルタリングはとても役立ちます。

手順

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）] を選択し、[侵入ルール（Intrusion Rules）] をクリックします。
- [オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]を選択します。

ステップ 2 フィルタリングする前に、次の選択を行います。

- 該当のルール グループを展開します。複数のルール グループにも、展開できるサブグループがあります。
  また、ルールがどのグループに含まれているか予想できる場合は、フィルタ処理前の元のページでそのグループを展開しておくと便利な場合があります。その後のフィルタ処理でそのフォルダ内の一致した結果が返されるとき、およびフィルタ消去アイコン（✖）をクリックしてフィルタ処理前のページに戻ったときに、グループが展開されたままになります。
- [グループ ルール（Group Rules By）] ドロップダウンリストから別のグループ メソッドを選択します。

ステップ 3 [グループ ルール（Group Rules By）] リストでフィルタ アイコン（🔍）の横にあるテキスト ボックスにフィルタ制約を入力します。

ステップ 4 Enter を押します。

（注） フィルタ クリア アイコン（✖）をクリックして、現在のフィルタ処理されたリストをクリアします。

侵入ルールのキーワードと引数

ルール言語では、キーワードを組み合わせることによってルールの動作を指定できます。キーワードとそれに関連する値（引数と呼ばれる）は、ルール エンジンによって検査されるパケットおよびパケット関連値をシステムがどのように評価するかを決定します。Firepower システムでは現在、コンテンツマッチング、プロトコル固有のパターンマッチング、状態固有のマッチングなどのインスペクション機能を実行するためのキーワードがサポートされています。キーワードあたり最大 100 個の引数を定義し、互換性のある任意の数のキーワードを組み合わせて非常に具体的なルールを作成できます。これにより、誤検出や検出漏れの可能性が減少し、受け取った侵入情報に集中的に取り組むことができます。

また、パッシブ展開でアダプティブ プロファイルを使用すると、ルール メタデータとホスト情報に基づいて特定のパケットに対するアクティブ ルール処理を動的に調整できます。

ここに記載されているキーワードは、ルール エディタの検出オプションとして表示されます。

関連トピック

アダプティブ プロファイルについて，（1429 ページ）

content キーワードと protected_content キーワード

content キーワードまたは protected_content キーワードを使用すると、パケット内から検出するコンテンツを指定できます。

ほとんどの場合、content または protected_content キーワードの後ろに修飾子を付けて、コンテンツを検索すべき場所、検索で大文字/小文字を区別するかどうか、およびその他のオプションを指定する必要があります。

ルールでイベントがトリガーとして使用されるためには、すべてのコンテンツ マッチングが真でなければならないことに注意してください。つまり、各コンテンツ マッチングは相互に AND 関係にあります。

また、インライン展開では、有害なコンテンツを照合した後でそれを同じ長さの独自のテキスト文字列に置き換えるルールをセットアップできることにも注意してください。

content

content キーワードを使用すると、ルール エンジンはパケット ペイロードまたはストリームでその文字列を検索します。たとえば、いずれかの content キーワードの値として /bin/sh と入力した場合、ルール エンジンはパケット ペイロード内で文字列 /bin/sh を検索します。

ASCII 文字列、16 進コンテンツ（バイナリ バイト コード）、またはその両方の組み合わせを使用してコンテンツを照合できます。キーワード値の中で 16 進コンテンツをパイプ文字（|）で囲みます。たとえば、|90C8 C0FF FFFF|/bin/sh のように 16 進コンテンツと ASCII コンテンツを混在させることができます。

1 つのルール内で複数のコンテンツ マッチングを指定できます。これを行うには、content キーワードの追加のインスタンスを使用します。コンテンツ マッチングごとに、ルールをトリガーとして使用させるにはパケット ペイロードまたはストリームでコンテンツ一致が見つからなければならないことを指定できます。

注意 Not オプションが選択された 1 つの content キーワードだけを含むルールを作成した場合、侵入ポリシーの効果がなくなる可能性があります。

protected_content

protected_content キーワードを使用すると、ルール引数を設定する前に、検索コンテンツ文字列をエンコードすることができます。キーワードを設定する前に、ルール作成者がハッシュ関数（SHA-512、SHA-256、または MD5）を使用して文字列をエンコードします。

content キーワードの代わりに protected_content キーワードを使用した場合でも、ルール エンジンがパケット ペイロードまたはストリームの中で文字列を検索する方法に違いはなく、ほとんど

のキーワード オプションが想定どおりに機能します。次の表は、protected_content キーワード オプションと content キーワード オプションの間の例外的な相違点を要約しています。

表 *105*：*protected_content* オプションの例外

オプション	説明
ハッシュ タイプ（Hash Type）	protected_content ルール キーワードの新しいオプション。
[大文字小文字の区別なし（Case Insensitive）]	未サポート
次の範囲内（Within）	未サポート
奥行き（Depth）	未サポート
長さ（Length）	protected_content ルール キーワードの新しいオプション。
高速パターン マッチ機能を使用（Use Fast Pattern Matcher）	未サポート
高速パターン マッチ機能のみ（Fast Pattern Matcher Only）	未サポート
高速パターン マッチ機能オフセットおよび長さ（Fast Pattern Matcher Offset and Length）	未サポート

Cisco では、protected_content キーワードを含むルールに 1 つ以上の content キーワードを含めることを推奨しています。こうすると、ルールエンジンが常に高速パターンマッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルール内の protected_content キーワードの前に content キーワードを配置します。ルールに 1 つ以上の content キーワードが含まれている場合は、content キーワードの Use Fast Pattern Matcher 引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。

注意 Not オプションが選択された 1 つの protected_content キーワードだけを含むルールを作成した場合、侵入ポリシーの効果がなくなる可能性があります。

関連トピック

カスタム ルールの作成, （1122 ページ）
基本コンテンツおよび protected_content キーワードの引数, （1137 ページ）

replace キーワード, （1149 ページ）

基本コンテンツおよび protected_content キーワードの引数

content または protected_content キーワードを変更するパラメータを使用すると、コンテンツ検索の位置や大文字/小文字の区別を制約できます。content または protected_content キーワードを変更するオプションを設定して、検索対象となるコンテンツを指定します。

[大文字小文字の区別なし（Case Insensitive）]

（注） このオプションは protected_content キーワードの設定では**サポートされません**。

ASCII 文字列でコンテンツ一致を検索するときに大文字/小文字の区別を無視するようルール エンジンに指示できます。検索で大文字と小文字を区別しないようにするには、コンテンツ検索の指定時に [大文字小文字の区別なし（Case Insensitive）] をオンにします。

Hash Type

（注） このオプションは protected_content キーワードで**のみ**設定できます。

[ハッシュ タイプ（Hash Type）] ドロップダウンを使用して、検索文字列のエンコードに使用されたハッシュ関数を特定します。protected_content 検索文字列のハッシュ方式として、SHA-512、SHA-256、および MD5 がサポートされています。選択したハッシュ タイプとハッシュされたコンテンツの長さが一致しない場合、システムはルールを保存**しません**。

自動的に Cisco 設定のデフォルト値が選択されます。[デフォルト（Default）] が選択される場合、ルールに特定のハッシュ関数は含まれず、SHA-512 がハッシュ関数であると見なされます。

Raw Data

[raw データ（Raw Data）] オプションを使用すると、ルール エンジンは、正規化されたペイロード データ（ネットワーク分析ポリシーによってデコードされたデータ）を分析する前にオリジナルのパケット ペイロードを分析します。引数値は使用されません。正規化の前に、ペイロード内の Telnet ネゴシエーション オプションを検査するために Telnet トラフィックを分析する場合に、このキーワードを使用できます。

同じ content または protected_content キーワードで、Raw Data オプションを HTTP コンテンツ オプションと一緒に使用することはできません。

ヒント HTTP トラフィックで raw データを検査するかどうか、また、どの程度の量の raw データを検査するかを決定するため、HTTP 検査プリプロセッサの [クライアント フローの深さ（Client Flow Depth）] オプションと [サーバ フローの深さ（Server Flow Depth）] オプションを設定することができます。

注

指定したコンテンツと一致しないコンテンツを検索するには、[一致しない（Not）]オプションを選択します。[一致しない（Not）]オプションが選択された `content` または `protected_content` キーワードを含むルールを作成する場合には、そのルール内に、[一致しない（Not）]オプションが選択されていない別の `content` または `protected_content` キーワードを 1 つ以上含める必要があります。

注意 `content` または `protected_content` キーワードに対して Not オプションをオンにした場合は、そのキーワードだけを含むルールを作成しないでください。侵入ポリシーの効果がなくなる可能性があります。

たとえば、SMTP ルール 1:2541: 9 に 3 つの `content` キーワードが含まれており、そのうちの 1 つで [一致しない（Not）] オプションが選択されているとします。[一致しない（Not）] オプションが選択されているキーワード以外のすべての `content` キーワードを削除すると、このルールに基づくカスタム ルールが無効になります。このようなルールを侵入ポリシーに追加すると、そのポリシーの効果がなくなる可能性があります。

ヒント 同じ `content` キーワードで、[Not] チェック ボックスと [Use Fast Pattern Matcher] チェック ボックスを同時に選択することはできません。

コンテンツ（content）および保護コンテンツ（protected_content）キーワード検索位置

検索位置オプションを使用すると、指定したコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

許可された組み合わせ：*content* 検索位置の引数

次のように、2つの `content` 位置ペアのいずれかを使用すると、指定したコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

- パケット ペイロードの先頭を基準にして検索する場合は、[オフセット（Offset）] と [奥行き（Depth）] を一緒に使用します。
- 現在の検索位置を基準にして検索する場合は、[距離（Distance）] と [次の範囲内（Within）] を一緒に使用します。

ペアに含まれるオプションのどちらか1つだけを指定した場合は、そのペアのもう1つのオプションのデフォルトが想定されます。

Offset および Depth オプションと、Distance および Within オプションを混合することはできません。たとえば、Offset と Within をペアにすることはできません。1 つのルール内で任意の数の位置オプションを使用できます。

位置が指定されない場合は、[オフセット（Offset）] と [奥行き（Depth）] のデフォルトが想定されます。つまり、コンテンツ検索はパケット ペイロードの先頭から始まってパケットの末尾まで続きます。

また、既存の `byte_extract` 変数を使用して位置オプションの値を指定することもできます。

ヒント 1 つのルール内で任意の数の位置オプションを使用できます。

関連トピック

byte_extract キーワード, （1155 ページ）

許可された組み合わせ：*protected_content* 検索位置の引数

次のように、必須の [長さ（Length）] `protected_content` 位置オプションを [オフセット（Offset）] または [距離（Distance）] 位置オプションと組み合わせて使用すると、指定されたコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

- パケット ペイロードの先頭を基準にして、保護された文字列を検索するには、[長さ（Length）] と [オフセット（Offset）] を一緒に使用します。
- 現在の検索位置を基準にして、保護された文字列を検索するには、[長さ（Length）] と [距離（Distance）] を一緒に使用します。

ヒント 1 つのキーワード設定内で [オフセット（Offset）] オプションと [距離（Distance）] オプションを併用することはできませんが、1 つのルール内では任意の数の位置オプションを使用できます。

位置が指定されない場合は、デフォルトが想定されます。つまり、コンテンツ検索はパケット ペイロードの先頭から始まってパケットの末尾まで続きます。

また、既存の `byte_extract` 変数を使用して位置オプションの値を指定することもできます。

関連トピック

byte_extract キーワード, （1155 ページ）

content および *protected_content* の検索位置の引数

奥行

（注） このオプションは、`content` キーワードを設定する場合に**のみ**サポートされます。

オフセット値の先頭からの（またはオフセットが設定されていない場合はパケット ペイロード先頭からの）コンテンツ検索の最大の深さをバイト単位で指定します。

たとえば、ルールのコンテンツ値が `cgi-bin/phf`、`offset` 値が `3`、`depth` 値が `22` である場合、ルール ヘッダーで指定されたパラメータを満たすパケット内で、`cgi-bin/phf` 文字列との一致の検索がバイト位置 3 から始まり、22 バイト処理した後（バイト位置 25 で）停止します。

指定したコンテンツの長さ以上の、最大 65535 バイトまでの値を指定する必要があります。値 0 は指定できません。

デフォルトの深さは、「パケットの末尾まで検索」です。

距離（Distance）

以前に見つかったコンテンツ一致から数えて、指定されたバイト数の後に出現する後続のコンテンツ一致を見つけるようルール エンジンに指示します。

Distance（距離）カウンタはバイト 0 から始まるため、最後に見つかったコンテンツ一致から順方向に移動すべきバイト数よりも 1 つ少ない数値を指定してください。たとえば 4 を指定した場合、5 番目のバイトから検索が始まります。

-65535 ～ 65535 バイトを値として指定できます。負の `Distance` 値を指定した場合は、検索を開始するバイト位置がパケットの先頭から外れる可能性があります。実際にはパケットの第 1 バイトから検索が開始されますが、計算ではパケットの外側のバイトも考慮されます。たとえば、パケット内の現在の位置が第 5 バイトで、次のコンテンツ ルール オプションで `Distance` 値 -10 および `Within` 値 20 が指定された場合、検索はペイロードの先頭から開始され、[Within] オプションが 15 に調整されます。

デフォルトの距離は 0 で、これは最後のコンテンツ一致の後のパケット内の現在位置という意味です。

長さ（Length）

（注） このオプションは `protected_content` キーワードを設定する場合に**のみ**サポートされます。

Length `protected_content` キーワード オプションは、ハッシュされていない検索文字列の長さをバイト単位で示します。

たとえば、コンテンツ `Sample1` を使ってセキュア ハッシュを生成した場合には、Length 値として `7` を使用します。このフィールドに値を入力することは**必須**です。

Offset

パケットペイロードの先頭を基準とする、コンテンツの検索を開始するパケットペイロード内の位置をバイト単位で指定します。65535 ～ 65535 バイトを値として指定できます。

オフセット カウンタはバイト 0 から始まるため、パケット ペイロードの先頭から順方向に移動すべきバイト数よりも 1 つ少ない数値を指定してください。たとえば 7 を指定した場合は、8 番目のバイトから検索が始まります。

デフォルトのオフセットは 0 で、これはパケットの先頭を意味します。

Within

（注） このオプションは、content キーワードを設定する場合に**のみ**サポートされます。

[次の範囲内（Within）]オプションを使用すると、ルールをトリガーとして使用させるには、最後に見つかったコンテンツ一致の末尾以降、指定のバイト数以内に次のコンテンツ一致が発生する必要があることを指示できます。たとえば Within 値として 8 を指定した場合、次のコンテンツ一致がパケット ペイロードの次の 8 バイト以内に発生する必要があります。発生しない場合は、ルールをトリガーとして使用する基準が満たされません。

指定したコンテンツの長さ以上の、最大 65535 バイトまでの値を指定できます。

[Within] のデフォルトは「パケットの末尾まで検索」です。

概要：HTTP content および protected_content キーワードの引数

HTTP content または protected_content キーワード オプションを使用すると、HTTP Inspect プリプロセッサによってデコードされた HTTP メッセージ内でコンテンツ一致を検索する位置を指定できます。

次の 2 つのオプションは、HTTP 応答内のステータス フィールドを検索します。

- HTTP ステータス コード（HTTP Status Code）
- HTTP ステータス メッセージ（HTTP Status Message）

ルール エンジンは未加工の正規化されていないステータス フィールドを検索しますが、ここでは、他の Raw HTTP フィールドと正規化された HTTP フィールドを併用する際に考慮すべき制限についての説明を簡略化するために、これらのオプションが別個に列挙されていることに注意してください。

次の 5 つのオプションは、必要に応じて HTTP 要求、応答、またはその両方の中で正規化フィールドを検索します。

- HTTP URI
- HTTP メソッド（HTTP Method）
- HTTP ヘッダー（HTTP Header）
- HTTP Cookie
- HTTP クライアント ボディ（HTTP Client Body）

次の 3 つのオプションは、必要に応じて HTTP 要求、応答、またはその両方の中で未加工の（正規化されていない）非ステータス フィールドを検索します。

- HTTP Raw URI
- HTTP Raw ヘッダー（HTTP Raw Header）
- HTTP Raw Cookie

HTTP `content` オプションを選択する場合は、次のガイドラインに従ってください。

- HTTP `content` オプションは TCP トラフィックにのみ適用されます。
- パフォーマンスへの悪影響を避けるために、指定したコンテンツが出現する可能性のあるメッセージ部分だけを選択してください。

  たとえば、ショッピング カート メッセージの場合のように大きな cookie がトラフィックに含まれている可能性がある場合は、HTTP cookie ではなく HTTP ヘッダーの中で指定のコンテンツを検索することができます。

- HTTP Inspect プリプロセッサの正規化機能を活用し、パフォーマンスを向上させるには、作成するすべての HTTP 関連ルールの中に少なくとも 1 つの `content` または `protected_content` キーワードを含め、それに対して HTTP URI、HTTP Method、HTTP Header、または HTTP Client Body オプションを選択します。

- HTTP `content` または `protected_content` キーワード オプションと組み合わせて `replace` キーワードを使用することはできません。

単一の正規化された HTTP オプションまたはステータス フィールドを指定できます。または、複数の正規化 HTTP オプションとステータス フィールドを任意に組み合わせて、コンテンツ領域をマッチング対象にすることもできます。ただし、HTTP フィールド オプションを使用する場合には次の制限事項に注意してください。

- 同じ `content` または `protected_content` キーワードの中で、[生データ（Raw Data）] オプションを HTTP オプションと一緒に使用することはできません。
- Raw HTTP フィールド オプション（[HTTP　Raw URI]、[HTTP Raw ヘッダー（HTTP Raw Header）]、または [HTTP Raw Cookie]）と、それぞれに対応する正規化されたオプション（[HTTP URI]、[HTTP ヘッダー（HTTP Header）]、または [HTTP Cookie]）を同じ `content` または `protected_content` キーワード内で一緒に使用することはできません。
- [高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] を、次の 1 つ以上の HTTP フィールド オプションと組み合わせて選択することはできません。

  [HTTP Raw URI]、[HTTP raw ヘッダー（HTTP Raw Header）]、[HTTP Raw Cookie]、[HTTP Cookie]、[HTTP メソッド（HTTP Method）]、[HTTP ステータス メッセージ（HTTP Status Message）]、[HTTP ステータス コード（HTTP Status Code）]

  ただし、次のいずれかの正規化フィールドを検索するために高速パターン マッチ機能を使用する `content` または `protected_content` キーワードでは、上記のオプションを含めることができます。

  [HTTP URI]、[HTTP ヘッダー（HTTP Header）]、[HTTP クライアント ボディ（HTTP Client Body）]

  たとえば、[HTTP Cookie]、[HTTP ヘッダー（HTTP Header）] 、[高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] を選択した場合、ルール エンジンは HTTP cookie と HTTP ヘッダーの両方でコンテンツを検索しますが、高速パターン マッチ機能は HTTP cookie ではなく、HTTP ヘッダーにのみ適用されます。

- 制限付きオプションと制限なしオプションを併用した場合、高速パターンマッチ機能は、指定された制限なしフィールドのみを検索することで、侵入ルールエディタにルールを渡して（制限付きフィールドの評価を含む）完全な評価を行うべきかどうかを検査します。

関連トピック

content キーワードの高速パターン マッチ機能の引数, （1146 ページ）

HTTP コンテンツと *protected_content* キーワードの引数

HTTP URI

正規化された要求 URI フィールド内でコンテンツ一致を検索するには、このオプションを選択します。

このオプションと `pcre` キーワードの HTTP URI（U）オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。

（注） パイプライン処理された HTTP 要求パケットには複数の URI が含まれています。[HTTP URI] が選択されている場合、パイプライン処理された HTTP 要求パケットをルール エンジンが検出すると、そのパケット内のすべての URI でコンテンツ一致が検索されます。

HTTP Raw URI

正規化された要求 URI フィールド内でコンテンツ一致を検索するには、このオプションを選択します。

このオプションと `pcre` キーワードの HTTP URI（U）オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。

（注） パイプライン処理された HTTP 要求パケットには複数の URI が含まれています。[HTTP URI] が選択されている場合、パイプライン処理された HTTP 要求パケットをルール エンジンが検出すると、そのパケット内のすべての URI でコンテンツ一致が検索されます。

HTTP メソッド

（URI で識別されるリソースに対して行う GET や POST などのアクションを特定する）要求メソッド フィールド内のコンテンツ一致を検索するには、このオプションを選択します。

HTTP Header

HTTP 要求内の（cookie を除く）正規化されたヘッダー フィールドでコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は応答内でも検索されます。

このオプションと pcre キーワードの HTTP 見出し（H）オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。

HTTP Raw Header

HTTP 要求内の（cookie を除く）raw ヘッダー フィールドでコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は応答内でも検索されます。

このオプションと pcre キーワードの HTTP 未加工見出し（D）オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。

HTTP Cookie

正規化された HTTP クライアント要求見出し内で識別される cookie でコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションが有効になっている場合は応答 set-cookie データ内でも検索されます。システムは、メッセージ本文に含まれる cookie を本文の内容として扱うことに注意してください。

cookie 内だけで一致を検索するには、HTTP Inspect プリプロセッサの [HTTP Cookie の検査（Inspect HTTP Cookies）] オプションを有効にする必要があります。これを有効にしない場合、ルール エンジンは cookie を含む見出し全体を検索します。

次の点に注意してください。

- このオプションと pcre キーワードの HTTP cookie（C）オプションを一緒に使用して、同じコンテンツを検索することはできません。
- Cookie: ヘッダー名と Set-Cookie: ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す CRLF は cookie の一部としてではなく、ヘッダーの一部として検査されます。

HTTP Raw Cookie

未加工 HTTP クライアント要求見出し内で識別される cookie でコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションが有効になっている場合は応答 set-cookie データ内でも検索されます。システムは、メッセージ本文に含まれる cookie を本文の内容として扱うことに注意してください。

cookie 内だけで一致を検索するには、HTTP Inspect プリプロセッサの [HTTP Cookie の検査（Inspect HTTP Cookies）] オプションを有効にする必要があります。これを有効にしない場合、ルール エンジンは cookie を含む見出し全体を検索します。

次の点に注意してください。

- このオプションと pcre キーワードの HTTP 未加工 cookie（K）オプションを一緒に使用して同じコンテンツを検索することはできません。

- `Cookie:` ヘッダー名と `Set-Cookie:` ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す `CRLF` は cookie の一部としてではなく、ヘッダーの一部として検査されます。

HTTP Client Body

HTTP クライアント要求内のメッセージ本文でコンテンツ一致を検索するには、このオプションを選択します。

このオプションが機能するためには、HTTP Inspect プリプロセッサの [HTTP クライアント ボディの抽出の深さ（HTTP Client Body Extraction Depth）] オプションで 0 ～ 65535 の値を指定する必要があることに注意してください。

HTTP ステータス コード（HTTP Status Code）

HTTP 応答内の 3 桁のステータス コードでコンテンツ一致を検索するには、このオプションを選択します。

このオプションで一致が返されるようにするには、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションを有効にする必要があります。

HTTP Status Message

HTTP応答のステータス コードに付加されるテキスト記述の中でコンテンツ一致を検索するには、このオプションを選択します。

このオプションで一致が返されるようにするには、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションを有効にする必要があります。

関連トピック

PCRE 修飾子のオプション，（1161 ページ）
サーバレベルの HTTP 正規化オプション，（1307 ページ）

概要：content キーワードによる高速パターン マッチ機能

（注） これらのオプションは、`protected_content` キーワードの設定では**サポートされません**。

高速パターンマッチ機能は、パケットをルールエンジンに渡す前に、評価するルールをすばやく決定します。この初期決定により、パケット評価で使用されるルール数が大幅に減るため、パフォーマンスが向上します。

デフォルトで、高速パターン マッチ機能は、ルールで指定された最長のコンテンツをパケットで検索します。これは、不必要なルール評価をできるだけ減らすためです。次の例のようなルール フラグメントがあるとします。

```
alert tcp any any -> any 80 (msg:"Exploit"; content:"GET";
http_method; nocase; content:"/exploit.cgi"; http_uri;
nocase;)
```

ほとんどすべての HTTP クライアント要求にはコンテンツ `GET` が含まれていますが、コンテンツ `/exploit.cgi` を含む要求は稀です。`GET` を高速パターン コンテンツとして使用した場合、ルール エンジンはほとんどのケースでこのルールを評価し、一致はほとんど検出されないでしょう。しかし、`/exploit.cgi` を使用するとほとんどのクライアントの `GET` 要求は評価されないため、パフォーマンスが向上します。

指定されたコンテンツが高速パターンマッチ機能で検出された場合にのみ、ルールエンジンはパケットをルールに照らして評価します。たとえば、ルール内の 1 つの `content` キーワードでコンテンツ `short` を指定し、別のキーワードで `longer`、さらに 3 番目のキーワードで `longest` を指定した場合、高速パターン マッチ機能はコンテンツ `longest` を使用し、ルール エンジンがペイロード内で `longest` を検出した場合にのみ、ルールが評価されます。

content キーワードの高速パターン マッチ機能の引数

Use Fast Pattern Matcher

使用する高速パターン マッチ機能の短い検索パターンを指定するには、このオプションを使用します。理論的には、指定したパターンの方が最長パターンよりもパケット内で見つかる可能性が低いため、より的を絞って対象のエクスプロイトを識別できます。

[高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] と他のオプションを同じ `content` キーワード内で選択する場合は、次の制限事項に注意してください。

- ルールごとに 1 回だけ、[高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] を指定できます。
- [高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] と [一致しない（Not）] を組み合わせて選択した場合は、[距離（Distance）]、[次の範囲内（Within）]、[オフセット（Offset）]、または [奥行き（Depth）] を使用できません。
- [高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] を、次のいずれかの HTTP フィールド オプションと組み合わせて選択することはできません。

  [HTTP Raw URI]、[HTTP raw ヘッダー（HTTP Raw Header）]、[HTTP raw クッキー（HTTP Raw Cookie）]、[HTTP クッキー（HTTP Cookie）]、[HTTP メソッド（HTTP Method）]、[HTTP ステータス メッセージ（HTTP Status Message）]、または [HTTP ステータス コード（HTTP Status Code）]

  ただし、次のいずれかの正規化フィールドを検索するために高速パターン マッチ機能を使用する `content` キーワードでは、上記のオプションを含めることができます。

  [HTTP URI]、[HTTP ヘッダー（HTTP Header）]、または [HTTP クライアント ボディ（HTTP Client Body）]

  たとえば、[HTTP Cookie]、[HTTP Header]、および [Use Fast Pattern Matcher] を選択した場合、ルール エンジンは HTTP cookie と HTTP ヘッダーの両方でコンテンツを検索しますが、高速パターン マッチ機能は HTTP cookie ではなく、HTTP ヘッダーにのみ適用されます。

  未加工 HTTP フィールド オプション（[HTTP Raw URI]、[HTTP raw ヘッダー（HTTP Raw Header）]、または [HTTP raw クッキー（HTTP Raw Cookie）]）と、それぞれに対応する正規化されたオプション（[HTTP URI]、[HTTP ヘッダー（HTTP Header）]、または [HTTP クッ

キー（HTTP Cookie）]）を同じ `content` キーワード内で一緒に使用できないことに注意してください。

制限付きオプションと制限なしオプションを併用した場合、高速パターンマッチ機能は、指定された制限なしフィールドのみを検索することで、ルール エンジンにパケットを渡して（制限付きフィールドの評価を含む）完全な評価を行うべきかどうかを検査します。

- オプションで、[高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] を選択した場合には [高速パターン マッチ機能のみ（Fast Pattern Matcher Only）] または [高速パターン マッチ機能オフセットおよび長さ（Fast Pattern Matcher Offset and Length）] を選択することもできますが、この両方は選択できません。
- Base64 データの検査時には高速パターン マッチ機能を使用できません。

Fast Pattern Matcher Only

このオプションを使用すると、`content` キーワードをルール オプションとしてではなく、高速パターンマッチ機能オプションとしてのみ使用できます。指定したコンテンツをルールエンジンで評価する必要がない場合、このオプションを使ってリソースを節約できます。たとえば、ペイロード内のいずれかの場所にコンテンツ `12345` が存在することだけを必要とするルールがあるとします。高速パターン マッチ機能でパターンが検出された場合に、ルール内の追加のキーワードに照らしてパケットを評価できます。パターン `12345` が含まれているかどうかを判断するために、ルール エンジンがパケットを再評価する必要はありません。

指定されたコンテンツに関連する他の条件がルールに含まれている場合は、このオプションを使用しないでください。たとえば、別のルール条件で `abcd` が `1234` の前に出現するかどうかを判断する場合には、このオプションを使ってコンテンツ `1234` を検索しないでください。[高速パターン マッチ機能のみ（Fast Pattern Matcher Only）] を指定すると、指定されたコンテンツがルール エンジンによって検索されないため、このケースではルール エンジンが相対的な位置を判断できません。

このオプションを使用するときには、次の条件に注意してください。

- 指定されたコンテンツは位置に依存しない、つまり、ペイロードのどこにでも出現する可能性があるため、位置オプション（[距離（Distance）]、[次の範囲内（Within）]、[オフセット（Offset）]、[奥行き（Depth）]、[高速パターンマッチ機能オフセットおよび長さ（Fast Pattern Matcher Offset and Length）]）を使用することはできません。
- このオプションを [一致しない（Not）] と組み合わせて使用することはできません。
- このオプションを [高速パターン マッチ機能オフセットおよび長さ（Fast Pattern Matcher Offset and Length）] と組み合わせて使用することはできません。
- 大文字/小文字を区別しない方法ですべてのパターンが高速パターン マッチ機能に挿入されるため、指定したコンテンツは「大文字/小文字の区別なし」として扱われます。これは自動的に処理されるため、このオプションの選択時に [大文字小文字の区別なし（Case Insensitive）] を選択する必要はありません。

- [高速パターン マッチ機能のみ（Fast Pattern Matcher Only）] オプションを使用する `content` キーワードの直後に、現在の検索位置を基準にして検索位置を設定する次のキーワードを続けないようにしてください。
  - `isdataat`
  - `pcre`
  - `content`（[距離（Distance）] または [次の範囲内（Within）] が選択されている場合）
  - `content`（[HTTP URI] が選択されている場合）
  - `asn1`
  - `byte_jump`
  - `byte_test`
  - `byte_extract`
  - `base64_decode`

Fast Pattern Matcher Offset and Length

[高速パターン マッチ機能オフセットおよび長さ（Fast Pattern Matcher Offset and Length）] オプションを使用すると、検索するコンテンツの一部分を指定できます。これにより、パターンが非常に長く、ルールの一致の可能性を判断するのにパターンの一部分だけで十分な場合に、メモリ消費を抑えることができます。高速パターン マッチ機能によってルールが選択されたときに、パターン全体がルールに照らして評価されます。

次の構文に従い、検索を開始する位置（オフセット）およびコンテンツ内をどれほど検索するか（長さ）をバイト単位で指定することにより、高速パターン マッチ機能で使用する部分を決定します。

`offset,length`
たとえば、次のコンテンツに対して

`1234567`
次のようにオフセットと長さのバイト数を指定した場合、

`1,5`
高速パターン マッチ機能はコンテンツ `23456` のみを検索します。

このオプションを [Fast Pattern Matcher Only] と一緒に使用できないことに注意してください。

関連トピック

概要：HTTP content および protected_content キーワードの引数, （1141 ページ）
base64_decode キーワードと base64_data キーワード, （1239 ページ）

replace キーワード

インライン導入で replace キーワードを使用すると、指定したコンテンツを置き換えることができます。

（注） Cisco SSL アプライアンスによって検出された SSL トラフィック内のコンテンツを置き換えるために replace キーワードを使用することは**できません**。置換データではなく、元の暗号化データが送信されます。詳細については、『*Cisco SSL Appliance Administration and Deployment Guide*』を参照してください。

replace キーワードを使用するには、content キーワードを使って特定の文字列を検索するカスタムの標準テキスト ルールを作成します。その後、replace キーワードを使用して、コンテンツを置き換える文字列を指定します。置換値とコンテンツ値は同じ長さである必要があります。

（注） protected_content キーワード内でハッシュされたコンテンツを置き換えるために replace キーワードを使用することは**できません**。

オプションで、以前の Firepower システム ソフトウェア バージョンとの下位互換性を維持するために、置換文字列を引用符で囲むことができます。引用符を含めない場合は、それらが自動的にルールに追加されるため、構文的に正しいルールになります。置換テキストの一部として先行引用符または後続引用符を含めるには、次の例に示すように、バックスラッシュを使ってエスケープする必要があります。

```
"replacement text plus \"quotation\" marks""
```

1 つのルール内に複数の replace キーワードを含めることができますが、content キーワードごとに 1 つずつしか含めることができません。ルールによって検出されたコンテンツの最初のインスタンスだけが置き換えられます。

次に、replace キーワードの使用例を示します。

- エクスプロイトを含んでいる着信パケットをシステムが検出した場合、有害な文字列を無害な文字列に置き換えることができます。このテクニックは、有害なパケットを単に破棄するよりも効果的である場合があります。破棄されたパケットを攻撃者が単に再送信し続け、やがてネットワーク防御を通り抜けるか、ネットワークを氾濫させるという攻撃シナリオがあります。パケットを破棄する代わりに別の文字列に置換することで、脆弱ではないターゲットに対して攻撃が実行されたと攻撃者に思い込ませることができます。
- （たとえばWebサーバの）脆弱なバージョンが稼働しているかどうかを調べる偵察攻撃が懸念される場合は、発信パケットを検出して、バナーを独自のテキストに置換できます。

（注） 置換ルールを使用するインライン侵入ポリシー内でルール状態が[イベントを生成する（Generate Events）]に設定されていることを確認してください。ルールを[ドロップしてイベントを生成する（Drop and Generate Events）]に設定した場合はパケットが破棄され、コンテンツが置き換えられません。

文字列置換プロセスでは、宛先ホストがエラーなしでパケットを受信できるように、パケットチェックサムがシステムによって自動的に更新されます。

`replace` キーワードは、HTTP 要求メッセージの `content` キーワード オプションと組み合わせて使用できないことに注意してください。

関連トピック

content キーワードと protected_content キーワード, （1135 ページ）
概要：HTTP content および protected_content キーワードの引数, （1141 ページ）

byte_jump キーワード

`byte_jump` キーワードは、指定されたバイト セグメントで定義されるバイト数を計算し、指定したオプションに応じて、指定されたバイトセグメントの末尾から、パケットペイロードの先頭から、あるいは最後のコンテンツ一致に対して相対的なポイントから順方向に、パケット内でそのバイト数だけスキップします。パケットの特定のバイト セグメントが、パケット内の可変データに含まれるバイト数を示す場合には、これが役立ちます。

次の表では、`byte_jump` キーワードで必要な引数を説明します。

表 *106*：*byte_jump* の必須引数

引数	説明
Bytes	パケットから抽出するバイト数。 DCE/RPC を指定せずに使用する場合、許可される値は 1 ～ 10 ですが、次の制限があります。 • • 1、2、または 4 以外のバイト数を指定する場合は、番号タイプ（16 進数、8 進数、または 10 進数）を指定する必要があります。 DCE/RPC とともに使用する場合、許可される値は 1、2、および 4 です。

引数	説明
Offset	ペイロード内で処理を開始するバイト数。`offset` カウンタはバイト 0 から始まるため、パケットペイロードの先頭、または最後に見つかったコンテンツ一致から順方向にジャンプさせるバイト数から 1 を差し引いて `offset` 値を計算してください。 -65535 ～ 65535 バイトを指定できます。 また、既存の `byte_extract` 変数を使用してこの引数の値を指定することもできます。

次の表で説明するオプションを使用すると、必須の引数に指定された値をシステムがどのように解釈するかを定義できます。

表 *107* : *byte_jump* の追加のオプション引数

引数	説明
Relative	最後に見つかったコンテンツ一致で検出された最後のパターンを基準にしてオフセットを計算します。
Align	変換されたバイト数を、次の 32 ビット境界に切り上げます。
Multiplier	ルール エンジンで最終的な `byte_jump` 値を算出するために、パケットから得られた `byte_jump` 値に掛ける値を示します。 つまり、ルール エンジンは、指定されたバイト セグメントで定義されるバイト数だけスキップする代わりに、Multiplier 引数で指定される整数を乗算したバイト数だけスキップします。
Post Jump Offset	他の `byte_jump` 引数を適用した後に、順方向または逆方向にスキップするバイト数（-65535 ～ 65535）。正の値は順方向にスキップし、負の値は逆方向にスキップします。無効にするには、フィールドを空白のままにするか、`0` を入力します。 DCE/RPC 引数を選択すると、一部の `byte_jump` 引数が適用されないことに注意してください。
From Beginning	ルール エンジンが、パケット内の現在の位置からではなく、パケット ペイロードの先頭からペイロード内の指定されたバイト数をスキップする必要があることを示します。

DCE/RPC、Endian、または Number Type のうち 1 つだけを指定できます。

バイト数を byte_extract キーワードでどのように計算するか定義するには、次の表の中から引数を選択します。バイト順引数を選択しなかった場合、ルールエンジンはビッグエンディアンのバイト順を使用します。

表 *108*：*byte_jump* のバイト順引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に byte_jump キーワードを指定します。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。Number Type 引数と Endian 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて byte_jump を使用することもできます。

次の表に示すいずれか 1 つの引数を使用して、パケット内のストリング データをシステムがどのように表示するかを定義します。

表 *109*：番号タイプ引数

引数	説明
Hexadecimal String	変換後のストリング データを 16 進形式で表現します。
Decimal String	変換後のストリング データを 10 進形式で表現します。
Octal String	変換後のストリング データを 8 進形式で表現します。

たとえば、次のような値を byte_jump に設定した場合、

- Bytes = 4
- Offset = 12
- Relative enabled
- Align enabled

ルール エンジンは、最後に見つかったコンテンツ一致から 13 バイト後に出現する 4 つのバイトで記述される数値を計算して、そのバイト数だけパケット内を順方向にスキップします。たとえば、ある特定のパケット内で計算される 4 つのバイトが 00 00 00 1F である場合、ルール エンジ

ンはこれを31に変換します。`align`が指定されている（次の32ビット境界まで移動するようエンジンに指示する）ため、ルール エンジンはパケット内を32バイト先までスキップします。

あるいは、次のような値を`byte_jump`に設定した場合、

- Bytes = 4
- Offset = 12
- From Beginning enabled
- Multiplier = 2

ルール エンジンは、パケットの先頭から13バイト後に出現する4つのバイトで記述される数値を計算します。その後、その数値に2を掛けてスキップする総バイト数を計算します。たとえば、ある特定のパケット内で計算される4つのバイトが`00 00 00 1F`である場合、ルール エンジンはこれを31に変換し、それに2を掛けて62にします。[From Beginning]が有効になっているため、ルール エンジンはパケット内の最初の63バイトをスキップします。

関連トピック

byte_extract キーワード, （1155 ページ）
DCE/RPC キーワード, （1192 ページ）

byte_test キーワード

`byte_test`キーワードは、指定されたバイト セグメントをValue引数およびその演算子に対してテストします。

次の表に、`byte_test`キーワードで必要な引数を説明します。

表 *110*：*byte_test* の必須引数

引数	説明
Bytes	パケットから計算するバイト数。 DCE/RPC を指定せずに使用する場合、許可される値は 1 ～ 10 です。ただし、1、2、または 4 以外のバイト数を指定する場合は、番号タイプ（16 進数、8 進数、または 10 進数）を指定する必要があります。 DCE/RPC とともに使用する場合、許可される値は 1、2、および 4 です。

引数	説明
値	テストする値（演算子を含む）。 サポートされている演算子：<、>、=、!、&、^、!>、!<、!=、!&、または !^。 たとえば `!1024` と指定した場合、`byte_test` は指定された数値を変換し、それが 1024 と等しくなければイベントが生成されます（他のすべてのキーワード パラメータが一致する場合）。 「!」と「!=」は等価であることに注意してください。 また、既存の `byte_extract` 変数を使用してこの引数の値を指定することもできます。
Offset	ペイロード内で処理を開始するバイト数。`offset` カウンタはバイト 0 から始まるため、パケット ペイロードの先頭、または最後に見つかったコンテンツ一致から順方向にカウントするバイト数から 1 を差し引いて `offset` 値を計算してください。 既存の `byte_extract` 変数 変数を使用して、この引数の値を指定することができます。

次の表に示す引数を使用すると、システムで `byte_test` 引数がどのように使用されるかをさらに定義できます。

表 *111*：*byte_test* の追加のオプション引数

引数	説明
Relative	最後に見つかったパターン一致を基準にしてオフセットを計算します。

DCE/RPC、Endian、または Number Type のうち 1 つだけを指定できます。

検査対象となるバイトを `byte_test` キーワードでどのように計算するか定義するには、次の表の中から引数を選択します。バイト順引数を選択しなかった場合、ルール エンジンはビッグ エンディアンのバイト順を使用します。

表 *112*：*byte_test* のバイト順引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。

引数	説明
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に `byte_test` キーワードを指定します。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアンバイト順を決定します。Number Type 引数と Endian 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて `byte_test` を使用することもできます。

次の表に示すいずれか 1 つの引数を使用して、パケット内のストリング データをシステムがどのように表示するかを定義できます。

表 *113* : *byte-test* の番号タイプ引数

引数	説明
Hexadecimal String	変換後のストリング データを 16 進形式で表現します。
Decimal String	変換後のストリング データを 10 進形式で表現します。
Octal String	変換後のストリング データを 8 進形式で表現します。

たとえば、次のような値を `byte_test` に指定した場合、

- Bytes = 4
- Operator and Value > 128
- Offset = 8
- Relative enabled

ルール エンジンは、最後に見つかったコンテンツ一致から（それを基準にして）9 バイト後に出現する 4 つのバイトで記述される数値を計算し、その計算値が 128 バイトを超えた場合に、ルールがトリガーとして使用されます。

関連トピック

byte_extract キーワード, （1155 ページ）
DCE/RPC キーワード, （1192 ページ）

byte_extract キーワード

`byte_extract` キーワードを使用すると、指定したバイト数をパケットから変数の中に読み込むことができます。後で、その変数を、同じルール内で他の検出キーワードの特定の引数の値として使用できます。

たとえば、パケット データに含まれるバイト数が特定のバイト セグメントで記述されている場合、パケットからデータ サイズを抽出するには、これが役立ちます。たとえば、特定のバイトセグメントにおいて、後続データが 4 バイト構成であると記述されている場合、データ サイズ 4 バイトを抽出して変数値として使用できます。

`byte_extract` を使用するとき、1 つのルール内で最大 2 つの異なる変数を同時に作成できます。`byte_extract` 変数を何回でも再定義できます。同じ変数名と別の変数定義を使って新しい `byte_extract` キーワードを入力した場合、その前の変数定義がオーバーライドされます。

次の表で、`byte_extract` キーワードで必要な引数について説明します。

表 *114*：*byte_extract* の必須引数

引数	説明
Bytes to Extract	パケットから抽出するバイト数。 1、2、または 4 以外のバイト数を指定する場合は、番号タイプ（16 進数、8 進数、または 10 進数）を指定する必要があります。
Offset	ペイロード内でデータの抽出を開始するバイト数。-65535 ～ 65535 バイトを指定できます。オフセットカウンタはバイト 0 から始まるため、順方向に数えるバイト数から 1 を差し引いてオフセット値を計算してください。たとえば、順方向に 8 バイト数えるには 7 を指定します。ルール エンジンは、パケット ペイロードの先頭から（Relative も一緒に指定した場合は最後に見つかったコンテンツ一致の後から）順方向に数えます。負の数は、Relative も指定した場合にのみ指定できます。
Variable Name	他の検出キーワードの引数で使用する変数名。英数字の文字列を指定できます（ただし文字で始まる必要があります）。

抽出対象のデータを見つける方法をさらに詳しく定義するには、次の表に示す引数を使用できます。

表 *115*：*byte_extract* の追加のオプション引数

引数	説明
Multiplier	パケットから抽出された値の乗数。0 ～ 65535 を指定できます。乗数を指定しない場合のデフォルト値は 1 です。
Align	抽出された値を最も近い 2 バイトまたは 4 バイト境界に切り上げます。Multiplier も一緒に選択した場合、システムはこの調整の前に乗数を適用します。
Relative	ペイロードの先頭ではなく、最後に見つかったコンテンツ一致の末尾を基準にして Offset を計算します。

DCE/RPC、Endian、または Number Type のうち 1 つだけを指定できます。

検査対象となるバイトを `byte_extract` キーワードでどのように計算するか定義するには、次の表の中から引数を選択できます。バイト順引数を選択しなかった場合、ルールエンジンはビッグエンディアンのバイト順を使用します。

表 *116*：*byte_extract* のバイト順引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に `byte_extract` キーワードを指定します。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。Number Type 引数と Endian 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて `byte_extract` を使用することもできます。

データを読み取るときの数値タイプを ASCII 文字列として指定できます。パケット内のストリング データをシステムがどのように認識するかを定義するには、次の表のいずれかの引数を選択できます。

表 *117*：*byte_extract* の番号タイプ引数

引数	説明
Hexadecimal String	抽出されたストリング データを 16 進形式で読み取ります。
Decimal String	抽出されたストリング データを 10 進形式で読み取ります。
Octal String	抽出されたストリング データを 8 進形式で読み取ります。

たとえば、`byte_extract` の値を次のように指定した場合、

- Bytes to Extract = 4
- Variable Name = var
- Offset = 8
- Relative = enabled

ルール エンジンは、最後に見つかったコンテンツ一致から（それを基準にして）9 バイト後に出現する、4 バイトで表現される数値を `var` という名前の変数の中に読み込みます。後でこの変数を、特定のキーワード引数の値としてルール内で指定できます。

`byte_extract` キーワードで定義した変数を指定できるキーワード引数を、次の表に列挙します。

表 *118*：*byte_extract* 変数を使用できる引数

キーワード	引数
content	Depth、Offset、Distance、Within
byte_jump	Offset
byte_test	Offset、Value
isdataat	Offset

関連トピック

DCE/RPC プリプロセッサ, （1278 ページ）
DCE/RPC キーワード, （1192 ページ）
基本コンテンツおよび protected_content キーワードの引数, （1137 ページ）
byte_jump キーワード, （1150 ページ）
byte_test キーワード, （1153 ページ）
パケット特性, （1217 ページ）

概要：pcre キーワード

`pcre` キーワードを使用すると、指定されたコンテンツをパケット ペイロード内で検査するために Perl 互換正規表現（PCRE）を使用できます。PCRE を使用すると、同じ内容のわずかなバリエーションにそれぞれ一致する複数のルールを作成する手間が省けます。

正規表現は、さまざまな方法で表現されることのあるコンテンツを検索する場合に役立ちます。パケットのペイロード内でコンテンツを検索するときには、コンテンツがさまざまな属性を持つ可能性があることを考慮すべき場合があります。

侵入ルールで使われる正規表現構文は完全な正規表現ライブラリのサブセットであり、完全なライブラリ内のコマンドで使用される構文とはいくつかの点で異なることに注意してください。侵入ルール エディタを使用して `pcre` キーワードを追加するときには、次の形式で完全な値を入力します。

```
!/pcre/ ismxAEGRBUIPHDMCKSY
```

引数の説明

- 「!」は否定オプションです（正規表現に**一致しない**パターンを照合する場合に使用します）。

- /pcre/ は Perl 互換正規表現です。
- ismxAEGRBUIPHDMCKSY は修飾子オプションの任意の組み合わせです。

また、次の表に示す文字をエスケープする必要があることに注意してください。これにより、パケット ペイロード内で特定のコンテンツを検索するために PCRE でこれらの文字を使用した場合、ルール エンジンがそれを正しく解釈するようになります。

表 *119*：エスケープする *PCRE* 文字

エスケープする必要のある文字	バックスラッシュを使用した場合	16 進コードを使用した場合
#（ナンバー記号）	\#	\x23
;（セミコロン）	\;	\x3B
|（縦棒）	\\|	\x7C
：（コロン）	\:	\x3A

m?regex? を使用することもできます。ここで、? は「/」以外のデリミタです。正規表現内でスラッシュと一致させる必要があり、バックスラッシュを使ってそれをエスケープしたくない場合には、これを使用できます。たとえば、「m?regex? ismxAEGRBUIPHDMCKSY」のように使用できます。regex は Perl 互換正規表現、ismxAEGRBUIPHDMCKSY は修飾子オプションの任意の組み合わせです。

ヒント オプションで、Perl 互換正規表現を引用符で囲むこともできます（例：pcre_expression または ‟pcre_expression‟）。引用符が任意ではなく必須であった旧バージョンに慣れている経験豊富なユーザのために、引用符を使用するオプションが提供されています。保存後のルールを侵入ルール エディタで表示すると、引用符が表示されません。

PCRE の構文

pcre キーワードでは、標準の Perl 互換正規表現（PCRE）構文を使用できます。以下の項では、この構文について説明します。

ヒント ここでは PCRE で使用可能な基本的な構文について説明しますが、Perl および PCRE 専用のオンライン リファレンスやブックで、さらに詳しい情報を参照することもできます。

メタ文字

メタ文字は正規表現内で特別な意味を持つリテラル文字です。メタ文字を正規表現内で使用するときには、その前にバックスラッシュを付けて「エスケープする」必要があります。

次の表に、PCRE で使用可能なメタ文字について説明し、それぞれの例を示します。

表 *120* : *PCRE* メタ文字

メタ文字	説明	例
.	改行以外の任意の文字と一致します。修飾オプションとして s が使用されている場合は、改行文字も含まれます。	abc. は、abcd、abc1、abc# などと一致します。
*	ある文字または式の 0 回以上の出現と一致します。	abc* は、abc、abcc、abccc、abcccccc などと一致します。
?	ある文字または式の 0 回または 1 回の出現と一致します。	abc? は abc に一致します。
+	ある文字または式の 1 回以上の出現と一致します。	abc+ は、abc、abcc、abccc、abcccccc などと一致します。
()	式をグループ化します。	(abc)+ は、abc、abcabc、abcabcabc などと一致します。
{}	ある文字または式の一致回数の限度を指定します。下限と上限を設定する場合には、下限と上限をカンマで区切ります。	a{4,6} は、aaaa、aaaaa、または aaaaaa と一致します。 (ab){2} は abab と一致します。
[]	文字クラスを定義できます。セットの中で記述される任意の文字または文字の組み合わせに一致します。	[abc123] は、a または b または c などと一致します。
^	文字列の先頭でコンテンツを照合します。また、文字クラスの中で否定としても使用されます。	^in は、info 内の「in」と一致しますが、bin では一致しません。[^a] は、a を含まない任意の文字列と一致します。
$	文字列の末尾でコンテンツを照合します。	ce$ は、announce 内の「ce」と一致しますが、cent では一致しません。
|	OR 式を示します。	(MAILTO|HELP) は、MAILTO または HELP と一致します。

メタ文字	説明	例
\	メタ文字を実際の文字として使用できます。また、事前定義された文字クラスを指定するためにも使われます。	\. はピリオドと一致し、* はアスタリスクと一致し、\\ はバックスラッシュと一致します。\d は数字と一致し、\w は英数字と一致します。

文字クラス

文字クラスには、英字、数字、英数字、および空白文字があります。大カッコで囲んで独自の文字クラスを作成できます。また、事前定義のクラスをさまざまな文字タイプのショートカットとして使用することもできます。追加の修飾子なしで文字クラスを使用すると、1 つの文字クラスは 1 桁または 1 文字に一致します。

次の表に、PCRE で使用できる事前定義の文字クラスの説明と例を示します。

表 *121*：*PCRE* 文字クラス

文字クラス	説明	文字クラスの定義
\d	数字（桁）と一致します。	[0-9]
\D	数字以外の任意の文字と一致します。	[^0-9]
\w	英数字（語）と一致します。	[a-zA-Z0-9_]
\W	英数字以外の任意の文字と一致します。	[^a-zA-Z0-9_]
\s	スペース、復帰、タブ、改行、および改ページを含む空白文字と一致します。	[\r\t\n\f]
\S	空白文字以外の任意の文字と一致します。	[^ \r\t\n\f]

PCRE 修飾子のオプション

pcre キーワードの値の中で正規表現構文を指定した後、修飾オプションを使用できます。これらの修飾子は、Perl、PCRE、および Snort 固有の処理機能を実行します。修飾子は、常に PCRE 値の末尾に、次の形式で出現します。

```
/pcre/ismxAEGRBUIPHDMCKSY
```

ここで、ismxAEGRBUPHMC には、次の表に示す任意の修飾オプションを含めることができます。

ヒント オプションで、正規表現と修飾オプションを引用符で囲むことができます（たとえば "/pcre/ismxAEGRBUIPHDMCKSY"）。引用符が任意ではなく必須であった旧バージョンに慣れている経験豊富なユーザのために、引用符を使用するオプションが提供されています。保存後のルールを侵入ルール エディタで表示すると、引用符が表示されません。

次の表に、Perl 処理機能を実行するために使用できるオプションを説明します。

表 *122* : *Perl* 関連の正規表現後オプション

オプション	説明
i	正規表現で大文字と小文字を区別しないようにします。
s	ドット文字（.）は、改行または \n 文字を除くすべての文字を表します。オプションとして "s" を使用すると、これをオーバーライドして、改行文字を含むすべての文字をドット文字に一致させることができます。
m	デフォルトで、1 つの文字列は複数文字からなる単一行として扱われ、^ と $ は特定の文字列の先頭および末尾に一致します。オプションとして "m" を使用すると、^ および $ はバッファの先頭または末尾だけでなく、バッファ内の改行文字の直前または直後のコンテンツとも一致します。
x	エスケープされた（バックスラッシュが先行する）場合、および文字クラスに含まれる場合を除き、空白データ文字がパターン内に出現してもそれを無視します。

次の表に、正規表現の後ろに使用できる PCRE 修飾子の説明を示します。

表 *123* : *PCRE* 関連の正規表現後オプション

オプション	説明
A	文字列の先頭でパターンが一致する必要があります（正規表現で ^ を使用した場合と同じ）。
E	対象の文字列の末尾でのみ一致するように $ を設定します。（E を伴わない $ は、それが改行である場合には最後の文字の直前とも一致しますが、他の改行文字の直前とは一致しません）。
G	デフォルトでは、* + と ? は「最長マッチ」を実行します。つまり、複数の一致が見つかった場合は最も長い一致が選択されます。G 文字を使用するとこの動作が変更され、常に最初の一致がこれらの文字で選択されます。ただし後ろに疑問符（?）が続く場合を除きます。たとえば、*? +? と ?? は G 修飾子を使った構造内で最長マッチを実行し、疑問符が付いていない *、+、または ? は最長マッチではありません。

次の表に、正規表現の後ろに使用できる Snort 固有の修飾子の説明を示します。

.

表 *124*：*Snort* 固有の正規表現後の修飾子

オプション	説明
R	ルールエンジンで見つかった最後の一致の末尾を基準にして、一致するコンテンツを検索します。
B	プリプロセッサによってデコードされる前のデータ内のコンテンツを検索します（このオプションは、`content` または `protected_content` キーワードとともに `生データ（Raw Data）` 引数を使用する場合に似ています）。
U	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージの URI 内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの HTTP URI オプションを一緒に使用して、同じコンテンツを検索することはできません。 パイプライン処理された HTTP 要求パケットには複数の URI が含まれていることに注意してください。U オプションを含む PCRE 式を使用すると、ルールエンジンは、パイプライン処理された HTTP 要求パケット内の最初の URI でのみコンテンツ一致を検索します。パケット内のすべての URI を検索するには、U オプションを使った PCRE 式を一緒に使用するかどうかに関係なく、[HTTP URI] を選択した `content` または `protected_content` キーワードを使用してください。
I	HTTP Inspect プリプロセッサによってデコードされた raw HTTP 要求メッセージの URI 内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの HTTP Raw URI オプションを一緒に使用して、同じコンテンツを検索することはできません。
P	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージ本文の中でコンテンツを検索します。
H	HTTP Inspect プリプロセッサによってデコードされた HTTP 要求または応答メッセージの（cookie を除く）ヘッダー内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの HTTP Header オプションを一緒に使用して、同じコンテンツを検索することはできません。

オプション	説明
D	HTTP Inspect プリプロセッサによってデコードされた未加工の HTTP 要求または応答メッセージの（cookie を除く）ヘッダー内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの HTTP Raw Header オプションを一緒に使用して、同じコンテンツを検索することはできません。
M	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージのメソッド フィールド内のコンテンツを検索します。メソッド フィールドは、URI で識別されるリソースに対して実行すべきアクション（GET、PUT、CONNECT など）を特定します。
C	HTTP Inspect プリプロセッサの [HTTP Cookie の検査（Inspect HTTP Cookies）] オプションが有効になっている場合は、HTTP 要求見出しの cookie 内の正規化済みコンテンツを検索します。さらに、プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションが有効になっている場合は、HTTP 応答見出しの set-cookie 内も検索します。[HTTP Cookie の検査（Inspect HTTP Cookies）] が有効になっていない場合は、cookie または set-cookie データを含む見出し全体を検索します。 次の点に注意してください。 • メッセージ本文に含まれる cookie は、本文のコンテンツとして扱われます。 • このオプションと `content` または `protected_content` キーワードの HTTP Cookie オプションを一緒に使用して、同じコンテンツを検索することはできません。 • `Cookie:` ヘッダー名と `Set-Cookie:` ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す `CRLF` は cookie の一部としてではなく、ヘッダーの一部として検査されます。

オプション	説明
K	HTTP Inspect プリプロセッサの [HTTP Cookie の検査（Inspect HTTP Cookies）] オプションが有効になっている場合は、HTTP 要求見出しの cookie 内の未加工コンテンツを検索します。さらに、プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションが有効になっている場合は、HTTP 応答見出しの set-cookie 内も検索します。[HTTP Cookie の検査（Inspect HTTP Cookies）] が有効になっていない場合は、cookie または set-cookie データを含む見出し全体を検索します。 次の点に注意してください。 • メッセージ本文に含まれる cookie は、本文のコンテンツとして扱われます。 • このオプションと `content` または `protected_content` キーワードの HTTP Raw Cookie オプションを一緒に使用して、同じコンテンツを検索することはできません。 • `Cookie:` ヘッダー名と `Set-Cookie:` ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す `CRLF` は cookie の一部としてではなく、ヘッダーの一部として検査されます。
S	HTTP 応答内の 3 桁のステータス コードを検索します。
Y	HTTP 応答内のステータス コードに付加されるテキスト記述を検索します。

（注） UオプションとRオプションを組み合わせて使用しないでください。パフォーマンスの問題が発生する可能性があります。また、他のHTTPコンテンツ オプション（I、P、H、D、M、C、K、S または Y）と組み合わせて U オプションを使用しないでください。

関連トピック

概要：HTTP content および protected_content キーワードの引数, （1141 ページ）

PCRE のキーワード値の例

次に、`pcre` で入力できる値の例を示し、それぞれの例で何が一致するかを説明します。

- /feedback[(\d{0,1})]?\.cgi/U

この例では、URI データにのみ配置された、`feedback` の後に 0 個または 1 個の数字、さらに `.cgi` が続くインスタンスをパケット ペイロード内で検索します。

この例は以下のものと一致します。

- `feedback.cgi`
- `feedback1.cgi`
- `feedback2.cgi`
- `feedback3.cgi`

この例は、以下のものとは一致**しません**。

- `feedbacka.cgi`
- `feedback11.cgi`
- `feedback21.cgi`
- `feedbackzb.cgi`

- /^ez(\w{3,5})\.cgi/iU

この例では、先頭の `ez` の後に 3 ～ 5 文字の単語、さらに `.cgi` が続く文字列をパケット ペイロード内で検索します。この検索では大文字と小文字を区別せず、URI データだけを検索します。

この例は以下のものと一致します。

- `EZBoard.cgi`
- `ezman.cgi`
- `ezadmin.cgi`
- `EZAdmin.cgi`

この例は、以下のものとは一致**しません**。

- `ezez.cgi`
- `fez.cgi`
- `abcezboard.cgi`
- `ezboardman.cgi`

- /mail(file|seek)\.cgi/U

この例では、URI データ内の `mail` の後に `file` と `seek` のどちらかが続く文字列をパケット ペイロードで検索します。

この例は以下のものと一致します。

- `mailfile.cgi`
- `mailseek.cgi`

この例は、以下のものとは一致**しません**。

- `MailFile.cgi`

- `mailfilefile.cgi`
- m?http\\x3a\x2f\x2f.*(\n|\t)+?U

この例では、任意の数の文字の後ろにある、HTTP 要求内のタブまたは改行文字を示す URI コンテンツをパケット ペイロード内で検索します。この例では、式で `m?`regex`?` を使用して、`http\:\/\/` を使用しないようにしています。コロンの前にバックスラッシュがあることに注意してください。

この例は以下のものと一致します。

- `http://www.example.com?scriptvar=x&othervar=\n\..\..`
- `http://www.example.com?scriptvar=\t`

この例は、以下のものとは一致**しません**。

- `ftp://ftp.example.com?scriptvar=&othervar=\n\..\..`
- `http://www.example.com?scriptvar=|/bin/sh -i|`
- m?http\\x3a\x2f\x2f.*=\|.*\|+?sU

この例では、（改行を含む）任意の数の文字の後に 1 つの等号、さらに任意の数の文字または空白を含むパイプ文字が続くという構成の URL をパケット ペイロード内で検索します。この例では、式で `m?`regex`?` を使用して、`http\:\/\/` を使用しないようにしています。

この例は以下のものと一致します。

- `http://www.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?input=|cat /etc/passwd|`

この例は、以下のものとは一致**しません**。

- `ftp://ftp.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?value=x&input?|cat /etc/passwd|`
- /[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}/i

この例では、MAC アドレスをパケット ペイロード内で検索します。コロン文字がバックスラッシュでエスケープされていることに注意してください。

metadata キーワード

`metadata` キーワードを使用すると、記述情報をルールに追加できます。また、`metadata` キーワードを `service` 引数とともに使用すると、ネットワーク トラフィック内のアプリケーションとポートを特定することができます。追加する情報を使用して、要件に適合するルールを編成または識別することができ、追加する情報や `service` 引数についてルールを検索することができます。

システムは次の形式の引数に基づいてメタデータを検証します。

key value

ここで、*key* と *value* は、スペースで区切られた記述の組み合わせです。これは、Cisco 提供のルールにメタデータを追加するために Cisco Talos Security Intelligence and Research Group（Talos） VRT で使用されている形式です。

または、次の形式を使用することもできます。

key = value

たとえば、*key value* 形式で次のようにカテゴリとサブカテゴリを使用し、作成者と日付によってルールを識別できます。

```
author SnortGuru_20050406
```

1 つのルール内で複数の `metadata` キーワードを使用できます。また、以下の例に示すように、単一の `metadata` キーワード内で複数の *key value* 引数をカンマで区切ることもできます。

```
author SnortGuru_20050406, revised_by SnortUser1_20050707,
revised_by SnortUser2_20061003,

revised_by SnortUser1_20070123
```

使用できる形式は *key value* と *key=value* だけに限定されません。ただし、これらの形式に基づく検証に起因する制限事項を把握しておく必要があります。

注意すべき制限のある文字

次の文字制限に注意してください。

- セミコロン（;）またはコロン（:）を使用しないでください。
- システムはコンマを、複数の *key value* 引数または *key=value* 引数の区切り文字であると解釈します。次に例を示します。

  key value,*key value*,*key value*

- システムは等号（=）または余白文字を、*key* と *value* の間の区切り文字であると解釈します。次に例を示します。

  key value

  key=value

その他のすべての文字が使用可能です。

注意すべき予約済みメタデータ

`metadata` キーワードでは、次の単語を単一の引数として、または *key value* 引数内の *key* として使用しないでください。これらは Talos 用に予約されています。

```
application
engine
impact_flag
os
policy
rule-type
rule-flushing
soid
```

（注） ローカル ルールを適切に機能させるために制限付きメタデータをどうしても追加する必要がある場合は、サポート担当にお問い合わせください。

影響レベル 1

`metadata` キーワードでは、次に示す予約済み *key value* 引数を使用できます。

`impact_flag red`
この *key value* 引数は、インポートしたローカル ルールまたは侵入ルール エディタを使って作成したカスタム ルールに関する影響フラグを赤（レベル 1）に設定します。

「送信元または宛先のホストがウイルス、トロイの木馬、その他の有害ソフトウェアによって侵害されている可能性があることを、ルールをトリガーしているパケットが示している」と Talos が判断した場合、Talos は Cisco 提供のルールに `impact_flag red` 引数を含めます。

関連トピック

ローカル侵入ルール ファイル インポート，（162 ページ）
侵入イベントのクリップボード，（2001 ページ）

サービス メタデータ

システムは、ネットワークのホストで動作しているアプリケーションを検出し、ネットワーク トラフィックにアプリケーション プロトコル情報を挿入します。これは、検出ポリシーの設定に関係なく実行されます。TCP または UDP ルールで `metadata` キーワード `service` 引数を使用して、ネットワーク トラフィックのアプリケーション プロトコルとポートを照合することができます。ルールで 1 つ以上の `service` アプリケーション引数を単一のポート引数と組み合わせることができます。

サービス アプリケーション

`metadata` キーワードとともに `service` を *key* として、アプリケーションを *value* として使用し、パケットを識別されたアプリケーション プロトコルと一致させることができます。たとえば、次に示す `metadata` キーワード内の *key value* 引数は、ルールを HTTP トラフィックに関連付けます。

`service http`
複数のアプリケーションをカンマで区切って指定することもできます。次に例を示します。

```
service http, service smtp, service ftp
```

注意 侵入ルールでサービス メタデータを使用するためには、適応型プロファイルの設定，（1431 ページ） で説明されているように、アダプティブ プロファイルを有効にする**必要があります**。

次の表に、`service` キーワードとともに使用される最も一般的なアプリケーション値を示します。

（注） 表にないアプリケーションを特定することが難しい場合は、サポートにお問い合わせください。

表 *125*：*service* 値

値	説明
cvs	Concurrent Versions System（バージョン管理システム）
dcerpc	分散コンピューティング環境/リモート プロシージャ コール システム
dns	ドメイン ネーム システム
finger	Finger User Information Protocol
FTP	File Transfer Protocol
ftp-data	File Transfer Protocol（データ チャネル）
http	ハイパーテキスト転送プロトコル
imap	Internet Message Access Protocol
isakmp	Internet Security Association and Key Management Protocol
mysql	My Structured Query Language（構造化照会言語）
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
netbios-ssn	NETBIOS Session Service
nntp	Network News Transfer Protocol
oracle	Oracle Net Services
shell	OS Shell
pop2	Post Office Protocol バージョン 2
pop3	Post Office Protocol バージョン 3
smtp	Simple Mail Transfer Protocol
snmp	簡易ネットワーク管理プロトコル

値	説明
ssh	セキュア シェル ネットワーク プロトコル
sunrpc	Sun リモート プロシージャ コール プロトコル
telnet	Telnet ネットワーク プロトコル
tftp	トリビアル ファイル転送プロトコル
x11	X Window システム

サービス ポート

Metadata キーワードとともに service を *key* として、指定したポート引数を *value* として使用し、ルールがアプリケーションと組み合わせてポートを照合する方法を定義できます。

次の表の任意のポート値を、ルールごとに 1 つ指定できます。

表 *126*：*service* ポート値

値	説明
else-ports または unknown	次の条件のいずれかが満たされるとルールが適用されます。 • パケット アプリケーションが既知で、ルール アプリケーションと一致する。 • パケット アプリケーションが不明で、パケット ポートがルール ポートと一致する。 else-ports および unknown の値では、service がポート修飾子なしでアプリケーション プロトコルを指定する場合にシステムで使用されるデフォルトの動作が生成されます。
and-ports	パケット アプリケーションが既知で、ルール アプリケーションと一致し、パケット ポートがルール ヘッダーのポートと一致する場合、ルールが適用されます。アプリケーションを指定しないルールで and-ports を使用することはできません。

値	説明
or-ports	次の条件のいずれかが満たされるとルールが適用されます。 • パケット アプリケーションが既知で、ルール アプリケーションと一致する。 • パケット アプリケーションが不明で、パケット ポートがルール ポートと一致する。 • パケット アプリケーションはルール アプリケーションと一致せず、パケット ポートはルール ポートと一致する。 • ルールはアプリケーションを指定せず、パケット ポートはルール ポートと一致する。

次の点に注意してください。

- service アプリケーション引数を service and-ports 引数とともに含める必要があります。
- ルールで上記の表の値が複数指定されている場合、ルールの一番最後にある値が適用されます。
- ポートおよびアプリケーション引数は任意の順序にすることができます。

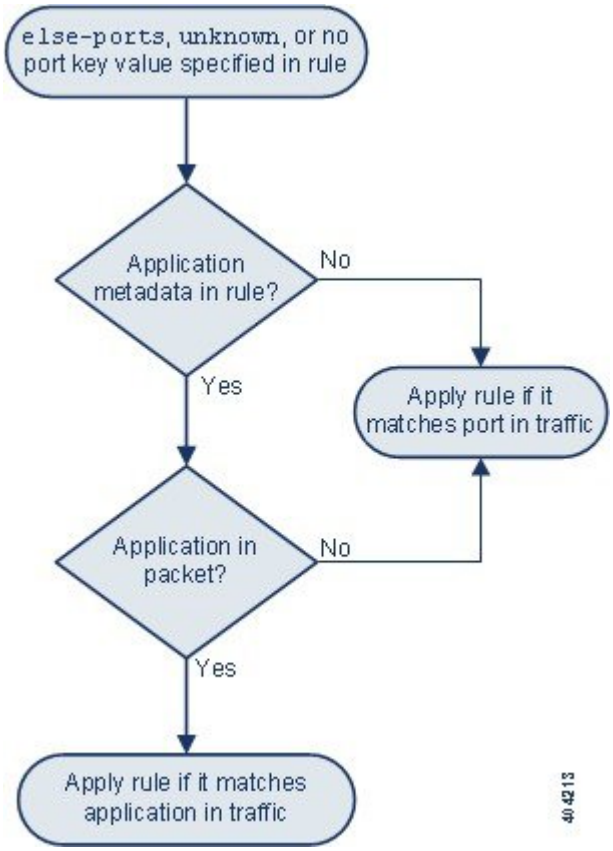
and-ports 値を除き、1 つ以上の service アプリケーション引数の有無にかかわらず、service ポート引数を含めることができます。次に例を示します。

```
service or-ports, service http, service smtp
```

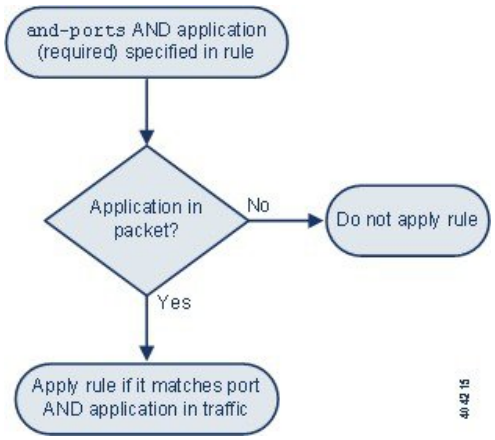
トラフィックのアプリケーションとポート

次の図は、侵入ルールでサポートされるアプリケーションとポートの組み合わせ、およびパケット データにこれらのルール制約を適用した結果を示しています。

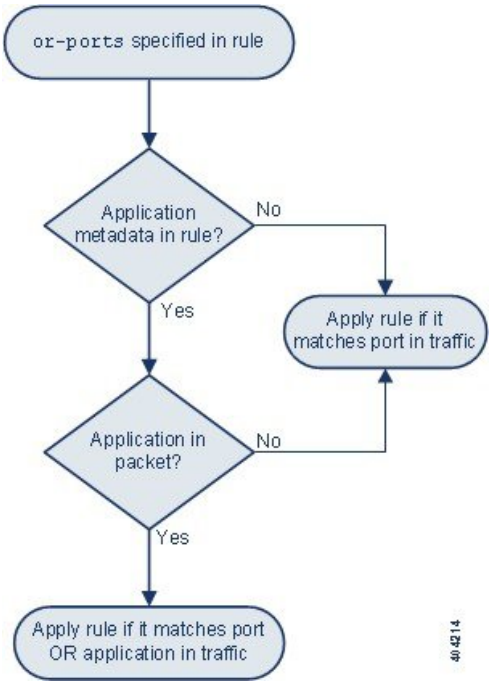
ホスト アプリケーション プロトコル **else** 送信元/宛先ポート：



ホスト アプリケーション プロトコル **and** 送信元/宛先ポート：



ホスト アプリケーション プロトコル or 送信元/宛先ポート：



一致する例

`metadata` キーワードを `service` 引数とともに使用した次のサンプル ルールを、一致するデータおよび一致しないデータの例とともに示します。

- `alert tcp any any -> any [80,8080] (metadata:service and-ports, service http, service smtp;)`

一致する例	一致しない例
• TCP ポート 80 経由の HTTP トラフィック • TCP ポート 8080 経由の HTTP トラフィック • TCP ポート 80 経由の SMTP トラフィック • TCP ポート 8080 経由の SMTP トラフィック	• ポート 80 または 8080 の POP3 トラフィック • ポート 80 または 8080 の不明なアプリケーション トラフィック • ポート 9999 の HTTP トラフィック

- `alert tcp any any -> any [80,8080] (metadata:service or-ports, service http;)`

一致する例	一致しない例
• あらゆるポートの HTTP トラフィック • ポート 80 の SMTP トラフィック • ポート 8080 の SMTP トラフィック • ポート 80 および 8080 の不明なアプリケーションのトラフィック	• 80 または 8080 以外のポートの非 HTTP および非 SMTP トラフィック

- 次のいずれかの規則：
  - `alert tcp any any -> any [80,8080] metadata:service else-ports, service http;)`
  - `alert tcp any any -> any [80,8080] metadata:service unknown, service http;)`
  - `alert tcp any any -> any [80,8080] metadata:service http;)`

一致する例	一致しない例
• あらゆるポートの HTTP トラフィック • パケット アプリケーションが不明な場合はポート 80 • パケット アプリケーションが不明な場合はポート 8080	• ポート 80 または 8080 の SMTP トラフィック • ポート 80 または 8080 の POP3 トラフィック

メタデータ検索のガイドライン

`metadata` キーワードを使用するルールを検索するには、ルールの [検索（Search）] ページで `metadata` キーワードを選択して、オプションで、メタデータの一部分を入力します。たとえば次のように入力できます。

- `search` と入力すると、*key* として `search` が使用されているすべてのルールが表示されます。
- `search http` と入力すると、*key* として `search`、*value* として `http` がそれぞれ使用されているすべてのルールが表示されます。
- `author snortguru` と入力すると、*key* として `author`、*value* として `SnortGuru` がそれぞれ使用されているすべてのルールが表示されます。
- `author s` と入力すると、*key* として `author`、さらに *value* として `SnortGuru`、`SnortUser1`、`SnortUser2` などの語が使用されているすべてのルールが表示されます。

ヒント *key* と *value* の両方を検索するときには、ルール内の *key value* 引数で使用されているのと同じ接続演算子（等号 [=] または空白文字）を検索で使用してください。*key* の後に等号（=）と空白文字のどちらを入力するかに応じて、異なる結果が検索で返されます。

なお、メタデータ追加のために使用する形式とは無関係に、システムはメタデータ検索語を *key value* または *key=value* 引数の全部または一部として解釈します。たとえば、次に示すメタデータは *key value* または *key=value* 形式に従っていませんが、有効なメタデータです。

```
ab cd ef gh
```

ただし、この例に含まれる各スペースは *key* と *value* の間の区切り文字としてシステムで解釈されます。次に示す並列語や単一語を検索で使用すると、この例のメタデータを含むルールを正しく検出できます。

```
cd ef
ef gh
ef
```

一方、次の検索を使用した場合、単一の *key value* 引数としてシステムによって解釈されるため、ルールを検出できません。

```
ab ef
```

関連トピック

ルールの検索, （1128 ページ）

IP ヘッダー値

キーワードを使用すると、パケットの IP ヘッダーの中で攻撃やセキュリティ ポリシー違反の可能性を識別できます。

fragbits

`fragbits` キーワードは、IP 見出し内のフラグメント ビットと予約ビットを検査します。パケットごとに、予約ビット、More Fragments ビット、および Don't Fragment ビットを任意に組み合わせて検査できます。

表 *127* : *Fragbits* 引数の値

引数	説明
R	予約済みビット
M	More Fragments ビット
D	Don’t Fragment ビット

fragbits キーワードを使ってルールを微調整するために、次の表に示す演算子をルール内の引数値の後ろに指定できます。

表 *128*：*Fragbit* 演算子

演算子	説明
プラス記号（+）	パケットは、指定されたすべてのビットと一致する必要があります。
アスタリスク（*）	パケットは、指定されたどのビットと一致することもできます。
感嘆符（!）	指定されたどのビットも設定されていない場合、パケットが基準を満たします。

たとえば、（他のビットの有無とは無関係に）少なくとも予約済みビットが設定されたパケットに対してイベントを生成するには、fragbits 値として R+ を使用します。

id

id キーワードは、キーワード引数で指定される値に照らして IP 見出しフラグメント識別フィールドを検査します。一部のサービス拒否ツールやスキャナは、このフィールドを、容易に検出できる特定の番号に設定します。たとえば、Synscan ポートスキャンを検出する SID 630 では、id 値が 39426（スキャナから伝送されるパケットの ID 番号として使われる静的な値）に設定されます。

（注） id 引数値は数値でなければなりません。

ipopts

IPopts キーワードを使用すると、指定された IP 見出しオプションをパケット内で検索できます。次の表に、使用可能な引数値を示します。

表 *129*：*IPoption* 引数

引数	説明
rr	経路を記録
eol	リストの末尾
nop	オペレーションなし
ts	タイム スタンプ

引数	説明
sec	IP セキュリティ オプション
lsrr	厳密でない送信元ルーティング
ssrr	厳密な送信元ルーティング
satid	ストリーム識別子

アナリストが最も頻繁に監視するのは、厳密な送信元ルーティングと厳密でない送信元ルーティングです。これらのオプションは送信元 IP アドレスのスプーフィングを示している可能性があるためです。

ip_proto

`ip_proto` キーワードを使用すると、キーワードの値として指定された IP プロトコルを含むパケットを識別できます。IP プロトコルは 0 ～ 255 の数値として指定できます。これらの番号を、`<`、`>`、または `!` 演算子と組み合わせることができます。たとえば、ICMP 以外のプロトコルを使用しているトラフィックを検査するには、`ip_proto` キーワードの値として `!1` を使用します。1 つのルール内で `ip_proto` キーワードを複数回にわたって使用できます。ただし、ルール エンジンはキーワードの複数インスタンスをブール和関係（AND）と解釈することに注意してください。たとえば、`ip_proto:!3; ip_proto:!6` を含むルールを作成した場合、このルールは GGP プロトコルおよび TCP プロトコルを使用するトラフィックを無視します。

tos

一部のネットワークでは、ネットワーク上を移動するパケットの優先度を設定するタイプ オブ サービス（ToS）値が使用されます。`tos` キーワードを使用すると、キーワードの引数で指定された値に照らしてパケットの IP 見出し ToS 値を検査できます。`tos` キーワードを使用するルールは、ToS が指定の値に設定され、しかもルール内の残りの基準を満たすパケットに対してトリガーとして使用されます。

（注） `tos` の引数値は数値でなければなりません。

[ToS] フィールドは IP ヘッダー プロトコルでは非推奨になり、[Differentiated Services Code Point (DSCP)] フィールドに置き換えられています。

ttl

パケットの存続可能時間（time-to-live、ttl）値は、パケットが破棄される前に生成できるホップ数を示します。`ttl` キーワードを使用すると、キーワードの引数として指定された値または値の範囲に照らしてパケットの IP 見出し ttl 値を検査できます。`ttl` キーワード パラメータを 0 や 1 などの低い値に設定すると役立つことがあります。これは、低い存続可能時間値がトレースルートや侵入回避の試みを示している場合があるためです。（ただし、このキーワードの適切な値は、管理

対象デバイスの配置やネットワーク トポロジによって異なります）。次のように構文を使用します。

- TTL 値に特定の 1 つの値を設定するには、0 ～ 255 の整数を使用します。値の前に等号（=）を付けることもできます（たとえば `5` または `=5` を指定できます）。
- TTL 値の範囲を指定するには、ハイフン（-）を使用します（たとえば、`0-2` は 0 ～ 2 のすべての値、`-5` は 0 ～ 5 のすべての値、`5-` は 5 ～ 255 のすべての値をそれぞれ指定します）。
- 特定の値より大きいTTL値を指定するには、「大なり」記号（>）を使用します（たとえば、`>3` は 3 より大きいすべての値を指定します）。
- 特定の値以上のTTL値を指定するには、「大なりイコール」記号（>=）を使用します（たとえば、`>=3` は 3 以上のすべての値を指定します）。
- 特定の値より小さいTTL値を指定するには、「小なり」記号（<）を使用します（たとえば、`<3` は 3 より小さいすべての値を指定します）。
- 特定の値以下のTTL値を指定するには、「小なりイコール」記号（<=）を使用します（たとえば、`<=3` は 3 以下のすべての値を指定します）。

ICMP ヘッダー値

Firepower システムでサポートされるキーワードを使用すると、ICMP パケット ヘッダー内の攻撃やセキュリティ ポリシー違反を識別できます。なお、ほとんどの ICMP タイプおよびコードを検出する事前定義ルールがあることに注意してください。既存のルールを有効にするか、既存のルールに基づいてローカル ルールを作成することを考慮してください。ICMP ルールを最初から作成するよりも、ニーズを満たすルールを見つける方が時間の節約になる可能性があります。

icmp_id と icmp_seq

ICMP の識別番号とシーケンス番号は、ICMP 応答と ICMP 要求を関連付けるうえで役立ちます。通常のトラフィックでは、これらの値はパケットに動的に割り当てられます。一部のコバート チャネルおよび Distributed Denial of Server（DDoS）プログラムは、静的な ICMP ID およびシーケンス値を使用します。次のキーワードを使用すると、静的な値を含む ICMP パケットを識別できます。

キーワード	定義（Definition）
icmp_id	ICMP エコー要求または応答パケットの ICMP ID 番号を検査します。ICMP ID 番号に対応する数値を `icmp_id` キーワードの引数として使用します。
icmp_seq	`icmp_seq` キーワードは、ICMP エコー要求または応答パケットの ICMP シーケンスを検査します。ICMP シーケンス番号に対応する数値を `icmp_seq` キーワードの引数として使用します。

itype

itype キーワードを使用して、特定の ICMP メッセージ タイプ値を含むパケットを検索します。有効な ICMP タイプ値と無効な ICMP タイプ値のいずれかを指定して、さまざまなタイプのトラフィックを検査できます。たとえば、サービス拒否攻撃やフラッディング攻撃を発生させるために攻撃者が範囲外の ICMP タイプ値を設定することがあります。

「小なり」（<）と「大なり」（>）を使用して itype 引数値の範囲を指定できます。

次に例を示します。

- <35
- >36
- 3<>55

icode

ICMP メッセージには、宛先が到達不能である場合の詳細を示すコード値が含まれることがあります。

icode キーワードを使用すると、特定の ICMP コード値を含むパケットを識別できます。有効な ICMP コード値と無効な ICMP コード値のいずれかを指定することにより、さまざまなタイプのトラフィックを検査できます。

「小なり」（<）と「大なり」（>）を使用して icode 引数値の範囲を指定できます。

次に例を示します。

- 35 より小さい値を検索するには <35 と指定します。
- 36 より大きい値を検索するには >36 と指定します。
- 3 ～ 55 の間にある値を検索するには、3<>55 と指定します。

ヒント　icode キーワードと itype キーワードを一緒に使用すると、両方に一致するトラフィックを識別できます。たとえば、ICMP 宛先到達不能コード タイプと ICMP ポート到達不能コード タイプを含む ICMP トラフィックを特定するには、値 3 の itype キーワード（宛先到達不能）と、値 3 の icode キーワード（ポート到達不能）を指定します。

TCP ヘッダー値とストリーム サイズ

Firepower システムでは、パケットの TCP ヘッダーと TCP ストリーム サイズを使って試行される攻撃を識別するためのキーワードを使用できます。

ack

ack キーワードを使用すると、パケットの TCP 確認応答番号と特定の値を比較できます。パケットの TCP 確認応答番号が、ack キーワードに指定された値と一致した場合に、ルールがトリガーとして使用されます。

ack の引数値は数値でなければなりません。

フラグ（Flags）

flags キーワードを使用すると、複数の TCP フラグを任意に組み合わせて指定できます。検査対象のパケットでこれらが設定されている場合、ルールがトリガーとして使用されます。

（注） 従来、flags の値として A+ を使用していたケースでは、代わりに flow キーワードおよび値 established を使用してください。一般に、フラグのすべての組み合わせが検出されるようにするには、フラグの使用時に flow キーワードおよび値 stateless を使用する必要があります。

次の表に示す flags キーワードの値を確認または無視することができます。

表 *130*：*flags* の引数

引数	TCP フラグ
ACK	データを確認応答します。
Psh	このパケットでデータが送信される必要があります。
Syn	新しい接続。
Urg	パケットに緊急データが含まれています。
Fin	接続が閉じられました。
Rst	接続が異常終了しました。
CWR	ECN 輻輳ウィンドウが減少しました。旧 R1 引数（下位互換性を維持するために引き続きサポートされています）。
ECE	ECN エコー。旧 R2 引数（下位互換性を維持するために引き続きサポートされています）。

flags キーワードを使用する場合、複数のフラグに対する照合方法をシステムに指示するための演算子を使用できます。次の表に、これらの演算子の説明を示します。

表 *131* : ***flags*** と一緒に使用する演算子

演算子	説明	例
すべて	パケットは、指定されたすべてのフラグを含んでいる必要があります。	`Urg` と `all` を選択すると、パケットが緊急フラグを含んでいる必要があること、および他のフラグが含まれる可能性があることを指定できます。
任意	パケットは、指定された任意のフラグを含むことができます。	`Ack`、`Psh`、および `any` を選択すると、ルールをトリガーとして使用するためには `Ack` と `Psh` のどちらか（または両方）のフラグが設定される必要があること、およびパケット内で他のフラグも設定されている可能性があることを指定できます。
ノット	パケットは、指定されたフラグセットを含んでは**なりません**。	`Urg` と `not` を選択すると、このルールをトリガーとして使用するパケットに関して緊急フラグが設定**されない**ことを指定できます。

flow

`flow` キーワードを使用すると、セッション特性に基づいてルールで検査されるパケットを選択できます。`flow` キーワードを使用することで、ルールの適用対象となるトラフィック フロー方向を指定して、クライアント フローとサーバ フローのどちらかにルールを適用できます。`flow` キーワードによるパケット検査の方法を指定するには、分析すべきトラフィックの方向、検査するパケットの状態、およびパケットが再構築ストリームの一部かどうかを設定できます。

ルールの処理時に、パケットのステートフルインスペクションが実行されます。ステートレス トラフィック（セッション コンテキストが確立されていないトラフィック）を TCP ルールで無視するには、`flow` キーワードをルールに追加して、そのキーワードで Established 引数を選択する必要があります。UDP ルールでステートレス トラフィックを無視するには、`flow` キーワードをルールに追加して、Established 引数と方向引数のどちらか（または両方）を選択する必要があります。これにより、TCP または UDP ルールでパケットのステートフル インスペクションが実行されます。

方向引数を追加した場合、ルール エンジンは、指定された方向と一致するフローを伴う確立された状態のパケットだけを検査します。たとえば、TCP または UDP 接続が検出されたときトリガーとして使用されるルールに、`flow` キーワードおよび `established` 引数と `From Client` 引数を追加した場合、ルール エンジンはクライアントから送信されたパケットだけを検査します。

ヒント パフォーマンスを最大にするには、必ず TCP ルールまたは UDP セッション ルールに `flow` キーワードを含めてください。

次の表に、`flow` キーワードで指定できるストリーム関連引数の説明を示します。

表 *132* : *flow* の状態関連引数

引数	説明
Established	確立された接続でトリガーとして使用されます。
Stateless	ストリーム プロセッサの状態に関係なくトリガーとして使用されます。

次の表に、`flow` キーワードで指定できる方向オプションの説明を示します。

表 *133* : *flow* の方向引数

引数	説明
To Client	サーバ応答でトリガーとして使用されます。
To Server	クライアント応答でトリガーとして使用されます。
From Client	クライアント応答でトリガーとして使用されます。
From Server	サーバ応答でトリガーとして使用されます。

`From Server` と `To Client` の機能が同じであること、および `To Server` と `From Client` の機能も同じであることに注意してください。これらのオプションは、ルールに文脈と読みやすさを加味するために提供されています。たとえば、サーバからクライアントへの攻撃を検出するよう設計されたルールを作成する場合は、`From Server` を使用します。一方、クライアントからサーバへの攻撃を検出するように設計されたルールを作成する場合は、`From Client` を使用します。

次の表に、`flow` キーワードで指定できるストリーム関連引数の説明を示します。

表 *134* : *flow* のストリーム関連引数

引数	説明
Ignore Stream Traffic	再構築されたストリーム パケットでトリガーとして使用されません。
Only Stream Traffic	再構築されたストリーム パケットでのみトリガーとして使用されます。

たとえば、`flow` キーワードの値として `To Server, Established, Only Stream Traffic` を使用すると、ストリーム プリプロセッサで再構築された、確立済みセッションでクライアントからサーバに移動するトラフィックを検出できます。

seq

seqキーワードを使用すると、静的なシーケンス番号値を指定できます。パケットのシーケンス番号が、指定された引数と一致する場合、そのキーワードを含むルールがトリガーとして使用されます。このキーワードはあまり使用されませんが、静的シーケンス番号付きの生成済みパケットを使用する攻撃やネットワーク スキャンを識別するうえでこれが役立ちます。

window

window キーワードを使用すると、特定の TCP ウィンドウ サイズを指定できます。このキーワードを含むルールは、指定されたTCPウィンドウサイズのパケットが検出されるたびにトリガーされます。このキーワードはあまり使用されませんが、静的TCPウィンドウサイズ付きの生成済みパケットを使用する攻撃やネットワーク スキャンを識別するうえでこれが役立ちます。

stream_size

次に示す形式で、stream_size キーワードとストリーム プリプロセッサを組み合わせて使用すると、TCP ストリームのサイズをバイト単位で特定できます。

```
direction,operator,bytes
```

ここで、bytes はバイト数です。引数内の各オプションをカンマ（,）で区切る必要があります。

次の表は、stream_size キーワードで指定できる大文字/小文字を区別しない方向オプションを示しています。

表 *135*：*stream_size* キーワードの方向引数

引数	説明
client	指定されたストリームサイズに一致するクライアントからのストリームでトリガーとして使用されます。
server	指定されたストリームサイズに一致するサーバからのストリームでトリガーとして使用されます。
both	指定されたストリームサイズに一致するクライアントからのトラフィックとサーバからのトラフィックの両方によってトリガーとして使用されます。 たとえば both, >, 200 という引数は、クライアントからのトラフィックが 200 バイトを超え、しかもサーバからのトラフィックが 200 バイトを超えている場合にトリガーとして使用されます。
either	指定されたストリームサイズに一致するクライアントまたはサーバからのトラフィック（どちらか先に出現した方）によってトリガーとして使用されます。 たとえば both, >, 200 という引数は、クライアントからのトラフィックが 200 バイトを超え、しかもサーバからのトラフィックが 200 バイトを超えている場合にトリガーとして使用されます。

次の表に、stream_size キーワードで使用できる演算子の説明を示します。

表 *136*：*stream_size* キーワードの引数演算子

演算子	説明
=	次の値と等しい
!=	等しくない
>	より大きい
<	より少ない
>=	右辺と比較して大きいか等しい
<=	右辺と比較して小さいか等しい

たとえば、クライアントからサーバに移動する 5001216 バイト以上の TCP ストリームを検出するには、stream_size キーワードの引数として client, >=, 5001216 を使用できます。

stream_reassembly キーワード

stream_reassemble キーワードを使用すると、接続での検査対象トラフィックがルールの条件と一致した場合に、1 つの接続の TCP ストリーム再構築を有効/無効にすることができます。オプションで、このキーワードを 1 つのルール内で複数回使用することができます。

ストリーム再構築を有効または無効にするには、次の構文を使用します。

```
enable|disable, server|client|both, option, option
```

次の表に、stream_reassemble キーワードで使用できるオプション引数の説明を示します。

表 *137*：*stream_reassemble* のオプション引数

引数	説明
noalert	ルールで他にどの検出オプションが指定されているかに関係なく、イベントを生成しません。
fastpath	一致の検出時に残りの接続トラフィックを無視します。

たとえば、次のルールは、HTTP 応答で 200 OK ステータス コードが検出される接続に対してイベントを生成せずに、TCP クライアント側ストリーム再構築を無効にします。

```
alert tcp any 80 -> any any (flow:to_client, established; content: "200 OK";
stream_reassemble:disable, client, noalert
```

SSL キーワード

SSL ルール キーワードを使用すると、Secure Sockets Layer（SSL）プリプロセッサを呼び出し、暗号化セッションのパケットから SSL のバージョンとセッション状態に関する情報を抽出できます。

SSL または Transport Layer Security（TLS）を使用する暗号化セッションを確立するためにクライアントとサーバが通信するとき、ハンドシェイク メッセージが交換されます。セッション中に伝送されるデータは暗号化されますが、ハンドシェイク メッセージは暗号化されません。

SSL プリプロセッサは、特定のハンドシェイク フィールドから状態とバージョンの情報を抽出します。ハンドシェイク内の 2 つのフィールドは、セッション暗号化に使われる SSL または TLS のバージョンとハンドシェイクのステージを示します。

ssl_state

`ssl_state` キーワードを使用すると、暗号化されたセッションの状態情報と照合することができます。同時に使用される複数の SSL バージョンを検査するには、1 つのルール内で複数の `ssl_version` キーワードを使用します。

ルールで `ssl_state` キーワードが使用されている場合、ルール エンジンは SSL プリプロセッサを呼び出して、トラフィック内の SSL 状態情報を検査します。

たとえば、チャレンジ長が非常に長く、データが多すぎる `ClientHello` メッセージを送信することによってサーバ上のバッファ オーバーフローを引き起そうとする攻撃者の試みを検出するには、`ssl_state` キーワードと引数 `client_hello` を使用し、異常に大きなパケットを検査することができます。

SSL 状態に関する複数の引数を指定するには、カンマ区切りのリストを使用します。複数の引数を列挙した場合、システムは OR 演算子を使ってそれらを評価します。たとえば、引数として `client_hello` および `server_hello` を指定すると、システムは `client_hello` または `server_hello` のどちらかを含むトラフィックに照らしてルールを評価します。

次のように、引数を除外することもできます。

```
!client_hello, !unknown
```

接続が一連の状態のそれぞれに到達したことを確認するには、ssl_state ルール オプションを使用する複数のルールを使う必要があります。`ssl_state` キーワードは、次の識別子を引数として受け入れます。

表 *138*：*`ssl_state`* の引数

引数	目的
`client_hello`	クライアントが暗号化セッションを要求する、メッセージ タイプ `ClientHello` のハンドシェイク メッセージを照合します。
`server_hello`	クライアントからの暗号化セッション要求に対してサーバが応答する、メッセージ タイプ `ServerHello` のハンドシェイク メッセージを照合します。

引数	目的
client_keyx	サーバからのキーの受信を確認するためにクライアントがサーバにキーを伝送する、メッセージタイプ ClientKeyExchange のハンドシェイク メッセージを照合します。
server_keyx	サーバからのキーの受信を確認するためにクライアントがサーバにキーを伝送する、メッセージタイプ ServerKeyExchange のハンドシェイク メッセージを照合します。
unknown	任意のハンドシェイク メッセージ タイプを照合します。

ssl_version

ssl_version キーワードを使用すると、暗号化されたセッションのバージョン情報と照合することができます。ルールで ssl_version キーワードが使用されている場合、ルール エンジンは SSL プリプロセッサを呼び出して、トラフィック内の SSL バージョン情報を検査します。

たとえば、SSL バージョン 2 にバッファ オーバーフロー脆弱性があることがわかっている場合、ssl_version キーワードで sslv2 引数を使用して、その SSL バージョンを使用するトラフィックを識別できます。

SSL バージョンに関する複数の引数を指定するには、カンマ区切りのリストを使用します。複数の引数を列挙した場合、システムは OR 演算子を使ってそれらを評価します。たとえば、SSLv2 を使用していない暗号化トラフィックを識別するには、ssl_version:ssl_v3,tls1.0,tls1.1,tls1.2 をルールに追加できます。このルールは、SSL バージョン 3、TLS バージョン 1.0、TLS バージョン 1.1、または TLS バージョン 1.2 を使用するトラフィックを評価します。

ssl_version キーワードは、次の SSL/TLS バージョン識別子を引数として受け入れます。

表 *139*：*ssl_version* の引数

引数	目的
sslv2	Secure Sockets Layer（SSL）バージョン 2 を使用してエンコードされたトラフィックを照合します。
sslv3	Secure Sockets Layer（SSL）バージョン 3 を使用してエンコードされたトラフィックを照合します。
tls1.0	Transport Layer Security（TLS）バージョン 1.0 を使用してエンコードされたトラフィックを照合します。
tls1.1	Transport Layer Security（TLS）バージョン 1.1 を使用してエンコードされたトラフィックを照合します。

引数	目的
`tls1.2`	Transport Layer Security（TLS）バージョン 1.2 を使用してエンコードされたトラフィックを照合します。

appid キーワード

パケットからアプリケーションプロトコル、クライアントアプリケーション、Webアプリケーションを特定するために `appid` キーワードを使用できます。たとえば、ある脆弱性をもつことが知られている特定のアプリケーションを検出することを考えます。

侵入ルールの `appid` キーワードの中で、[AppID の設定（Configure AppID）] をクリックし、検出するアプリケーションを 1 つまたは複数選択します。

使用可能なアプリケーションの参照

条件の作成を初めて開始するときは、[使用可能なアプリケーション（Available Applications）] リストは制約されておらず、システムが検出するすべてのアプリケーションをページごとに 100 個ずつ表示します。

- アプリケーションを確認していくには、リストの下にある矢印をクリックします。
- アプリケーションの特性に関するサマリー情報と参照できるインターネットの検索リンクが示されているポップアップ ウィンドウを表示するには、アプリケーションの横にある情報アイコン（  ）をクリックします。

アプリケーション フィルタの使用

照合するアプリケーションを見つけやすくするために、[使用可能なアプリケーション（Available Applications）] リストを次のように制約できます。

- アプリケーションを検索するには、リスト上部にある [名前で検索（Search by name）] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するアプリケーションが表示されます。
- フィルタを適用してアプリケーションを制約するには、[アプリケーション フィルタ（Application Filters）] リストを使用します。フィルタを適用すると、[使用可能なアプリケーション（Available Applications）] リストが更新されます。便宜上、システムはロック解除アイコン（  ）を使用して、復号化されたトラフィック（暗号化されているトラフィックまたは暗号化されていないトラフィックではなく）でのみ識別できるアプリケーションをマークします。

（注） [アプリケーション フィルタ（Application Filters）] リストで 1 つ以上のフィルタを選択し、しかも [使用可能なアプリケーション（Available Applications）] リストを検索した場合、選択内容と検索フィルタ適用後の [使用可能なアプリケーション（Available Applications）] リストが AND 演算を使って結合されます。

アプリケーションの選択

アプリケーションを 1 つだけ選択するには、そのアプリケーションを選択し、[ルールへの追加（Add to Rule）] をクリックします。フィルタで限定されている現在の表示のすべてのアプリケーションを選択するには、右クリックして [すべて選択（Select All）] を選択します。

アプリケーション層プロトコル値

アプリケーション層プロトコル値の正規化と検査はほとんどがプリプロセッサによって実行されますが、種々のプリプロセッサ オプションを使用して、アプリケーション層値をさらに検査できます。

RPC キーワード

`rpc` キーワードは、TCP または UDP パケットでオープン ネットワーク コンピューティング リモート プロシージャ コール（ONC RPC）サービスを識別します。これにより、ホスト上の RPC プログラムの識別試行を検出することができます。ネットワークで実行中のいずれかの RPC サービスを悪用できるかどうか判断するために、侵入者は RPC ポートマッパーを使用できます。また、ポートマッパーを使用せずに RPC を実行中の他のポートへのアクセスを試みることもできます。次の表に、`rpc` キーワードで使用できる引数を列挙します。

表 *140*：*rpc* キーワードの引数

引数	説明
アプリケーション	RPC アプリケーション番号
手順	呼び出される RPC プロシージャ
version	RPC バージョン

`rpc` キーワードの引数を指定するには、次の構文を使用します。

```
application,procedure,version
```

ここで、application は RPC アプリケーション番号、procedure は RPC プロシージャ番号、version は RPC バージョン番号です。`rpc` キーワードのすべての引数を指定する必要があります。引数のいずれかを指定できない場合は、アスタリスク（`*`）で置き換えてください。

たとえば、任意のプロシージャまたはバージョンのRPCポートマッパー（100000という番号で示されるRPCアプリケーション）を検索するには、引数として`100000,*,*`を使用します。

ASN.1 キーワード

`asn1`キーワードを使用すると、さまざまな有害エンコードを検索しながら、パケットまたはパケットの一部分をデコードできます。

次の表に、`asn1`キーワードの引数について説明します。

表 *141*：*asn.1* キーワードの引数

引数	説明
Bitstring Overflow	無効な、リモートで悪用可能なビットストリング エンコードを検出します。
Double Overflow	標準バッファより大きい二重ASCIIエンコードを検出します。これはMicrosoft Windowsの悪用可能な機能であることが知られていますが、現時点でどのサービスが悪用可能であるかは不明です。
Oversize Length	指定された引数より大きいASN.1タイプ長を検出します。たとえばOversize Lengthを500に設定した場合、500を上回るASN.1タイプによってルールがトリガーとして使用されます。
Absolute Offset	パケットペイロードの先頭からの絶対オフセットを設定します（offsetカウンタがバイト0から始まることに注意してください）。たとえばSNMPパケットをデコードするには、Absolute Offsetを0に設定し、Relative Offsetを設定しません。Absolute Offsetとして正または負の値が可能です。
Relative Offset	これは、最後に見つかったコンテンツ一致、`pcre`、または`byte_jump`からの相対オフセットです。コンテンツ "foo" の直後のASN.1シーケンスをデコードするには、Relative Offsetを0に設定し、Absolute Offsetを設定しません。Relative Offsetとして正または負の値が可能です。（オフセット カウンタが0から始まることに注意してください。）

たとえば、Microsoft ASN.1ライブラリにおける既知の脆弱性ではバッファ オーバーフローが発生し、攻撃者は特別に細工した認証パケットを使ってその状態を悪用できます。システムがasn.1データをデコードするとき、パケット内のexploitコードは、システム レベル特権付きでホスト上で動作したり、DoS状態を引き起こしたりすることができます。次のルールは、`asn1`キーワードを使用して、この脆弱性を悪用する試みを検出します。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445
(flow:to_server, established; content:"|FF|SMB|73|";
nocase; offset:4; depth:5;
asn1:bitstring_overflow,double_overflow,oversize_length 100,
relative_offset 54;)
```

上記のルールの場合、任意のポートおよび$EXTERNAL_NET変数で定義された任意のIPアドレスから発信され、ポート445を使用する$HOME_NET変数で定義された任意のIPアドレスに向かうTCPトラフィックに対して、イベントが生成されます。加えて、サーバへのTCP接続が確立された時点でのみルールを実行します。その後、ルールは特定の位置にある特定のコンテンツを

検査します。最後に、ルールは asn1 キーワードを使用して、ビットストリングエンコードと二重 ASCII エンコードを検出し、最後に見つかったコンテンツ一致の末尾から 55 バイト目以降、長さ 100 バイトを超える asn.1 タイプ長を識別します。（offset カウンタがバイト 0 から始まることに注意してください。）

urilen キーワード

urilen キーワードと HTTP Inspect プリプロセッサを組み合わせて使用すると、特定の長さ、最大長を下回る、最小長を上回る、または指定された範囲内の URI を HTTP トラフィック内で検査できます。

HTTP Inspect プリプロセッサがパケットを正規化して検査した後、ルール エンジンはルールに照らしてそのパケットを評価し、urilen キーワードで指定された長さ条件に URI が一致するかどうか判断します。このキーワードを使用すると、URI 長の脆弱性をエクスプロイトしようとする試みを検出できます。たとえばバッファ オーバーフローを発生させて、攻撃者が DoS 状態を引き起こしたり、システム レベル特権付きでホスト上でコードを実行したりしようと試みる可能性があります。

ルール内で urilen キーワードを使用するときには、次の点に注意してください。

- 必ず flow:established キーワードおよび他の 1 つ以上のキーワードを組み合わせて、urilen キーワードを使用してください。
- ルール プロトコルは常に TCP です。
- ターゲット ポートは常に HTTP ポートです。

URI 長を指定するときには、10 進のバイト数、「小なり」（<）、および「大なり」（>）を使用します。

次に例を示します。

- 5 バイト長の URI を検出するには、5 を指定します。
- 5 バイト長を下回る URI を検出するには、< 5 （1 つの空白文字で区切る）を指定します。
- 5 バイト長を上回る URI を検出するには、> 5（1 つの空白文字で区切る）を指定します。
- 3 ～ 5 バイト長の URI を検出するには、3 <> 5（<> の前後に空白文字を 1 つずつ含む）を指定します。

たとえば、Novell の eDirectory バージョン 8.8 に付属のサーバ モニタリングおよび診断ユーティリティ iMonitor バージョン 2.4 には、脆弱性があることが知られています。長すぎる URI を含むパケットはバッファ オーバーフローを発生させるため、攻撃者はシステム レベル特権付きでホスト上で動作したり、DoS 状態を引き起こしたりできる特別に細工したパケットを使ってその状態をエクスプロイトできます。次のルールは、urilen キーワードを使用して、この脆弱性を悪用する試みを検出します。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"EXPLOIT eDirectory 8.8 Long URI iMonitor buffer
overflow attempt"; flow:to_server,established;
urilen:> 8192; uricontent:"/nds/"; nocase;
classtype:attempted-admin; sid:x; rev:1;)
```

上記のルールの場合、任意のポートおよび $EXTERNAL_NET 変数で定義された任意の IP アドレスから発信され、$HTTP_PORTS 変数で定義されたポートを使用して、$HOME_NET 変数で定義された任意の IP アドレスに向かう TCP トラフィックに対して、イベントが生成されます。加えて、サーバへの TCP 接続が確立された時点でのみ、パケットがルールに照らして評価されます。ルールは、`urilen` キーワードを使用して、長さ 8192 バイトを超える URI を検出します。最後に、ルールは URI を検索して、大文字/小文字を区別しない特定のコンテンツ `/nds/` を探します。

関連トピック

侵入ルール ヘッダー プロトコル, （1109 ページ）
侵入ルール ヘッダーの送信元および宛先ポート, （1114 ページ）
定義済みデフォルト変数, （400 ページ）

DCE/RPC キーワード

次の表で説明する 3 つの DCE/RPC キーワードを使用して、DCE/RPC セッション トラフィックのエクスプロイトをモニタできます。これらのキーワードを含むルールを処理するとき、システムは DCE/RPC プリプロセッサを呼び出します。

表 *142* : *DCE/RPC* キーワード

使用するフィルタ	使用方法	検出対象
`dce_iface`	単独	特定の DCE/RPC サービスを特定するパケット
`dce_opnum`	`dce_iface` の後ろ	特定の DCE/RPC サービス オペレーションを特定するパケット
`dce_stub_data`	`dce_iface` + `dce_opnum` の後ろ	特定の処理要求または応答を定義するスタブ データ

表に示されているように、`dce_opnum` の前に必ず `dce_iface` を配置し、`dce_stub_data` の前に必ず `dce_iface` + `dce_opnum` を配置する必要があることに注意してください。

また、これらの DCE/RPC キーワードを他のルール キーワードと組み合わせて使用することもできます。DCE/RPC ルールでは、DCE/RPC の引数が選択された状態で `byte_jump`、`byte_test`、`byte_extract` の各キーワードを使用することに注意してください。

シスコでは、DCE/RPC キーワードを含むルールに 1 つ以上の `content` キーワードを含めることを推奨しています。こうすると、ルールエンジンが常に高速パターンマッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルールに 1 つ以上の `content` キーワードが含まれている場合は、`content` キーワードの [高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] 引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。

次のケースでは、DCE/RPC バージョンおよび隣接ヘッダー情報を一致コンテンツとして使用できます。

- ルールに他の content キーワードが含まれていない
- ルールにもう 1 つ content キーワードが含まれているが、DCE/RPC バージョンおよび隣接情報が、他方の content よりも特有のパターンを表している

  たとえば、DCE/RPC バージョンおよび隣接情報は通常、1 バイトのコンテンツよりも特有です。

次に示すバージョンおよび隣接情報コンテンツ一致のいずれか 1 つを使用して、ルール限定を終了する必要があります。

- コネクション型 DCE/RPC ルールでは、コンテンツ |05 00 00|（メジャー バージョン 05、マイナー バージョン 00、および要求 PDU（プロトコル データ ユニット）タイプ 00）を使用します。
- コネクションレス型 DCE/RPC ルールでは、コンテンツ |04 00|（バージョン 04、要求 PDU タイプ 00）を使用します。

いずれの場合も、DCE/RPC プリプロセッサで完了済みの処理を繰り返すことなく高速パターンマッチ機能を呼び出すために、ルール内の最後のキーワードとしてバージョンおよび隣接情報の content キーワードを配置してください。ルールの末尾に配置される content キーワードは、高速パターンマッチ機能を呼び出す手段として使われるバージョン コンテンツに当てはまりますが、ルール内の他のコンテンツ一致には必ずしも当てはまらないことに注意してください。

関連トピック

DCE/RPC プリプロセッサ, （1278 ページ）
content キーワードと protected_content キーワード, （1135 ページ）
content キーワードの高速パターン マッチ機能の引数, （1146 ページ）
概要：byte_jump および byte_test キーワード
byte_extract キーワード, （1155 ページ）

dce_iface

dce_iface キーワードを使用すると、特定の DCE/RPC サービスを識別できます。

オプションで、dce_iface キーワードを dce_opnum キーワードおよび dce_stub_data キーワードと組み合わせて使用すると、検査する DCE/RPC トラフィックをさらに限定することができます。

固定型 16 バイト Universally Unique Identifier（UUID）は、それぞれの DCE/RPC サービスに割り当てられるアプリケーション インターフェイスを識別します。たとえば、UUID 4b324fc8-670-01d3-1278-5a47bf6ee188 は、srvsvc サービスとしても知られる DCE/RPC lanmanserver サービスを識別します。このサービスは、ピアツーピア プリンタ、ファイル、および SMB 名前付きパイプを共有するためのさまざまな管理機能を提供します。DCE/RPC プリプロセッサは UUID および関連するヘッダー値を使用して DCE/RPC セッションを追跡します。

インターフェイス UUID は、次のように、ハイフンで区切られた 5 つの 16 進文字列で構成されます。

```
<4hexbytes>-<2hexbytes>-<2hexbytes>-<2hexbytes>-<6hexbytes>
```

次に示す netlogon インターフェイスの UUID のように、ハイフンを含む UUID 全体を入力することで、インターフェイスを指定します。

```
12345678-1234-abcd-ef00-01234567cffb
```

UUID 内の最初の 3 つの文字列はビッグ エンディアン バイト順で指定される必要があることに注意してください。通常、公開されたインターフェイス リストやプロトコル アナライザには UUID が正しいバイト順で表示されますが、それを入力する前に UUID バイト順を変更しなければならない場合もあります。次に示すメッセンジャー サービス UUID の場合、リトル エンディアン バイト順の最初の 3 つの文字列を含む未加工 ASCII テキストで表示されることがあります。

```
f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc
```

この同じ UUID を `dce_iface` キーワードに指定するには、次のようにハイフンを挿入し、最初の 3 つの文字列をビッグ エンディアン バイト順で配置できます。

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

1 つの DCE/RPC セッションに複数のインターフェイスへの要求を含めることができますが、1 つのルールには 1 つの `dce_iface` キーワードだけを含めてください。追加のインターフェイスを検出するには、追加のルールを作成します。

DCE/RPC アプリケーション インターフェイスにはインターフェイス バージョン番号も割り当てられます。オプションで、インターフェイス バージョンを指定できます。その際、バージョンが指定値に等しい、等しくない、指定値より小さい、または大きいことを示す演算子を使用します。

TCP セグメンテーションや IP フラグメンテーションに加えて、コネクション型とコネクションレス型の両方の DCE/RPC をフラグメント化することができます。通常、先頭以外の DCE/RPC フラグメントを指定のインターフェイスに関連付けるのはあまり効率的ではありません。このようにすると、多数の誤検出が発生する可能性があります。ただし、柔軟性を維持するために、オプションで、指定されたインターフェイスに照らしてすべてのフラグメントを評価できます。

次の表に、`dce_iface` キーワードの引数を要約します。

表 *143* : *`dce_iface`* の引数

引数	説明
Interface UUID	DCE/RPC トラフィック内で検出対象となる特定のサービスのアプリケーション インターフェイスを識別する、ハイフンを含む UUID。指定されたインターフェイスに関連付けられた任意の要求がインターフェイス UUID に一致します。
Version	オプションで、アプリケーション インターフェイス バージョン番号 0 ～ 65535 と、検出対象のバージョンが指定値より大きい（>）、小さい（<）、等しい（=）、または等しくない（!）を示す演算子。

引数	説明
All Fragments	オプションで、関連するすべての DCE/RPC フラグメント内のインターフェイスの照合、およびインターフェイスバージョン（指定されている場合）での照合を有効にします。この引数はデフォルトで無効になっています。これは、最初のフラグメントまたはフラグメント化されていないパケット全体が指定のインターフェイスに関連付けられている場合にのみ、キーワードが一致することを意味します。この引数を有効にすると、誤検出が発生する可能性があることに注意してください。

dce_opnum キーワード

`dce_opnum` キーワードを DCE/RPC プリプロセッサと組み合わせて使用すると、DCE/RPC サービスが提供する 1 つ以上の特定のオペレーションを識別するパケットを検出できます。

クライアント関数呼び出しは、DCE/RPC 仕様で「オペレーション」と呼ばれる特定のサービス関数を要求します。オペレーション番号（opnum）は DCE/RPC ヘッダー内の特定のオペレーションを識別します。エクスプロイトは特定のオペレーションを標的にすることがあります。

たとえば UUID 12345678-1234-abcd-ef00-01234567cffb は、数十種類のオペレーションを提供する netlogon サービスのインターフェイスを識別します。その 1 つがオペレーション 6（NetrServerPasswordSet オペレーション）です。

オペレーション用のサービスを識別するには、`dce_opnum` キーワードの前に `dce_iface` キーワードを指定する必要があります。

特定のオペレーションを示す 1 つの 10 進数値（0 ～ 65535 の範囲）、ハイフンで区切られたオペレーション範囲、またはカンマ区切りのオペレーション/範囲リストを任意の順序で指定できます。

次の例は、すべて有効な netlogon オペレーション番号を表しています。

```
15
15-18
15, 18-20
15, 20-22, 17
15, 18-20, 22, 24-26
```

dce_stub_data キーワード

`dce_stub_data` キーワードを DCE/RPC プリプロセッサと組み合わせて使用すると、他のルール オプションとは無関係に、スタブデータの先頭からインスペクションを開始するようルールエンジンに指示できます。`dce_stub_data` キーワードの後に続くパケット ペイロード ルール オプションは、スタブ データ バッファを基準にして適用されます。

DCE/RPC スタブ データは、クライアント プロシージャ コールと DCE/RPC ランタイム システム（DCE/RPC の中核をなすルーチンとサービスを提供するメカニズム）の間のインターフェイスを提供します。DCE/RPC エクスプロイトは、DCE/RPC パケットのスタブ データ部分で識別されます。スタブ データは特定のオペレーションまたは関数呼び出しに関連付けられているため、必ず `dce_stub_data` の前に `dce_iface` と `dce_opnum` を指定して、関連するサービスとオペレーションを識別してください。

`dce_stub_data` キーワードには引数がありません。

SIP キーワード

4 つの SIP キーワードを使用すると、SIP セッション トラフィックでエクスプロイトを監視できます。

SIP プロトコルはサービス拒否（DoS）攻撃に対して脆弱であることに注意してください。このような攻撃に対処するルールでは、レート ベースの攻撃防御を活用できます。

sip_header キーワード

`sip_header` キーワードを使用すると、抽出された SIP 要求または応答ヘッダーの先頭から検査を開始し、検査対象をヘッダー フィールドに限定することができます。

`sip_header` キーワードには引数がありません。

次の例のルール フラグメントは SIP ヘッダーを指し示し、CSeq ヘッダー フィールドに一致します。

```
alert udp any any -> any 5060 ( sip_header; content:"CSeq"; )
```

関連トピック

動的侵入ルール状態, （1071 ページ）
レート ベースの攻撃防御, （1415 ページ）

sip_body キーワード

`sip_body` キーワードを使用すると、抽出された SIP 要求または応答メッセージ本文の先頭から検査を開始し、検査対象をメッセージ本文に限定することができます。

`sip_body` キーワードには引数がありません。

次の例のルール フラグメントは SIP メッセージ本文を指し示し、抽出された SDP データの c（接続情報）フィールド内の特定の IP アドレスに一致します。

```
alert udp any any -> any 5060 ( sip_body; content:"c=IN 192.168.12.14"; )
```

ルールが SDP コンテンツの検索だけに限定されないことに注意してください。 SIP プリプロセッサはメッセージ本文全体を抽出し、それをルール エンジンで使用できるようにします。

sip_method キーワード

各 SIP 要求内の *method* フィールドは要求の目的を識別します。`sip_method` キーワードを使用すると、SIP 要求の中で特定のメソッドを検査することができます。複数のメソッドはカンマで区切ります。

次に示す現在定義されている SIP メソッドを指定できます。

```
ack, benotify, bye, cancel, do, info, invite, join, message, notify, options, prack,
publish, quath, refer, register, service, sprack, subscribe, unsubscribe, update
```

メソッドでは大文字と小文字が区別されません。複数のメソッドをカンマで区切ることができます。

今後、新しい SIP メソッドが定義される可能性があるため、カスタム メソッド、つまり現在定義されている SIP メソッド以外のメソッドを指定することもできます。可能なフィールド値は RFC 2616 で定義されています。=、(、) などの制御文字と区切り文字を除いて、すべての文字を使用できます。除外されている区切り文字の完全なリストについては、RFC 2616 を参照してください。指定されたカスタムメソッドがトラフィックで検出されると、システムはパケットヘッダーを検査しますが、メッセージは検査されません。

システムでは最大 32 個のメソッド（現在定義されている 21 個のメソッドと追加の 11 個のメソッド）がサポートされます。システムは、設定される未定義のメソッドをすべて無視します。合計 32 個のメソッドには、SIP プリプロセッサのオプション [検査するメソッド（Methods to Check）] を使って指定されるメソッドが含まれることに注意してください。

否定を使用する場合は、1 つのメソッドだけを指定できます。次に例を示します。

```
!invite
```

ただし、1 つのルール内の複数の `sip_method` キーワードが AND 演算で結合されることに注意してください。たとえば、`invite` と `cancel` を除くすべての抽出されたメソッドを検査するには、次のような 2 つの否定付き `sip_method` キーワードを使用します。

```
sip_method: !invite
sip_method: !cancel
```

Cisco では、`sip_method` キーワードを含むルールに 1 つ以上の `content` キーワードを含めることを推奨しています。こうすると、ルールエンジンが常に高速パターンマッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルールに 1 つ以上の `content` キーワードが含まれている場合は、`content` キーワードの [高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] 引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。

関連トピック

SIP プリプロセッサのオプション, （1326 ページ）
content キーワードと protected_content キーワード, （1135 ページ）
content キーワードの高速パターン マッチ機能の引数, （1146 ページ）

sip_stat_code キーワード

各 SIP 応答内の 3 桁のステータス コードは、要求されたアクションの結果を示します。`sip_stat_code` キーワードを使用すると、SIP 応答の中で特定のステータス コードを検査することができます。

1 桁の応答タイプ番号 1 ～ 9、特定の 3 桁の番号 100 ～ 999、またはこれらを任意に組み合わせたカンマ区切りリストを指定できます。リスト内のいずれか 1 つの番号が SIP 応答内のコードに一致する場合、そのリストが一致します。

次の表に、指定可能な SIP ステータス コード値の説明を示します。

表 *144* : *sip_stat_code* の値

検出対象	指定する内容	例	検出結果
1 つの特定のステータス コード	3 桁のステータス コード	189	189
指定された 1 桁で始まる 3 桁のコード	1 桁	1	1xx、つまり 100、101、102 など
値のリスト	特定のコードおよび 1 桁を任意に組み合わせてカンマで区切る	222, 3	222 および 300、301、302 など

また、ルールに content キーワードが含まれているかどうかに関係なく、sip_stat_code キーワードを使って指定された値を検索するためにルールエンジンが高速パターンマッチ機能を使用しないことにも注意してください。

GTP キーワード

3 つの GSRP トンネリング プロトコル（GTP）キーワードを使用すると、GTP バージョン、メッセージ タイプ、および情報要素をコマンド チャネル内で検査できます。content や byte_jump などの他の侵入ルール キーワードと組み合わせて GTP キーワードを使用することはできません。gtp_info または gtp_type キーワードを使用するそれぞれのルールで、gtp_version キーワードを使用する**必要があります**。

gtp_version キーワード

gtp_version キーワードを使用すると、GTP 制御メッセージの中で GTP バージョン 0、1、または 2 を検査することができます。

定義されているメッセージ タイプと情報要素は GTP バージョンによって異なるため、gtp_type または gtp_info キーワードを使用するときには、gtp_version を使用する必要があります。値として 0、1、または 2 を指定できます。

gtp_type キーワード

それぞれの GTP メッセージは、数値と文字列で構成されるメッセージタイプによって識別されます。gtp_type キーワードを使用すると、特定の GTP メッセージ タイプのトラフィックを検査できます。定義されているメッセージ タイプと情報要素は GTP バージョンによって異なるため、gtp_type または gtp_info キーワードを使用するときには、gtp_version も使用する必要があります。

次の例に示すように、メッセージ タイプとして定義済みの 10 進数値、定義済み文字列、あるいはどちらか（または両方）を任意に組み合わたカンマ区切りリストを指定できます。

```
10, 11, echo_request
```

リスト内のそれぞれの値または文字列を照合するとき、システムは OR 演算を使用します。値と文字列を列挙する順序は重要ではありません。 リスト内のいずれか 1 つの値または文字列の一致により、キーワードが一致します。認識されない文字列または範囲外の値を含むルールを保存しようとすると、エラーが発生します。

表に示されているように、GTP バージョンに応じて、同じメッセージ タイプの値が異なる場合があることに注意してください。たとえば `sgsn_context_request` メッセージ タイプの値は GTPv0 と GTPv1 では 50 ですが、GTPv2 では 130 です。

パケット内のバージョン番号に応じて、`gtp_type` キーワードは異なる値と一致します。上記の例の場合、GTPv0 または GTPv1 パケットではキーワードがメッセージ タイプ値 50 と一致しますが、GTPv2 パケットでは値 130 と一致します。パケット内のメッセージ タイプ値が、パケットで指定されたバージョンの既知の値でない場合は、キーワードがパケットと一致しません。

メッセージ タイプに整数を指定した場合、パケット内で指定されたバージョンとは無関係に、キーワード内のメッセージタイプが GTP パケット内の値と一致すればキーワードが一致します。

次の表に、GTP メッセージ タイプごとにシステムで認識される定義済みの値と文字列を示します。

表 *145*：*GTP* メッセージ タイプ

値	Version 0	Version 1	Version 2
1	echo_request	echo_request	echo_request
2	echo_response	echo_response	echo_response
3	version_not_supported	version_not_supported	version_not_supported
4	node_alive_request	node_alive_request	該当なし
5	node_alive_response	node_alive_response	該当なし
[6]	redirection_request	redirection_request	該当なし
7	redirection_response	redirection_response	該当なし
16	create_pdp_context_request	create_pdp_context_request	該当なし
17	create_pdp_context_response	create_pdp_context_response	該当なし
18	update_pdp_context_request	update_pdp_context_request	該当なし
19	update_pdp_context_response	update_pdp_context_response	該当なし
20	delete_pdp_context_request	delete_pdp_context_request	該当なし
21	delete_pdp_context_response	delete_pdp_context_response	該当なし

値	Version 0	Version 1	Version 2
22	create_aa_pdp_context_request	init_pdp_context_activation_request	該当なし
23	create_aa_pdp_context_response	init_pdp_context_activation_response	該当なし
24	delete_aa_pdp_context_request	該当なし	該当なし
25	delete_aa_pdp_context_response	該当なし	該当なし
26	error_indication	error_indication	該当なし
27	pdu_notification_request	pdu_notification_request	該当なし
36	pdu_notification_response	pdu_notification_response	該当なし
29	pdu_notification_reject_request	pdu_notification_reject_request	該当なし
30	pdu_notification_reject_response	pdu_notification_reject_response	該当なし
31	該当なし	supported_ext_header_notification	該当なし
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response
36	note_ms_present_request	note_ms_present_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	該当なし	該当なし	change_notification_request
39	該当なし	該当なし	change_notification_response
48	identification_request	identification_request	該当なし
49	identification_response	identification_response	該当なし
50	sgsn_context_request	sgsn_context_request	該当なし
51	sgsn_context_response	sgsn_context_response	該当なし
52	sgsn_context_ack	sgsn_context_ack	該当なし

値	Version 0	Version 1	Version 2
53	該当なし	forward_relocation_request	該当なし
54	該当なし	forward_relocation_response	該当なし
55	該当なし	forward_relocation_complete	該当なし
72	該当なし	relocation_cancel_request	該当なし
57	該当なし	relocation_cancel_response	該当なし
58	該当なし	forward_srns_contex	該当なし
59	該当なし	forward_relocation_complete_ack	該当なし
60	該当なし	forward_srns_contex_ack	該当なし
64	該当なし	該当なし	modify_bearer_command
65	該当なし	該当なし	modify_bearer_failure_indication
66	該当なし	該当なし	delete_bearer_command
67	該当なし	該当なし	delete_bearer_failure_indication
68	該当なし	該当なし	bearer_resource_command
69	該当なし	該当なし	bearer_resource_failure_indication
70	該当なし	ran_info_relay	downlink_failure_indication
71	該当なし	該当なし	trace_session_activation
72	該当なし	該当なし	trace_session_deactivation
73	該当なし	該当なし	stop_paging_indication
95	該当なし	該当なし	create_bearer_request
96	該当なし	mbms_notification_request	create_bearer_response
97	該当なし	mbms_notification_response	update_bearer_request
98	該当なし	mbms_notification_reject_request	update_bearer_response
99	該当なし	mbms_notification_reject_response	delete_bearer_request

値	Version 0	Version 1	Version 2
100	該当なし	create_mbms_context_request	delete_bearer_response
101	該当なし	create_mbms_context_response	delete_pdn_request
102	該当なし	update_mbms_context_request	delete_pdn_response
103	該当なし	update_mbms_context_response	該当なし
104	該当なし	delete_mbms_context_request	該当なし
105	該当なし	delete_mbms_context_response	該当なし
112	該当なし	mbms_register_request	該当なし
113	該当なし	mbms_register_response	該当なし
114	該当なし	mbms_deregister_request	該当なし
115	該当なし	mbms_deregister_response	該当なし
116	該当なし	mbms_session_start_request	該当なし
117	該当なし	mbms_session_start_response	該当なし
118	該当なし	mbms_session_stop_request	該当なし
119	該当なし	mbms_session_stop_response	該当なし
120	該当なし	mbms_session_update_request	該当なし
121	該当なし	mbms_session_update_response	該当なし
128	該当なし	ms_info_change_request	identification_request
129	該当なし	ms_info_change_response	identification_response
130	該当なし	該当なし	sgsn_context_request
131	該当なし	該当なし	sgsn_context_response
132	該当なし	該当なし	sgsn_context_ack
133	該当なし	該当なし	forward_relocation_request
134	該当なし	該当なし	forward_relocation_response

値	Version 0	Version 1	Version 2
135	該当なし	該当なし	forward_relocation_complete
136	該当なし	該当なし	forward_relocation_complete_ack
137	該当なし	該当なし	forward_access
138	該当なし	該当なし	forward_access_ack
139	該当なし	該当なし	relocation_cancel_request
140	該当なし	該当なし	relocation_cancel_response
141	該当なし	該当なし	configuration_transfer_tunnel
149	該当なし	該当なし	detach
150	該当なし	該当なし	detach_ack
151	該当なし	該当なし	cs_paging
152	該当なし	該当なし	ran_info_relay
153	該当なし	該当なし	alert_mme
154	該当なし	該当なし	alert_mme_ack
155	該当なし	該当なし	ue_activity
156	該当なし	該当なし	ue_activity_ack
160	該当なし	該当なし	create_forward_tunnel_request
161	該当なし	該当なし	create_forward_tunnel_response
162	該当なし	該当なし	suspend
163	該当なし	該当なし	suspend_ack
164	該当なし	該当なし	復帰
165	該当なし	該当なし	resume_ack
166	該当なし	該当なし	create_indirect_forward_tunnel_request
167	該当なし	該当なし	create_indirect_forward_tunnel_response

値	Version 0	Version 1	Version 2
168	該当なし	該当なし	delete_indirect_forward_tunnel_request
169	該当なし	該当なし	delete_indirect_forward_tunnel_response
170	該当なし	該当なし	release_access_bearer_request
171	該当なし	該当なし	release_access_bearer_response
176	該当なし	該当なし	downlink_data
177	該当なし	該当なし	downlink_data_ack
179	該当なし	該当なし	pgw_restart
180	該当なし	該当なし	pgw_restart_ack
200	該当なし	該当なし	update_pdn_request
201	該当なし	該当なし	update_pdn_response
211	該当なし	該当なし	modify_access_bearer_request
212	該当なし	該当なし	modify_access_bearer_response
231	該当なし	該当なし	mbms_session_start_request
232	該当なし	該当なし	mbms_session_start_response
233	該当なし	該当なし	mbms_session_update_request
234	該当なし	該当なし	mbms_session_update_response
235	該当なし	該当なし	mbms_session_stop_request
236	該当なし	該当なし	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	該当なし
241	data_record_transfer_response	data_record_transfer_response	該当なし
254	該当なし	end_marker	該当なし
255	pdu	pdu	該当なし

gtp_info キーワード

1 つの GTP メッセージには多数の情報要素が含まれることがあり、それぞれの要素は定義済み数値および定義済み文字列によって識別されます。`gtp_info` キーワードを使用すると、指定された情報要素の先頭から検査を開始し、検査対象を指定の情報要素に限定することができます。定義されているメッセージタイプと情報要素はGTPバージョンによって異なるため、このキーワードを使用するときには、`gtp_version` も使用する必要があります。

情報要素に対して定義された10進数値と定義された文字列のどちらでも指定できます。単一の値または文字列を指定することも、1 つのルール内で複数の `gtp_info` キーワードを使って複数の情報要素を検査することもできます。

1 つのメッセージに同じタイプの複数の情報要素が含まれている場合は、すべてが照合対象として検査されます。情報要素が無効な順序で出現する場合は、最後のインスタンスだけが検査されます。

GTP バージョンに応じて、同じ情報要素の値が異なる場合があることに注意してください。たとえば `cause` 情報要素の値は GTPv0 と GTPv1 では 1 ですが、GTPv2 では 2 です。

パケット内のバージョン番号に応じて、`gtp_info` キーワードは異なる値と一致します。上記の例の場合、GTPv0 またはGTPv1 パケットではキーワードが情報要素値 1 と一致しますが、GTPv2 パケットでは値 2 と一致します。パケット内の情報要素値が、パケットで指定されたバージョンの既知の値でない場合は、キーワードがパケットと一致しません。

情報要素に整数を指定した場合、パケット内で指定されたバージョンとは無関係に、キーワード内のメッセージ タイプが GTP パケット内の値と一致すればキーワードが一致します。

次の表に、GTP 情報要素ごとにシステムで認識される値と文字列を示します。

表 *146*：*GTP* 情報要素

値	Version 0	Version 1	Version 2
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	recovery
4	tlli	tlli	該当なし
5	p_tmsi	p_tmsi	該当なし
[6]	qos	該当なし	該当なし
8	recording_required	recording_required	該当なし
9	認証	認証	該当なし
11	map_cause	map_cause	該当なし

値	Version 0	Version 1	Version 2
12	p_tmsi_sig	p_tmsi_sig	該当なし
13	ms_validated	ms_validated	該当なし
18	recovery	recovery	該当なし
15	selection_mode	selection_mode	該当なし
16	flow_label_data_1	teid_1	該当なし
17	flow_label_signalling	teid_control	該当なし
18	flow_label_data_2	teid_2	該当なし
19	ms_unreachable	teardown_ind	該当なし
20	該当なし	nsapi	該当なし
21	該当なし	ranap	該当なし
22	該当なし	rab_context	該当なし
23	該当なし	radio_priority_sms	該当なし
24	該当なし	radio_priority	該当なし
25	該当なし	packet_flow_id	該当なし
26	該当なし	charging_char	該当なし
27	該当なし	trace_ref	該当なし
36	該当なし	trace_type	該当なし
29	該当なし	ms_unreachable	該当なし
71	該当なし	該当なし	apn
72	該当なし	該当なし	ambr
73	該当なし	該当なし	ebi
74	該当なし	該当なし	ip_addr
75	該当なし	該当なし	mei

値	Version 0	Version 1	Version 2
76	該当なし	該当なし	msisdn
77	該当なし	該当なし	indication
78	該当なし	該当なし	pco
79	該当なし	該当なし	paa
80	該当なし	該当なし	bearer_qos
80	該当なし	該当なし	flow_qos
82	該当なし	該当なし	rat_type
83	該当なし	該当なし	serving_network
84	該当なし	該当なし	bearer_tft
85	該当なし	該当なし	tad
86	該当なし	該当なし	uli
87	該当なし	該当なし	f_teid
88	該当なし	該当なし	tmsi
89	該当なし	該当なし	cn_id
90	該当なし	該当なし	s103pdf
91	該当なし	該当なし	s1udf
92	該当なし	該当なし	delay_value
93	該当なし	該当なし	bearer_context
94	該当なし	該当なし	charging_id
95	該当なし	該当なし	charging_char
96	該当なし	該当なし	trace_info
97	該当なし	該当なし	bearer_flag
99	該当なし	該当なし	pdn_type

値	Version 0	Version 1	Version 2
100	該当なし	該当なし	pti
101	該当なし	該当なし	drx_parameter
103	該当なし	該当なし	gsm_key_tri
104	該当なし	該当なし	umts_key_cipher_quin
105	該当なし	該当なし	gsm_key_cipher_quin
106	該当なし	該当なし	umts_key_quin
107	該当なし	該当なし	eps_quad
108	該当なし	該当なし	umts_key_quad_quin
109	該当なし	該当なし	pdn_connection
110	該当なし	該当なし	pdn_number
111	該当なし	該当なし	p_tmsi
112	該当なし	該当なし	p_tmsi_sig
113	該当なし	該当なし	hop_counter
114	該当なし	該当なし	ue_time_zone
115	該当なし	該当なし	trace_ref
116	該当なし	該当なし	complete_request_msg
117	該当なし	該当なし	guti
118	該当なし	該当なし	f_container
119	該当なし	該当なし	f_cause
120	該当なし	該当なし	plmn_id
121	該当なし	該当なし	target_id
123	該当なし	該当なし	packet_flow_id
124	該当なし	該当なし	rab_contex

値	Version 0	Version 1	Version 2
125	該当なし	該当なし	src_rnc_pdcp
126	該当なし	該当なし	udp_src_port
127	charge_id	charge_id	apn_restriction
128	end_user_address	end_user_address	selection_mode
129	mm_context	mm_context	src_id
130	pdp_context	pdp_context	該当なし
131	apn	apn	change_report_action
132	protocol_config	protocol_config	fq_csid
133	gsn	gsn	channel
134	msisdn	msisdn	emlpp_pri
135	該当なし	qos	node_type
136	該当なし	authentication_qu	fqdn
137	該当なし	tft	ti
138	該当なし	target_id	mbms_session_duration
139	該当なし	utran_trans	mbms_service_area
140	該当なし	rab_setup	mbms_session_id
141	該当なし	ext_header	mbms_flow_id
142	該当なし	trigger_id	mbms_ip_multicast
143	該当なし	omc_id	mbms_distribution_ack
144	該当なし	ran_trans	rfsp_index
145	該当なし	pdp_context_pri	uci
146	該当なし	addi_rab_setup	csg_info
147	該当なし	sgsn_number	csg_id

値	Version 0	Version 1	Version 2
148	該当なし	common_flag	cmi
149	該当なし	apn_restriction	service_indicator
150	該当なし	radio_priority_lcs	detach_type
151	該当なし	rat_type	ldn
152	該当なし	user_loc_info	node_feature
153	該当なし	ms_time_zone	mbms_time_to_transfer
154	該当なし	imei_sv	throttling
155	該当なし	camel	arp
156	該当なし	mbms_ue_context	epc_timer
157	該当なし	tmp_mobile_group_id	signalling_priority_indication
158	該当なし	rim_routing_addr	tmgi
159	該当なし	mbms_config	mm_srvcc
160	該当なし	mbms_service_area	flags_srvcc
161	該当なし	src_rnc_pdcp	nmbr
162	該当なし	addi_trace_info	該当なし
163	該当なし	hop_counter	該当なし
164	該当なし	plmn_id	該当なし
165	該当なし	mbms_session_id	該当なし
166	該当なし	mbms_2g3g_indicator	該当なし
167	該当なし	enhanced_nsapi	該当なし
168	該当なし	mbms_session_duration	該当なし
169	該当なし	addi_mbms_trace_info	該当なし
170	該当なし	mbms_session_repetition_num	該当なし

値	Version 0	Version 1	Version 2
171	該当なし	mbms_time_to_data	該当なし
173	該当なし	bss	該当なし
174	該当なし	cell_id	該当なし
175	該当なし	pdu_num	該当なし
177	該当なし	mbms_bearer_capab	該当なし
178	該当なし	rim_routing_disc	該当なし
179	該当なし	list_pfc	該当なし
180	該当なし	ps_xid	該当なし
181	該当なし	ms_info_change_report	該当なし
182	該当なし	direct_tunnel_flags	該当なし
183	該当なし	correlation_id	該当なし
184	該当なし	bearer_control_mode	該当なし
185	該当なし	mbms_flow_id	該当なし
186	該当なし	mbms_ip_multicast	該当なし
187	該当なし	mbms_distribution_ack	該当なし
188	該当なし	reliable_inter_rat_handover	該当なし
189	該当なし	rfsp_index	該当なし
190	該当なし	fqdn	該当なし
191	該当なし	evolved_allocation1	該当なし
192	該当なし	evolved_allocation2	該当なし
193	該当なし	extended_flags	該当なし
194	該当なし	uci	該当なし
195	該当なし	csg_info	該当なし

値	Version 0	Version 1	Version 2
196	該当なし	csg_id	該当なし
197	該当なし	cmi	該当なし
198	該当なし	apn_ambr	該当なし
199	該当なし	ue_network	該当なし
200	該当なし	ue_ambr	該当なし
201	該当なし	apn_ambr_nsapi	該当なし
202	該当なし	ggsn_backoff_timer	該当なし
203	該当なし	signalling_priority_indication	該当なし
204	該当なし	signalling_priority_indication_nsapi	該当なし
205	該当なし	high_bitrate	該当なし
206	該当なし	max_mbr	該当なし
251	charging_gateway_addr	charging_gateway_addr	該当なし
255	private_extension	private_extension	private_extension

SCADA キーワード

ルール エンジンは Modbus および DNP3 ルールを使用して特定のプロトコル フィールドにアクセスします。

Modbus キーワード

Modbus キーワードを単独で使用することも、`content` や `byte_jump` など他のキーワードと組み合わせて使用することもできます。

modbus_data

`modbus_data` キーワードを使用すると、Modbus 要求または応答内の [Data] フィールドの先頭を指し示すことができます。

modbus_func

`modbus_func` キーワードを使用すると、Modbus アプリケーション層要求または応答見出し内の [Function Code（機能コード）] フィールドを照合できます。Modbus 機能コードとして、1 つの定義済み 10 進数値または 1 つの定義済み文字列を指定できます。

次の表に、Modbus 機能コードとしてシステムで認識される定義済みの値と文字列を示します。

表 *147*：*Modbus* 機能コード

値	文字列
1	read_coils
2	read_discrete_inputs
3	read_holding_registers
4	read_input_registers
5	write_single_coil
[6]	write_single_register
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
17	report_slave_id
20	read_file_record
21	write_file_record
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue
43	encapsulated_interface_transport

modbus_unit

modbus_unit キーワードを使用すると、Modbus 要求または応答ヘッダー内の [Unit ID] フィールドで 1 つの 10 進数値を照合できます。

DNP3 キーワード

DNP3 キーワードを単独で使用することも、content や byte_jump など他のキーワードと組み合わせて使用することもできます。

dnp3_data

dnp3_data キーワードを使用すると、再構築された DNP3 アプリケーション層フラグメントの先頭を指し示すことができます。

DNP3 プリプロセッサは、リンク層フレームをアプリケーション層フラグメントに再構築します。dnp3_data キーワードは、各アプリケーション層フラグメントの先頭を指し示します。他のルールオプションは、16 バイトごとにデータを分離してチェックサムを追加せずに、フラグメント内の再構築されたデータを照合することができます。

dnp3_func

dnp3_func キーワードを使用すると、DNP3 アプリケーション層要求または応答ヘッダー内の [機能コード（Function Code）] フィールドを照合できます。DNP3 機能コードとして、1 つの定義済み 10 進数値または 1 つの定義済み文字列を指定できます。

次の表に、DNP3 機能コードとしてシステムで認識される定義済みの値と文字列を示します。

表 *148* : *DNP3* 機能コード

値	文字列
[0]	confirm
1	read
2	write
3	選択
4	operate
5	direct_operate
[6]	direct_operate_nr
7	immed_freeze
8	immed_freeze_nr
9	freeze_clear

値	文字列
10	freeze_clear_nr
11	freeze_at_time
12	freeze_at_time_nr
13	cold_restart
18	warm_restart
15	initialize_data
16	initialize_appl
17	start_appl
18	stop_appl
19	save_config
20	enable_unsolicited
21	disable_unsolicited
22	assign_class
23	delay_measure
24	record_current_time
25	open_file
26	close_file
27	delete_file
36	get_file_info
29	authenticate_file
30	abort_file
31	activate_config
32	authenticate_req
33	authenticate_err

値	文字列
129	response
130	unsolicited_response
131	authenticate_resp

dnp3_ind

dnp3_ind キーワードを使用すると、DNP3 アプリケーション層応答ヘッダー内の [Internal Indications] フィールド内のフラグを照合できます。

1 つの既知のフラグ、または次の例のようなカンマ区切りのフラグ リストを示す文字列を指定できます。

```
class_1_events, class_2_events
```

複数のフラグを指定した場合、キーワードはリスト内の任意のフラグと一致します。いくつかのフラグの組み合わせを検出するには、1 つのルール内で dnp3_ind キーワードを複数回使用します。

定義済みの DNP3 内部通知フラグとしてシステムによって認識される文字列構文を以下に示します。

```
class_1_events
class_2_events
class_3_events
need_time
local_control
device_trouble
device_restart
no_func_code_support
object_unknown
parameter_error
event_buffer_overflow
already_executing
config_corrupt
reserved_2
reserved_1
```

dnp3_obj

dnp3_obj キーワードを使用すると、要求または応答内の DNP3 オブジェクト ヘッダーを照合できます。

DNP3 データは、アナログ入力やバイナリ入力など、さまざまなタイプの一連の DNP3 オブジェクトで構成されます。各タイプは、それぞれ10進数値で識別されるグループを使って区別されます（アナログ入力グループ、バイナリ入力グループなど）。各グループ内のオブジェクトは、それぞれオブジェクトデータ形式を指定するオブジェクトバリエーションによってさらに区別されます（16 ビット整数、32 ビット整数、短精度浮動小数点など）。また、オブジェクト バリエーションの各タイプは 10 進数値でも識別可能です。

オブジェクト ヘッダーを識別する際には、オブジェクト ヘッダー グループのタイプを示す 10 進数値とオブジェクト バリエーションのタイプを示す 10 進数値を指定します。この 2 つの組み合わせによって DNP3 オブジェクトの特定のタイプが定義されます。

パケット特性

特定のパケット特性を持つパケットに対してのみイベントを生成するルールを作成できます。

dsize

dsize キーワードはパケット ペイロード サイズを検査します。「大なり」演算子と「小なり」演算子（<、>）を使って値の範囲を指定することができます。次の構文をに従って範囲を指定できます。

```
>number_of_bytes
<number_of_bytes
number_of_bytes<>number_of_bytes
```

たとえば、400 バイトを超えるパケット サイズを指定するには、dtype 値として >400 を使用します。500 バイト未満のパケット サイズを指定するには、<500 を使用します。400 ～ 500 バイトのパケットに対してルールをトリガーとして使用するよう指定するには、400<>500 を使用します。

注意 dsize キーワードは、プリプロセッサによってデコードされる前のパケットを検査します。

isdataat

isdataat キーワードは、ペイロード内の特定の位置にデータが存在することを確認するよう、ルール エンジンに指示します。

次の表に、isdataat キーワードで使用可能な引数を列挙します。

表 *149*：*isdataat* の引数

引数	タイプ（Type）	説明
Offset	必須（Required）	ペイロード内の特定の位置。たとえば、パケット ペイロード内のバイト位置 50 にデータが出現することを検査するには、オフセット値として 50 を指定します。! 修飾子は isdataat 検査の結果を否定します。特定量のデータがペイロードに存在しない場合は警告が出されます。 また、既存の byte_extract 変数を使用してこの引数の値を指定することもできます。
Relative	オプション	最後に見つかったコンテンツ一致を基準にして相対的な位置を計算します。相対位置を指定する場合は、カウンタがバイト 0 から始まることに注意してください。最後に見つかったコンテンツ一致から順方向に移動するバイト数から 1 を差し引いて位置を計算します。たとえば、最後に見つかったコンテンツ一致から 9 バイト後にデータが出現すべきことを指定するには、相対オフセットとして 8 を指定します。

引数	タイプ（Type）	説明
Raw Data	オプション	Firepower システム プリプロセッサによるデコードやアプリケーション層の正規化が行われる前の、元のパケット ペイロードにデータが配置されていることを指定します。前のコンテンツ一致が未加工パケット データ内に存在していた場合は、この引数を Relative と一緒に使用できます。

たとえば、`foo` というコンテンツを検索するルールで `isdataat` の値が次のように指定される場合、

- Offset = !10
- Relative = enabled

ルール エンジンが `foo` の後ろからペイロード末尾までに 10 バイトを検出しない場合、システムは警告を出します。

sameip

`sameip` キーワードは、パケットの送信元 IP アドレスと宛先 IP アドレスが同じであることを検査します。このキーワードは引数を受け入れません。

fragoffset

`fragoffset` キーワードは、フラグメント化されたパケットのオフセットを検査します。一部の exploit（WinNuke サービス拒否攻撃など）では、特定のオフセットを持つ手動生成されたパケット フラグメントが使われるため、このキーワードが役立ちます。

たとえば、フラグメント化されたパケットのオフセットが 31337 バイトかどうかを検査するには、`fragoffset` 値として `31337` を指定します。

`fragoffset` キーワードの引数を指定するときには、次の演算子を使用できます。

表 *150*：*fragoffset* キーワードの引数演算子

演算子	説明
!	ノット
>	より大きい
<	より少ない

否定（!）演算子を < や > と組み合わせて使用できないことに注意してください。

cvs

`cvs` キーワードは、Concurrent Versions System（CVS）トラフィック内で不正な形式の CVS エントリを検査します。攻撃者は不正な形式のエントリを使用して、ヒープ オーバーフローを強制的に

発生させ、CVSサーバ上で有害コードを実行することができます。このキーワードを使用すると、2 つの既知の CVS 脆弱性 CVE-2004-0396（CVS 1.11.x ～ 1.11.15 と 1.12.x ～ 1.12.7）および CVS-2004-0414（CVS 1.12.x ～ 1.12.8 と 1.11.x ～ 1.11.16）に対する攻撃を識別できます。`cvs` キーワードは、正しい形式のエントリであることを検査して、不正な形式のエントリが検出された場合はアラートを生成します。

CVS が動作するポートをルールに含める必要があります。さらに、トラフィックが発生する可能性のあるポートをTCPポリシー内のストリーム再構築用のポートリストに追加することで、CVS セッションの状態を保持できるようにする必要があります。ストリーム再構築が行われるクライアント ポートのリストには、TCP ポート 2401（`pserver`）と 514（`rsh`）が含まれています。ただし、サーバが `xinetd` サーバ（つまり pserver）として動作する場合は、任意の TCP ポート上で動作できることに注意してください。すべての非標準ポートを、ストリーム再構築の[クライアントポート（Client Ports）] リストに追加します。

関連トピック

byte_extract キーワード, （1155 ページ）
TCP ストリームのプリプロセス オプション, （1393 ページ）

アクティブ応答のキーワード

システムは、トリガーとして使用されたTCPルールに応答してTCP接続を閉じるために、またはトリガーとして使用された UDP ルールに応答して UDP セッションを閉じるために、アクティブ応答を開始できます。2 つのキーワードにより、別々の方法でアクティブ応答を開始できます。どちらかのキーワードを含むルールをパケットがトリガーとして使用すると、システムは 1 つのアクティブ応答を開始します。`config response` コマンドを使用して、アクティブ応答インターフェイスおよびパッシブ展開で試行する TCP リセットの回数を設定することもできます。

リセットは接続やセッションに影響を与えるのに間に合うまでに到着する可能性が高いため、アクティブ応答はインライン展開で最も効果を発揮します。たとえば、インライン展開での `react` キーワードに応答して、システムは接続の両端用のトラフィックに TCP リセット（RST）パケットを直接挿入し、通常はこれによって接続が閉じます。

（パッシブ展開ではシステムがパケットを挿入できない、攻撃者がアクティブ応答を無視または回避するよう選択する可能性があるなど）さまざまな理由で、アクティブ応答はファイアウォールの代わりとして想定されていません。

アクティブ応答は戻って来ることがあるため、システムはTCPリセットによるTCPリセットの開始を許可しません。これにより、アクティブ応答が無限に続くことを防止できます。また、システムは、標準的な慣行に従って ICMP 到達不能パケットによる ICMP 到達不能パケットの開始を許可しません。

侵入ルールがアクティブ応答をトリガーとして使用した後、接続またはセッションで追加のトラフィックを検出するよう、TCP ストリーム プリプロセッサを設定できます。追加のトラフィックが検出されると、プリプロセッサは、指定された最大値まで、追加のアクティブ応答を接続またはセッションの両端に送信します。

関連トピック

侵入廃棄ルールでのアクティブ応答, （1366 ページ）

resp キーワード

resp キーワードを使用すると、ルール ヘッダーで TCP プロトコルと UDP プロトコルのどちらが指定されているかに基づいて、TCP 接続または UDP セッションにアクティブに（能動的に）応答できます。

キーワード引数を使用すると、パケットの方向、および TCP リセット（RST）パケットと ICMP 到達不能パケットのどちらをアクティブ応答として使用するかを指定できます。

任意の TCP リセット引数または ICMP 到達不能引数を使用して、TCP 接続を閉じることができます。UDP セッションを閉じるには、ICMP 到達不能引数だけを使用する必要があります。

また、さまざまな TCP リセット引数を使用することで、パケットの送信元、宛先、またはその両方にアクティブ応答を送ることができます。すべての ICMP 到達不能引数はパケット送信元に送られます。ICMP ネットワーク、ホスト、またはポートのどの到達不能パケットを使用するか（または 3 つすべてを使用するか）を指定できます。

ルールがトリガーとして使用されたときに Firepower システムで実行されるアクションを正確に指定するために、resp キーワードで使用できる引数を次の表に列挙します。

表 *151*：*resp* 引数

引数	説明
reset_source	ルールをトリガーとして使用したパケットを送信元エンドポイントに TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている rst_snd を指定することもできます。
reset_dest	ルールをトリガーとして使用したパケットの宛先であるエンドポイントに TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている rst_rcv を指定することもできます。
reset_both	送信側エンドポイントと受信側エンドポイントの両方に TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている rst_all を指定することもできます。
icmp_net	送信側に ICMP ネットワーク到達不能メッセージを送ります。
icmp_host	送信側に ICMP ホスト到達不能メッセージを送ります。
icmp_port	送信側に ICMP ポート到達不能メッセージを送ります。この引数は、UDP トラフィックを終了するために使われます。

引数	説明
icmp_all	送信側に次の ICMP メッセージを転送します。 • ネットワーク到達不能 • ホスト到達不能 • ポート到達不能

たとえば、ルールがトリガーとして使用されたときに接続の両側をリセットするようルールを設定するには、`resp` キーワードの値として `reset_both` を使用します。

次のように、カンマ区切りのリストを使用して複数の引数を指定できます。

```
argument,argument,argument
```

`config response` コマンドを使用すると、使用するアクティブ応答インターフェイス、およびパッシブ展開で試行する TCP リセットの回数を設定することができます。

関連トピック

config response コマンド, （1222 ページ）

react キーワード

`react` キーワードを使用すると、パケットがルールをトリガーとして使用した時点でデフォルト HTML ページを TCP 接続クライアントに送信できます。HTML ページの送信後に、システムは TCP リセット パケットを使って接続の両端へのアクティブ応答を開始します。`react` キーワードは UDP トラフィックのアクティブ応答をトリガーとして使用しません。

オプションで、次の引数を指定できます。

```
msg
```

`msg` 引数を使用する `react` ルールがパケットによってトリガーとして使用されると、HTML ページにルール イベント メッセージが表示されます。

`msg` 引数を指定しない場合、HTML ページには次のメッセージが含まれます。

```
You are attempting to access a forbidden site.
Consult your system administrator for details.
```

（注） アクティブ応答は戻されることがあるため、HTML 応答ページによって `react` ルールがトリガーとして使用されないようにしてください（結果としてアクティブ応答が無限に続く可能性があります）。Cisco では、`react` ルールを十分にテストしてから実稼動環境でアクティブにするよう推奨しています。

`config response` コマンドを使用すると、使用するアクティブ応答インターフェイス、およびパッシブ展開で試行する TCP リセットの回数を設定することができます。

関連トピック

ルールの詳細, （1106 ページ）
config response コマンド, （1222 ページ）

config response コマンド

config response コマンドを使用すると、resp ルールと react ルールによって開始される TCP リセットの動作を詳細に設定できます。また、このコマンドは、廃棄ルールによって開始されるアクティブ応答の動作にも影響を与えます。

config response コマンドを使用するには、高度な USER_CONF 変数内の別個の 1 行にこれを挿入します。

次のように、USER_CONF 拡張変数の別の行に config response コマンドの形式を挿入します。

- アクティブ応答の試行回数のみを指定するには、次のコマンドを挿入します。

  `config response: attempts`att

  例：`config response: attempts 10`

- アクティブ応答インターフェイスのみを指定するには、次のコマンドを挿入します。

  `config response: device` dev

  例：`config response: device eth0`

- アクティブ応答の試行回数とアクティブ応答インターフェイスの両方を指定するには、次のコマンドを挿入します。

  `config response: attempts` att, `device` dev

  引数の説明

  - att は、受信側ホストにパケットを受け入れさせるために、現在の接続枠で各 TCP リセットパケットを挿入する試行回数（1 ～ 20）です。この連続試行はパッシブ展開でのみ効果があります。インライン展開の場合、システムはトリガーパケットの代わりにリセットパケットをストリームに直接挿入します。ICMP 到着可能な 1 つのアクティブ応答のみが送信されます。
  - dev は、パッシブ展開でシステムからアクティブ応答を送信したり、インライン展開でアクティブ応答を挿入したりするための代替インターフェイスです。

    例：`config response: attempts 10, device eth0`

注意 機能の説明またはサポート担当の指示に従う場合を除き、侵入ポリシー機能を設定するために高度な USER_CONF 変数を**使用しない**でください。競合または重複する設定が存在すると、システムが停止します。

関連トピック

侵入廃棄ルールでのアクティブ応答, （1366 ページ）
拡張変数, （407 ページ）

detection_filter キーワード

`detection_filter` キーワードを使用すると、指定された時間内に指定された数のパケットがルールをトリガーとして使用しない限り、ルールでイベントが生成されないようにすることができます。これにより、早すぎるタイミングでルールがイベントを生成することを回避できます。たとえば、数秒間にログイン試行が 2 ～ 3 回失敗することは想定の範囲内ですが、同じ時間内に多数の試行が発生した場合はブルートフォース アタックを示唆している可能性があります。

`detection_filter` キーワードの必須の引数は、送信元/宛先のどちらの IP アドレスをシステムで追跡するか、イベントをトリガーする前に検出基準が満たされるべき回数、およびカウントの継続時間を定義します。

イベントのトリガーを遅らせるには、次の構文を使用します。

```
track by_src/by_dst, count count, seconds number_of_seconds
```

`track` 引数は、ルールの検出基準を満たすパケット数をカウントするときに、パケットの送信元 IP アドレスと宛先 IP アドレスのどちらを使用するかを指定します。システムでイベント インスタンスを追跡する方法を指定するには、次の表の中から引数値を選択します。

表 *152*：*detection_filter* の追跡引数

引数	説明
by_src	送信元 IP アドレスによる検出基準カウント。
by_dst	宛先 IP アドレスによる検出基準カウント。

`count` 引数は、ルールでイベントを生成する前に、指定された時間内に指定された IP アドレスのルールをトリガーすべきパケットの数を指定します。

`seconds` 引数は、ルールでイベントを生成する前に、指定された数のパケットがルールをトリガーすべき時間枠を秒数で指定します。

パケット内でコンテンツ `foo` を検索するルールが、次の引数を含む `detection_filter` キーワードを使用するとします。

```
track by_src, count 10, seconds 20
```

この例のルールは、特定の送信元 IP アドレスから 20 秒以内に 10 個のパケットで `foo` を検出するまでは、イベントを生成しません。システムが最初の 20 秒以内に `foo` を含むパケットを 7 つしか検出しなかった場合は、イベントが生成されません。 しかし、最初の 20 秒間で `foo` が 40 回出現した場合は、ルールで 30 個のイベントが生成され、20 秒が経過するとカウントが再開されます。

しきい値と detection_filter キーワードの比較

detection_filter キーワードは、非推奨の threshold キーワードに代わるものです。threshold キーワードは、下位互換性を維持するために引き続きサポートされていますが、侵入ポリシー内で設定されるしきい値と同じ機能です。

detection_filter キーワードは、パケットがルールをトリガーとして使用する前に適用される検出機能です。ルールは、指定されたパケットカウントの前に検出されたトリガーパケットに関してイベントを生成しません。また、インライン展開では、パケットを破棄するようルールで設定されていても、そのようなパケットを破棄しません。逆に、指定されたパケットカウントの後に出現する、ルールをトリガーとして使用するパケットに関してルールはイベントを生成します。また、インライン展開でパケットを破棄するよう設定されている場合は、そのようなパケットを破棄します。

しきい値は、検出アクションを発生させないイベント通知機能です。これは、パケットがイベントをトリガーとして使用した後に適用されます。インライン展開において、パケットを破棄するよう設定されたルールは、ルールしきい値とは無関係に、ルールをトリガーとして使用するすべてのパケットを破棄します。

侵入ポリシー内で detection_filter キーワードを侵入イベントしきい値、侵入イベント抑制、および Rate-Based 攻撃防御機能と任意に組み合わせて使用できることに注意してください。また、侵入ポリシー内の侵入イベントしきい値機能と組み合わせて非推奨の threshold キーワードを使用するインポートされたローカル ルールを有効にした場合、ポリシー検証が失敗することに注意してください。

関連トピック

侵入イベントのしきい値, （1064 ページ）
侵入ポリシーの抑制の設定, （1068 ページ）
[ルール（Rule）] ページからの動的ルール状態の設定, （1073 ページ）
ローカル侵入ルール ファイル インポート, （162 ページ）

tag キーワード

ホストまたはセッションに関する追加のトラフィックをログに記録するようシステムに指示するには、tag キーワードを使用します。tag キーワードを使って検出するトラフィックのタイプと量を指定するときには、次の構文を使用します。

```
tagging_type, count, metric, optional_direction
```

次の 3 つの表に、その他の使用可能な引数について説明します。

2 つのタイプのタグ機能から選択できます。次の表に、これらのタグ機能の説明を示します。侵入ルールでルール ヘッダー オプションのみを設定した場合、session タグ引数タイプによって、同じセッションからのパケットが別のセッションからのパケットのように記録されることに注意してください。同じセッションからのパケットをまとめてグループ化するには、同じ侵入ルール内で 1 つ以上のルール オプション（flag キーワードや content キーワードなど）を設定します。

表 *153*：*tag* の引数

引数	説明
session	ルールをトリガーとして使用したセッション内のパケットをログに記録します。
ホスト	ルールをトリガーとして使用したパケットを送信したホストからのパケットをログに記録します。ホストからのトラフィックのみ（`src`）、またはホストへのトラフィックのみ（`dst`）を記録する方向修飾子を追加できます。

ログに記録するトラフィック量を指定するには、次の引数を使用します。

表 *154*：カウント引数

引数	説明
count	ルールがトリガーとして使用された後にログに記録するパケット数または秒数。 この単位を指定するには、count 引数の後に測定基準引数を使用します。

次の表の中から、トラフィックの時間または量ごとにログで使用する測定基準を選択してください。

注意 高帯域ネットワークでは、1 秒あたり数千パケットが発生する可能性があり、多数のパケットにタグを付けるとパフォーマンスに重大な影響が及ぶ可能性があるため、必ずネットワーク環境に合わせてこの設定を調整してください。

表 *155*：ログの測定基準引数

引数	説明
packets	ルールのトリガー後に、カウントで指定されるパケット数をログに記録します。
秒	ルールのトリガー後に、カウントで指定される秒数の間、トラフィックを記録します。

たとえば、次の `tag` キーワード値を使用するルールがトリガーとして使用された場合、

```
host, 30, seconds, dst
```

次の 30 秒間にクライアントからホストに送信されるすべてのパケットがログに記録されます。

flowbits キーワード

状態名をセッションに割り当てるには、flowbits キーワードを使用します。すでに名前が付けられた状態に基づいてセッション内の後続パケットを分析することにより、システムは単一セッション内で複数のパケットに及ぶエクスプロイトを検出して警告を出すことができます。

flowbits状態名は、セッションの特定部分でパケットに割り当てられるユーザ定義のラベルです。パケットの内容に基づいてパケットに状態名を付けると、警告の必要のないパケットと有害なパケットを区別しやすくなります。管理対象デバイスごとに最大1024個の状態名を定義できます。たとえば、ログイン成功後にのみ発生することがわかっている有害パケットについて警告するには、flowbits キーワードを使用して、初期ログイン試行を構成するパケットを除去することにより、有害パケットに焦点を絞ることができます。このような機能を実装するには、まず、セッション内のすべてのログイン確立済みパケットにlogged_in 状態のラベルを付けるルールを作成した後、2 番目のルールを作成し、最初のルールで設定された状態を持つパケットを検査してそのようなパケットだけを処理する flowbits をそのルールに含めます。

オプションの *group name* を使用すると、状態のグループに状態名を含めることができます。1 つの状態名は複数のグループに属することができます。グループに関連付けられていない状態は相互排他的ではないため、トリガーとして使用されたルールがグループに関連付けられていない状態を設定した場合、現在設定されている他の状態には影響がありません。

flowbits キーワードのオプション

次の表に、flowbits キーワードで使用できる演算子、状態、およびグループのさまざまな組み合わせについて説明します。なお、状態名には、英数字、ピリオド（.）、アンダースコア（_）、およびダッシュ（-）を含めることができます。

表 *156* : *flowbits* のオプション

演算子	状態オプション	グループ	説明
set	state_name	オプション	パケットに関する指定された状態を設定します。グループが定義されている場合は、指定されたグループ内で状態を設定します。
set	state_name&state_name	オプション	パケットに関する指定された状態を設定します。グループが定義されている場合は、指定されたグループ内で状態を設定します。
setx	state_name	入力必須	指定されたグループ内でパケットに関して指定された状態を設定し、グループ内の他のすべての状態を解除します。
setx	state_name&state_name	入力必須	指定されたグループ内でパケットに関して指定された状態を設定し、グループ内の他のすべての状態を解除します。
unset	state_name	グループなし	パケットに関する指定された状態を解除します。
unset	state_name&state_name	グループなし	パケットに関する指定された状態を解除します。
unset	all	入力必須	指定されたグループ内のすべての状態を解除します。
toggle	state_name	グループなし	指定された状態が設定されている場合はそれを解除し、指定された状態が解除されている場合にはそれを設定します。
toggle	state_name&state_name	グループなし	指定された複数の状態が設定されている場合はそれらを解除し、指定された複数の状態が解除されている場合はそれらを設定します。
toggle	all	入力必須	指定されたグループ内で設定されているすべての状態を解除し、指定されたグループ内で解除されているすべての状態を設定します。
isset	state_name	グループなし	指定された状態がパケット内で設定されているかどうかを判別します。
isset	state_name&state_name	グループなし	指定された複数の状態がパケット内で設定されているかどうかを判別します。
isset	state_name|state_name	グループなし	指定されたいずれかの状態がパケット内で設定されているかどうかを判別します。

演算子	状態オプション	グループ	説明
isset	any	入力必須	指定されたグループ内で、いずれかの状態が設定されているかどうかを判別します。
isset	all	入力必須	指定されたグループ内で、すべての状態が設定されているかどうかを判別します。
isnotset	state_name	グループなし	指定された状態がパケット内で設定されていないかどうかを判別します。
isnotset	state_name&state_name	グループなし	指定された複数の状態がパケット内で設定されていないかどうかを判別します。
isnotset	state_name|state_name	グループなし	指定されたいずれかの状態が、パケット内で設定されていないかどうかを判別します。
isnotset	any	入力必須	パケット内でいずれかの状態が設定されていないかどうかを判別します。
isnotset	all	入力必須	パケット内ですべての状態が設定されていないかどうかを判別します。
reset	（状態なし）	オプション	すべてのパケットのすべての状態を解除します。グループが指定されている場合、グループ内のすべての状態を解除します。
noalert	（状態なし）	グループなし	イベント生成を抑制するには、これを他の演算子と組み合わせて使用します。

flowbits キーワードの使用に関するガイドライン

flowbits キーワードを使用するときには、次の点に注意してください。

- setx 演算子を使用する場合、指定した状態は、指定したグループ以外のグループに属することができません。
- setx 演算子を複数回定義して、それぞれのインスタンスで別々の状態と同じグループを指定できます。
- setx 演算子を使用してグループを指定する場合、そのグループに対して set、toggle、unset 演算子を使用することはできません。
- isset 演算子と isnotset 演算子は、指定された状態がグループに含まれるかどうかに関係なく、その状態を評価します。

- 侵入ポリシーの保存時、侵入ポリシーの再適用時、および（アクセス コントロール ポリシーで参照される侵入ポリシー数に関係なく）アクセス コントロール ポリシーの適用時には、グループ指定の**ない** `isset` または `isnotset` 演算子を含むルールを有効にした場合、対応する状態名とプロトコルに関する `flowbits` 割り当て（`set`、`setx`、`unset`、`toggle`）に影響する 1 つ以上のルールを有効にしないと、対応する状態名の `flowbits` 割り当てに影響するすべてのルールが有効になります。
- 侵入ポリシーの保存時、侵入ポリシーの再適用時、および（アクセス コントロール ポリシーで参照される侵入ポリシー数に関係なく）アクセス コントロール ポリシーの適用時には、グループを指定**した** `isset` 演算子または `isnotset` 演算子を含むルールを有効にした場合、`flowbits` 割り当て（`set`、`setx`、`unset`、`toggle`）に影響し、対応するグループ名を定義するすべてのルールもまた有効になります。

flowbits キーワードの例

この項では、`flowbits` キーワードを使用する 3 つの例を示します。

flowbits キーワードの例：*state_name* を使用した設定

これは、`state_name` を使用した flowbits 設定の例です。

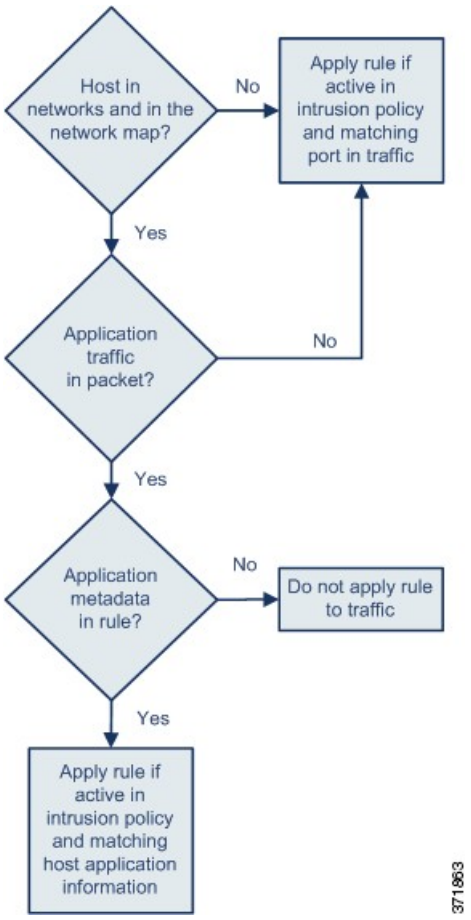
Bugtraq ID #1110 に記述されている IMAP 脆弱性について考えてみます。この脆弱性は、IMAP の実装（具体的にはLIST、LSUB、RENAME、FIND、およびCOPY コマンド）で見られます。ただし、攻撃者がこの脆弱性を悪用するには、IMAP サーバにログインする必要があります。IMAP サーバからの LOGIN 確認とそれに続く exploit は必然的に別々のパケットに存在するため、この exploit を検出する非フロー ベースのルールを作成するのは困難です。`flowbits` キーワードを使って一連のルールを作成すると、ユーザが IMAP サーバにログイン済みかどうかを追跡し、ログイン済みの場合は、いずれかの攻撃が検出された時点でイベントを生成することができます。ユーザがログイン済みでない場合、攻撃によって脆弱性が悪用されることはないため、イベントが生成されません。

下記の 2 つのルール フラグメントはこの例を示しています。最初のルール フラグメントは IMAP サーバからの IMAP ログイン確認を検索します。

```
alert tcp any 143 -> any any (msg:"IMAP login"; content:"OK

LOGIN"; flowbits:set,logged_in; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

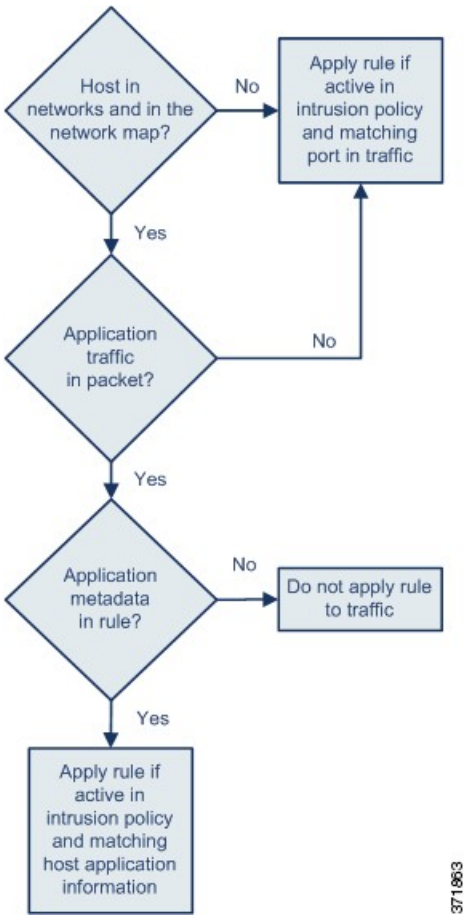


`flowbits:set` は `logged_in` 状態を設定しますが、`flowbits:noalert` がアラートを抑制することに注意してください。これは、IMAP サーバ上で多数の無害なログイン セッションが見つかる可能性があるためです。

次のルール フラグメントは LIST 文字列を検索しますが、セッション内の先行パケットの結果として logged_in 状態が設定済みでない限り、イベントを生成しません。

```
alert tcp any any -> any 143 (msg:"IMAP LIST";
content:"LIST"; flowbits:isset,logged_in;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。



この場合、最初のフラグメントを含むルールが先行パケットによってトリガーとして使用した場合、2 番目のフラグメントを含むルールがトリガーとして使用し、イベントを生成します。

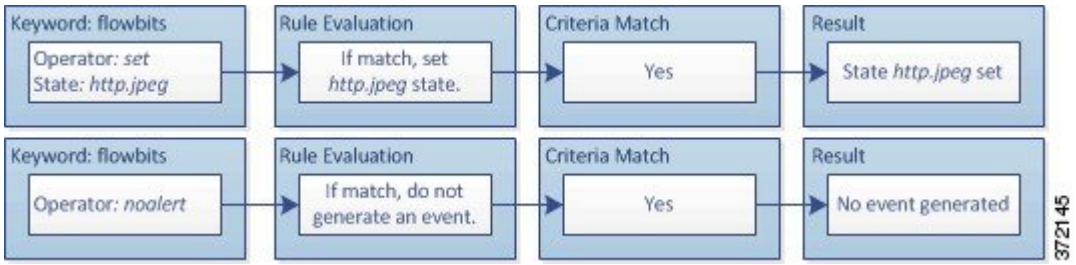
flowbits キーワードの例：誤検出イベントを引き起こす設定

後続パケット内コンテンツが、効力を失った状態を持つルールに一致することによって誤検出イベントが発生する可能性があります。複数のルールで設定された複数の状態名をグループに含めることでこれを回避できます。次の例は、複数の状態名をグループに含めない場合に誤検出が発生する可能性があることを示しています。

1 つのセッションで次の 3 つのルール フラグメントがこの順序でトリガーとして使用される場合を考えてみます。

```
(msg:"JPEG transfer";
content:"image/";pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:set,http.jpeg; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

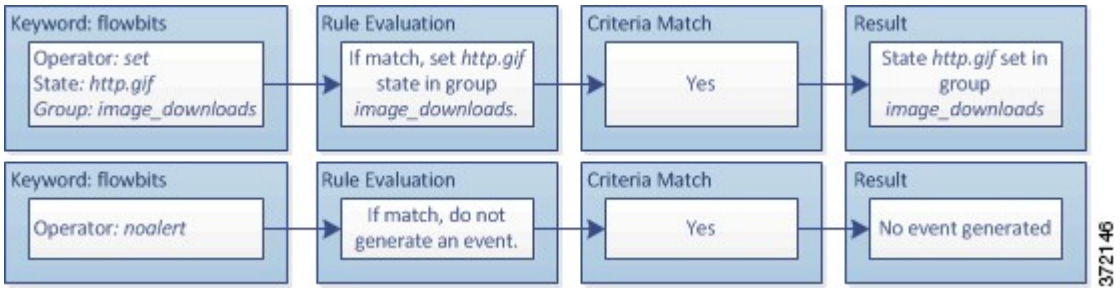


最初のルール フラグメント内の `content` キーワードと `pcre` キーワードが JPEG ファイル ダウンロードに一致し、`flowbits:set,http.jpeg` が `http.jpeg flowbits` ステートを設定し、`flowbits:noalert` はルールでのイベント生成を抑制します。イベントが生成されない理由は、このルールの目的がファイル ダウンロードを検出して `flowbits` 状態を設定することだからです。これにより、1 つ以上のコンパニオン ルールで状態名を検査して有害コンテンツを探し、有害コンテンツが検出された時点でイベントを生成できます。

次のルール フラグメントは、上記の JPEG ファイル ダウンロードに続く GIF ファイル ダウンロードを検出します。

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:set,http.jpg,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

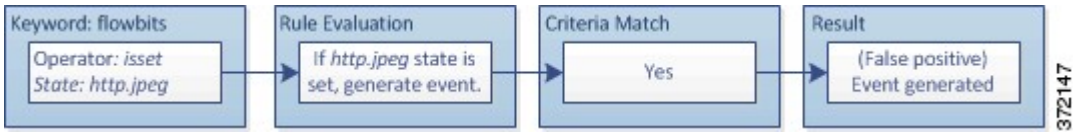


2 番目のルール内の `content` キーワードと `pcre` キーワードは GIF ファイル ダウンロードを照合し、`flowbits:set,http.jpg` は `http.jpg` flowbit ステートを設定し、`flowbits:noalert` はルールでのイベント生成を抑制します。最初のルール フラグメントで設定された `http.jpeg` 状態が不要になっても引き続き設定されていることに注意してください。これは、後続の GIF ダウンロードが検出されたときに JPEG ダウンロードが既に終了しているはずであるためです。

次に示す 3 番目のルール フラグメントは最初のルール フラグメントのコンパニオンです。

```
(msg:"JPEG exploit";?flowbits:isset,http.jpeg;content:"|FF|";
pcre:"?/\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。



3 番目のルール フラグメントでは、もはや無意味になった `http.jpeg` ステートが設定されていることを `flowbits:isset,http.jpeg` が判別し、`content` と `pcre` は（GIF ファイルでは無害でも）JPEG ファイル内では有害とみなされるコンテンツを照合します。3 番目のルール フラグメントによって、JPEG ファイル内に存在しないエクスプロイトに関する誤検出イベントが生成されます。

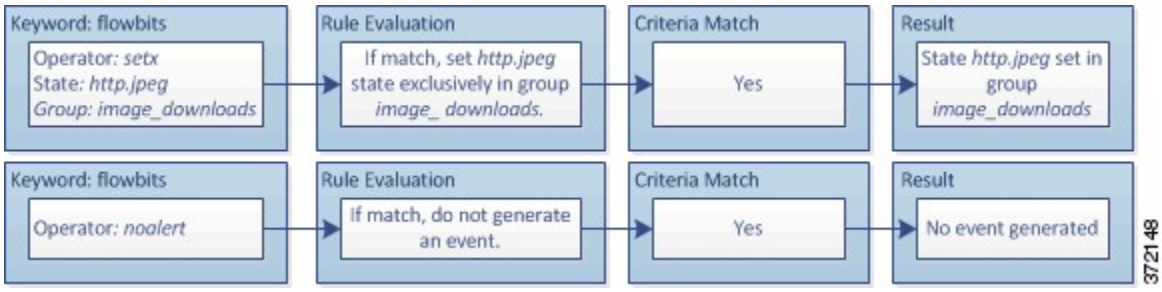
flowbits キーワードの例：誤検出イベントを防ぐための設定

次の例は、状態名をグループに含めて `setx` 演算子を使用することで、どのように誤検出を防止できるかを示しています。

前の例とほぼ同じケースを考えます。ただし、最初の 2 つのルールで、同じ状態グループに 2 つの異なる状態名が含まれるようになった点が異なります。

```
(msg:"JPEG transfer";
content:"image/";pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:setx,http.jpeg,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

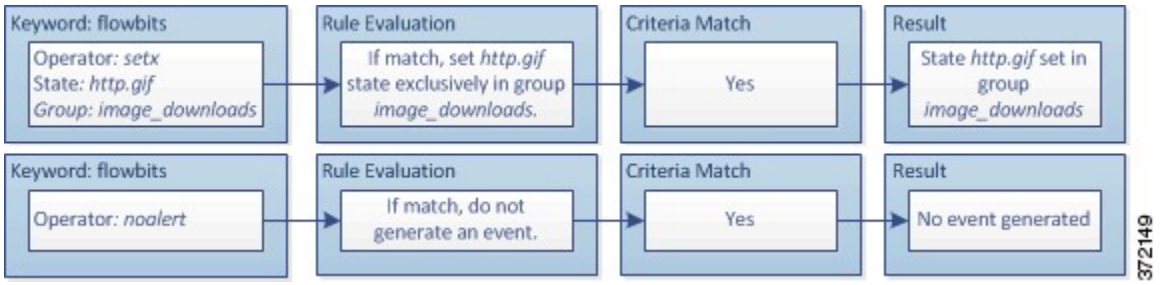


最初のルール フラグメントが JPEG ファイル ダウンロードを検出すると、`flowbits:setx,http.jpeg,image_downloads` キーワードが `flowbits` 状態を `http.jpeg` に設定し、その状態を `image_downloads` グループに含めます。

その後、次のルールが後続の GIF ファイル ダウンロードを検出します。

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:setx,http.jpg,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

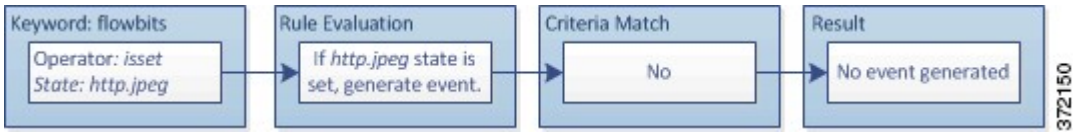


2 番目のルール フラグメントが GIF ダウンロードに一致すると、`flowbits:setx,http.jpg,image_downloads` キーワードが `http.jpg flowbits` ステートを設定し、グループ内の他のステートである `http.jpeg` を解除します。

次に示す 3 番目のルール フラグメントで誤検出は発生しません。

```
(msg:"JPEG exploit"; ?flowbits:isset,http.jpeg;content:"|FF|";
pcre:"/?\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。



`flowbits:isset,http.jpeg` が false であるため、ルール エンジンはルールの処理を停止し、イベントは生成されません。こうして、GIF ファイル内のコンテンツが JPEG ファイルに関するエクスプロイト コンテンツと一致した場合でも誤検出が回避されます。

http_encode キーワード

`http_encode` キーワードを使用すると、HTTP URI、HTTP ヘッダー内の非 cookie データ、HTTP 要求ヘッダー内の cookie、HTTP 応答内の set-cookie データのいずれかにおいて、正規化前の HTTP 要求または応答内のエンコード タイプに基づいてイベントを生成できます。

HTTP 応答と HTTP cookie を検査し、`http_encode` キーワードを使用しているルールに一致したものを返すように、HTTP Inspect プリプロセッサを設定する必要があります。

また、侵入ルール内の `http_encode` キーワードで特定のエンコード タイプによってイベントがトリガーとして使用されるようにするには、HTTP Inspect プリプロセッサ設定で個々の特定のエンコードタイプのデコードオプションとアラートオプションの両方を有効にする必要があります。

次の表は、このオプションでイベントを生成できる、HTTP URI、ヘッダー、cookie、set-cookie のエンコード タイプを説明しています。

表 *157* : *http_encode* エンコード タイプ

エンコードタイプ	説明
utf8	HTTP Inspect プリプロセッサによるデコードで UTF-8 エンコード タイプが有効になっている場合、指定された場所で UTF-8 エンコードを検出します。
double_encode	HTTP Inspect プリプロセッサによるデコードで二重エンコード タイプが有効になっている場合、指定された場所で二重エンコードを検出します。
non_ascii	非 ASCII 文字が検出されても、検出されたエンコード タイプが有効になっていない場合に、指定された場所で非 ASCII 文字を検出します。
uencode	HTTP Inspect プリプロセッサによるデコードで Microsoft %u エンコード タイプが有効になっている場合、指定された場所で Microsoft %u エンコードを検出します。

エンコードタイプ	説明
bare_byte	HTTP Inspect プリプロセッサによるデコードで空白バイト エンコード タイプが有効になっている場合、指定された場所で空白バイト エンコードを検出します。

関連トピック

HTTP Inspect プリプロセッサ, （1305 ページ）
サーバレベルの HTTP 正規化オプション, （1307 ページ）

http_encode キーワードの構文

エンコーディングの場所

HTTP URI、ヘッダー、または set-cookie などの Cookie で指定されたエンコーディング タイプを検索するかどうかを指定します。

エンコード タイプ

次のいずれかの形式を使用して、1 つ以上のエンコード タイプを指定します。

```
encode_type
encode_type|encode_type|encode_type...
```

ここで、`encode_type` は次のいずれかです。

```
utf8
double_encode
non_ascii
uencode
bare_byte.
```

否定（!）演算子と OR（|）演算子を一緒に使用できないことに注意してください。

http_encode キーワードの例：2 つの http_endcode キーワードを使用した 2 つのエンコーディングの検索

次に、同じルールで 2 つの `http_encode` キーワードを使用して、UTF-8 および Microsoft IIS %u エンコーディングの HTTP URI を検索する例を示します。

最初に、`http_encode` キーワードを使用します。

- エンコーディングの場所：`HTTP URI`
- エンコーディングのタイプ：`utf8`

次に、追加の `http_encode` キーワードを使用します。

- エンコーディングの場所：`HTTP URI`
- エンコーディングのタイプ：`uencode`

概要：file_type および file_group キーワード

file_type と file_group キーワードを使用すると、タイプとバージョンに基づいて、FTP、HTTP、SMTP、IMAP、POP3、NetBIOS-ssn（SMB）を介して伝送されるファイルを検出できます。1 つの侵入ルール内で複数の file_type キーワードや file_group キーワードを使用**しない**でください。

ヒント　脆弱性データベース（VDB）を更新すると、最新のファイル タイプ、バージョン、グループが侵入ルール エディタに表示されます。

（注）　システムは、file_type および file_group キーワードに値を代入するためにプリプロセッサを自動的に有効にすることはしません。

file_type または file_group キーワードに一致するトラフィックに対して イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、特定のプリプロセッサを有効にする**必要があります**。

表 *158*：*file_type* および *file_group* の侵入イベントの生成

プロトコル	必要なプリプロセッサまたはプリプロセッサ オプション
FTP	FTP/Telnet プリプロセッサおよび [TCP ペイロードの正規化（Normalize TCP Payload）] インライン正規化プリプロセッサ オプション
HTTP	HTTP トラフィックでの侵入イベントを生成する HTTP Inspect プリプロセッサ。
SMTP	HTTP トラフィックでの侵入イベントを生成する SMTP プリプロセッサ
IMAP	IMAP プリプロセッサ
POP3	POP プリプロセッサ
NetBIOS-ssn（SMB）	DCE/RPC プリプロセッサおよび [SMB ファイル インスペクション（SMB File Inspection）] DCE/RPC プリプロセッサ オプション

関連トピック

脆弱性データベースの更新，（155 ページ）
FTP/Telnet デコーダ，（1295 ページ）
インライン正規化プリプロセッサ，（1371 ページ）
HTTP Inspect プリプロセッサ，（1305 ページ）
SMTP プリプロセッサ，（1340 ページ）

IMAP プリプロセッサ, （1333 ページ）
POP プリプロセッサ, （1337 ページ）
DCE/RPC プリプロセッサ, （1278 ページ）

file_type キーワードと file_group キーワード

file_type

file_type キーワードを使用すると、トラフィック内で検出対象となるファイルのタイプとバージョンを指定できます。ファイル タイプ引数（JPEG や PDF など）は、トラフィックで検出するファイルの形式を識別します。

（注） 同じ侵入ルール内で file_type キーワードを別の file_type キーワードまたは file_group キーワードと一緒に使用**しない**でください。

デフォルトでは [任意のバージョン（Any Version）] が選択されますが、一部のファイル タイプではバージョン オプション（たとえば PDF バージョン 1.7）を選択することにより、トラフィックで検出対象となる特定のファイル タイプ バージョンを識別できます。

file_group

file_group キーワードを使用すると、トラフィック内で検出する類似のファイル タイプからなる Cisco 定義のグループを選択できます（マルチメディア、オーディオなど）。また、ファイル グループには、グループ内の各ファイル タイプに関する Cisco 定義のバージョンも含まれています。

（注） 同じ侵入ルール内で file_group キーワードを別の file_group キーワードまたは file_type キーワードと一緒に使用**しない**でください。

file_data キーワード

file_data キーワードは、content、byte_jump、byte_test、pcre などの他のキーワードで使用可能な位置引数の参照として機能するポインタです。file_data キーワードが指し示すデータのタイプは、検出されるトラフィックによって決まります。file_data キーワードを使用すると、次のペイロード タイプの先頭を指し示すことができます。

- HTTP 応答本文

  HTTP 応答パケットを検査するには、HTTP Inspect プリプロセッサを有効にして、HTTP 応答を検査するようプリプロセッサを設定する必要があります。HTTP Inspect プリプロセッサが HTTP 応答本文データを検出した場合に、file_data キーワードが一致します。

- 非圧縮 gzip ファイル データ

HTTP 応答本文内の非圧縮 gzip ファイルを検査するには、HTTP Inspect プリプロセッサを有効にする必要があり、さらに HTTP 応答を検査して HTTP 応答本文内の gzip 圧縮ファイルを復元するようプリプロセッサを設定する必要があります。詳細については、サーバレベルの HTTP 正規化オプション [HTTP 応答の検査（Inspect HTTP Responses）] および [圧縮データの検査（Inspect Compressed Data）] を参照してください。`file_data` キーワードは、HTTP Inspect プリプロセッサが HTTP 応答本文内で非圧縮 gzip データを検出した場合に一致します。

- 正規化された JavaScript

  正規化された JavaScript データを検査するには、HTTP Inspect プリプロセッサを有効にして、HTTP 応答を検査するようプリプロセッサを設定する必要があります。`file_data` キーワードは、HTTP Inspect プリプロセッサが応答本文データ内で JavaScript を検出した場合に一致します。

- SMTP ペイロード

  SMTP ペイロードを検査するには、SMTP プリプロセッサを有効にする必要があります。`file_data` キーワードは、SMTP プリプロセッサが SMTP データを検出した場合に一致します。

- SMTP、POP、または IMAP トラフィック内のエンコードされた電子メール添付ファイル

  SMTP、POP、または IMAP トラフィック内の電子メール添付ファイルを検査するには、それぞれ SMTP、POP、または IMAP プリプロセッサを単独で、または任意に組み合わせて有効にする必要があります。その後、有効にしたプリプロセッサごとに、デコード対象のそれぞれの添付ファイル エンコード タイプをデコードするようプリプロセッサが設定されていることを確認する必要があります。プリプロセッサごとに設定可能な添付ファイル デコード オプションは、[Base64 復号の深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリ復号の深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted Printable 復号の深さ（Quoted-Printable Decoding Depth）]、および [UNIX 間復号の深さ（Unix-to-Unix Decoding Depth）] です。

  1 つのルール内で複数の `file_data` キーワードを使用できます。

関連トピック

HTTP Inspect プリプロセッサ, （1305 ページ）
サーバレベルの HTTP 正規化オプション, （1307 ページ）
SMTP プリプロセッサ, （1340 ページ）
IMAP プリプロセッサ, （1333 ページ）

pkt_data キーワード

`pkt_data` キーワードは、`content`、`byte_jump`、`byte_test`、`pcre` などの他のキーワードで使用可能な位置引数の参照として機能するポインタです。

正規化された FTP、Telnet、または SMTP トラフィックが検出された場合、`pkt_data` キーワードは、正規化されたパケット ペイロードの先頭を指します。その他のトラフィックが検出された場合、`pkt_data` キーワードは、未加工の TCP または UDP ペイロードの先頭を指します。

侵入ルールで検査するために、該当するトラフィックをシステムで正規化するには、次の正規化オプションを有効にする必要があります。

- 検査のために FTP トラフィックを正規化するには、FTP & Telnet プリプロセッサの [FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape codes within FTP commands）] オプションを有効にします。
- 検査のために Telnet トラフィックを正規化するには、FTP & Telnet プリプロセッサの Telnet の [正規化（Normalize）] オプションを有効にします。
- 検査のために SMTP トラフィックを正規化するには、SMTP プリプロセッサの [正規化（Normalize）] オプションを有効にします。

1 つのルール内で複数の `pkt_data` キーワードを使用できます。

関連トピック

クライアントレベルの FTP オプション, （1301 ページ）
Telnet オプション, （1296 ページ）
SMTP プリプロセッサのオプション, （1341 ページ）

base64_decode キーワードと base64_data キーワード

`base64_decode` キーワードと `base64_data` キーワードを組み合わせて使用すると、指定したデータを Base64 データとしてデコードおよび検査するようルール エンジンに指示できます。たとえば HTTP PUT および POST 要求内の Base64 エンコード HTTP 認証要求見出しと Base64 エンコード データを検査する場合に、これが役立つ可能性があります。

これらのキーワードは特に、HTTP 要求内の Base64 データをデコードして検査するうえで役立ちます。また、長いヘッダー行を複数行に拡張するために HTTP で使われるのと同じ方法でスペース文字やタブ文字を使用する SMTP などのプロトコルでも、これらを使用できます。この行拡張（折り返しとも言う）を使用するプロトコル内に行拡張が存在しない場合、後続スペース/タブを伴わない復帰または改行が出現した箇所で検査が終了します。

base64_decode

`base64_decode` キーワードは、パケット データを Base64 データとしてデコードするようルール エンジンに指示します。オプションの引数を使用すると、デコードするバイト数と、デコードを開始するデータ内の位置を指定できます。

`base64_decode` キーワードは 1 つのルール内で 1 回だけ使用可能です。また、少なくとも 1 つの `base64_data` キーワードのインスタンスの前にこれを配置する必要があります。

Base64データをデコードする前に、ルール エンジンは、複数行にわたって折り返された長いヘッダーを元どおりに広げます。ルール エンジンが次のいずれかに遭遇するとデコードが終了します。

- ヘッダー行の末尾
- デコード対象として指定されたバイト数

- パケットの末尾

次の表に、base64_decode キーワードで使用可能な引数の説明を示します。

表 *159*：*base64_decode* のオプション引数

引数	説明
Bytes	デコードするバイト数を指定します。これを指定しない場合、ヘッダー行の末尾またはパケットペイロード末尾のどちらかが先に出現するまでデコードが続行されます。ゼロ以外の正の値を指定できます。
Offset	パケット ペイロードの先頭を基準にしたオフセットを決定します。さらに Relative も指定した場合は、現在の検査位置を基準にしたオフセットを決定します。ゼロ以外の正の値を指定できます。
Relative	現在の検査位置を基準にして検査することを指定します。

base64_data

base64_data キーワードは、base64_decode キーワードを使ってデコードされた Base64 データを検査するための参照を提供します。base64_data キーワードは、デコードされた Base64 データの先頭から検査を開始するよう設定します。オプションで、content や byte_test などの他のキーワードで使用可能な位置引数を使用して、検査位置をさらに指定することもできます。

base64_decode キーワードを使用した後に base64_data キーワードを 1 回以上使用する必要があります。オプションで、base64_data を複数回使用して、デコードされた Base64 データの先頭に戻ることができます。

Base64 データを検査するときには、次の点に注意してください。

- 高速パターン マッチ機能は使用できません。
- 中間的な HTTP コンテンツ引数を使ってルール内で Base64 検査を中断する場合は、Base64 データをさらに検査する前に、別の base64_data キーワードをルールに挿入する必要があります。

関連トピック

概要：HTTP content および protected_content キーワードの引数, （1141 ページ）
content キーワードの高速パターン マッチ機能の引数, （1146 ページ）

第 55 章

侵入防御パフォーマンスの調整

以下のトピックでは、侵入防御のパフォーマンスを調整する方法について説明します。

侵入防御のパフォーマンス チューニングについて

Cisco では、侵入行為のトラフィックを分析する際のシステムのパフォーマンスを向上するための機能を提供しています。次の操作を実行できます。

- イベントキューで許可するパケット数を指定できます。ストリーム再構成の前後に、より大きなストリームに再構築されるパケットのインスペクションを有効または無効にできます。
- パケットペイロードの内容を検査するための侵入ルールで使用される PCRE のデフォルトの一致および再帰の制限をオーバーライドできます。
- 複数のイベントが生成された場合にパケットまたはパケットストリームごとに複数のイベントをルールエンジンがログに記録するようにして、レポートされるイベント以外の情報も収集できます。
- デバイスの遅延をパケットおよびルール遅延しきい値構成の許容レベルで保持する必要性とセキュリティのバランスを保つことができます。

- デバイスがそのパフォーマンスをモニタおよび報告する動作に関する基本的なパラメータを設定できます。システムがデバイスのパフォーマンス統計情報を更新する間隔を指定できます。

これらのパフォーマンス設定は、各アクセスコントロールポリシーごとに設定し、その設定はその親のアクセスコントロールポリシーによって呼び出されるすべての侵入ポリシーに適用されます。

侵入に対するパターン一致の制限

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

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [パフォーマンス設定（Performance Settings）] の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 3 [パフォーマンス設定（Performance Settings）] ポップアップ ウィンドウ内の [パターン一致の制限（Pattern Matching Limits）] タブをクリックします。

ステップ 4 [パケットごとに分析するパターン状態の最大値（Maximum Pattern States to Analyze Per Packet）] フィールドに、キューに含めるイベントの最大数の値を入力します。

ステップ 5 ストリーム再構成の前後で、データのより大きなストリームに再構築されるパケットのインスペクションを無効にするには、[今後の再構成の対象となるトラフィックでコンテンツチェックを無効にする（Disable Content Checks on Traffic Subject to Future Reassembly）] チェックボックスをオンにします。再構成の前後の検査はより多くの処理オーバーヘッドを必要とするため、パフォーマンスが低下する可能性があります。

ステップ 6 [OK] をクリックします。

ステップ 7 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

正規表現による侵入ルールのオーバーライドの制限

デフォルトの正規表現の制限によってパフォーマンスの最低レベルが確保されます。これらの制限をオーバーライドすると、セキュリティが向上する可能性がありますが、非効率的な正規表現に対してパケット評価を許可することで、パフォーマンスが著しく影響を受ける可能性もあります。

注意 非効率的なパターンの影響に関する知識があり、侵入ルールの作成経験が豊富であるユーザ以外は、デフォルトの PCRE の制限をオーバーライドしないでください。

表 *160*：正規表現の制約オプション

オプション	説明
検索結果の制限状態（Match Limit State）	[制限に合わせる（Match Limit）] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [デフォルト（Default）] を選択して、[制限に合わせる（Match Limit）] に設定した値を使用する • [無制限（Unlimited）] を選択して、無制限の数の試行を許可する • [カスタム（Custom）] を選択して、[制限に合わせる（Match Limit）] に対して 1 以上の制限を指定するか、または PCRE の一致の評価を完全に無効化するために 0 を指定する
制限に合わせる（Match Limit）	PCRE 正規表現で定義されたパターンに一致することを試行する回数を指定します。
検索結果の再起制限状態（Match Recursion Limit State）	[再起制限に合わせる（Match Recursion Limit）] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [デフォルト（Default）] を選択して、[再起制限に合わせる（Match Recursion Limit）] に設定した値を使用する • [無制限（Unlimited）] を選択して、無制限の数の再帰を許可する • [カスタム（Custom）] を選択して、[再起制限に合わせる（Match Recursion Limit）] に対して 1 以上の制限を指定するか、または PCRE の再帰を完全に無効化するために 0 を指定する [再起制限に合わせる（Match Recursion Limit）] が意味を持つためには、[制限に合わせる（Match Limit）] よりも小さい必要があることに注意してください。

オプション	説明
再起制限に合わせる（Match Recursion Limit）	パケット ペイロードに対して PCRE 正規表現を評価する際の再帰数を指定します。

侵入ルールの正規表現制限のオーバーライド

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

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [パフォーマンス設定（Performance Settings）]の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 3 [パフォーマンス設定（Performance Settings）] ポップアップ ウィンドウ内の [正規表現の制限（Regular Expression Limits）] タブをクリックします。

ステップ 4 正規表現による侵入ルールのオーバーライドの制限, （1243 ページ） に示したオプションを変更できます。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ） を参照してください。

パケットごとの侵入イベント生成の制限

侵入ルール エンジンがルールに対してトラフィックを評価する場合、特定のパケットまたはパケット ストリームに生成されたイベントをイベント キューに配置し、キュー内の上位のイベント

をユーザインターフェイスに報告します。侵入イベントロギングの制限を設定する場合、キュー内に配置可能なイベントの数および記録されるイベントの数を指定できます。また、キュー内のイベントの順序を決定する条件を選択できます。

表 *161*：侵入イベント ロギング制限のオプション

オプション	説明
パケットごとに保存されるイベントの最大数（Maximum Events Stored Per Packet）	特定のパケットまたはパケット ストリームに対して保存できるイベントの最大数。
パケットごとにログに記録されるイベントの最大数（Maximum Events Logged Per Packet）	特定のパケットまたはパケット ストリームに対して記録されるイベントの数。これは、[パケットごとに保存されるイベントの最大数（Maximum Events Stored Per Packet）] 値を超えてはいけません。
イベント ロギングの順位決定の基準（Prioritize Event Logging By）	イベント キュー内のイベントの順序を決定するために使用する値。最上位のイベントがユーザ インターフェイスから報告されます。次の中から選択できます。 • `priority`。イベントの優先順位によってキュー内のイベントを並べ替えます。 • `content_length`。最も長い識別コンテンツの一致によってイベントを並べ替えます。イベントがコンテンツ長によって並べ替えられる場合、ルールイベントは常にデコーダイベントおよびプリプロセッサイベントよりも優先されます。

パケットごとに生成される侵入イベントの制限

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

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [パフォーマンス設定（Performance Settings）] の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 3 [パフォーマンス設定（Performance Settings）] ポップアップ ウィンドウ内の [侵入イベントのログ制限（Intrusion Event Logging Limits）] タブをクリックします。

ステップ 4 パケットごとの侵入イベント生成の制限, （1244 ページ） に示したオプションを変更できます。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

パケットおよび侵入ルールの遅延しきい値構成

各アクセスコントロールポリシーには、しきい値を使用してパケットとルールの処理パフォーマンスを管理する、遅延ベースの設定があります。

パケット遅延しきい値構成は、該当するデコーダ、プリプロセッサ、およびルールによるパケット処理の総経過時間を測定し、処理時間が設定可能なしきい値を超えるとパケットのインスペクションを終了します。

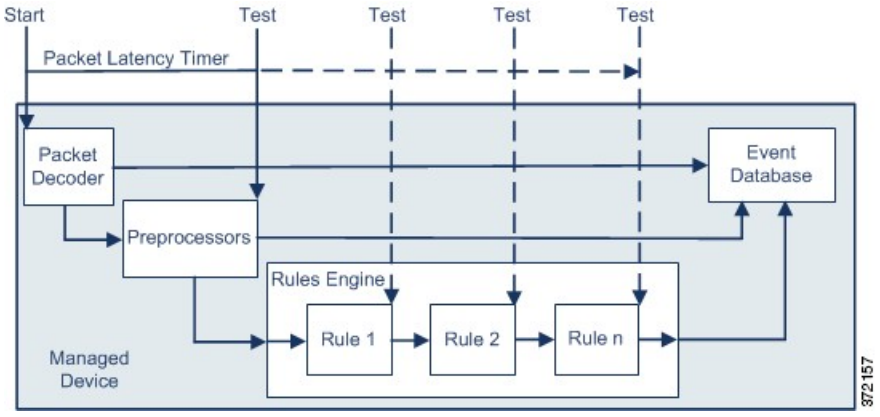
ルール遅延しきい値構成は、各ルールが個別のパケットの処理に費やした時間を測定し、処理時間が遅延しきい値ルールをある回数（設定可能）連続して超えた場合は、そのルールに違反した処理を、関連するルールのグループとともに指定された期間中断し、中断期間終了後にルールを回復します。

パケット遅延しきい値構成

パケット遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値はソフトウェアベースの遅延の実装であり、厳密なタイミングを適用するわけではありません。

遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。ただし、パケット遅延しきい値構成では、セキュリティと接続性のバランスを取るために使用可能なツールが用意されています。

デコーダの処理の開始時に各パケットのタイマーが起動します。タイミングは、パケットのすべての処理が終了するか、または処理時間がタイミングテストポイントでしきい値を超えるまで継続します。



上の図に示すように、パケット遅延タイミングは次のテスト ポイントでテストされます。

- すべてのデコーダおよびプリプロセッサの処理の完了後、ルールの処理が開始される前
- 各ルールによる処理の後

処理時間が任意のテスト ポイントでしきい値を超えると、パケットの検査は停止します。

ヒント　パケットの合計処理時間にルーチン TCP ストリームまたは IP フラグメント再構成の時間は含まれません。

パケット遅延しきい値構成は、パケットを処理するデコーダ、プリプロセッサ、またはルールによってトリガーされるイベントに影響を与えません。該当するデコーダ、プリプロセッサ、またはルールは、パケットが完全に処理されるか、または遅延しきい値を超えたためにパケット処理が終了されるか、どちらか先に発生した時点まで通常通りトリガーされます。廃棄ルールがインライン展開の侵入を検知すると、その廃棄ルールがイベントをトリガーし、パケットは廃棄されます。

（注）　パケット遅延しきい値違反のためにパケットの処理が終了した後は、ルールに対してパケットは評価されません。イベントを引き起こす可能性があったルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

パケット遅延のしきい値は、パッシブおよびインライン展開の両方でシステムのパフォーマンスを向上させ、インライン展開では過度の処理時間を必要とするパケットの検査を停止することにより遅延を低減できます。これらのパフォーマンス上のメリットは、以下のような場合にもたらされます。

- パッシブ展開およびインライン展開の両方で、複数のルールによるパケットの順次検査に長時間かかる場合

- インライン展開で、ユーザが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット処理を遅らせる場合

パッシブ展開では、パケットの処理を停止しても、処理が単に次のパケットに移るだけで、ネットワーク パフォーマンスの回復につながらない可能性があります。

パケット遅延しきい値構成の注意事項

表 *162*：パケット遅延しきい値構成オプション

オプション	説明
しきい値（マイクロ秒）（Threshold (microseconds)）	パケットのインスペクションが終了する時間をマイクロ秒単位で指定します。

ルール 134:3 を有効にして、パケット遅延しきい値を超えたためにシステムがパケットのインスペクションを終了する場合に イベントを生成し、インライン展開では、違反パケットをドロップします。 できます。詳細については、侵入ルールの状態オプション，（1062 ページ）を参照してください。

システム パフォーマンスおよびパケット遅延の測定に影響する要因は、CPU 速度、データ レート、パケットサイズ、プロトコルタイプなど多数あります。このためシスコは、ユーザ独自の計算によってご自身のネットワーク環境に合った設定を行うまで、次の表のしきい値設定を使用することを推奨します。

表 *163*：最小のパケット遅延しきい値設定

データ レート	最小しきい値設定（マイクロ秒）
1 Gbps	100
100 Mbps	250
5 Mbps	[1000]

独自の設定を計算する場合は、次の項目を決定します。

- 1 秒あたりの平均パケット数
- 1 パケットあたりの平均マイクロ秒数

パケット インスペクションを不必要に中断することがないように、ネットワークの 1 パケットあたりの平均マイクロ秒数に重要な安全係数を乗算します。

たとえば、シスコは 1 ギガビット環境で 100 マイクロ秒の最小パケット遅延しきい値を推奨しています。この最小推奨値は、1 秒あたり平均 250,000 パケットを示すテスト データに基づいてい

ます。これは、1 マイクロ秒あたり 0.25 パケット、言い換えると 1 パケットあたり 4 マイクロ秒に相当します。25 倍すると推奨最小しきい値の 100 マイクロ秒が得られます。

パケット遅延しきい値の設定

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

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 3 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] ポップアップ ウィンドウで [パケット処理（Packet Handling）] タブをクリックします。

ステップ 4 推奨される最小しきい値の設定については、パケット遅延しきい値構成の注意事項, （1248 ページ）を参照してください。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ルール遅延しきい値構成

ルール遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値はソフトウェアベースの遅延の実装であり、厳密なタイミングを適用するわけではありません。

遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。ただし、ルール遅延しきい値構成では、セキュリティと接続性のバランスを取るために使用可能なツールが用意されています。

パケットがルールのグループに対して処理されるたびに、タイマーが処理時間を測定します。ルール処理時間が指定されたルール遅延しきい値を超えると、システムでカウンタが増加します。連続したしきい値違反の数が指定した数に達すると、システムは次のアクションを実行します。

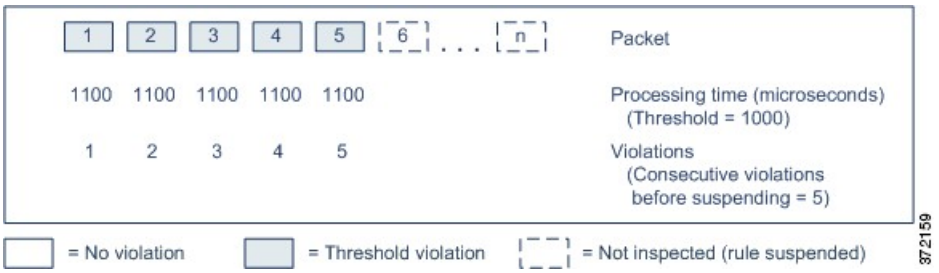
- 指定された時間、ルールを一時停止する
- ルールが一時停止されたことを示すイベントをトリガーとして使用する
- 一時停止期間が過ぎたらルールを再度有効にする
- ルールが再び有効になったことを示すイベントをトリガーとして使用する

ルールのグループが一時停止しているか、またはルール違反が連続していない場合は、カウンタがゼロになります。ルールを一時停止する前に連続する違反の一部を許可することにより、パフォーマンスへの影響がわずかであると考えられる散発的なルール違反を無視し、繰り返しルール遅延しきい値を超えるルールのより重大な影響に焦点を当てることができます。

次の例は、ルールが一時停止にならない、5 つの連続したルール処理時間を示します。

上の例で、最初の 3 個の各パケットの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反し、違反カウンタは各違反のたびに増加します。4 個目のパケット処理はしきい値に違反しないので、違反カウンタはゼロにリセットされます。5 個目のパケットはしきい値に違反し、違反カウンタは 1 から再開します。

次の例は、ルールが一時停止になる、5 つの連続したルール処理時間を示します。



2 番目の例で、5 個のパケットのそれぞれの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反します。各パケットの 1100 マイクロ秒というルール処理時間が指定された連続する 5 回の違反に対する 1000 マイクロ秒というしきい値に違反するため、ルールのグループは一時停止されます。図中のパケット 6 から n で表される後続のパケットは、一時停止期間が経過するまで、一時停止されたルールに対して検査されません。ルールが再有効化された後にさらにパケットが発生すると、違反カウンタはゼロから再開されます。

ルール遅延しきい値構成は、パケットを処理するルールによってトリガーされる侵入イベントに影響を及ぼしません。ルール処理時間がしきい値を超えるかどうかにかかわらず、パケット内で検出されるすべての侵入に対して、ルールはイベントをトリガーします。侵入を検知するルールがインライン展開の廃棄ルールである場合、パケットは廃棄されます。廃棄ルールがパケット内で侵入を検出し、その結果ルールが一時停止されると、廃棄ルールは侵入イベントをトリガーし、パケットは廃棄され、そのルールと関連するすべてのルールが一時停止されます。

（注） パケットは一時停止されたルールに対して評価されません。イベントを引き起こす可能性があった一時停止ルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

ルール遅延しきい値構成は、パッシブとインラインの両方の展開でシステムのパフォーマンスを向上することができます。また、パケットの処理に最も多くの時間を必要とするルールを一時停止することで、インライン展開の遅延を減らすことができます。設定可能な時間が過ぎるまで、パケットは一時停止されたルールに対して再度評価されず、過負荷のデバイスに回復の時間が与えられます。これらのパフォーマンス上のメリットは、以下のような場合にもたらされます。

- 短期間で作成され、ほとんどテストされていないルールが過剰な処理時間を必要とする場合
- ユーザが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット インスペクションを遅らせる場合

ルール遅延しきい値構成の注記

ルール遅延しきい値、一時停止されるルールの一時停止時間、ルールを一時停止する前に発生する必要がある連続したしきい値違反の回数の変更を行うことができます。

ルールによるパケット処理時間が、[ルール停止前の連続しきい値違反（Consecutive Threshold Violations Before Suspending Rule）] で指定された回数連続して [しきい値（Threshold）] を超えると、ルール遅延しきい値構成は [停止時間（Suspension Time）] で指定された時間、ルールを一時停止します。

ルール 134:1 を有効にして、ルールが一時停止されるときにイベントを生成できます。また、ルール 134:2 を有効にして、一時停止されたルールが有効化されるときにイベントを生成できます。侵入ルールの状態オプション，（1062 ページ）を参照してください。

表 *164*：ルール遅延しきい値構成のオプション

オプション	説明
しきい値（Threshold）	ルールがパケットを検査する際に超えることができない時間をマイクロ秒単位で指定します。

オプション	説明
ルール停止前の連続しきい値違反（Consecutive Threshold Violations Before Suspending Rule）	ルールが一時停止される前に、ルールによるパケットの検査時間が [しきい値（Threshold）] で設定された時間を超えることができる、連続した回数を指定します。
停止時間（Suspension Time）	ルールのグループを一時停止する秒数を指定します。

システムパフォーマンスの測定に影響する要因は、CPU速度、データ レート、パケットサイズ、プロトコル タイプなど多数あります。このためシスコは、ユーザ独自の計算によってご自身のネットワーク環境に合った設定を行うまで、次の表のしきい値設定を使用することを推奨します。

表 *165*：最小のルール遅延しきい値設定

データ レート	最小しきい値設定（マイクロ秒）
1 Gbps	500
100 Mbps	1250
5 Mbps	[5000]

独自の設定を計算する場合は、次の項目を決定します。

- 1 秒あたりの平均パケット数
- 1 パケットあたりの平均マイクロ秒数

ルールを不必要に一時停止することがないように、ネットワークの 1 パケットあたりの平均マイクロ秒数に重要な安全係数を乗算します。

ルール遅延しきい値の設定

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

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 3 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] ポップアップ ウィンドウで [ルール処理（Rule Handling）] タブをクリックします。

ステップ 4 ルール遅延しきい値構成の注記, （1251 ページ）の任意のオプションを設定できます。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- イベントを生成するには、遅延ルール（134:1 と 134:2）を有効にします。詳細については、侵入ルールの状態オプション, （1062 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

侵入パフォーマンス統計情報のロギング設定

[サンプル時間（秒）（Sample time (seconds)）] と [パケットの最小数（Minimum number of packets）]

パフォーマンス統計情報の各更新の間で指定した秒数が経過すると、システムは指定したパケット数を分析したかを検証します。分析していた場合、システムはパフォーマンス統計情報を更新します。それ以外の場合、システムは指定したパケット数を分析するまで待機します。

トラブルシューティング オプション：[ログ セッション/プロトコル分布（Log Session/Protocol Distribution）]

トラブルシューティングの電話中に、プロトコル分布、パケット長、およびポートの統計情報のログを取るようにサポートから依頼される場合があります。

注意 サポートによって指示された場合を除き、[ログセッション/プロトコル分布（Log Session/Protocol Distribution）] を有効にしないでください。注：[ログ セッション/プロトコル分布（Log Session/Protocol Distribution）] の有効化または無効化 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

トラブルシューティング オプション：[概要（Summary）]

トラブルシューティングの電話中に、Snort プロセスのシャットダウンまたは再起動時に限り、パフォーマンス統計情報を計算するようにシステムを設定するようにサポートから依頼される場合があります。このオプションを有効にするには、[ログ セッション/プロトコル分布（Log Session/Protocol Distribution）] トラブルシューティング オプションも有効にする必要があります。

注意 サポートから指示された場合を除き、[概要（Summary）] を有効にしないでください。

侵入パフォーマンス統計情報のロギングの設定

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

手順

ステップ 1 アクセス コントロール ポリシー エディタで [詳細（Advanced）] タブをクリックし、[パフォーマンス設定（Performance Settings）] の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 2 表示されるポップアップ ウィンドウの [パフォーマンス統計情報（Performance Statistics）] タブをクリックします。

ステップ 3 前述のように、[サンプル時間（Sample time）] または [パケットの最小数（Minimum number of packets）] を変更します。

ステップ 4 任意で、サポートによって求められた場合にのみ、[トラブルシューティング オプション（Troubleshoot Options）] セクションを展開し、そのオプションを変更します。

注意 [ログ セッション/プロトコル配布（Log Session/Protocol Distribution）] を有効にするか、無効にする 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

ステップ 5 [OK] をクリック

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 XV 部

高度なネットワーク分析と前処理

第 56 章

ネットワーク分析/侵入ポリシーのための高度なアクセス制御の設定

以下のトピックでは、ネットワーク分析ポリシーと侵入ポリシー用の高度な設定を行う手順を示します。

ネットワーク分析および侵入ポリシーのアクセスコントロールの詳細設定について

アクセスコントロールポリシーにおける詳細設定の多くは、設定のために特定の専門知識を要する侵入検知設定と予防設定を制御します。通常、詳細設定はほとんど、あるいはまったく変更する必要がありません。詳細設定は導入環境ごとに異なります。

デフォルトの侵入ポリシー

各アクセスコントロールポリシーは、システムがトラフィックを検査する方法を正確に決定する前に、デフォルトの侵入ポリシーを使用してそのトラフィックを最初に検査します。これは、場合によってシステムがトラフィックを処理するアクセスコントロールルール（存在する場合）を決定する前に、接続の最初の数パケットを処理し**通過を許可する**必要があるため必要となります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。デフォルトでは、デフォルトの侵入ポリシーでデフォルトの変数セットが使用されます。

システムはクライアントとサーバの間で接続が完全に確立される前にアプリケーションを識別したり URL をフィルタ処理することはできないので、デフォルトの侵入ポリシーは、アプリケー

ション制御およびURLフィルタリングを実行する場合に特に有用です。たとえば、パケットがアプリケーションまたはURL条件を持つアクセス コントロール ルールのその他のすべての条件に一致する場合、そのパケットと後続のパケットは、接続が確立されてアプリケーションまたはURLの識別が完了するまで通過することを許可されます。通常は3～5パケットです。

システムはこれらの許可されたパケットをデフォルトの侵入ポリシーで検査し、これによってイベントを生成したり、インラインで配置されている場合は、悪意のあるトラフィックをブロックできます。システムが接続を処理する必要があるアクセスコントロールルールまたはデフォルトアクションを識別した後、接続内の残りのパケットが適宜処理され検査されます。

アクセスコントロールポリシーを作成する場合、そのデフォルトの侵入ポリシーは**最初に**選択したデフォルトアクションによって異なります。アクセスコントロールの初期のデフォルト侵入ポリシーは次のとおりです。

- [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）]（システムによって提供されるポリシー）は、最初に [侵入防御（Intrusion Prevention）] デフォルト アクションを選択した場合のアクセス コントロール ポリシーのデフォルトの侵入ポリシーです。
- 最初に [すべてのトラフィックをブロック（Block all traffic）] または [ネットワーク検出（Network Discovery）] デフォルト アクションを選択した場合、アクセス コントロール ポリシーのデフォルトの侵入ポリシーは No Rules Active になります。このオプションを選択すると、前述の許可されたパケットでの侵入インスペクションが無効になりますが、侵入データが必要なければ、パフォーマンスを向上できます。

（注） （たとえば、検出専用の導入において）侵入インスペクションを実行していない場合は、デフォルトの侵入ポリシーとして No Rules Active ポリシーを保持してください。

アクセス コントロール ポリシーを作成した後にデフォルト アクションを変更する場合、デフォルトの侵入ポリシーは自動的には変更され**ません**。手動で変更するには、アクセス コントロール ポリシーの詳細オプションを使用します。

システムによって作成されたポリシーまたはユーザが作成したポリシーを選択できます。

（注） 最初に一致したネットワーク分析ルールに関連付けられているネットワーク分析ポリシーが、デフォルトの侵入ポリシーに対してトラフィックを前処理します。ネットワーク分析ルールがない場合、あるいはどのルールも一致しない場合は、デフォルトのネットワーク分析ポリシーが使用されます。

デフォルトの侵入ポリシーの設定

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

注意 アクセス コントロール ポリシーによって使用される侵入ポリシーの総数の変更 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作，（326 ページ）を参照してください。 現在使用されていない侵入ポリシーを追加するか、侵入ポリシーの最後のインスタンスを削除することで、侵入ポリシーの総数を変更します。アクセス コントロール ルールで侵入ポリシーをデフォルトのアクションまたはデフォルトの侵入ポリシーとして使用できます。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細設定（Advanced）] タブをクリックし、[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] セクションの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 2 [アクセス制御ルールが決定される前に使用されている侵入ポリシー（ntrusion Policy used before Access Control rule is determined）] ドロップダウン リストから、侵入ポリシーを選択します。

ユーザが作成したポリシーを選択した場合は、編集アイコン（）をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

ステップ 3 必要に応じて、[侵入ポリシーの変数セット（Intrusion Policy Variable Set）] ドロップダウン リストから別の変数セットを選択します。変数セットの横にある編集アイコン（）を選択して、変数セットを作成および編集することもできます。変数セットを変更しない場合、システムはデフォルトのセットを使用します。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ネットワーク分析プロファイルの詳細設定

ネットワーク分析ポリシーは、特に侵入の試みの前兆となるかもしれない異常トラフィックに対し、そのトラフィックがさらに評価されるようにトラフィックをデコードおよび前処理する方法を制御します。トラフィックの前処理は、セキュリティ インテリジェンスのブラックリスト登録およびトラフィックの復号化の後、侵入ポリシーによるパケット インスペクションの前に行われます。デフォルトでは、システム提供の [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] ネットワーク分析ポリシーが、デフォルト ネットワーク分析ポリシーです。

ヒント　システムによって提供される [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] ネットワーク分析ポリシーおよび [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] 侵入ポリシーは共に機能し、侵入ルールの更新の際に両方とも更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。

前処理を調整する簡単な方法は、カスタム ネットワーク分析ポリシーを作成し、それをデフォルトとして使用することです。複雑な環境での高度なユーザの場合は、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを別々に前処理するように調整することができます。さらに、トラフィックのセキュリティ ゾーン、ネットワーク、または VLAN に応じて前処理が制御されるようにこれらのポリシーを設定できます。

これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。ネットワーク分析ルールは、これらの条件に一致するトラフィックを前処理する方法を指定する設定および条件の単純なセットにすぎません。既存のアクセス コントロール ポリシーの詳細オプションでネットワーク分析ルールを作成および編集します。各ルールは 1 つのポリシーにのみ属します。

各ルールに含まれる内容は、次のとおりです。

- 一連のルール条件。前処理の対象となる特定のトラフィックを識別します
- 関連付けられたネットワーク分析ポリシー。すべてのルールの条件を満たすトラフィックを前処理するために使用できます

システムがトラフィックを前処理するときに、パケットはルール番号の上位から下位の順序でネットワーク分析ルールに照合されます。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

デフォルトのネットワーク分析ポリシーの設定

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

システムによって作成されたポリシーまたはユーザが作成したポリシーを選択できます。

（注） プリプロセッサを無効にしているが、システムは有効になっている侵入ルールまたはプリプロセッサ ルールと照合して前処理されたパケットを評価する必要がある場合、システムはプリプロセッサを自動的に有効にして使用します。しかし、ネットワーク分析ポリシー Web インターフェイスでは無効のままです。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。前処理および侵入インスペクションは密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーが互いに補完することを許可する場合は慎重になる**必要があります**。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細設定（Advanced）] タブをクリックし、[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] セクションの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 2 [デフォルトのネットワーク分析ポリシー（Default Network Analysis Policy）] ドロップダウンリストから、デフォルトのネットワーク分析ポリシーを選択します。

ユーザが作成したポリシーを選択した場合は、編集アイコン（）をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

注意 アクセス コントロール ポリシーによって使用されるネットワーク分析ポリシーの総数を変更すると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326ページ）を参照してください。現在使用されていないポリシーを追加するか、ネットワーク分析ポリシーの最後のインスタンスを削除することで、ネットワーク分析ポリシーの総数を変更します。ネットワーク分析ポリシーは、ネットワーク分析ルールと一緒に使用することもできれば、デフォルトのネットワーク分析ポリシーとして使用することもできます。

ステップ 3 [OK] をクリックします。

ステップ 4 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ネットワーク分析ルール

アクセスコントロールポリシーの詳細設定で、ネットワーク分析ルールを使用してネットワークトラフィックへの前処理設定を調整できます。

ネットワーク分析ルールには 1 から番号が付けられます。システムがトラフィックを前処理するときに、パケットはルール番号の昇順で上から順にネットワーク分析ルールに照合され、すべてのルールの条件が一致する最初のルールに従ってトラフィックが前処理されます。

ルールには、ゾーン、ネットワーク、VLAN タグの条件を追加できます。ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。たとえば、ネットワーク条件を持つがゾーン条件を持たないルールは、その入力または出力インターフェイスに関係なく、送信元または宛先 IP アドレスに基づいてトラフィックを評価します。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

ネットワーク分析ルールの設定

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

手順

ステップ 1 アクセス コントロール ポリシー エディタで [詳細（Advanced）] タブをクリックし、[ネットワーク分析（Network Analysis）] および [侵入ポリシー（Intrusion Policies）] セクションの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ヒント [ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックし、既存のカスタム ネットワーク分析ポリシーを表示および編集します。

ステップ 2 [ネットワーク分析ルール（Network Analysis Rules）] の横にある、所持しているカスタム ルールの数を示したステートメントをクリックします。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 追加する条件に対応するタブをクリックして、ルールの条件を設定します。ルール条件タイプ, （341 ページ）を参照してください。

ステップ 5 [ネットワーク分析（Network Analysis）] タブをクリックし、このルールに一致するトラフィックの前処理に使用する [ネットワーク分析ポリシー（Network Analysis Policy）] を選択します。

編集アイコン（  ）をクリックして、新しいウィンドウでカスタム ポリシーを編集します。システムによって提供されたポリシーは編集できません。

注意 アクセス コントロール ポリシーによって使用されるネットワーク分析ポリシーの総数を変更すると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。現在使用されていないポリシーを追加するか、ネットワーク分析ポリシーの最後のインスタンスを削除することで、ネットワーク分析ポリシーの総数を変更します。ネットワーク分析ポリシーは、ネットワーク分析ルールと一緒に使用することもできれば、デフォルトのネットワーク分析ポリシーとして使用することもできます。

ステップ 6 [追加（Add）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ネットワーク分析ルールの管理

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

ネットワーク分析ルールは、これらの条件に一致するトラフィックを前処理する方法を指定する設定および条件の単純なセットにすぎません。既存のアクセスコントロールポリシーの詳細オプションでネットワーク分析ルールを作成および編集します。各ルールは 1 つのポリシーにのみ属します。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックして、[侵入およびネットワーク分析ポリシー（Intrusion and Network Analysis Policies）] セクションの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 2 [ネットワーク分析ルール（Network Analysis Rules）] の横にある、所持しているカスタム ルールの数を示したステートメントをクリックします。

ステップ 3 カスタム ルールを編集します。次の選択肢があります。

- ルールの条件を編集する、またはルールによって呼び出されるネットワーク分析ポリシーを変更するには、ルールの横にある編集アイコン（）をクリックします。
- ルールの評価順序を変更するには、ルールをクリックして正しい位置にドラッグします。複数のルールを選択するには、Shift キーおよび Ctrl キーを使用します。
- ルールを削除するには、ルールの横にある削除アイコン（）をクリックします。

ヒント ルールを右クリックするとコンテキスト メニューが表示され、新しいネットワーク分析ルールの切り取り、コピー、貼り付け、編集、削除、および追加を実行できます。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

第 57 章

ネットワーク分析ポリシーの使用を開始するには

ここでは、ネットワーク分析ポリシーの使用を開始する方法について説明します。

ネットワーク分析ポリシーの基本

ネットワーク分析ポリシーは、多数のトラフィックの前処理オプションを制御し、アクセス コントロール ポリシーの詳細設定で呼び出されます。ネットワーク分析に関連する前処理は、Security Intelligence によるブラックリスト化や SSL 復号化の後、侵入またはファイル検査の開始前に実行されます。

デフォルトでは、システムは *Balanced Security and Connectivity* ネットワーク分析ポリシーを使用して、アクセス コントロール ポリシーによって処理されるすべてのトラフィックを前処理します。ただし、この前処理を実行するために別のデフォルトのネットワーク分析ポリシーを選択できます。便宜を図るため、システムによっていくつかの変更不可能なネットワーク分析ポリシーが提供されます。これらのポリシーは、Cisco Talos Security Intelligence and Research Group（Talos）によってセキュリティおよび接続の一定のバランスがとれるように調整されています。カスタム前処理設定を使用して、カスタム ネットワーク分析ポリシーを作成することもできます。

ヒント システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。ネットワーク分析ポリシーと侵入ポリシーが連動してトラフィックを検査します。

複数のカスタム ネットワーク分析ポリシーを作成し、それらに異なるトラフィックの前処理を割り当てることにより、特定のセキュリティ ゾーン、ネットワーク、VLAN 用に前処理オプションを調整できます。（ただし、ASA FirePOWER VLAN による前処理を制限することはできないことに注意してください）。

ネットワーク分析ポリシーの管理

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

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 ネットワーク分析ポリシーを管理します。

- [比較（Compare）]：[ポリシーの比較（Compare Policies）] をクリックします（ポリシーの比較, （331 ページ） を参照）。
- 作成：新しいネットワーク分析ポリシーを作成する場合は、[ポリシーの作成（Create Policy）] をクリックして、カスタム ネットワーク分析ポリシーの作成, （1269 ページ） で説明する手順を実行します。
- 削除：ネットワーク分析ポリシーを削除する場合は、削除アイコン（）をクリックして、ポリシーの削除を確認します。アクセス コントロール ポリシーが参照しているネットワーク分析ポリシーは削除できません。

  コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 展開：[展開（Deploy）] をクリックします（設定変更の導入, （320 ページ） を参照）。

- 編集:既存のネットワーク分析ポリシーを編集する場合は、編集アイコン（  ）をクリックして、ネットワーク分析ポリシーの設定とキャッシュされた変更, （1271 ページ）で説明する手順を実行します。

  代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- [レポート（Report）]：レポート アイコン（  ）をクリックします（現在のポリシー レポートの生成, （333 ページ） を参照）。

カスタム ネットワーク分析ポリシーの作成

新しいネットワーク分析ポリシーを作成するときは、一意の名前を付け、基本ポリシーを指定し、インライン モードを選択する必要があります。

基本ポリシーはネットワーク分析ポリシーのデフォルト設定を定義します。新しいポリシーの設定の変更は、基本ポリシーの設定を変更するのではなく、オーバーライドします。システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

ネットワーク分析ポリシーのインライン モードでは、プリプロセッサでトラフィックを変更（正規化）したりドロップしたりして、攻撃者が検出を回避する可能性を最小限にすることができます。パッシブな展開では、インラインモードに関係なく、システムはトラフィック フローに影響を与えることができないことに注意してください。

関連トピック

基本レイヤ, （1017 ページ）
インライン導入でのプリプロセッサによるトラフィックの変更, （1274 ページ）
カスタム ネットワーク分析ポリシーの作成, （1269 ページ）
ネットワーク分析ポリシーの編集, （1272 ページ）

カスタム ネットワーク分析ポリシーの作成

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

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。別のポリシー内に未保存の変更が存在する場合は、[ネットワーク分析ポリシー（Network Analysis Policy）] ページに戻るかどうか尋ねられたときに [キャンセル（Cancel）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力します。
マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 [基本ポリシー（Base Policy）] で最初の基本ポリシーを選択します。システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

ステップ 6 プリプロセッサがインライン導入でのトラフィックに影響するようにする場合は、[インライン モード（Inline Mode）] を有効化します。

ステップ 7 ポリシーを作成します。

- 新しいポリシーを作成して [ネットワーク分析ポリシー（Network Analysis Policy）] ページに戻るには、[ポリシーの作成（Create Policy）] をクリックします。新しいポリシーには基本ポリシーと同じ設定項目が含まれています。
- ポリシーを作成し、高度なネットワーク分析ポリシー エディタでそれを開いて編集するには、[ポリシーの作成と編集（Create and Edit Policy）] をクリックします。

関連トピック

カスタム ユーザ ロールの作成, （72 ページ）

ネットワーク分析ポリシーの管理

[ネットワーク分析ポリシー（Network Analysis Policy）] ページ（[ポリシー（Policies）] > [アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。、または[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。）で、現在のカスタム ネットワーク分析ポリシーを次の情報とともに確認できます。

- ポリシーが最後に変更された日時（ローカル時間）とそれを変更したユーザ

- プリプロセッサがトラフィックに影響を与えることを許可する [インライン モード（Inline Mode）] 設定が有効になっているかどうか
- どのアクセス コントロール ポリシーとデバイスが、ネットワーク分析ポリシーを使用してトラフィックを前処理しているか
- ポリシーに保存されていない変更があるかどうか、およびポリシーを現在編集している人（いれば）に関する情報

お客様が独自に作成するカスタムポリシーに加えて、システムは初期インラインポリシーと初期パッシブ ポリシーの 2 つのカスタム ポリシーを提供しています。これら 2 つのネットワーク分析ポリシーは、基本ポリシーとして「Balanced Security and Connectivity」ネットワーク分析ポリシーを使用します。両者の唯一の相違点はインラインモードの設定です。インラインポリシーではプリプロセッサによるトラフィックの影響が有効化され、パッシブ ポリシーでは無効化されています。これらのシステム付属のカスタム ポリシーは編集して使用できます。

ただし、Firepower システムのユーザ アカウントの権限が侵入ポリシーまたは修正侵入ポリシーに限定されている場合は、ネットワーク分析ポリシーに加えて、侵入ポリシーを作成して編集できます。

関連トピック

カスタム ネットワーク分析ポリシーの作成, （1269 ページ）
ネットワーク分析ポリシーの編集, （1272 ページ）

ネットワーク分析ポリシーの設定とキャッシュされた変更

新しいネットワーク分析ポリシーを作成すると、そのポリシーには基本ポリシーと同じ設定が付与されます。

ネットワーク分析ポリシーの調整時、特にプリプロセッサを無効化するときは、プリプロセッサおよび侵入ルールによっては、トラフィックを特定の方法で最初にデコードまたは前処理する必要があることに留意してください。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

（注） 前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な** タスクです。

システムは、ユーザごとに 1 つのネットワーク分析ポリシーをキャッシュします。ネットワーク分析ポリシーの編集中に、任意のメニューまたは別のページへの他のパスを選択した場合、変更内容はそのページを離れてもシステム キャッシュにとどまります。

関連トピック

ポリシーが侵入についてトラフィックを検査する仕組み, （996 ページ）

カスタム ポリシーの制限, （1007 ページ）

ネットワーク分析ポリシーの編集

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

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 設定するネットワーク分析ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ネットワーク分析ポリシーを編集します。

- 基本ポリシーの変更：基本ポリシーを変更するには、[ポリシー情報（Policy Information）] ページの [基本ポリシー（Base Policy）] ドロップダウン リストから、ポリシーを選択します。
- ポリシー階層の管理：ポリシー階層を管理するには、ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。
- プリプロセッサの変更：プリプロセッサの設定有効または無効にするか、あるいは編集するには、ナビゲーション パネルで [設定（Settings）] をクリックします。
- トラフィックの変更：プリプロセッサがトラフィックを変更またはドロップできるようにするには、[ポリシー情報（Policy Information）] ページで [インライン モード（Inline Mode）] チェックボックスをオンにします。

- 設定の表示：基本ポリシーの設定を表示するには、[ポリシー情報（Policy Information）] ページで [基本ポリシーの管理（Manage Base Policy）] をクリックします。

ステップ 4 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] を選択して、[変更を確定（Commit Changes）] をクリックします。変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次の作業

- プリプロセッサで イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、プリプロセッサのルールを有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

基本レイヤ, （1017 ページ）
ベースポリシーの変更, （1019 ページ）
ネットワーク分析ポリシーでのプリプロセッサの設定, （1273 ページ）
インライン導入でのプリプロセッサによるトラフィックの変更, （1274 ページ）
レイヤの管理, （1023 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

ネットワーク分析ポリシーでのプリプロセッサの設定

プリプロセッサ は、トラフィックを正規化し、プロトコルの異常を識別することで、トラフィックの詳細な検査に備えます。プリプロセッサは、ユーザが設定したプリプロセッサ オプションをパケットがトリガーしたときに、プリプロセッサ イベントを生成できます。デフォルトで有効になるプリプロセッサや、それぞれのデフォルト設定は、ネットワーク分析ポリシーの基本ポリシーに応じて決まります。

（注） 多くの場合、プリプロセッサの設定には特定の専門知識が必要で、通常は、ほとんどあるいはまったく変更を必要としません。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。

プリプロセッサの設定を変更するには、その設定とネットワークへの潜在的影響を理解する必要があります。

トランスポート/ネットワーク プリプロセッサの詳細設定は、アクセス コントロール ポリシーを展開するすべてのネットワーク、ゾーン、VLAN にグローバルに適用されることに注意してくだ

さい。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。

また、侵入ポリシーでは ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出する機密データ プリプロセッサを設定することにも注意してください。

関連トピック

DCE/RPC プリプロセッサ, （1278 ページ）
DNP3 プリプロセッサ, （1362 ページ）
DNS プリプロセッサ, （1291 ページ）
FTP/Telnet デコーダ, （1295 ページ）
GTP プリプロセッサ, （1331 ページ）
HTTP Inspect プリプロセッサ, （1305 ページ）
IMAP プリプロセッサ, （1333 ページ）
インライン正規化プリプロセッサ, （1371 ページ）
IP 最適化プリプロセッサ, （1379 ページ）
Modbus プリプロセッサ, （1359 ページ）
パケット デコーダ, （1385 ページ）
POP プリプロセッサ, （1337 ページ）
機密データ検出の基本, （1083 ページ）
SIP プリプロセッサ, （1325 ページ）
SMTP プリプロセッサ, （1340 ページ）
SSH プリプロセッサ, （1348 ページ）
SSL プリプロセッサ, （1352 ページ）
Sun RPC プリプロセッサ, （1323 ページ）
TCP ストリームの前処理, （1390 ページ）
UDP ストリームの前処理, （1402 ページ）
カスタム ポリシーの制限, （1007 ページ）

インライン導入でのプリプロセッサによるトラフィックの変更

インライン導入（つまり、ルーテッドインターフェイス、スイッチドインターフェイス、トランスペアレントインターフェイス、あるいはインラインインターフェイスのペアを使用して関連する設定をデバイスに展開する導入）では、一部のプリプロセッサがトラフィックを変更およびブロックできます。次に例を示します。

- インライン正規化プリプロセッサは、パケットを正規化し、他のプリプロセッサおよび侵入ルール エンジンで分析されるようにパケットを準備します。ユーザは、プリプロセッサの [これらの TCP オプションを許可（Allow These TCP Options）] と [回復不能な TCP ヘッダーの異常をブロック（Block Unresolvable TCP Header Anomalies）] オプションを使用して、特定のパケットをブロックすることもできます。
- システムは無効なチェックサムを持つパケットをドロップできます。

- システムはレート ベースの攻撃防御設定に一致するパケットをドロップできます。

ネットワーク分析ポリシーに設定したプリプロセッサがトラフィックに影響を与えるようにするには、プリプロセッサを有効にして正しく設定するとともに、管理対象デバイスをインラインで正しく展開する必要があります。最後に、ネットワーク分析ポリシーの[インライン モード（Inline Mode）] 設定を有効にする必要があります。

ネットワーク分析ポリシーの注記におけるプリプロセッサの設定

ネットワーク分析ポリシーのナビゲーション パネルで[設定（Settings）] を選択すると、ポリシーによりタイプ別のプリプロセッサがリストされます。[設定（Settings）] ページで、ネットワーク分析ポリシーのプリプロセッサを有効または無効にしたり、プリプロセッサの設定ページにアクセスしたりできます。

プリプロセッサを設定するには、それを有効にする必要があります。プリプロセッサを有効にすると、そのプリプロセッサに関する設定ページへのサブリンクがナビゲーション パネル内の [設定（Settings）] リンクの下に表示され、この設定ページへの [編集（Edit）] リンクが [設定（Settings）] ページのプリプロセッサの横に表示されます。

ヒント プリプロセッサの設定を基本ポリシーの設定に戻すには、プリプロセッサ設定ページで[デフォルトに戻す（Revert to Defaults）] をクリックします。プロンプトが表示されたら、復元することを確認します。

プリプロセッサを無効にすると、サブリンクと [編集（Edit）] リンクは表示されなくなりますが、設定は保持されます。特定の分析を実行するには、多くのプリプロセッサおよび侵入ルールで、トラフィックをまず特定の方法でデコードまたは前処理する必要があることに注意してください。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

実際にトラフィックを変更せずに、設定がインライン展開でどのように機能するかを評価する場合は、インライン モードを無効にできます。タップ モードでのパッシブ展開またはインライン展開では、インライン モード設定に関係なくシステムがトラフィックに影響を及ぼすことはありません。

（注） インライン モードを無効にすることで、侵入イベントのパフォーマンス統計グラフに影響を及ぼす可能性があります。インライン展開でインライン モードが有効の場合、侵入イベント パフォーマンス ページ（[概要（Overview）] > [概要（Summary）] > [侵入イベント パフォーマンス（Intrusion Event Performance）]）には、正規化し、ブロックされたパケットを示すグラフが表示されます。インライン モードが無効の場合、またはパッシブ展開である場合、多くのグラフによりシステムが正規化するか、またはドロップするトラフィックに関するデータが表示されます。

（注） インライン展開では、インライン モードを有効にし、[TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にして、インライン正規化プリプロセッサを設定することをお勧めします。パッシブ展開では、アダプティブ プロファイルを使用することをお勧めします。

関連トピック

トランスポート/ネットワーク プリプロセッサの詳細設定, （1366 ページ）
チェックサム検証, （1369 ページ）
インライン正規化プリプロセッサ, （1371 ページ）
チェックサム検証, （1369 ページ）
侵入イベントのパフォーマンス統計情報グラフの種類, （2007 ページ）

第 58 章

アプリケーション層プリプロセッサ

次のトピックでは、アプリケーション層プリプロセッサおよびその設定方法について説明します。

アプリケーション層のプリプロセッサの概要

アプリケーション層プロトコルにより、同一データをさまざまな方法で表すことができます。Firepower システムは、特定タイプのパケット データを侵入ルール エンジンが分析可能なフォーマットに正規化する、アプリケーション層プロトコル デコーダを提供しています。アプリケーション層プロトコルエンコードを正規化することにより、ルールエンジンでさまざまなデータ形式のパケットに同じコンテンツ関連ルールを効果的に適用し、有意な結果を得ることができます。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。

ほとんどの場合、侵入ルールで関連するプリプロセッサ ルールが有効になっていないと、プリプロセッサはイベントを生成しません。

DCE/RPC プリプロセッサ

DCE/RPC プロトコルにより、別々のネットワーク ホスト上のプロセスが、同一ホストに配置されている場合と同様に通信できます。通常、このようなプロセス間通信はホスト間で TCP および UDP 経由で転送されます。TCP 転送では、DCE/RPC が Windows Server Message Block（SMB）プロトコルまたは Samba でさらにカプセル化されることがあります。Samba は、Windows や UNIX/Linux 系のオペレーティング システムから構成される混合環境でプロセス間通信に使用されるオープンソースの SMB 実装です。また、ネットワーク上の Windows IIS Web サーバでは IIS RPC over HTTP が使用されることがあります。IIS RPC over HTTP は、プロキシ TCP により伝送される DCE/RPC トラフィックに、ファイアウォールを介して分散通信を提供します。

DCE/RPC プリプロセッサ オプションとその機能の説明には、Microsoft による DCE/RPC の実装である MSRPC が含まれることに注意してください。SMB のオプションと機能についての説明は、SMB と Samba の両方に当てはまります。

ほとんどの DCE/RPC エクスプロイトは、DCE/RPC サーバ（ネットワーク上の Windows または Samba が稼働している任意のホスト）を対象とした DCE/RPC クライアント要求で発生します。またエクスプロイトはサーバ応答でも発生することがあります。DCE/RPC プリプロセッサは、TCP、UDP、および SMB トランスポートでカプセル化された DCE/RPC 要求と応答を検出します。これには、RPC over HTTP バージョン 1 を使用して TCP により伝送される DCE/RPC も含まれます。プリプロセッサは DCE/RPC データ ストリームを分析し、DCE/RPC トラフィックにおける異常な動作と回避技術を検出します。また、SMB データ ストリームを分析し、異常な SMB 動作と回避技術を検出します。

IP 最適化プリプロセッサによる IP 最適化および TCP ストリーム プリプロセッサによる TCP ストリームの再構成に加えて、DCE/RPC プリプロセッサは、SMB のセグメント化解除と DCE/RPC の最適化も行います。

最後に、DCE/RPC プリプロセッサはルール エンジンで処理できるように DCE/RPC トラフィックを正規化します。

コネクションレス型およびコネクション型 DCE/RPC トラフィック

DCE/RPC メッセージは、2 種類の DCE/RPC Protocol Data Unit（PDU）の 1 つに準拠します。

コネクション型 DCE/RPC PDU プロトコル

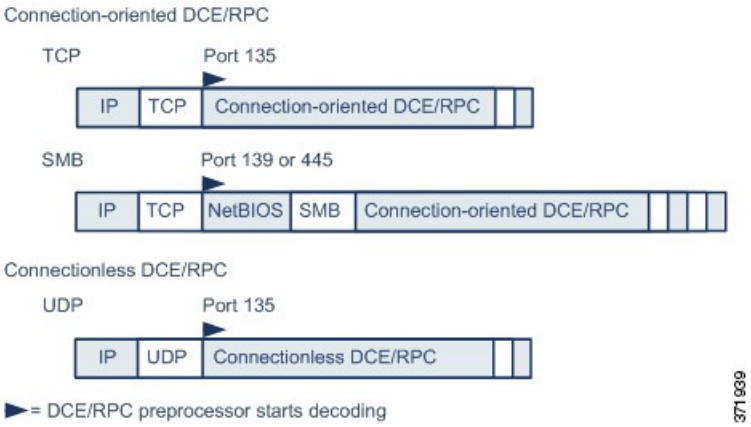
DCE/RPC プリプロセッサは、TCP、SMB、および RPC over HTTP トランスポートでコネクション型 DCE/RPC を検出します。

コネクションレス型 DCE/RPC PDU プロトコル

DCE/RPC プリプロセッサは、UDP トランスポートでコネクションレス型 DCE/RPC を検出します。

この 2 つの DCE/RPC PDU プロトコルには、それぞれ固有のヘッダーとデータ特性があります。たとえば、コネクション型 DCE/RPC のヘッダーの長さは通常は 24 バイトですが、コネクションレス型 DCE/RPC のヘッダーの長さは 80 バイト（固定）です。また、フラグメント化コネクションレス型 DCE/RPC のフラグメントの正しい順序は、コネクションレス型トランスポートでは処理できないため、代わりに、コネクションレス型 DCE/RPC ヘッダーの値によって維持する必要があります。これとは対照的に、コネクション型 DCE/RPC の正しいフラグメント順序はトランスポートプロトコルによって維持されます。DCE/RPC プリプロセッサは、これらや他のプロトコル固有の特性を使用して、両方のプロトコルで異常やその他の回避技術をモニタし、トラフィックをデコードおよび復号化してからルール エンジンに渡します。

次の図は、DCE/RPC プリプロセッサが各種トランスポートの DCE/RPC トラフィックの処理を開始するポイントを示します。



この図の次の点に注意してください。

- ウェルノウン TCP または UDP ポート 135 は、TCP および UDP トランスポートの DCE/RPC トラフィックを特定します。
- この図には RPC over HTTP は含まれていません。

  RPC over HTTP の場合、コネクション型 DCE/RPC は、図に示すように、HTTP を介した初期設定シーケンスの後、TCP 経由で直接伝送されます。
- DCE/RPC プリプロセッサは通常、NetBIOS セッション サービス用のウェルノウン TCP ポート 139 か、同様に実装されたウェルノウン Windows ポート 445 で SMB トラフィックを受信します。

  SMB には DCE/RPC 伝送以外にも多数の機能があるため、プリプロセッサは SMB トラフィックが DCE/RPC トラフィックを伝送しているかどうかをまず検査します。伝送していない場合は処理を停止し、伝送している場合は処理を続行します。
- IP によりすべての DCE/RPC トランスポートがカプセル化されます。

- TCP は、すべてのコネクション型 DCE/RPC を伝送します。
- UDP はコネクションレス型 DCE/RPC を伝送します。

DCE/RPC ターゲット ベース ポリシー

Windows および Samba の DCE/RPC の実装は大きく異なります。たとえば、Windows のすべてのバージョンは、DCE/RPC トラフィックの最適化時に最初のフラグメントの DCE/RPC コンテキスト ID を使用しますが、Samba のすべてのバージョンは、最後のフラグメントのコンテキスト ID を使用します。また、特定の関数呼び出しを識別するために、Windows Vista では最初のフラグメントの opnum（操作番号）ヘッダー フィールドを使用しますが、Samba とその他のすべてのバージョンの Windows では最後のフラグメントの opnum フィールドを使用します。

Windows と Samba の SMB の実装にも、大きな違いがあります。たとえば、Windows は名前付きパイプの操作時に SMB OPEN および READ コマンドを認識しますが、Samba はこれらのコマンドを認識しません。

DCE/RPC プリプロセッサを有効にすると、デフォルトのターゲットベース ポリシーが自動的に有効になります。必要に応じて、異なる Windows や Samba バージョンを実行する他のホストを対象としたターゲットベース ポリシーを追加できます。デフォルトのターゲットベース ポリシーは、別のターゲットベース ポリシーに含まれていないホストに適用されます。

各ターゲットベースのポリシーでは次の設定が可能です。

- 1 つ以上のトランスポートを有効にし、それぞれについて検出ポートを指定します。
- 自動検出ポートを有効にして指定します。
- 指定した 1 つ以上の共有 SMB リソースへの接続が試行された場合にそのことを検出するように、プリプロセッサを設定します。
- SMB トラフィックでファイルを検出し、検出されたファイルで指定されたバイト数を検査するように、プリプロセッサを設定します。
- SMB プロトコルの知識を持つユーザだけが変更すべき拡張オプションを変更できます。このオプションでは、連結された SMB AndX コマンドの数が指定された最大数を超えた場合にそのことを検出するようにプリプロセッサを設定します。

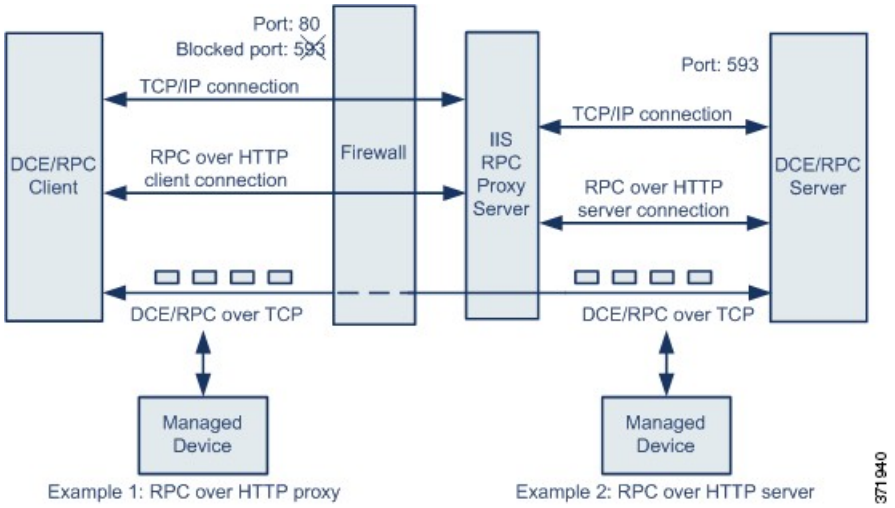
DCE/RPC プリプロセッサで SMB トラフィック ファイル検出を有効にするほかに、オプションでこれらのファイルをキャプチャしてブロックするか、またはダイナミック分析のために Cisco AMP クラウドに送信するように、ファイル ポリシーを設定できます。そのポリシー内で、[アクション（Action）] として [ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] を選択し、[アプリケーション プロトコル（Application Protocol）] として [任意（Any）] または [NetBIOS-ssn (SMB)] を選択して、ファイル ルールを作成する必要があります。

関連トピック

ファイル ポリシーの作成, （965 ページ）

RPC over HTTP トランスポート

Microsoft RPC over HTTP では、次の図に示すように、DCE/RPC トラフィックをトンネリングして、ファイアウォールを通過させることができます。DCE/RPC プリプロセッサは Microsoft RPC over HTTP バージョン 1 を検出します。



Microsoft IIS プロキシ サーバと DCE/RPC サーバは、同じホストまたは別々のホストにインストールできます。いずれの場合でも、個別のプロキシオプションとサーバオプションがあります。この図の次の点に注意してください。

- DCE/RPC サーバはポート 593 で DCE/RPC クライアント トラフィックをモニタしますが、ファイアウォールはこのポート 593 をブロックします。

  通常、ファイアウォールではデフォルトでポート 593 がブロックされます。

- RPC over HTTP は、ファイアウォールによって許可される可能性が高いウェルノウン HTTP ポート 80 を使用して、HTTP 経由で DCE/RPC を伝送します。

- 例 1 のように、DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間のトラフィックをモニタする場合は、[RPC over HTTP プロキシ（RPC over HTTP proxy）] オプションを選択します。

- 例 2 のように、Microsoft IIS RPC プロキシ サーバと DCE/RPC サーバが異なるホスト上にあり、デバイスが 2 つのサーバ間のトラフィックをモニタしている場合は、[RPC over HTTP サーバ（RPC over HTTP server）] オプションを選択します。

- RPC over HTTP により DCE/RPC クライアントとサーバ間でのプロキシ セットアップが完了した後、トラフィックは TCP を経由したコネクション型 DCE/RPC だけで構成されます。

DCE/RPC グローバル オプション

グローバル DCE/RPC プリプロセッサ オプションは、プリプロセッサの機能を制御します。[到達したメモリ容量（Memory Cap Reached）] および [SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] オプション以外のオプションを変更すると、パフォーマンスまたは検出

機能に悪影響を及ぼす可能性があります。プリプロセッサについて、またプリプロセッサと有効にされているDCE/RPCルールとの間の相互作用について十分に理解していない場合は、これらのオプションを変更しないでください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

最大フラグメント サイズ（Maximum Fragment Size）

[最適化の有効化（Enable Defragmentation）] が選択されている場合、DCE/RPC フラグメントの許容最大長を指定します。これよりも大きなフラグメントの場合、プリプロセッサは処理のためにフラグメントの一部を切り捨て、指定のサイズにしてから最適化を行いますが、実際のパケットは変更されません。空白フィールドの場合、このオプションは無効になります。

[最大フラグメント サイズ（Maximum Fragment Size）] オプションは、ルールが検出する必要がある深さと同じかそれ以上にしてください。

リアセンブリしきい値（Reassembly Threshold）

[最適化の有効化（Enable Defragmentation）] が選択されている場合、0 を指定するとこのオプションは無効になります。あるいは、フラグメント化されたDCE/RPCの最小バイト数を、該当する場合は、再構成されたパケットをルールエンジンに送信する前にキューに入れるセグメント化SMBのバイト数を指定します。低い値を指定すると、早期検出の可能性が高くなりますが、パフォーマンスに悪影響を及ぼす可能性があります。このオプションを有効にする場合は、パフォーマンスの影響をテストしておく必要があります。

[リアセンブリしきい値（Reassembly Threshold）] オプションは、ルールが検出する必要がある深さと同じかそれ以上にしてください。

最適化の有効化（Enable Defragmentation）

フラグメント化された DCE/RPC トラフィックを最適化するかどうかを指定します。無効にすると、プリプロセッサは引き続き異常を検出して DCE/RPC データをルール エンジンに送信しますが、フラグメント化された DCE/RPC データでのエクスプロイトを見落とすリスクがあります。

このオプションには、DCE/RPC トラフィックを最適化しないという柔軟性がありますが、ほとんどのDCE/RPCエクスプロイトでは、フラグメント化を利用してエクスプロイトを隠ぺいする試みが行われます。このオプションを無効にすると、ほとんどの既知のエクスプロイトがバイパスされ、検出漏れが大量に発生します。

到達したメモリ容量（Memory Cap Reached）

プリプロセッサに割り当てられた最大メモリ制限に達したか、またはこの制限を超過したことを検出します。最大メモリ制限に達したか、またはこの制限を超過した場合、プリプロセッサはメモリ キャップイベントを引き起こしたセッションに関連付けられているすべての保留データを解放し、セッションのそれ以降の部分を無視します。

ルール 133:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）

SMB `Session Setup AndX` 要求および応答に指定されている Windows または Samba のバージョンを検出します。検出されたバージョンが、[ポリシー（Policy）]設定オプションで設定されている Windows または Samba のバージョンと異なる場合、そのセッションに限り、検出されたバージョンが設定バージョンをオーバーライドします。

たとえば、[ポリシー（Policy）] に Windows XP を設定した場合に、プリプロセッサが Windows Vista を検出すると、プリプロセッサはそのセッションでは Windows Vista ポリシーを使用します。その他の設定は引き続き有効です。

DCE/RPC トランスポートが SMB ではない場合は（トランスポートが TCP または UDP の場合）、バージョンを検出できず、ポリシーを自動的に設定できません。

このオプションを有効にするには、ドロップダウン リストで次のいずれかを選択します。

- サーバ/クライアント トラフィックでポリシー タイプを検査するには、[クライアント（Client）] を選択します。
- クライアント/サーバ トラフィックでポリシー タイプを検査するには、[サーバ（Server）] を選択します。
- サーバ/クライアント トラフィックとクライアント/サーバ トラフィックの両方でポリシー タイプを検査するには、[両方（Both）] を選択します。

レガシー SMB 検査モード（Legacy SMB Inspection Mode）

検査する SMB バージョンを指定します。[レガシー SMB 検査モード（Legacy SMB Inspection Mode）] が有効になっている場合、DCE/RPC プリプロセッサは、SMB バージョン 1 のトラフィックのみを検査します。このオプションを無効にすると、DCE/RPC プリプロセッサは、SMB バージョン 1、2、および 3 を使用するトラフィックを調査します。

関連トピック

基本コンテンツおよび protected_content キーワードの引数, （1137 ページ）
概要：byte_jump および byte_test キーワード

DCE/RPC ターゲットベース ポリシー オプション

各ターゲットベース ポリシーでは、TCP、UDP、SMB、および RPC over HTTP トランスポートのうち 1 つ以上を有効にできます。トランスポートを有効にする場合は、1 つ以上の検出ポート（DCE/RPC トラフィックを伝送することがわかっているポート）を指定する必要があります。

シスコでは、デフォルトの検出ポート（ウェルノウン ポートまたは各プロトコルで一般に使用されているポート）を使用することを推奨しています。検出ポートを追加するのは、デフォルト以外のポートで DCE/RPC トラフィックを検出した場合だけです。

Windows のターゲットベース ポリシーでは、ネットワークのトラフィックに一致するように、1 つ以上の任意のトランスポートのポートを任意の組み合わせで指定できます。しかし、Samba のターゲットベース ポリシーでは SMB トランスポートのポートだけを指定できます。

（注） 少なくとも 1 つのトランスポートが有効になっている DCE/RPC ターゲットベース ポリシーを追加した場合を除き、デフォルトのターゲットベースポリシーでは少なくとも 1 つの DCE/RPC トランスポートを有効にする必要があります。たとえば、すべての DCE/RPC 実装に対してホストを指定し、未指定のホストにはデフォルトのターゲットベース ポリシーを展開したくない場合があります。そのような場合は、デフォルトのターゲットベース ポリシーのトランスポートを有効化しないようにします。

（任意）自動検出ポートを有効にして指定できます。プリプロセッサは、自動検出ポートとして指定されたポートを最初にテストして、そのポートが DCE/RPC トラフィックを伝送しているかどうかを判別し、DCE/RPC トラフィックを検出した場合にのみ処理を続行します。

自動検出ポートを有効にする場合は、エフェメラル ポート範囲全体に対応するよう、自動検出ポートが 1025 から 65535 の範囲に設定されていることを確認してください。

自動検出は、トランスポート検出ポートによって識別されていないポートでのみ発生する点にも注意してください。

[RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）] オプションまたは [SMB 自動検出ポート（SMB Auto-Detect Ports）] オプションで自動検出ポートを有効にしたり指定したりすることはほとんどありません。これは、指定されているデフォルト検出ポートを除き、どちらの場合もトラフィックが発生することはほとんどなく、その見込みも少ないためです。

各ターゲットベース ポリシーでは、次に示すさまざまなオプションを指定できます。以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

ネットワーク

DCE/RPC ターゲットベース サーバ ポリシーを展開するホストの IP アドレス。また、ターゲットベース ポリシーを追加する場合は、[ターゲットの追加（Add Target）] ポップアップ ウィンドウの [サーバ アドレス（Server Address）] フィールドに指定した名前。

単一の IP アドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを設定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は

指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、any を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

ポリシー

モニタ対象ネットワークセグメントのターゲットホストが使用する Windows または Samba DCE/RPC の実装。

[SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] グローバル オプションを有効にすると、SMB が DCE/RPC トランスポートの場合に、このオプションの設定をセッションごとに自動的にオーバーライドできます。

SMB の無効な共有（SMB Invalid Shares）

指定した共有リソースへの接続が試行されると、プリプロセッサが検出する 1 つ以上の SMB 共有リソースを識別します。複数の共有をカンマで区切って指定できます。また必要に応じて、共有を引用符で囲むこともできます。これは、以前のソフトウェア バージョンでは必須でしたが、現在は必須ではありません。次に例を示します。

```
"C$", D$, "admin", private
```

[SMB ポート（SMB Ports）] が有効に設定されている場合、プリプロセッサは SMB トラフィックで無効な共有を検出します。

ほとんどの場合、Windows により名前が指定されたドライブを無効な共有として指定するには、このドライブにドル記号を付加する必要があることに注意してください。たとえば、ドライブ C は C$ または "C$" として指定します。

SMB の無効な共有を検出するには、[SMB ポート（SMB Ports）] か、[SMB 自動検出ポート（SMB Auto-Detect Ports）] を有効にする必要があることにも注意してください。

ルール 133:26 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

SMB 最大 AndX チェーン（SMB Maximum AndX Chain）

連結された SMB AndX コマンドの許容最大数です。通常、多数の連結 AndX コマンドは異常な動作を表し、場合によっては回避試行を示している可能性があります。連結コマンドを許可しない場合は 1 を指定し、連結コマンドの数の検出を無効にするには 0 を指定します。

プリプロセッサは最初に連結コマンドの数をカウントし、関連する SMB プリプロセッサ ルールが有効であり、連結コマンドの数が設定されている値と等しいかそれ以上の場合にはイベントを生成することに注意してください。その後、処理が続行されます。

注意 SMB プロトコルに詳しいユーザだけが [SMB AndX の最大チェーン（SMB Maximum AndX Chains）] オプションのデフォルト設定を変更するようにしてください。

ルール 133:20 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

RPC プロキシ トラフィックのみ（RPC proxy traffic only）

[RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）] が有効である場合、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみであるか、または他の Web サーバ トラフィックを含んでいる可能性があるかどうかを示します。たとえば、ポート 80 はプロキシ トラフィックとその他の Web サーバ トラフィックの両方を伝送する可能性があります。

このオプションが無効になっている場合は、プロキシ トラフィックとその他の Web サーバ トラフィックの両方が想定されます。たとえばサーバが専用プロキシ サーバである場合などに、このオプションを有効にします。有効にすると、プリプロセッサはトラフィックを調べて DCE/RPC を伝送しているかどうかを判別し、伝送していない場合はそのトラフィックを無視し、伝送している場合は処理を続行します。このオプションを有効にすることで機能が追加されるのは、[RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）] チェック ボックスも有効にされている場合だけであることに注意してください。

RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）

管理対象デバイスが DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間に配置されている場合に、指定の各ポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの検出を有効にします。

有効である場合、DCE/RPC トラフィックが確認されるポートを追加できますが、Web サーバは一般に DCE/RPC トラフィックとその他のトラフィックの両方にデフォルト ポートを使用するため、この操作が必要になることはあまりありません。有効である場合、[RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）] は有効にしませんが、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみであり、その他の Web サーバ トラフィックを含んでいない場合は、[RPC プロキシ トラフィックのみ（RPC Proxy Traffic Only）] を有効にします。

（注） このオプションを選択することがあるとすれば、きわめて稀なケースです。

RPC over HTTP サーバ ポート（RPC over HTTP Server Ports）

Microsoft IIS RPC プロキシ サーバと DCE/RPC サーバが異なるホスト上に配置されており、デバイスがこの 2 つのサーバ間のトラフィックをモニタしている場合、指定の各ポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの検出を有効にします。

一般に、このオプションを有効にするときは、ネットワーク上のプロキシ Web サーバに注意を払わない場合でも、1025 ～ 65535 のポート範囲で [RPC over HTTP サーバ自動検出ポート（RPC over HTTP Server Auto-Detect Ports）] も有効にする必要があります。場合によっては RPC over HTTP サーバポートを再設定することがあり、その際には再設定したサーバポートをこのオプションのポート リストに追加する必要があることに注意してください。

TCP ポート（TCP Ports）

指定の各ポートでの TCP の DCE/RPC トラフィックの検出を有効にします。

正当なDCE/RPCトラフィックとエクスプロイトは、さまざまなポートを使用する可能性があります。ポート1024より大きい番号のポートが一般的です。通常、このオプションを有効にする場合は、1025 ～ 65535 のポート範囲で [TCP 自動検出ポート（TCP Auto-Detect Ports）] も有効にする必要があります。

UDP ポート

指定の各ポートでの UDP の DCE/RPC トラフィックの検出を有効にします。

正当なDCE/RPCトラフィックとエクスプロイトは、さまざまなポートを使用する可能性があります。ポート1024より大きい番号のポートが一般的です。通常、このオプションを有効にする場合は、1025 ～ 65535 のポート範囲で [UDP 自動検出ポート（UDP Auto-Detect Ports）] も有効にする必要があります。

SMB ポート（SMB Ports）

指定の各ポートでの SMB の DCE/RPC トラフィックの検出を有効にします。

デフォルトの検出ポートを使用したSMBトラフィックが発生することがあります。他のポートはほとんどありません。通常はデフォルト設定を使用してください。

[SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] グローバル オプションを有効にすると、SMB が DCE/RPC トランスポートの場合に、ターゲット ポリシーに対して設定されているポリシー タイプをセッションごとに自動的にオーバーライドできます。

RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）

管理対象デバイスが DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間に配置されている場合に、指定のポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの自動検出を有効にします。

有効である場合は、一時ポート範囲全体をカバーするため、一般にポート範囲として 1025 から 65535 を指定します。

RPC over HTTP サーバ自動検出ポート（RPC over HTTP Server Auto-Detect Ports）

Microsoft IIS RPC プロキシ サーバおよび DCE/RPC サーバが異なるホスト上に配置されており、デバイスがこの 2 つのサーバ間のトラフィックをモニタしている場合、指定のポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの自動検出を有効にします。

TCP 自動検出ポート（TCP Auto-Detect Ports）

指定のポートで TCP の DCE/RPC トラフィックの自動検出を有効にします。

UDP 自動検出ポート（UDP Auto-Detect Ports）

指定の各ポートで UDP の DCE/RPC トラフィックの自動検出を有効にします。

SMB 自動検出ポート（SMB Auto-Detect Ports）

SMB の DCE/RPC トラフィックの検出を有効にします。

（注） このオプションを選択することがあるとすれば、きわめて稀なケースです。

SMB ファイル インスペクション（SMB File Inspection）

ファイル検出のためのSMBトラフィックのインスペクションを有効にします。次の選択肢があります。

- ファイル インスペクションを無効にするには、[オフ（Off）] を選択します。
- SMB でファイルデータを検査するが、DCE/RPC トラフィックは検査しない場合は、[ファイルのみ（Only）] を選択します。このオプションを選択すると、ファイルと DCE/RPC トラフィックの両方を検査する場合よりもパフォーマンスが向上する可能性があります。
- SMB でファイルと DCE/RPC トラフィックの両方を検査するには、[オン（On）] を選択します。このオプションを選択すると、パフォーマンスに影響する可能性があります。

SMB トラフィックでの次のファイルについてのインスペクションはサポートされていません。

- このオプションを有効にしてポリシーを適用する前に確立された TCP または SMB セッションで転送されたファイル
- 1 つの TCP または SMB セッションで同時に転送されたファイル
- 複数の TCP または SMB セッションにわたって転送されたファイル
- メッセージ署名のネゴシエート時など、非連続データを使用して転送されたファイル
- 同一オフセットに異なるデータが含まれており、データがオーバーラップしている転送ファイル
- リモート クライアントがファイル サーバに保存し、そのクライアントで編集用に開かれたファイル

SMB ファイル インスペクションの深さ（SMB File Inspection Depth）

[SMB ファイル インスペクション（SMB File Inspection）] が [ファイルのみ（Only）] または [オン（On）]に設定されている場合に、SMBトラフィックでファイルが検出された時に検査されるデータのバイト数です。次のいずれかを指定します。

- 正の値
- `0`：ファイル全体を検査する場合
- `-1`：ファイル インスペクションを無効にする場合

アクセス コントロール ポリシーの [詳細（Advanced）] タブの [ファイルおよびマルウェアの設定（File and Malware Settings）] セクションで定義された値以下になるように、このフィールドに値を入力します。[ファイルタイプを検知する前に検閲するバイト数制限（Limit the number of bytes inspected when doing file type detection）] で定義されている値よりも大きい値をこのオプションに設定すると、アクセス コントロール ポリシーの設定が、有効な最大値として使用されます。

[SMB ファイル インスペクション（SMB File Inspection）] が [オフ（Off）] に設定されている場合、このフィールドは無効になります。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）

トラフィックに関連する DCE/RPC ルール

ほとんどの DCE/RPC プリプロセッサ ルールでは、SMB、コネクション型 DCE/RPC、またはコネクションレス型 DCE/RPC のトラフィックで検出される異常や検知回避技術に対してトリガーします。トラフィック タイプ別に有効にできるルールを次の表に示します。

表 *166*：トラフィックに関連する *DCE/RPC* ルール

トラフィック	プリプロセッサ ルール GID:SID
SMB	133:2 ～ 133:26、133:48 ～ 133:57
コネクション型 DCE/RPC	133:27 ～ 133:39
コネクションレス型 DCE/RPC の検出	133:40 ～ 133:43

DCE/RPC プリプロセッサの設定

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

DCE/RPC プリプロセッサを設定するには、プリプロセッサの機能を制御するグローバル オプションを変更するか、IP アドレスと稼働している Windows または Samba のバージョンによってネットワーク上の DCE/RPC サーバを識別する 1 つ以上のターゲットベース サーバ ポリシーを指定します。ターゲットベース ポリシー構成では、トランスポート プロトコルの有効化、DCE/RPC トラフィックをホストに伝送するポートの指定、およびその他のサーバ固有オプションの設定も行います。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

はじめる前に

- カスタム ターゲットベースのポリシーで指定するネットワークが一致しているか、または親のネットワーク分析ポリシーで処理されるネットワーク、ゾーン、およびVLANのサブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定, （1262 ページ）を参照してください。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。または[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 左側のナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [DCE/RPC の構成（DCE/RPC Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [DCE/RPC の構成（DCE/RPC Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 [グローバル設定（Global Settings）] セクションのオプションを変更します。DCE/RPC グローバル オプション, （1281 ページ）を参照してください。

ステップ 7 次の選択肢があります。

- サーバ プロファイルの追加：[サーバ（Servers）] の横にある追加アイコン（）をクリックします。1 つ以上の IP アドレスを [サーバ アドレス（Server Address）] フィールドに指定し、[OK] をクリックします。
- サーバ プロファイルの削除：ポリシーの横にある削除アイコン（）をクリックします。
- サーバ プロファイルの編集：[サーバ（Servers）] の下にあるプロファイルの設定済みアドレスをクリックするか、[デフォルト（default）] をクリックします。[設定（Configuration）] セクションの設定を変更できます。DCE/RPC ターゲットベース ポリシー オプション, （1283 ページ）を参照してください。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次の作業

- 侵入イベントを生成する場合は、DCE/RPC プリプロセッサ ルール（GID 132 または 133）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）、DCE/RPC グローバル オプション, （1281 ページ）、DCE/RPC ターゲットベース ポリシー オプション, （1283 ページ）、およびトラフィックに関連する DCE/RPC ルール, （1289 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）
ファイルおよびマルウェアのインスペクション パフォーマンスとストレージのオプション, （988 ページ）
DCE/RPC キーワード, （1192 ページ）
レイヤの管理, （1023 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

DNS プリプロセッサ

DNS プリプロセッサは、DNS ネーム サーバ応答を検査し、次に示す特定のエクスプロイトがあるかどうかを確認します。

- RData テキスト フィールドに対するオーバーフローの試行
- 古い DNS リソース レコード タイプ
- 試験的な DNS リソース レコード タイプ

最も一般的なタイプの DNS ネーム サーバ応答には、応答を求めたクエリ内のドメイン名に対応する 1 つ以上の IP アドレスが示されています。その他のタイプのサーバ応答には、たとえば、電子メール メッセージの宛先や、元のクエリの対象のサーバからは取得できない情報を提供できるネーム サーバの位置などが記述されています。

DNS 応答には以下の構成要素があります。

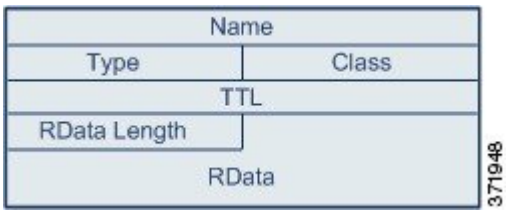
- メッセージ ヘッダー
- 1 つ以上の要求が含まれる [質問（Question）] セクション
- [質問（Question）] セクションの要求に応答する 3 つのセクション
  - 応答
  - 権限（Authority）
  - その他の情報（Additional Information）

この 3 セクションの応答には、ネーム サーバに保持されているリソース レコード（RR）の情報が反映されます。次の表で、これらの 3 つのセクションについて説明します。

表 *167* : *DNS* ネーム サーバ *RR* 応答

セクション	内容	例
応答	クエリに対する特定の回答を提供する 1 つ以上のリソース レコード（オプション）	ドメイン名に対応する IP アドレス
権限	権威ネーム サーバを指し示す 1 つ以上のリソース レコード（オプション）	応答の権威ネーム サーバの名前
その他の情報	[応答（Answer）] セクションに関連する追加情報を提供する 1 つ以上のリソース レコード（オプション）	クエリ対象の別のサーバの IP アドレス

さまざまなタイプのリソース レコードがありますが、これらはすべて一貫して次の構造を保っています。



理論上、すべてのタイプのリソース レコードを、ネーム サーバ応答メッセージの [応答（Answer）]、[権威（Authority）]、または [追加情報（Additional Information）] セクションで使用できます。DNS プリプロセッサは、検出されたエクスプロイトについて、3 つの各応答セクションのすべてのリソース レコードを検査します。

[タイプ（Type）] および [RData] リソース レコード フィールドは、DNS プリプロセッサでは特に重要です。[タイプ（Type）] フィールドは、リソース レコードのタイプを示します。[RData]（リソース データ）フィールドは、応答の内容を示します。[RData] フィールドのサイズと内容は、リソース レコードのタイプによって異なります。

DNS メッセージは通常、UDP トランスポート プロトコルを使用しますが、信頼性のある配信を必要とするメッセージ タイプである場合や、メッセージ サイズが UDP で処理可能なサイズを超えている場合は、TCP を使用します。DNS プリプロセッサは、UDP および TCP の両方のトラフィックで DNS サーバ応答を検査します。

DNS プリプロセッサは、ミッドストリームで検出された TCP セッションを検査せず、ドロップされたパケットが原因でセッションの状態が失われるとインスペクションを終了します。

DNS プリプロセッサ オプション

ポート

このフィールドは、送信元ポート、または DNS プリプロセッサが DNS サーバ応答をモニタする必要があるポートを指定します。複数のポートを指定する場合は、カンマで区切ります。

DNS プリプロセッサ用に設定する一般的なポートは、ウェルノウン ポート 53 です。これは、DNS ネーム サーバが UDP および TCP の両方で DNS メッセージに使用するポートです。

RData テキスト フィールドでのオーバーフローの試行の検出

リソース レコード タイプが TXT（テキスト）の場合、RData フィールドは可変長の ASCII テキスト フィールドになります。

このオプションを選択した場合は、MITRE の Current Vulnerabilities and Exposures データベースの CVE-2006-3441 エントリで指定した特定の脆弱性を検出します。これは、Microsoft Windows 2000 Service Pack 4、Windows XP Service Pack 1 および Service Pack 2、Windows Server 2003 Service Pack 1 の既知の脆弱性です。攻撃者はこの脆弱性を悪用して、[RData] テキスト フィールドの長さの誤算を引き起こし、結果としてバッファ オーバーフローを発生させるよう悪意をもって作られたネーム サーバ応答をホストに送信するか受信させることで、ホストを完全に制御できます。

アップグレードによってこの脆弱性が修正されていないオペレーティング システムが稼働しているホストがネットワーク内に含まれている可能性がある場合は、このオプションを有効にする必要があります。

ルール 131:3 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定，（1063 ページ）を参照してください。

古い DNS RR タイプの検知

RFC 1035 ではさまざまなリソース レコード タイプが古いタイプとして指定されています。これらは古いレコードタイプであるため、一部のシステムはこれらのレコードタイプに対応しておらず、エクスプロイトの対象となることがあります。このようなレコード タイプを含めるようにネットワークを意図的に設定している場合を除き、通常の DNS 応答でこのようなレコード タイプが検出されることは想定されません。

既知の古いリソース レコードタイプを検出するようにシステムを設定できます。次の表に、これらのレコード タイプとその説明を示します。

表 *168*：古い *DNS* リソース レコード タイプ

RR タイプ	コード（Code）	説明
3	MD	メールの宛先
4	MF	メールのフォワーダ

ルール131:1を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

試験的な DNS RR タイプの検出

RFC 1035 ではさまざまなリソース レコード タイプが試験的なタイプとして指定されています。これらは試験的なレコードタイプであるため、一部のシステムはこれらのレコードタイプに対応しておらず、エクスプロイトの対象となることがあります。このようなレコード タイプを含めるようにネットワークを意図的に設定している場合を除き、通常のDNS応答でこのようなレコードタイプが検出されることは想定されません。

既知の試験的なレコード タイプを検出するようにシステムを設定できます。次の表に、これらのレコード タイプとその説明を示します。

表 *169* : 試験的な *DNS* リソース レコード タイプ

RR タイプ	コード（Code）	説明
7	MB	メールボックスのドメイン名
8	MG	メール グループ メンバー
9	MR	メール リネーム ドメイン名
10	NUL	空白のリソース レコード

ルール131:2を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

DNS プリプロセッサの設定

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

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [DNS の構成（DNS Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [DNS の構成（DNS Configuration）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 DNS プリプロセッサ オプション, （1293 ページ）で説明されている設定を変更します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次の作業

- 侵入イベントを生成する場合は、DNS プリプロセッサ ルール（GID 131）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）およびDNS プリプロセッサ オプション, （1293 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

侵入ポリシーおよびネットワーク分析ポリシーのレイヤ, （1015 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

FTP/Telnet デコーダ

FTP/Telnet デコーダは FTP および Telnet データ ストリームを分析して、ルール エンジンによる処理の前に FTP および Telnet コマンドを正規化します。

グローバル FTP および Telnet オプション

FTP/Telnet デコーダがパケットのステートフル インスペクションまたはステートレス インスペクションを実行するかどうか、デコーダが暗号化 FTP または Telnet セッションを検出するかどうか、およびデコーダが暗号化データの検出後にデータ ストリームの検査を続行するかどうかを決定するグローバル オプションを設定できます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ステートフル インスペクション（Stateful Inspection）

選択されている場合、FTP/Telnet デコーダは状態を保存し、各パケットにセッション コンテキストを提供し、再構成されたセッションだけを検査します。選択されていない場合、セッション コンテキストなしで個々のパケットを分析します。

FTP データ転送を検査するには、このオプションを選択する必要があります。

暗号化トラフィックの検出（Detect Encrypted Traffic）

暗号化 Tenet および FTP セッションを検出します。

ルール 125:7 と 126:2 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

暗号化データの検査を続行（Continue to Inspect Encrypted Data）

プリプロセッサに対し、データ ストリームの暗号化後もデータ ストリームの検査を続行し、最終的に処理できるデコードされたデータを検索するように指示します。

Telnet オプション

FTP/Telnet デコーダによる Telnet コマンドの正規化を有効または無効にし、特定の異常ケースを有効または無効にし、許容可能な Are You There（AYT）攻撃数のしきい値を設定できます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

Telnet トラフィックを正規化するポートを示します。通常、Telnet は TCP ポート 23 に接続します。インターフェイスで、複数のポートをカンマで区切って指定します。

注意 暗号化トラフィック（SSL）はデコードできないので、ポート 22（SSH）を追加すると、予想外の結果が生じる可能性があります。

正規化（Normalize）

指定のポートへの Telnet トラフィックを正規化します。

異常検知（Detect Anomalies）

対応するSE（サブネゴシエーション終了）がないTelnetSB（サブネゴシエーション開始）の検出を有効にします。

Telnet がサポートするサブネゴシエーションは、SB（サブネゴシエーション開始）で開始し、SE（サブネゴシエーション終了）で終了していなければなりません。しかし、一部の Telnet サーバ実装では、対応する SE のない SB が無視されます。これは、回避事例につながるおそれのある異常な動作です。FTP はコントロール接続で Telnet プロトコルを使用するため、FTP もこの動作の影響を受けます。

ルール 126:3 を有効にすることでイベントを生成でき、インライン展開では、この異常が Telnet トラフィックで検出される場合に違反パケットをドロップできます。FTP コマンド チャネルで検出される場合はルール 125:9 を有効にできます。侵入ルール状態の設定, （1063 ページ）を参照してください。

Are You There 攻撃のしきい値（Are You There Attack Threshold Number）

連続する AYT コマンドの数が指定のしきい値を超えた場合にそのことを検出します。Cisco は、AYT しきい値としてデフォルト値以下の値を設定することを推奨します。

ルール 126:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

サーバレベルの FTP オプション

複数のFTPサーバでデコードオプションを設定できます。作成する各サーバプロファイルには、トラフィックをモニタするサーバのサーバIPアドレスとポートが含まれます。検証するFTPコマンドと、特定のサーバで無視する FTP コマンドを指定し、コマンドの最大パラメータ長を設定できます。また、デコーダが特定のコマンドで検証する特定のコマンド構文を設定し、代替最大コマンド パラメータ長を設定することもできます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ネットワーク

FTP サーバの 1 つ以上の IP アドレスを指定するには、このオプションを使用します。

1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。設定できる最大文字数は 1024 文字です。デフォルト プロファイルを含め最大 255 個のプロファイルを設定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたはアドレス ブロックは指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

ポート

管理対象デバイスがトラフィックをモニタする FTP サーバのポートを指定するには、このオプションを使用します。インターフェイスで、複数のポートをカンマで区切って指定します。ポート 21 は FTP トラフィック用のウェルノウン ポートです。

File Get コマンド（File Get Commands）

サーバからクライアントにファイルを転送するために使用する FTP コマンドを定義するには、このオプションを使用します。サポートからの指示がない限り、これらの値を変更しないでください。

注意 サポートからの指示がない限り、[File Get コマンド（File Get Commands）] フィールドを変更しないでください。

File Put コマンド（File Put Commands）

クライアントからサーバにファイルを転送するために使用する FTP コマンドを定義するには、このオプションを使用します。サポートからの指示がない限り、これらの値を変更しないでください。

注意 サポートからの指示がない限り、[File Put コマンド（File Put Commands）] フィールドを変更しないでください。

追加 FTP コマンド（Additional FTP Commands）

デコーダが検出するコマンドを追加で指定するには、この行を使用します。複数のコマンドを追加する場合は、コマンドをスペースで区切ってください。

追加できるコマンドには、`XPWD`、`XCWD`、`XCUP`、`XMKD`、`XRMD` があります。これらのコマンドの詳細については、RFC 775（Network Working Group によるディレクトリに基づく FTP コマンドの仕様）を参照してください。

デフォルト最大パラメータ長（Default Max Parameter Length）

代替最大パラメータ長が設定されていないコマンドの最大パラメータ長を検出するには、このオプションを使用します。代替最大パラメータ長は、必要な数だけ追加できます。

ルール 125:3 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定，（1063 ページ）を参照してください。

代替最大パラメータ長（Alternate Max Parameter Length）

異なる最大パラメータ長を検出するコマンドを指定し、それらのコマンドの最大パラメータ長を指定するには、このオプションを使用します。[追加（Add）]をクリックして行を追加し、特定のコマンドで検出する異なる最大パラメータ長を指定します。

フォーマット文字列攻撃の検査コマンド（Check Commands for String Format Attacks）

指定されたコマンドでフォーマット文字列攻撃を検査するには、このオプションを使用します。

ルール 125:5 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定，（1063 ページ）を参照してください。

コマンドの妥当性（Command Validity）

特定のコマンドの有効な形式を入力するには、このオプションを使用します。[追加（Add）]をクリックして、コマンド検証行を追加します。

ルール 125:2 と 125:4 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定，（1063 ページ）を参照してください。

FTP 転送を無視（Ignore FTP Transfers）

データ転送チャネルで状態インスペクション以外のすべてのインスペクションを無効にして FTP データ転送のパフォーマンスを改善するには、このオプションを使用します。

（注） データ転送を検査するには、グローバル FTP/Telnet オプション [ステートフル インスペクション（Stateful Inspection）] を選択する必要があります。

FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）

FTP コマンド チャネルで Telnet コマンドが使用された場合にそのことを検出するには、このオプションを使用します。

ルール 125:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定，（1063 ページ）を参照してください。

正規化時に消去コマンドを無視（Ignore Erase Commands during Normalization）

[FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）] が選択されている場合に、FTP トラフィックの正規化時に Telnet の文字および行の消去コマンドを無視するには、このオプションを使用します。この設定は、FTP サーバによる Telnet 消去コマンドの処理方法と一致する必要があります。一般に、新しい FTP サーバは Telnet 消去コマンドを無視しますが、ほとんどの古いサーバは Telnet 消去コマンドを処理する点に注意してください。

トラブルシューティング オプション：FTP コマンドの検証設定のログを記録（Troubleshooting Options：Log FTP Command Validation Configuration）

トラブルシューティングについてサポートに問い合わせた際に、サーバ用にリストされている FTP コマンドごとに設定情報を出力するように、システムを設定することを指示される場合があります。

注意 サポートからの指示がない限り [FTP コマンドの検証設定のログを記録（Log FTP Command Validation Configuration）] を有効にしないでください。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）
FTP コマンドの検証ステートメント, （1300 ページ）

FTP コマンドの検証ステートメント

FTP コマンドに対する検証ステートメントを設定するときには、複数の代替パラメータをスペースで区切って指定できます。2つのパラメータ間にバイナリ OR 関係を作成するには、検証ステートメントでこの2つのパラメータをパイプ文字（|）で区切って指定します。パラメータを大カッコ（[]）で囲むと、これらのパラメータがオプションであることを示します。パラメータを中カッコ（{}）で囲むと、これらのパラメータが必須であることを示します。

FTP 通信の一部として受信したパラメータの構文を検証する FTP コマンド パラメータ検証ステートメントを作成できます。

FTP コマンド パラメータ検証ステートメントに使用できるパラメータを次の表に示します。

表 *170*：*FTP* コマンド パラメータ

使用するパラメータ	実行される検証
`int`	示されるパラメータが整数である必要があります。
`number`	示されるパラメータが 1 ～ 255 の範囲内の整数である必要があります。

使用するパラメータ	実行される検証
`char` _chars	示されるパラメータが単一文字であり、かつ _chars 引数に指定した文字の 1 つである必要があります。 たとえば、検証引数 `char` SBC を使用して `MODE` のコマンド検証を定義すると、`MODE` コマンドのパラメータが、文字 `S`（Stream モードを示す）、文字 `B`（Block モードを示す）、または文字 `C`（Compressed モードを示す）を含んでいるかどうかが検証されます。
`date` _datefmt	_datefmt に `#` が含まれている場合、示されるパラメータは数値である必要があります。 _datefmt に `C` が含まれている場合、示されるパラメータは文字である必要があります。 _datefmt にリテラル文字列が含まれている場合、示されるパラメータはリテラル文字列に一致している必要があります。
`string`	示されるパラメータが文字列である必要があります。
`host_port`	示されるパラメータは、RFC 959（Network Working Group による File Transfer Protocol 仕様）で定義されている有効なホスト ポート指定子である必要があります。

上記の表の構文を必要に応じて組み合わせることにより、トラフィックを検証する必要がある各 FTP コマンドを正しく検証するパラメータ検証ステートメントを作成できます。

（注） TYPE コマンドに複合式を含める場合は、式をスペースで囲んでください。また、式内の各オペランドをスペースで囲んでください。たとえば、`char A|B` ではなく `char A | B` と入力します。

関連トピック

サーバレベルの FTP オプション，（1297 ページ）

クライアントレベルの FTP オプション

カスタム FTP クライアント プロファイルを設定するには、これらのオプションを使用します。オプション記述にプリプロセッサルールが含まれない場合、そのオプションはプリプロセッサルールに関連付けられません。

ネットワーク

FTP クライアントの 1 つ以上の IP アドレスを指定するには、このオプションを使用します。

1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト プロファイルを含め最大 255 個のプロファイルを設定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたはアドレス ブロックは指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

最大応答長（Max Response Length）

このオプションを使用して、クライアントが受け入れる FTP コマンドに許可される最大応答長を指定します。これにより、基本的なバッファ オーバーフローを検出できます。

ルール 125:6 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

FTP バウンス試行の検出（Detect FTP Bounce Attempts）

FTP バウンス攻撃を検出するには、このオプションを使用します。

ルール 125:8 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

FTP バウンスの許可（Allow FTP Bounce to）

FTP PORT コマンドを FTP バウンス攻撃として扱わない追加のホストとそれらのホスト上のポートのリストを設定するには、このオプションを使用します。

FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）

FTP コマンド チャネルで Telnet コマンドが使用された場合にそのことを検出するには、このオプションを使用します。

ルール 125:1 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

正規化時に消去コマンドを無視（Ignore Erase Commands during Normalization）

[FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）] が選択されている場合に、FTP トラフィックの正規化時に Telnet の文字および行の消去コマンドを無視するには、このオプションを使用します。この設定は、FTP クライアントによる Telnet 消去コマンドの処理方法に一致している必要があります。一般に、新しい FTP クライ

アントは Telnet 消去コマンドを無視しますが、ほとんどの古いクライアントは Telnet 消去コマンドを処理する点に注意してください。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）

FTP/Telnet デコーダの設定

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

クライアントからの FTP トラフィックをモニタするように、FTP クライアントのクライアント プロファイルを設定できます。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

はじめる前に

- カスタム ターゲットベース ポリシーで識別するネットワークが、親ネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、および VLAN のサブセットと一致するか、サブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定, （1262 ページ）を参照してください。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。または[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [FTP と Telnet の構成（FTP and Telnet Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [FTP と Telnet の構成（FTP and Telnet Configuration）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 グローバル FTP および Telnet オプション, （1296 ページ）の説明に従って、[グローバル設定（Global Settings）] セクションのオプションを設定します。

ステップ 7 Telnet オプション, （1296 ページ）の説明に従って、[Telnet の設定（Telnet Settings）] セクションのオプションを設定します。

ステップ 8 FTP サーバ プロファイルを管理します。

- サーバ プロファイルの追加：[FTP サーバ（FTP Server）] の横にある追加アイコン（  ）をクリックします。クライアントの 1 つ以上の IP アドレスを [サーバアドレス（Server Address）] フィールドに指定し、[OK] をクリックします。単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト ポリシーを含め最大 255 個のポリシーを設定できます。
- サーバ プロファイルの編集：[FTP サーバ（FTP Server）] の下にあるカスタム プロファイルの設定済みアドレスをクリックするか、[デフォルト（default）] をクリックします。[設定（Configuration）] セクションの設定を変更できます。サーバレベルの FTP オプション, （1297 ページ）を参照してください。
- サーバ プロファイルの削除：プロファイルの横にある削除アイコン（  ）をクリックします。

ステップ 9 FTP クライアント プロファイルを管理します。

- クライアント プロファイルの追加：[FTP クライアント（FTP Client）] の横にある追加アイコン（  ）をクリックします。クライアントの 1 つ以上の IP アドレスを [クライアント アドレス（Client Address）] フィールドに指定し、[OK] をクリックします。単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト ポリシーを含め最大 255 個のポリシーを設定できます。
- クライアント プロファイルの編集：[FTP クライアント（FTP Client）] の下にあるプロファイルの設定済みアドレスをクリックするか、[デフォルト（default）] をクリックします。[設定（Configuration）] ページ エリアの設定を変更できます。クライアントレベルの FTP オプション, （1301 ページ）を参照してください。

- クライアント プロファイルの削除：カスタム プロファイルの横にある削除アイコン（  ）をクリックします。

ステップ 10 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次の作業

- 侵入イベントを生成する場合は、FTP および telnet プリプロセッサ ルール（GID 125 および 126）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）
レイヤの管理, （1023 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

HTTP Inspect プリプロセッサ

HTTP Inspect プリプロセッサは、次の処理を行います。

- ネットワーク上の Web サーバに送信される HTTP 要求と Web サーバから受信する HTTP 応答をデコードおよび正規化する。
- HTTP 関連の侵入ルールのパフォーマンス向上のために、Web サーバに送信されたメッセージを URI、非 cookie ヘッダー、cookie ヘッダー、メソッド、メッセージ本文の各コンポーネントに分ける。
- HTTP 関連の侵入ルールのパフォーマンス向上のために、Web サーバから受信したメッセージをステータス コード、ステータス メッセージ、非 set-cookie ヘッダー、cookie ヘッダー、応答本文の各コンポーネントに分ける。
- URI エンコード攻撃の可能性を検出する。
- 正規化データを追加ルール処理に使用できるようにする。

HTTP トラフィックはさまざまな形式でエンコードされている可能性があり、このことが、ルールによる適切な検査の実施を困難にしています。HTTP Inspect は 14 種類のエンコードをデコードし、HTTP トラフィックが最良のインスペクションを受けられるようにします。

HTTP Inspect のオプションは、グローバルに設定するか、1 つのサーバで設定するか、またはサーバ リストに対して設定することができます。

プリプロセッサ エンジンは HTTP の正規化をステートレスに実行することに注意してください。つまり、パケット単位で HTTP 文字列を正規化し、TCP ストリーム プリプロセッサにより再構成された HTTP 文字列のみを処理できます。

グローバル HTTP 正規化オプション

HTTP Inspect プリプロセッサのグローバル HTTP オプションは、プリプロセッサの機能を制御します。Web サーバ ポートとして指定されていないポートが HTTP トラフィックを受信する場合の HTTP 正規化を有効または無効にするには、このオプションを使用します。

次の点に注意してください。

- [無制限の圧縮解除（Unlimited Decompression）] を有効にすると、変更のコミット時に [圧縮データの最大深さ（Maximum Compressed Data Depth）] および [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] オプションが自動的に 65535 に設定されます。
- 最大値は、[圧縮データの最大深さ（Maximum Compressed Data Depth）] または [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] の値が異なる場合に使用されます。
  - デフォルトのネットワーク分析ポリシー
  - 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

異常な HTTP サーバの検出（Detect Anomalous HTTP Servers）

Web サーバ ポートとして指定されていないポートに送信された HTTP トラフィックまたはこのポートで受信した HTTP トラフィックを検出します。

（注） このオプションをオンにする場合は、[HTTP 設定（HTTP Configuration）] ページで、HTTP トラフィックを受信するすべてのポートがサーバ プロファイルにリストされていることを確認してください。確認せずにこのオプションと関連するプリプロセッサ ルールを有効にすると、サーバとの間の通常のトラフィックによってイベントが生成されます。デフォルトのサーバ プロファイルには、HTTP トラフィックに一般に使用されるすべてのポートが含まれていますが、このプロファイルを変更した場合は、イベントの生成を防ぐために別のプロファイルにそれらのポートを追加する必要があります。

ルール 120:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定，（1063 ページ）を参照してください。

HTTP プロキシ サーバの検出（Detect HTTP Proxy Servers）

[HTTP プロキシの使用を許可（Allow HTTP Proxy Use）] オプションで定義されていないプロキシ サーバを使用する HTTP トラフィックを検出します。

ルール 119:17 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

圧縮データの最大深さ（Maximum Compressed Data Depth）

[圧縮データの検査（Inspect Compressed Data）]（および任意で、[SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））]、[SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））]、または [PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））]）が有効な場合に、圧縮解除する圧縮データの最大サイズを設定します。

圧縮解除データの最大深さ（Maximum Decompressed Data Depth）

[圧縮データの検査（Inspect Compressed Data）]（および任意で、[SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））]、[SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））]、または [PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））]）が有効な場合に、正規化された圧縮データの最大サイズを設定します。

サーバレベルの HTTP 正規化オプション

サーバレベルのオプションは、モニタ対象サーバごとに設定するか、すべてのサーバに対してグローバルに設定するか、またはサーバ リストに対して設定することができます。また、事前定義のサーバ プロファイルを使用してこれらのオプションを設定するか、またはご使用の環境のニーズに合わせて個別に設定することができます。これらのオプション、またはこれらのオプションを設定するデフォルト プロファイルの 1 つを使用して、トラフィックを正規化する HTTP サーバ ポート、正規化するサーバ応答ペイロードの量、および正規化するエンコードのタイプを指定します。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ネットワーク

1 つ以上のサーバの IP アドレスを指定するには、このオプションを使用します。1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。

デフォルト プロファイルを含めてプロファイルの合計数は最大 255 ですが、さらに、HTTP サーバ リストに最大 496 文字（約 26 エントリ）を含めることができ、すべてのサーバ プロファイルに対して合計 256 のアドレス エントリを指定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

ポート

プリプロセッサ エンジンが HTTP トラフィックを正規化するポート。ポート番号が複数ある場合は、カンマで区切ります。

サイズ超過のディレクトリ長（Oversize Dir Length）

指定された値よりも長い URL ディレクトリを検出します。

ルール 119:15 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

クライアント フローの深さ（Client Flow Depth）

[ポート（Ports）] で定義されているクライアント側 HTTP トラフィックについて、ルールで検査される raw HTTP パケットのバイト数（ヘッダーとペイロードデータを含む）を指定します。ルール内の HTTP コンテンツ ルール オプションによって要求メッセージの特定の部分が検査される場合は、[クライアント フローの深さ（Client Flow Depth）] は適用されません。

次のいずれかを指定します。

- 正の値によって、最初のパケットで指定のバイト数が検査されます。最初のパケットのバイト数が指定のバイト数よりも少ない場合は、パケット全体が検査されます。指定された値は、セグメント化されたパケットと再構成されたパケットの両方に適用されることに注意してください。

  また、値 300 を指定すると、通常は、多くのクライアント要求ヘッダーの終わりにある大きな HTTP Cookie のインスペクションが排除されることにも注意してください。

- 0 を指定すると、すべてのクライアント側トラフィックが検査されます。これにはセッション内の複数のパケットが含まれ、必要な場合にはバイトの上限を超えることもあります。この値はパフォーマンスに影響する可能性があることに注意してください。

- -1 を指定すると、クライアント側のすべてのトラフィックが無視されます。

サーバ フローの深さ（Server Flow Depth）

[ポート（Ports）] で指定されているサーバ側 HTTP トラフィックについて、ルールで検査される raw HTTP パケットのバイト数を指定します。[HTTP 応答の検査（Inspect HTTP Responses）] が無効である場合は raw ヘッダーとペイロードが検査され、[HTTP 応答の検査（Inspect HTTP Response）] が有効である場合は、raw 応答ボディのみが検査されます。

[サーバ フローの深さ（Server Flow Depth）] では、[ポート（Ports）] で定義されているサーバ側 HTTP トラフィックについて、ルールで検査されるセッション内の raw サーバ応答データのバイ

ト数を指定します。このオプションを使用して、HTTP サーバ応答データのインスペクションのレベルとパフォーマンスのバランスを調整できます。ルール内の HTTP コンテンツ オプションによって要求メッセージの特定の部分が検査される場合は、Server Flow Depth は適用されません。

クライアント フローの深さ（Client Flow Depth）とは異なり、サーバ フローの深さ（Server Flow Depth）では、ルールが検査するバイト数を、HTTP 要求パケットごとではなく、HTTP 応答ごとのバイト数として指定します。

次のいずれかの値を指定できます。

- 正の値：

  [HTTP 応答の検査（Inspect HTTP Responses）] が**有効**である場合、raw HTTP 応答ボディのみが検査され、raw HTTP ヘッダーは検査されません。また、[圧縮データの検査（Inspect Compressed Data）] が有効である場合は、圧縮解除データも検査されます。

  [HTTP 応答の検査（Inspect HTTP Responses）] が**無効**である場合、raw パケット ヘッダーとペイロードが検査されます。

  セッションの応答バイト数が指定の値よりも少ない場合は、そのセッションで、ルールにより（必要に応じて複数パケットにわたって）すべての応答パケットが完全に検査されます。セッションの応答バイト数が指定の値よりも多い場合、そのセッションで、ルールにより（必要に応じて複数パケットにわたって）指定のバイト数だけが検査されます。

  フローの深さ（Flow Depth）の値が小さいと、[ポート（Ports）] で定義されているサーバ側トラフィックを対象とするルールで、検出漏れが発生する可能性があります。これらのルールのほとんどは HTTP ヘッダーまたはコンテンツ（通常、非ヘッダー データの先頭の約 100 バイト以内）を対象とします。通常はヘッダーの長さは 300 バイト未満ですが、ヘッダー サイズは異なることがあります。

  指定された値は、セグメント化されたパケットと再構成されたパケットの両方に適用されることにも注意してください。

- 0 を指定すると、[ポート（Port）] で定義されているすべての HTTP サーバ側トラフィックでパケット全体が検査されます。これにはセッションでの 65535 バイトよりも大きな応答データも含まれます。

  この値はパフォーマンスに影響する可能性があることに注意してください。

- -1

  [HTTP 応答の検査（Inspect HTTP Responses）] が**有効**な場合、raw HTTP ヘッダーだけが検査され、raw HTTP 応答ボディは検査されません。

  [HTTP 応答の検査（Inspect HTTP Responses）] が**無効**である場合、[ポート（Ports）] で定義されているすべてのサーバ側トラフィックは無視されます。

最大ヘッダー長（Maximum Header Length）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効である場合は、HTTP 要求、および HTTP 応答で、指定されている最大バイト数よりも長いヘッダー フィールドを検出します。値 0 を指定すると、このオプションが無効になります。これを有効にするため正の値を指定します。

ルール 119:19 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定,（1063 ページ）を参照してください。

最大ヘッダー数（Maximum Number of Headers）

HTTP 要求でヘッダー数がこの設定を超えている場合にそのことを検出します。値 0 を指定すると、このオプションが無効になります。これを有効にするため正の値を指定します。

ルール 119:20 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定,（1063 ページ）を参照してください。

最大スペース数（Maximum Number of Spaces）

折りたたみ行のスペースの数が HTTP 要求のこの設定と等しいか、超えている場合にそのことを検出します。値 0 を指定すると、このオプションが無効になります。これを有効にするため正の値を指定します。

ルール 119:26 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定,（1063 ページ）を参照してください。

HTTP クライアント ボディの抽出の深さ（HTTP Client Body Extraction Depth）

HTTP クライアント要求のメッセージ ボディから抽出するバイト数を指定します。侵入ルールを使用して抽出データを検査するには、`content` または `protected_content` キーワードを [HTTP クライアント ボディ（HTTP Client Body）] オプションと共に選択します。

クライアント ボディを無視するには、-1 を指定します。クライアント ボディ全体を抽出するには、0 を指定します。抽出対象のバイト数を指定すると、システム パフォーマンスが向上することがある点に注意してください。また、侵入ルールで [HTTP クライアント ボディ（HTTP Client Body）] オプションが機能するためには、0 か 0 より大きい値を指定する必要があることに注意してください。

小さいチャンク サイズ（Small Chunk Size）

チャンクが小さいとみなされるサイズの最大バイト数を指定します。正の値を指定します。値 0 を指定すると、異常な小さなセグメントの連続の検出が無効になります。詳細については、[連続する小さいチャンク（Consecutive Small Chunks）] オプションを参照してください。

連続する小さいチャンク（Consecutive Small Chunks）

チャンク転送エンコードを使用するクライアント トラフィックまたはサーバ トラフィックで異常に大量であるとみなされる、連続する小さなチャンクの数を指定します。[小さいチャンク サイズ（Small Chunk Size）] オプションは、小さなチャンクの最大サイズを指定します。

たとえば、10 バイト以下のチャンクが 5 つ連続していることを検出するには、[小さいチャンク サイズ（Small Chunk Size）] に 10 を設定し、[連続する小さいチャンク（Consecutive Small Chunks）] に 5 を設定します。

大量の小さなチャンクが検出される場合にイベントを生成し、インライン展開では、違反パケットをドロップします。するには、クライアントトラフィックの場合はプリプロセッサルール119:27を有効にし、サーバトラフィックの場合はルール120:7を有効にします。[小さいチャンクサイズ（Small Chunk Size）]が有効であり、このオプションが0または1に設定されている場合にこれらのルールを有効にすると、指定されたサイズ以下のすべてのチャンクでイベントがトリガーとして使用されます。

HTTP メソッド（HTTP Methods）

システムがトラフィックで検出すると予期される、GETおよびPOST以外のHTTP要求メソッドを指定します。複数の値はカンマで区切ります。

侵入ルールでは、HTTPメソッドのコンテンツを検索するために、`content`または`protected_content`キーワードがHTTP Method引数と共に使用されます。GET、POST、およびこのオプションで設定されているメソッド以外のメソッドがトラフィックで検出される場合イベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール119:31を有効にします。侵入ルール状態の設定，（1063 ページ）を参照してください。

アラートなし（No Alerts）

関連するプリプロセッサルールが有効である場合に、侵入イベントを無効にします。

（注） このオプションは、HTTPの標準テキストルールと共有するオブジェクトルールを無効にしません。

HTTP ヘッダーの正規化（Normalize HTTP Headers）

[HTTP応答の検査（Inspect HTTP Responses）]が有効な場合は、要求ヘッダーと応答ヘッダーの非cookieデータの正規化が有効になります。[HTTP応答の検査（Inspect HTTP Responses）]が有効**ではない**場合は、要求ヘッダーと応答ヘッダーでcookieを含むHTTPヘッダー全体の正規化が有効になります。

HTTP Cookie の検査（Inspect HTTP Cookies）

HTTP要求ヘッダーからのcookieの抽出を有効にします。また、[HTTP応答の検査（Inspect HTTP Responses）]が有効な場合は、応答ヘッダーからのset-cookieデータの抽出も有効になります。cookieの抽出が不要な場合は、このオプションを無効にするとパフォーマンスが向上します。

`Cookie:`および`Set-Cookie:`のヘッダー名、ヘッダー行の先頭のスペース、およびヘッダー行の末尾の`CRLF`は、cookieの一部ではなくヘッダーの一部として検査されます。

HTTP ヘッダーの Cookie の正規化（Normalize Cookies in HTTP headers）

HTTP要求ヘッダーのcookieの正規化を有効にします。[HTTP応答の検査（Inspect HTTP Responses）]が有効な場合も、応答ヘッダーのset-cookieデータの正規化を有効にします。このオプションを選択する前に、[HTTP Cookieの検査（Inspect HTTP Cookies）]を選択する必要があります。

HTTP プロキシの使用を許可（Allow HTTP Proxy Use）

モニタ対象 Web サーバを HTTP プロキシとして使用できるようにします。このオプションは、HTTP 要求のインスペクションでのみ使用されます。

URI のみの検査（Inspect URI Only）

正規化された HTTP 要求パケットの URI 部分のみを検査します。

HTTP 応答の検査（Inspect HTTP Responses）

HTTP応答の拡張インスペクションが有効になり、プリプロセッサは、HTTP要求メッセージのデコードと正規化の他に、ルール エンジンによるインスペクションのために応答フィールドを抽出します。このオプションを有効にすると、応答ヘッダー、ボディ、ステータス コードなどがシステムにより抽出されます。また [HTTP Cookie の検査（Inspect HTTP Cookies）] が有効な場合は、set-cookie データも抽出されます。

ルール 120:2 と 120:3 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

UTF エンコードの UTF-8 への正規化（Normalize UTF Encodings to UTF-8）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効である場合、HTTP 応答で UTF-16LE、UTF-16BE、UTF-32LE、および UTF32-BE エンコードが検出され、UTF-8 に正規化されます。

ルール 120:4 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

圧縮データの検査（Inspect Compressed Data）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合は、HTTP 応答ボディ内の gzip および deflate 互換圧縮データの圧縮解除と、正規化された圧縮解除データのインスペクションが有効になります。システムは、チャンク HTTP 応答データと非チャンク HTTP 応答データを検査します。システムは、必要に応じて複数のパケットにわたり圧縮解除データをパケット単位で検査します。つまり、システムが異なるパケットの圧縮解除データをインスペクションのために結合させることはありません。[圧縮データの最大深さ（Maximum Compressed Data Depth）]、[圧縮解除データの最大深さ（Maximum Decompressed Data Depth）]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバ フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、`file_data` ルール キーワードを使用できます。

ルール 120:6 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

無制限の圧縮解除（Unlimited Decompression）

[圧縮データの検査（Inspect Compressed Data）]（および任意で、[SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））]、[SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））]、または [PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））]）が有効な場合、複数のパケットにわたって [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] がオーバーライドされます。つまり、このオプションにより、複数のパケットにわたる無制限の圧縮解除が有効になります。このオプションを有効にしても、単一パケット内での [圧縮データの最大深さ（Maximum Compressed Data Depth）] または [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] には影響しないことに注意してください。また、このオプションを有効にすると、変更のコミット時に、[圧縮データの最大深さ（Maximum Compressed Data Depth）] と [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] が 65535 に設定されることにも注意してください。

Javascript の正規化（Normalize Javascript）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合、HTTP 応答ボディ内での Javascript の検出と正規化を有効にします。プリプロセッサは unescape 関数や decodeURI 関数、String.fromCharCode メソッドなどの難読化 Javascript データを正規化します。プリプロセッサは、unescape、decodeURI、および decodeURIComponent 関数内の次のエンコードを正規化します。

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

プリプロセッサは連続するスペースを検出し、1 つのスペースに正規化します。このオプションが有効である場合、設定フィールドでは、難読化 Javascript データで許容する連続スペースの最大数を指定できます。入力できる値は、1 ～ 65535 です。値 0 を指定すると、このフィールドに関連付けられているプリプロセッサ ルール（120:10）が有効かどうかに関係なく、イベントの生成が無効になります。

プリプロセッサは、Javascript の正符号（+）演算子も正規化し、この演算子を使用して文字列を連結します。

`file_data` 侵入ルール キーワードを使用して、正規化された Javascript データに対し侵入ルールを指し示すことができます。

イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、次に示すように、ルール 120:9、120:10、および 120:11 を有効にします。

表 *171*：*[Javascript* の正規化（*Normalize Javascript*）*]* オプションのルール（*Normalize Javascript Option Rules*）

ルール	以下の場合にトリガーする
120:9	プリプロセッサ内の難読化レベルが 2 以上である。

ルール	以下の場合にトリガーする
120:10	Javascript 難読化データで連続するスペースの数が、許容される連続スペースの最大数として設定された値以上である。
120:11	エスケープされたデータまたはエンコードされたデータに、複数のエンコードタイプが含まれている。

SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））および SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））

[HTTP Inspect の応答（HTTP Inspect Responses）] が有効な場合、これらのオプションは、HTTP 要求の HTTP 応答ボディ内にあるファイルの圧縮部分を圧縮解除します。

（注） HTTP GET 応答で見つかったファイルの圧縮部分**のみ**を圧縮解除できます。

- [SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））] は、Adobe ShockWave Flash（.swf）ファイルの LZMA 互換の圧縮部分を圧縮解除します。
- [SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））] は、Adobe ShockWave Flash（.swf）ファイルの deflate 互換の圧縮部分を圧縮解除します。

[圧縮データの最大深さ（Maximum Compressed Data Depth）]、[圧縮解除データの最大深さ（Maximum Decompressed Data Depth）]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバ フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、file_data 侵入ルール キーワードを使用できます。

イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、次に示すように、ルール 120:12 および 120:13 を有効にします。

表 *172*：*[SWF ファイルの圧縮解除（Decompress SWF File）] オプションのルール（Decompress SWF File Option Rules）*

ルール	以下の場合にトリガーする
120:12	deflate ファイルの圧縮解除に失敗
120:13	LZMA ファイルの圧縮解除に失敗

PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））

[HTTP Inspect の応答（HTTP Inspect Responses）] が有効な場合、[PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate）] は、HTTP 要求の HTTP 応答ボディ内にある Portable Document Format（.pdf）ファイルの deflate 互換の圧縮部分を圧縮解除します。システムは、/FlateDecode

ストリームフィルタが付いたPDFファイルだけを圧縮解除できます。他のフィルタ（`/FlateDecode /FlateDecode` など）はサポートしていません。

（注） HTTP GET 応答で見つかったファイルの圧縮部分**のみ**を圧縮解除できます。

[圧縮データの最大深さ（Maximum Compressed Data Depth）]、[圧縮解除データの最大深さ（Maximum Decompressed Data Depth）]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバ フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、`file_data` 侵入ルール キーワードを使用できます。

イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、次に示すように、ルール 120:14、120:15、120:16、および 120:17 を有効にします。

表 *173*：*[PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））]オプションのルール（Decompress PDF File (Deflate) Option Rules）*

ルール	以下の場合にトリガーする
120:14	ファイルの圧縮解除に失敗
120:15	圧縮タイプがサポート対象外のタイプであるため、ファイルの圧縮解除に失敗
120:16	PDF ストリーム フィルタがサポート対象外のフィルタであるため、ファイルの圧縮解除に失敗
120:17	ファイルの解析に失敗

元のクライアント IP アドレスの抽出（Extract Original Client IP Address）

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーから、元のクライアント IP アドレスを抽出できるようにします。侵入イベント テーブル ビューで、抽出された元のクライアント IP アドレスを表示できます。

ルール 119:23、119:29 および 119:30 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定，（1063 ページ）を参照してください。

XFF ヘッダーの優先順位（XFF Header Priority）

[元のクライアント IP アドレスの抽出（Extract Original Client IP Address）] が有効な場合、システムが元のクライアント IP の HTTP ヘッダーを処理する順序を指定します。モニタ対象ネットワークで、X-Forwarded-For（XFF）または True-Client-IP 以外の元のクライアント IP ヘッダーが発生すると予測される場合は、[追加（Add）]をクリックしてプライオリティ リストに追加のヘッダー名を追加します。追加したら、各ヘッダー タイプの横にある上下矢印アイコンを使用して、優先

順位を調整します。HTTP要求に複数のXFFヘッダーがある場合は、優先順位が最も高いヘッダーだけが処理されます。

URI のログ（Log URI）

raw URI が存在する場合に、HTTP 要求パケットから raw URI を抽出できるようにし、このセッションで生成されるすべての侵入イベントにこの URI を関連付けます。

このオプションが有効である場合、侵入イベント テーブル ビューの [HTTP URI] 列に、抽出された URI の先頭 50 文字を表示できます。パケット ビューでは、URI 全体（最大 2048 バイト）を表示できます。

ホスト名のログ（Log Hostname）

ホスト名が存在する場合に、HTTP 要求の Host ヘッダーからホスト名を抽出できるようにし、このセッションで生成されるすべての侵入イベントにこのホスト名を関連付けます。複数の Host ヘッダーがある場合は、1 番目のヘッダーからホスト名を抽出します。

このオプションが有効である場合、侵入イベント テーブル ビューの [HTTP ホスト名（HTTP Hostname）] 列に、抽出されたホスト名の先頭 50 文字を表示できます。パケット ビューでは、ホスト名全体（最大 256 バイト）を表示できます。

ルール 119:25 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

有効にすると、このオプションの設定に関係なく、HTTP 要求で複数のホスト ヘッダーが検出された場合、ルール 119:24 がトリガーされます。

プロファイル（Profile）

HTTP トラフィック向けに正規化されたエンコードのタイプを指定します。システムには、ほとんどのサーバに適用できるデフォルト プロファイル、Apache サーバと IIS サーバ用のデフォルト プロファイル、およびモニタ対象トラフィックのニーズに合わせて調整できるカスタムのデフォルト設定があります。

- すべてのサーバに対して適切な標準のデフォルト プロファイルを使用するには、[すべて（All）] を選択します。
- システムによって提供される IIS プロファイルを使用するには、[IIS] を選択します。
- システムによって提供される Apache プロファイルを使用するには、[Apache] を選択します。
- 独自のサーバ プロファイルを作成するには、[カスタム（Custom）] を選択します。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）
概要：HTTP content および protected_content キーワードの引数, （1141 ページ）
http_encode キーワード, （1234 ページ）
file_data キーワード, （1237 ページ）

サーバレベルの HTTP 正規化エンコード オプション

HTTP サーバレベルの [プロファイル（Profile）] オプションを `Custom` に設定すると、HTTP トラフィックに対して正規化されるエンコード タイプを指定できます。また、HTTP のプリプロセッサ ルールを有効にして、異なるエンコードタイプを含むトラフィックに対してイベントを生成できます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ASCII エンコード

エンコードされた ASCII 文字をデコードし、ルール エンジンが ASCII エンコード URI でイベントを生成するかどうかを指定します。

ルール 119:1 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

UTF-8 エンコード

URI の標準 UTF-8 Unicode シーケンスをデコードします。

ルール 119:6 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

Microsoft %U エンコード

%u とその後に続く 4 文字を使用する IIS %u エンコード スキームをデコードします。この 4 文字は、IIS Unicode コードポイントに関連する 16 進数のエンコード値です。

ヒント 正規のクライアントが %u エンコードを使用することはほとんどないため、シスコは、%u エンコードによってエンコードされている HTTP トラフィックをデコードすることを推奨します。

ルール 119:3 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

ベア バイト UTF-8 エンコード

ベア バイト エンコードをデコードします。ベア バイト エンコードは、UTF-8 値のデコード時に非 ASCII 文字を有効な値として使用します。

ヒント　ベア バイト エンコードにより、ユーザは IIS サーバをエミュレートし、非標準エンコードを正しく解釈することができます。正規のクライアントはこの方法で UTF-8 をエンコードしないため、シスコは、このオプションを有効にすることを推奨します。

ルール 119:4 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

Microsoft IIS エンコード

Unicode コードポイント マッピングを使用してデコードします。

ヒント　これは主に攻撃と回避の試行で見られるため、シスコはこのオプションを有効にすることを推奨します。

ルール 119:7 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

二重符号化

要求 URI を 2 回通過し、それぞれでデコードを実行するようにすることで、IIS 二重エンコードトラフィックをデコードします。これは通常は攻撃シナリオでのみ検出されるため、シスコはこのオプションを有効にすることを推奨します。

ルール 119:2 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

マルチスラッシュ オブファスケーション

1 つの行内の複数のスラッシュを 1 つのスラッシュに正規化します。

ルール 119:8 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

IIS バックスラッシュ オブファスケーション

バックスラッシュをスラッシュに正規化します。

ルール 119:9 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

ディレクトリ トラバーサル

ディレクトリ トラバーサルおよび自己参照用ディレクトリを正規化します。一部の Web サイトはディレクトリ トラバーサルを使用してファイルを参照するため、このタイプのトラフィックに対してイベントを生成するために、関連するプリプロセッサ ルールを有効にすると、誤検出が発生する可能性があります。

ルール 119:10 と 119:11 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

タブ オブファスケーション

スペース区切り記号としてタブを使用する非 RFC 標準を正規化します。Apache やその他の非 IIS Web サーバは、URL の区切り文字としてタブ文字（0x09）を使用します。

（注） このオプションの設定に関係なく、空白文字（0x20）がタブの前にある場合、HTTP Inspect プリプロセッサはそのタブをスペースとして扱います。

ルール 119:12 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

無効な RFC 区切り文字

URI データの改行（\ n）を正規化します。

ルール 119:13 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

Webroot ディレクトリ トラバーサル

URL の初期ディレクトリを越えて横断するディレクトリ トラバーサルを検出します。

ルール 119:18 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

タブ区切り（URI）

URI の区切り文字としてタブ文字（0x09）を有効にします。Apache、新しいバージョンの IIS、およびその他の一部の Web サーバは、URL の区切り文字としてタブ文字を使用します。

（注） このオプションの設定に関係なく、空白文字（0x20）がタブの前にある場合、HTTP Inspect プリプロセッサはそのタブをスペースとして扱います。

非 RFC 文字

対応するフィールドに追加された非RFC文字リストが、着信または発信URIデータ内に含まれている場合にそれを検出します。このフィールドを変更する場合は、バイト文字を表す16進表記を使用します。このオプションを設定する場合は、値を慎重に設定してください。非常に一般的な文字を使用すると、イベントが大量に発生する可能性があります。

ルール 119:14 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

チャンク形式の最大エンコード サイズ

URI データで異常に大きなチャンク サイズを検出します。

ルール 119:16 と 119:22 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

パイプライン デコードの無効化

パイプライン処理された要求の HTTP デコードを無効にします。このオプションが無効である場合、パイプラインで待機する HTTP 要求には、デコードおよび分析は行われず、汎用パターンマッチングを使用した検査のみが行われるため、パフォーマンスが向上します。

Non-Strict URI 解析

Non-Strict URI 解析を有効にします。このオプションは、「GET /index.html abc xo qr \n」という形式の非標準 URI を受け入れるサーバでのみ使用します。このオプションを使用すると、デコーダは URI が 1 番目のスペースと 2 番目のスペースで囲まれているものと想定します。これは、2 番目のスペースの後に有効な HTTP 識別子がない場合でも同様です。

拡張 ASCII エンコード

HTTP 要求 URI の拡張 ASCII 文字の解析を有効にします。このオプションは、カスタム サーバ プロファイルでのみ使用可能であり、Apache、IIS、またはすべてのサーバ向けに提供されるデフォルト プロファイルでは使用できないことに注意してください。

関連トピック

概要：HTTP content および protected_content キーワードの引数, （1141 ページ）

HTTP 検査プリプロセッサの設定

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

システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際のIPアドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

はじめる前に

- カスタム ターゲットベース ポリシーで識別するネットワークが、親ネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、およびVLANのサブセットと一致するか、サブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定, （1262 ページ）を参照してください。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に[ネットワーク分析ポリシー（Network Analysis Policy）]をクリックします。 または[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に[ネットワーク分析ポリシー（Network Analysis Policy）]をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで[設定（Settings）]をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）]の下の[HTTPの設定（HTTP Configuration）]が無効になっている場合は、[有効化（Enabled）]をクリックします。

ステップ 5 [HTTPの設定（HTTP Configuration）]の横にある編集アイコン（）をクリックします。

ステップ 6 [グローバル設定（Global Settings）]ページ エリアのオプションを変更します。グローバル HTTP 正規化オプション, （1306 ページ）を参照してください。

ステップ 7 次の 3 つの選択肢があります。

- サーバプロファイルの追加：[サーバ（Servers）]セクションの追加アイコン（）をクリックします。クライアントの 1 つ以上の IP アドレスを[サーバ アドレス（Server Address）]フィールドに指定し、[OK] をクリックします。単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。リストに入力できる文字数は最大 496 文字、すべてのサーバプロファイルで指定できるアドレス項目の総数は 256、作成できるプロファイルの総数はデフォルト プロファイルを含めて 255 です。
- サーバプロファイルの編集：[サーバ（Servers）]の下で追加したプロファイルの設定済みアドレスをクリックするか、[デフォルト（default）]をクリックします。[設定（Configuration）]セクションの設定を変更できます。サーバレベルの HTTP 正規化オプション, （1307 ページ）を参照してください。プロファイル値で[カスタム（Custom）]を選択した場合は、サーバレ

ベルの HTTP 正規化エンコードオプション, （1317 ページ）で説明されているエンコーディング オプションを変更することもできます。

- サーバプロファイルの削除：カスタムプロファイルの横にある削除アイコン（）をクリックします。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

次の作業

- イベントを生成し、インライン展開では、違反パケットをドロップします。 する場合は、HTTP プリプロセッサ ルール（GID 119）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

レイヤの管理, （1023 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

その他の HTTP 検査プリプロセッサ ルール

特定の設定オプションに関連付けられていない HTTP Inspect プリプロセッサ ルールのイベントを生成するには、次の表の 「プリプロセッサ ルール GID：SID」列のルールを有効にできます。

表 *174*：その他の *HTTP* 検査プリプロセッサ ルール

プリプロセッサルール GID:SID	説明
120:5	HTTP 応答トラフィックで UTF-7 エンコードが検出された場合にイベントが生成されます。UTF-7 は、SMTP トラフィックなどで 7 ビット パリティが必要な場合にのみ使用してください。
119:21	HTTP 要求ヘッダーに複数の `content-length` フィールドがある場合にイベントが生成されます。
119:24	HTTP 要求に複数の Host ヘッダーがある場合に、イベントが生成されます。
119:28 120:8	これらのルールを有効にする場合、イベントは生成されません。

プリプロセッサルール GID:SID	説明
119:32	トラフィックで HTTP バージョン 0.9 が検出されると、イベントが生成されます。TCP ストリームの設定も有効にする必要があることに注意してください。
119:33	エスケープされていないスペースが HTTP URI に含まれている場合に、イベントが生成されます。
119:34	TCP 接続に 24 以上のパイプライン処理された HTTP 要求が含まれている場合に、イベントが生成されます。

Sun RPC プリプロセッサ

リモート プロシージャ コール（RPC）の正規化では、フラグメント化された複数の RPC レコードを取得し、それらを 1 つのレコードに正規化するので、ルール エンジンがそのレコード全体を検査できます。たとえば、攻撃者が RPC `admind` が実行されているポートの検出を試行するとします。一部の UNIX ホストは、RPC `admind` を使用してリモート分散システム タスクを実行します。ホストが弱い認証を実行する場合、悪意のあるユーザがリモート管理のコントロールを獲得できることがあります。Snort ID（SID）575 の標準テキスト ルール（GID：1）では、特定のロケーションでコンテンツを検索して、不適切な `portmap GETPORT` 要求を特定することで、この攻撃を検出します。

Sun RPC プリプロセッサのオプション

ポート

トラフィックを正規化するポートを示します。インターフェイスで、複数のポートをカンマで区切って指定します。一般的な RPC ポートは 111 および 32771 です。ネットワークが他のポートに RPC トラフィックを送信する場合は、それらのポートの追加を検討してください。

RPC フラグメント化レコードの検出（Detect fragmented RPC records）

RPC フラグメント化レコードを検出します。

ルール 106:1 と 106:5 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定，（1063 ページ）を参照してください。

1 パケットの複数レコードの検出（Detect multiple records in one packet）

パケット（または再構成されたパケット）ごとに、複数の RPC 要求を検出します。

ルール106:2を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

1 フラグメントを超えるフラグメント化レコード合計の検出（Detect fragmented record sums which exceed one fragment）

現在のパケット長を超える再構成されたフラグメント化レコード長を検出します。

ルール106:3を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

1パケットのサイズを超える単一フラグメント レコードの検出（Detect single fragment records which exceed the size of one packet）

部分的なレコードを検出します。

ルール106:4を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

Sun RPC プリプロセッサの設定

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

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に[ネットワーク分析ポリシー（Network Analysis Policy）]をクリックします。 または[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に[ネットワーク分析ポリシー（Network Analysis Policy）]をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [Sun RPC の構成（Sun RPC Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [Sun RPC の構成（Sun RPC Configuration）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 Sun RPC プリプロセッサのオプション, （1323 ページ）で説明されている設定を変更します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

次の作業

- イベントを生成し、インライン展開では、違反パケットをドロップします。 する場合は、Sun RPC プリプロセッサ ルール（GID 106）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

レイヤの管理, （1023 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

SIP プリプロセッサ

Session Initiation Protocol（SIP）は、インターネット テレフォニー、マルチメディア会議、インスタント メッセージング、オンライン ゲーム、ファイル転送などのクライアント アプリケーションの 1 人以上のユーザに対し、1 つ以上のセッションのコールのセットアップ、変更、およびティアダウンを提供します。各 SIP 要求の *method* フィールドは要求の目的を示し、Request-URI に要求の送信先が指定されます。各 SIP 応答のステータス コードは、要求されたアクションの結果を示します。

SIP を使用してコールがセットアップされた後、後続の音声およびビデオによる通信は Real-time Transport Protocol（RTP）により処理されます。セッションのこの部分は、コール チャネル、データ チャネル、または音声/ビデオデータ チャネルと呼ばれることがあります。RTP は、データチャネル パラメータ ネゴシエーション、セッション通知、およびセッションへの招待のために、SIP メッセージ ボディ内で Session Description Protocol（SDP）を使用します。

SIP プリプロセッサは次の処理を実行します。

- SIP 2.0 トラフィックのデコードおよび分析
- SDP データが存在する場合はこのデータを含む SIP ヘッダーとメッセージ ボディを抽出し、抽出したデータを今後のインスペクションのためにルール エンジンに受け渡す

- 次の状態が検出され、対応するプリプロセッサ ルールが有効な場合にイベントを生成する
  - SIP パケット内の異常と既知の脆弱性
  - 順序が間違っているコール シーケンスと無効なコール シーケンス
- コール チャネルの無視（オプション）

プリプロセッサは、SIP メッセージ ボディに組み込まれている SDP メッセージに示されているポートに基づいて RTP チャネルを識別しますが、RTP プロトコル インスペクションを実行しません。

SIP プリプロセッサを使用するときは、次の点に注意してください。

- UDP は通常、SIP でサポートされるメディア セッションを伝送します。UDP ストリームの前処理により、SIP プリプロセッサに対し SIP セッション トラッキングが提供されます。
- SIP ルール キーワードにより、SIP パケット ヘッダーまたはメッセージ ボディを指し示し、検出対象を特定の SIP メソッドまたはステータス コードのパケットに限定できます。

SIP プリプロセッサのオプション

次のオプションでは、1 から 65535 バイトの正の値を指定するか 0 を指定して、関連するルールが有効にされているかどうかにかかわらず、オプションのイベント生成を無効にできます。

- 要求 URI の最大長（Maximum Request URI Length）
- コール ID の最大長（Maximum Call ID Length）
- 要求名の最大長（Maximum Request Name Length）
- 送信元の最大長（Maximum From Length）
- 送信先の最大長（Maximum To Length）
- 経由の最大長（Maximum Via Length）
- 連絡先の最大長（Maximum Contact Length）
- コンテンツの最大長（Maximum Content Length）

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

SIP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。ポート番号が複数ある場合は、カンマで区切ります。

検査するメソッド（Methods to Check）

検出する SIP メソッドを指定します。次に示す現在定義されている SIP メソッドを指定できます。

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

メソッドでは大文字と小文字が区別されません。メソッド名には英字、数字、下線文字を使用できます。その他の特殊文字は使用できません。複数のメソッドはカンマで区切ります。

新しい SIP メソッドが今後定義される可能性があるため、設定には、現在定義されていない英字文字列を含めることができます。 システムでは最大 32 個のメソッド（現在定義されている 21 個のメソッドと追加の 11 個のメソッド）がサポートされます。システムは、設定される未定義のメソッドをすべて無視します。

合計 32 個のメソッドには、このオプションに指定するメソッドの他に、侵入ルールで `sip_method` キーワードを使用して指定するメソッドも含まれることに注意してください。

セッション内のダイアログ最大数（Maximum Dialogs within a Session）

ストリーム セッション内で許容されるダイアログの最大数を指定します。この数より多くのダイアログが作成されると、ダイアログの数が、指定されている最大数以下になるまで、最も古いダイアログから順に削除されます。1 ～ 4194303 の整数を指定できます。

ルール 140:27 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定, （1063 ページ）を参照してください。

要求 URI の最大長（Maximum Request URI Length）

[要求 URI（Request-URI）] ヘッダー フィールドの最大許容バイト数を指定します。ルール 140:3 が有効である場合、URI が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[要求 URI（Request-URI）] フィールドは、要求の宛先のパスまたはページを示します。

コール ID の最大長（Maximum Call ID Length）

[要求または応答のコール ID（request or response Call-ID）] ヘッダー フィールドの最大許容バイト数を指定します。ルール 140:5 が有効である場合、Call-ID が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[コール ID（Call-ID）] フィールドによって、要求や応答内の SIP セッションが一意に識別されます。

要求名の最大長（Maximum Request Name Length）

要求名で許容される最大バイト数を指定します。要求名は、CSeq トランザクション ID に指定されるメソッドの名前です。ルール 140:7 が有効である場合、リクエスト名が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。

送信元の最大長（Maximum From Length）

要求または応答の [送信元（From）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:9 が有効である場合、[送信元（From）] が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[送信元（From）] フィールドは、メッセージの発信側を識別します。

送信先の最大長（Maximum To Length）

要求または応答の [送信先（To）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:11 が有効である場合、[送信先（To）] が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[送信先（To）] フィールドは、メッセージの受信側を識別します。

経由の最大長（Maximum Via Length）

要求または応答の [経由（Via）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:13 が有効である場合、[経由（Via）] が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[経由（Via）] フィールドには要求がたどるパスが示され、応答の場合は受信者情報が示されます。

連絡先の最大長（Maximum Contact Length）

要求または応答の [連絡先（Contact）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:15 が有効である場合、[連絡先（Contact）] が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[連絡先（Contact）] フィールドには、後続のメッセージについての連絡先を指定する URI が示されます。

コンテンツの最大長（Maximum Content Length）

要求または応答のメッセージ ボディのコンテンツで許容される最大バイト数を指定します。ルール 140:16 が有効である場合、コンテンツが長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。

音声/ビデオ データ チャネルを無視（Ignore Audio/Video Data Channel）

データ チャネル トラフィックのインスペクションを有効または無効にします。このオプションを有効にすると、プリプロセッサはその他の非データ チャネル SIP トラフィックのインスペクションを続行するので注意してください。

関連トピック

SIP キーワード, （1196 ページ）

SIP プリプロセッサの設定

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

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SIP の設定（SIP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [SIP の設定（SIP Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 SIP プリプロセッサのオプション, （1326 ページ）の説明に従ってオプションを変更します。

ステップ 7 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

次の作業

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、SIP プリプロセッサ ルール（GID 140）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

レイヤの管理, （1023 ページ）

競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

その他の SIP プリプロセッサ ルール

次の表に示す SIP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。その他の SIP プリプロセッサ ルールと同様に、これらのルールによってイベントを生成し、インライン展開では、違反パケットをドロップします。 する場合は、これらのルールを有効にする必要があります。

表 *175*：その他の *SIP* プリプロセッサ ルール

プリプロセッサルール GID:SID	以下の場合にトリガーする
140:1	プリプロセッサがモニタしている SIP セッションの数が、システムで許容される最大数である。
140:2	SIP 要求で [要求 URI（Request URI）] 必須フィールドが空である。
140:4	SIP 要求または応答の Call-ID ヘッダー フィールドが空である。
140:6	SIP 要求または応答の CSeq フィールドのシーケンス番号値が、231 未満の 32 ビット符号なし整数ではない。
140:8	SIP 要求または応答の [送信元（From）] 必須フィールドが空である。
140:10	SIP 要求または応答の [送信先（To）] ヘッダー フィールドが空である。
140:12	SIP 要求または応答の [経由（Via）] ヘッダー フィールドが空である。
140:14	SIP 要求または応答で [連絡先（Contact）] 必須フィールドが空である。
140:17	UDP トラフィック内の 1 つの SIP 要求または応答パケットに複数のメッセージが含まれている。SIP の旧バージョンでは複数メッセージがサポートされていますが、SIP 2.0 ではパケットあたり 1 メッセージだけがサポートされていることに注意してください。
140:18	UDP トラフィック内の SIP 要求または応答のメッセージ本文の実際の長さが SIP 要求または応答の [コンテンツ長（Content-Length）] ヘッダー フィールドに指定されている値と一致しない。
140:19	プリプロセッサが SIP 応答の [CSeq] フィールドのメソッド名を認識しない。
140:20	SIP サーバが、認証済み招待メッセージに対してチャレンジを送信しない。これは InviteReplay 請求攻撃の場合に発生することに注意してください。
140:21	呼び出しが設定される前に、セッション情報が変更される。これは FakeBusy 請求攻撃の場合に発生することに注意してください。

プリプロセッサルール GID:SID	以下の場合にトリガーする
140:22	応答ステータス コードが 3 桁の数字でない。
140:23	[コンテンツ タイプ（Content-Type）] ヘッダー フィールドにコンテンツ タイプが指定されておらず、メッセージ ボディにデータが含まれている。
140:24	SIP バージョンが 1、1.1、2.0 でない。
140:25	SIP 要求で、[CSeq] ヘッダーで指定されたメソッドとメソッド フィールドが一致しない。
140:26	プリプロセッサが SIP 要求のメソッド フィールドに指定されたメソッドを認識しない。

GTP プリプロセッサ

General Packet Radio Service（GPRS）Tunneling Protocol（GTP）により、GTP コア ネットワークを介した通信が実現します。GTP プリプロセッサは、GTP トラフィックの異常を検出し、コマンド チャネル シグナリング メッセージをインスペクションのためにルール エンジンに転送します。GTP コマンド チャネル トラフィックでエクスプロイトがあるかどうかを検査するには、`gtp_version`、`gtp_type`、および `gtp_info` ルール キーワードを使用します。

1 つの構成オプションで、プリプロセッサが GTP コマンド チャネル メッセージを検査するポートのデフォルト設定を変更できます。

関連トピック

GTP キーワード, （1198 ページ）

GTP プリプロセッサ ルール

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、次の表に示す GTP プリプロセッサ ルールを有効にする必要があります。

表 *176* : *GTP* プリプロセッサ ルール

プリプロセッサルール GID:SID	説明
143:1	プリプロセッサが無効なメッセージの長さを検出すると、イベントが生成されます。
143:2	プリプロセッサが無効な情報要素の長さを検出すると、イベントが生成されます。
143:3	プリプロセッサが誤った順序の情報要素を検出すると、イベントが生成されます。

GTP プリプロセッサの設定

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

GTP プリプロセッサが GTP コマンド メッセージをモニタするポートを変更するには、次の手順を使用します。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。または[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 左側のナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [GTP コマンド チャネル構成（GTP Command Channel Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [GTP コマンド チャネル構成（GTP Command Channel Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 ポート値を入力します。
複数のポートを指定する場合は、カンマで区切ります。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次の作業

- 侵入イベントを有効にする場合は、GTP プリプロセッサ ルール（GID 143）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）を参照してください。

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

IMAP プリプロセッサ

Internet Message Application Protocol（IMAP）は、リモート IMAP サーバから電子メールを取得するときに使用されます。IMAP プリプロセッサはサーバ/クライアント IMAP4 トラフィックを検査し、関連するプリプロセッサ ルールが有効な場合は、異常なトラフィックがあるとイベントを生成します。プリプロセッサは、クライアント/サーバ IMAP4 トラフィックの電子メール添付ファイルを抽出してデコードし、添付ファイルデータをルールエンジンに送信することもできます。添付ファイル データを指し示すには、侵入ルールで `file_data` キーワードを使用します。

抽出とデコードでは、複数の添付ファイル（存在する場合）や、複数パケットにまたがる大きな添付ファイルなども処理されます。

IMAP プリプロセッサ オプション

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 デコーディングの深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）] オプションの値が以下のポリシーで異なる場合は、最も大きい値が使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

注意 [Base64 復号の深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリ復号化の深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [UNIX 間復号の深さ（Unix-to-Unix Decoding Depth）] の値の変更設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

IMAP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。ポート番号が複数ある場合は、カンマで区切ります。

Base64 デコーディングの深さ（Base64 Decoding Depth）

各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはすべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

このオプションが有効である場合、ルール 141:4 を有効にすると、デコードの失敗時に イベントを生成し、インライン展開では、違反パケットをドロップします。 することができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）

デコードを必要としない各 MIME 電子メール添付ファイルから抽出するデータの最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。正値またはパケット内のすべてのデータを抽出するには 0 を指定できます。非デコード データを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 141:6 を有効にすると、抽出の失敗時に イベントを生成し、インライン展開では、違反パケットをドロップします。 することができます（たとえばデータの破損のために抽出が失敗することがあります）。

Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）

各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはパケットのすべての QP エンコード済みデータを復号化する場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 141:5 を有効にすると、デコードの失敗時に イベントを生成し、インライン展開では、違反パケットをドロップします。 することができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）

各 Unix-to-Unix エンコード（UU エンコード）電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。パケットのすべての UU エンコード データをデコードするには、正値を指定するか、0 を指定できます。UU エンコードデータを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 141:7 を有効にして、デコードの失敗時に イベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

関連トピック

file_data キーワード, （1237 ページ）

IMAP プリプロセッサの設定

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

注意 [Base64 復号の深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリ復号化の深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [UNIX 間復号の深さ（Unix-to-Unix Decoding Depth）] の値の変更設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。または[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [IMAP の構成（IMAP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [IMAP の構成（IMAP Configuration）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 IMAP プリプロセッサ オプション, （1333 ページ）で説明されている設定を変更します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次の作業

- 侵入イベントを有効にする場合は、IMAP プリプロセッサ ルール（GID 141）を有効にします。侵入ルール状態の設定, （1063 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

侵入ポリシーおよびネットワーク分析ポリシーのレイヤ, （1015 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

その他の IMAP プリプロセッサ ルール

次の表に示す IMAP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。他の IMAP プリプロセッサ ルールの場合と同様に、これらのルールでイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、ルールを有効にする必要があります。

表 *177*：その他の *IMAP* プリプロセッサ ルール

プリプロセッサルール GID:SID	説明
141:1	プリプロセッサが RFC 3501 に定義されていないクライアント コマンドを検出すると、イベントが生成されます。
141:2	プリプロセッサが RFC 3501 に定義されていないサーバ応答を検出すると、イベントが生成されます。
141:3	プリプロセッサが使用しているメモリの量が、システムでの最大許容量に達している場合に、イベントが生成されます。この時点で、プリプロセッサはメモリが使用可能になるまでデコードを停止します。

POP プリプロセッサ

Post Office Protocol（POP）は、リモート POP メール サーバから電子メールを取得するときに使用されます。POP プリプロセッサは、サーバからクライアントへの POP3 トラフィックを検査し、関連付けられているプリプロセッサ ルールが有効な場合は、異常なトラフィックについてのイベントを生成します。プリプロセッサは、クライアントからサーバへの POP3 トラフィック内の電子メールの添付ファイルを抽出して復号化（デコード）し、添付ファイルデータをルールエンジンに送信することもできます。添付ファイルデータを指し示すには、侵入ルールで `file_data` キーワードを使用します。

抽出とデコードでは、複数の添付ファイル（存在する場合）や、複数パケットにまたがる大きな添付ファイルなども処理されます。

POP プリプロセッサ オプション

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 デコーディングの深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）] オプションの値が以下のポリシーで異なる場合は、最も大きい値が使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

注意 [Base64 復号の深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリ復号化の深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [UNIX 間復号の深さ（Unix-to-Unix Decoding Depth）] の値の変更設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

POP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。ポート番号が複数ある場合は、カンマで区切ります。

Base64 デコーディングの深さ（Base64 Decoding Depth）

各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはすべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

このオプションが有効である場合、ルール 142:4 を有効にして、デコードの失敗時に イベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）

デコードを必要としない各 MIME 電子メール添付ファイルから抽出するデータの最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。正値またはパケット内のすべてのデータを抽出するには 0 を指定できます。非デコード データを無視するには、-1 を指定します。

このオプションが有効であれば、抽出が失敗したときにルール 142:6 を有効にして イベントを生成し、インライン展開では、違反パケットをドロップします。 できます。抽出は、たとえば、データの破損により失敗することがあります。

Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）

各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはパケットのすべての QP エンコード済みデータを復号化する場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 142:5 を有効にして、デコードの失敗時に イベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）

各 Unix-to-Unix エンコード（UU エンコード）電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。パケットのすべての UU エンコード データをデコードするには、正値を指定するか、0 を指定できます。UU エンコードデータを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 142:7 を有効にして、デコードの失敗時に イベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

関連トピック

レイヤの管理, （1023 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）
file_data キーワード, （1237 ページ）

POP プリプロセッサの設定

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

注意 [Base64 復号の深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリ復号化の深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [UNIX 間復号の深さ（Unix-to-Unix Decoding Depth）] の値の変更設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作，（326 ページ）を参照してください。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。または[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [POP の構成（POP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [POP の構成（POP Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 POP プリプロセッサ オプション，（1337 ページ）で説明されている設定を変更します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次の作業

- 侵入イベントを有効にする場合は、POPプリプロセッサルール（GID 142）を有効にします。詳細については、侵入ルール状態の設定，（1063 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

関連トピック

レイヤの管理，（1023 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー，（1011 ページ）

その他の POP プリプロセッサ ルール

次の表に示すPOPプリプロセッサルールは、特定の設定オプションに関連付けられていません。その他の POP プリプロセッサ ルールと同様に、これらのルールによって イベントを生成し、インライン展開では、違反パケットをドロップします。 する場合は、これらのルールを有効にする必要があります。

表 *178*：その他の *POP* プリプロセッサ ルール

プリプロセッサルール GID:SID	説明
142:1	プリプロセッサが RFC 1939 に定義されていないクライアント コマンドを検出すると、イベントが生成されます。
142:2	プリプロセッサがRFC 1939に定義されていないサーバ応答を検出すると、イベントが生成されます。
142:3	プリプロセッサが使用しているメモリの量が、システムでの最大許容量に達している場合に、イベントが生成されます。この時点で、プリプロセッサはメモリが使用可能になるまでデコードを停止します。

SMTP プリプロセッサ

SMTPプリプロセッサはルールエンジンに対し、SMTPコマンドを正規化するように指示します。このプリプロセッサは、クライアントからサーバへのトラフィック内の電子メールの添付ファイルを抽出して復号化（デコード）することもできます。またソフトウェアのバージョンによっては、SMTP トラフィックによりトリガーされた侵入イベントの表示時にコンテキストを提供するために、電子メールのファイル名、アドレス、およびヘッダー データも抽出します。

SMTP プリプロセッサのオプション

正規化を有効または無効にし、SMTP デコーダが検出する異常トラフィックのタイプを制御するオプションを設定できます。

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 デコーディングの深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）] オプションの値が以下のポリシーで異なる場合は、最も大きい値が使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

注意 [Base64 復号の深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリ復号化の深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [UNIX 間復号の深さ（Unix-to-Unix Decoding Depth）] の値の変更設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

SMTP トラフィックを正規化するポートを指定します。0以上の値を指定できます。複数のポートを指定する場合は、カンマで区切ります。

ステートフル インスペクション（Stateful Inspection）

選択されている場合、SMTP デコーダは状態を保存し、各パケットのセッション コンテキストを提供し、再構成されたセッションだけを検査します。選択されていない場合、セッション コンテキストなしで個々のパケットを分析します。

正規化（Normalize）

[すべて（All）]に設定すると、すべてのコマンドが正規化されます。コマンドの後に複数のスペース文字があるかどうかを確認します。

[なし（None）] に設定すると、コマンドは正規化されません。

[Cmds] に設定すると、[カスタム コマンド（Custom Commands）] にリストされているコマンドが正規化されます。

カスタム コマンド（Custom Commands）

[正規化（Normalize）] が [Cmds] に設定されている場合に、リストされているコマンドが正規化されます。

正規化する必要があるコマンドをテキスト ボックスに指定します。コマンドの後に複数のスペース文字があるかどうかを確認します。

スペース文字（ASCII 0x20）とタブ文字（ASCII 0x09）は、正規化のためにスペース文字としてカウントされます。

データを無視（Ignore Data）

メール データを処理せず、MIME メール ヘッダー データだけを処理します。

TLS データを無視（Ignore TLS Data）

Transport Layer Security プロトコルで暗号化されたデータを処理しません。

アラートなし（No Alerts）

関連するプリプロセッサ ルールが有効である場合に、侵入イベントを無効にします。

不明なコマンドの検出（Detect Unknown Commands）

SMTP トラフィックで不明なコマンドを検出します。

このオプションに関する イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 124:5 を有効にできます。

コマンドラインの最大長（Max Command Line Len）

SMTP コマンドラインがこの値より長い場合にそのことを検出します。コマンドラインの長さを検出しない場合は、0 を指定します。

RFC 2821（Network Working Group による Simple Mail Transfer Protocol 仕様）では、コマンドラインの最大長として 512 が推奨されています。

このオプションに関する イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 124:1 を有効にできます。

ヘッダー行の最大長（Max Header Line Len）

SMTP データ ヘッダー行がこの値より長い場合にそのことを検出します。データ ヘッダー行の長さを検出しない場合は、0 を指定します。

このオプションに関して イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 124:2 および 124:7 を有効にします。

応答行の最大長（Max Response Line Len）

SMTP応答行がこの値より長い場合にそのことを検出します。応答行の長さを検出しない場合は、0 を指定します。

RFC 2821 では、応答行の最大長として 512 が推奨されています。

ルール 124:3 を有効にすると、このオプションに関して、および [代替のコマンドラインの最大長（Alt Max Command Line Len）] オプション（有効になっている場合）に関して イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

代替のコマンドラインの最大長（Alt Max Command Line Len）

指定のコマンドの SMTP コマンドラインがこの値より長い場合にそのことを検出します。指定したコマンドのコマンドライン長を検出しない場合は、0を指定します。多数のコマンドに対して、さまざまなデフォルト ライン長が設定されています。

この設定は、指定されたコマンドの [コマンドラインの最大長（Max Command Line Len）] の設定をオーバーライドします。

ルール 124:3 を有効にすると、このオプションに関して、および [応答行の最大長（Max Response Line Len）] オプション（有効になっている場合）に関してイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

無効なコマンド（Invalid Commands）

これらのコマンドがクライアント側から送信された場合にそのことを検出します。

ルール 124:6 を有効にすると、このオプションに関して、および [無効なコマンド（Invalid Commands）] に関して イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

有効なコマンド（Valid Commands）

このリストのコマンドを許可します。

このリストが空の場合でも、プリプロセッサにより許可される有効なコマンドは、ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR です。

（注） RCPT TO および MAIL FROM は SMTP コマンドです。プリプロセッサ設定では、コマンド名 RCPT と MAIL がそれぞれ使用されます。プリプロセッサはコード内で RCPT および MAIL を正しいコマンド名にマッピングします。

ルール 124:4 を有効にすると、このオプションに関して、および [無効なコマンド（Invalid Commands）] オプション（設定済みの場合）に関してイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

データ コマンド（Data Commands）

RFC 5321 に基づく SMTP DATA コマンドによるデータの送信と同じ方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

バイナリ データ コマンド（Binary Data Commands）

RFC 3030 に基づく BDAT コマンドによるデータの送信と類似の方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

認証コマンド（Authentication Commands）

クライアントおよびサーバ間で認証交換を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

xlink2state の検出（Detect xlink2state）

X-Link2State Microsoft Exchange バッファ データ オーバーフロー攻撃の一部であるパケットを検出します。インライン展開では、システムはこれらのパケットをドロップすることもできます。

このオプションに関する イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 124:8 を有効にできます。

Base64 デコーディングの深さ（Base64 Decoding Depth）

[データを無視（Ignore Data）] が無効である場合、各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。正の値から指定するか 0 を指定して、すべての Base64 データをデコードします。Base64 データを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータをデコードしません。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

このオプションが有効である場合、ルール 124:10 を有効にすると、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

このオプションは、廃止されたオプション [MIME デコーディングの有効化（Enable MIME Decoding）] および [MIME デコーディングの最大の深さ（Maximum MIME Decoding Depth）] の代わりに使用されます。廃止されたこれらのオプションは、既存の侵入ポリシーでは後方互換性を維持する目的で引き続きサポートされています。

7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）

[データを無視（Ignore Data）] が無効である場合、デコードを必要としない各 MIME 電子メール添付ファイルから抽出する最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。正値またはパケット内のすべてのデータを

抽出するには0を指定できます。非デコードデータを無視するには、-1を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータを抽出しません。

Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）

[データを無視（Ignore Data）] が無効な場合、各 quoted-printable（QP）エンコードMIME電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。

1 ～ 65535 バイトを指定するか、または、パケットのすべての QP エンコード データをデコードする場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータをデコードしません。

このオプションが有効である場合、ルール 124:11 を有効にすると、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。 することができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）

[データを無視（Ignore Data）] が無効な場合、各 UNIX 間エンコード（UU エンコード）電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての UU エンコード データをデコードする場合は 0 を指定します。UUエンコードデータを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータをデコードしません。

このオプションが有効である場合、ルール 124:13 を有効にすると、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。 することができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

MIME 添付ファイル名のログ（Log MIME Attachment Names）

MIME Content-Dispositionヘッダーからの MIME 添付ファイル名の抽出を有効にして、セッションで生成されるすべての侵入イベントにこのファイル名を関連付けます。複数ファイル名がサポートされています。

このオプションが有効である場合、侵入イベントのテーブル ビューの [電子メール添付（Email Attachment）] 列に、イベントに関連付けられているファイル名が表示されます。

受信者アドレスのログ（Log To Addresses）

SMTP RCPT TO コマンドからの受信者の電子メール アドレスの抽出を有効にし、セッションで生成されるすべての侵入イベントにこの受信者アドレスに関連付けます。複数の受信者がサポートされます。

このオプションが有効である場合、侵入イベントのテーブル ビューの [電子メール受信者（Email Recipient）] 列に、イベントに関連付けられている受信者が表示されます。

送信者アドレスのログ（Log From Addresses）

SMTP MAIL FROM コマンドからの送信者の電子メール アドレスの抽出を有効にし、セッションで生成されるすべての侵入イベントにこの送信者アドレスを関連付けます。複数の送信者アドレスがサポートされます。

このオプションが有効である場合、侵入イベントのテーブル ビューの [電子メール送信者（Email Sender）] 列に、イベントに関連付けられている送信者が表示されます。

ヘッダーのログ（Log Headers）

電子メール ヘッダーの抽出を有効にします。抽出されるバイト数は、[ヘッダーのログの深さ（Header Log Depth）] に指定されている値によって決まります。

キーワード `content` または `protected_content` を使用して、電子メール ヘッダー データをパターンとして使用する侵入ルールを作成できます。侵入イベント パケット ビューに、抽出された電子メール ヘッダーが表示されます。

ヘッダーのログの深さ（Header Log Depth）

[ヘッダーのログ（Log Headers）] が有効である場合、抽出する電子メールヘッダーのバイト数を指定します。0 ～ 20480 バイトを指定できます。値 0 を指定すると、[ヘッダーのログ（Log Headers）] が無効になります。

関連トピック

基本コンテンツおよび protected_content キーワードの引数, （1137 ページ）

SMTP デコードの設定

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

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

注意 [Base64 復号の深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリ復号化の深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [UNIX 間復号の深さ（Unix-to-Unix Decoding Depth）] の値の変更設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。または[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SMTP の設定（SMTP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [SMTP の設定（SMTP Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 SMTP プリプロセッサのオプション, （1341 ページ）の説明に従ってオプションを変更します。

ステップ 7 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

次の作業

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、SMTP プリプロセッサ ルール（GID 124）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

レイヤの管理, （1023 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

SSH プリプロセッサ

SSH プリプロセッサでは、次の攻撃を検出します。

- チャレンジレスポンス バッファ オーバーフロー エクスプロイト
- CRC-32 エクスプロイト
- SecureCRT SSH クライアント バッファ オーバーフロー エクスプロイト
- プロトコル不一致
- 不正な SSH メッセージの方向
- バージョン 1 または 2 以外のすべてのバージョン文字列

チャレンジレスポンス バッファ オーバーフロー攻撃と CRC--32 攻撃はいずれもキー交換の後に発生するので、暗号化されています。いずれの攻撃でも、20 KB を超える普通よりも大きなペイロードが認証チャレンジ直後にサーバに送信されます。CRC--32 攻撃の対象となるのは SSH バージョン 1 のみであり、チャレンジレスポンス バッファ オーバーフロー エクスプロイトの対象となるのは SSH バージョン 2 のみです。バージョン文字列は、セッションの開始時に読み取られます。バージョン文字列の違いを除き、この両方の攻撃は同様に扱われます。

SecureCRT SSH エクスプロイトとプロトコル不一致攻撃は、鍵交換前に接続をセキュリティで保護しようとするときに発生します。SecureCRT エクスプロイトでは、非常に長いプロトコル ID 文字列がクライアントに送信され、これが原因でバッファ オーバーフローが発生します。プロトコル不一致は、非 SSH クライアント アプリケーションがセキュア SSH サーバに接続しようとした場合、またはサーバとクライアントのバージョン番号が一致しない場合に発生します。

SSH プリプロセッサは、指定のポートまたはポートのリストでトラフィックを検査するか、または SSH トラフィックを自動的に検出するように設定できます。指定バイト数に達するまでに指定数の暗号化パケットが渡されたか、指定パケット数に達するまでにバイト数が指定最大バイト数を超えるまで、SSH トラフィックの検査が続行されます。最大バイト数を超えた場合は、CRC--32（SSH バージョン 1）攻撃またはチャレンジレスポンス バッファ オーバーフロー（SSH バージョン 2）攻撃が発生したとみなされます。プリプロセッサは、設定していない場合でもバージョン 1 または 2 以外のバージョン文字列を検出することに注意してください。

SSH プリプロセッサでは、ブルートフォース攻撃が処理されないことにも注意してください。

SSH プリプロセッサのオプション

次のいずれかが発生すると、プリプロセッサはセッションのトラフィックの検査を停止します。

- この数の暗号化パケットで、サーバとクライアント間で有効な交換が行われた場合。接続は続行します。

- 検査対象の暗号化パケットの数に達する前に、[サーバ応答がないまま送信されたバイト数（Number of Bytes Sent Without Server Response）] に達した場合。この場合、攻撃があったものと想定されます。

[検査する暗号化パケットの数（Number of Encrypted Packets to Inspect）] に達するまでの有効な各サーバ応答により、[サーバ応答がないまま送信されたバイト数（Number of Bytes Sent Without Server Response）] がリセットされ、パケット カウントが続行します。

次に示す SSH のプリプロセッサの設定例で説明します。

- [サーバ ポート（Server Ports）]：22
- [自動検出ポート（Autodetect Ports）]：off
- [プロトコル バージョン ストリングの最大長（Maximum Length of Protocol Version String）]：80
- [検査する暗号化パケットの数（Number of Encrypted Packets to Inspect）]：25
- [サーバ応答がないまま送信されたバイト数（Number of Bytes Sent Without Server Response）]：19,600
- 検出オプションはすべて有効です。

この例では、プリプロセッサはポート22のトラフィックだけを検査します。つまり、自動検出が無効であるため、指定されたポートでのみ検査をします。

また、次のいずれかが発生すると、この例のプリプロセッサはトラフィックの検査を停止します。

- クライアントが 25 個の暗号化パケットを送信したが、すべてのパケットのデータ合計が 19,600 バイト以下であった。攻撃はなかったと想定されます。
- クライアントが、25 個の暗号化パケットで 19,600 バイトを超えるデータを送信した。この場合、この例のセッションはSSHバージョン2セッションであるため、プリプロセッサはこの攻撃がチャレンジレスポンス バッファ オーバーフロー攻撃であるとみなします。

この例のプリプロセッサは、トラフィックの処理時に以下の状況が発生しているかどうかも検出します。

- 80バイトより長いバージョン文字列によりトリガーとして使用されるサーバオーバーフロー（これは SecureCRT エクスプロイトを示します）
- プロトコルの不一致
- 誤った方向に流れるパケット

最後に、プリプロセッサは、バージョン 1 または 2 以外のすべてのバージョン文字列を自動的に検出します。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

サーバ ポート（Server Ports）

SSH プリプロセッサがトラフィックを検査する必要があるポートを指定します。

1 つのポート、または複数のポートをカンマで区切ったリストを設定できます。

自動検出ポート（Autodetect Ports）

SSH トラフィックを自動的に検出するようにプリプロセッサを設定します。

このオプションが選択されている場合、プリプロセッサはすべてのトラフィックで SSH バージョン番号を検査します。クライアントパケットにもサーバパケットにもバージョン番号が含まれていない場合は、処理が停止します。無効である場合、プリプロセッサは [サーバ ポート（Server Ports）] オプションで指定されているトラフィックだけを検査します。

検査する暗号化パケットの最大数（Number of Encrypted Packets to Inspect）

セッションあたりの検査対象の暗号化パケットの数を指定します。

このオプションをゼロに設定すると、すべてのトラフィックの通過が許可されます。

検査対象の暗号化パケットの数を減らすと、一部の攻撃が検出されなくなることがあります。検査対象の暗号化パケットの数を増やすと、パフォーマンスに悪影響を及ぼす可能性があります。

サーバ応答がないまま送信されたバイト数（Number of Bytes Sent Without Server Response）

SSH クライアントが、応答なしでサーバに送信できる最大バイト数を指定します。この最大バイト数を超えると、チャレンジレスポンス バッファ オーバーフロー攻撃または CRC-32 攻撃が想定されます。

プリプロセッサがチャレンジレスポンス バッファ オーバーフローまたは CRC-32 エクスプロイトを誤検出する場合は、このオプションの値を増やしてください。

プロトコル バージョン ストリングの最大長（Maximum Length of Protocol Version String）

サーバのバージョン文字列の最大許容バイト数を指定します。この値を超えると、SecureCRT エクスプロイトとみなされます。

チャレンジレスポンス バッファ オーバーフロー攻撃の検出（Detect Challenge-Response Buffer Overflow Attack）

チャレンジレスポンス バッファ オーバーフロー エクスプロイトの検出を有効または無効にします。

このオプションに関する イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:1 を有効にできます。

SSH1 CRC-32 攻撃の検出（Detect SSH1 CRC-32 Attack）

CRC-32 エクスプロイトの検出を有効または無効にします。

このオプションに関する イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:2 を有効にできます。

サーバ オーバーフローの検出（Detect Server Overflow）

SecureCRT SSH クライアント バッファ オーバーフロー エクスプロイトの検出を有効または無効にします。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 128:3 を有効にします。

プロトコル不一致の検出（Detect Protocol Mismatch）

プロトコル不一致の検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:4 を有効にできます。

正しくないメッセージ方向の検出（Detect Bad Message Direction）

トラフィックのフロー方向が正しくない場合（つまり、推定されるサーバがクライアント トラフィックを生成したり、クライアントがサーバ トラフィックを生成したりした場合）の検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:5 を有効にできます。

特定のペイロードに正しくないペイロード サイズの検出（Detect Payload Size Incorrect for the Given Payload）

SSH パケットに指定された長さが IP ヘッダーに指定されている合計長と矛盾する場合や、メッセージが切り捨てられる場合、つまり完全な SSH ヘッダーを形成できる十分なデータがない場合などの、誤ったペイロード サイズのパケットの検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:6 を有効にできます。

正しくないバージョン ストリングの検出（Detect Bad Version String）

有効である場合、プリプロセッサは、設定していない場合でもバージョン 1 または 2 以外のバージョン文字列を検出することに注意してください。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:7 を有効にできます。

SSH プリプロセッサの設定

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

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SSH の構成（SSH Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [SSH の構成（SSH Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 SSH プリプロセッサのオプション, （1348 ページ）の説明に従ってオプションを変更します。

ステップ 7 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次の作業

- 侵入イベントを有効にする場合は、SSH プリプロセッサ ルール（GID 128）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

レイヤの管理, （1023 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

SSL プリプロセッサ

SSL プリプロセッサでは、SSL インスペクション（検査）を設定できます。SSL インスペクションでは、暗号化トラフィックのブロック、暗号化トラフィックの復号化、またはアクセス コントロール（アクセス制御）によるトラフィックの検査を実行します。SSL インスペクションが設定されているかどうかに関係なく、SSL プリプロセッサでは、トラフィックで検出された SSL ハンドシェイク メッセージも分析し、セッションを暗号化するタイミングを決定します。暗号化トラ

フィックを識別することにより、システムは暗号化ペイロードの侵入およびファイル インスペクションを停止できます。これによって、誤検出が減少し、パフォーマンスが向上します。

SSL プリプロセッサは、暗号化トラフィックを検査して Heartbleed バグを悪用する試みを検出し、そのような悪用の検出時にイベントを生成することもできます。

セッションが暗号化されると、侵入およびマルウェアに対するトラフィックの検査を一時停止できます。SSL インスペクションを設定した場合、SSL プリプロセッサでは、ユーザがアクセス コントロールによってブロック、復号化、または検査を行える暗号化トラフィックも識別します。

SSL プリプロセッサを使用して暗号化トラフィックを復号化するために、ライセンスは必要ありません。マルウェアおよび侵入に対する暗号化ペイロードのインスペクションの停止、Heartbleed バグの悪用の検出など、他のすべての SSL プリプロセッサ機能には保護ライセンスが必要です。

関連トピック

SSL インスペクションの要件, （868 ページ）

SSL 前処理の仕組み

SSL インスペクションを設定すると、SSL プリプロセッサは暗号化データに対する侵入およびファイル インスペクションを停止して、SSL ポリシーにより暗号化トラフィックを検査します。これにより誤検出を排除できます。SSL プリプロセッサは、SSL ハンドシェイクを検査するときに状態情報を保持し、そのセッションの状態と SSL バージョンの両方を追跡します。セッションの状態が暗号化されていることをプリプロセッサが検出すると、そのセッションのトラフィックは暗号化されているものとしてシステムによりマークされます。暗号化が確定した場合に暗号化セッションにおけるすべてのパケット処理を停止し、Heartbleed のバグを悪用する試みが検出された場合にイベントを生成するように、システムを設定できます。

パケットごとに、IP ヘッダー、TCP ヘッダー、および TCP ペイロードがトラフィックに含まれており、このトラフィックが SSL 前処理用に指定されているポートで発生することが SSL プリプロセッサにより確認されます。次に示す状況では、対象トラフィックについて、トラフィックが暗号化されているかどうかが判別されます。

- システムがセッションのすべてのパケットを監視し、[サーバ側のデータを信頼する（Server side data is trusted）] が有効にされておらず、サーバとクライアントの両方からの完了メッセージ、および Application レコードが存在するが Alert レコードがない各側からの 1 つ以上のパケットが、セッションに含まれている。
- システムがトラフィックの一部を検出せず、[サーバ側のデータを信頼する（Server side data is trusted）] が有効にされておらず、Alert レコードによる応答がない Application レコードが存在する各側からの 1 つ以上のパケットが、セッションに含まれている。
- システムがセッションのすべてのパケットを監視し、[サーバ側のデータを信頼する（Server side data is trusted）] が有効であり、クライアントからの完了メッセージ、および Application レコードが存在するが Alert レコードがないクライアントからの 1 つ以上のパケットが、セッションに含まれている。

- システムがトラフィックの一部を検出せず、[サーバ側のデータを信頼する（Server side data is trusted）] が有効であり、Alert レコードによる応答がない Application レコードが存在するクライアントからの 1 つ以上のパケットが、セッションに含まれている。

暗号化トラフィックの処理を停止することを選択する場合、セッションが暗号化されているものとしてマークされると、そのセッションのその後のパケットは無視されます。

また、SSL ハンドシェイク時、プリプロセッサはハートビート要求と応答をモニタします。プリプロセッサは、以下を検出したときにイベントを生成します。

- ペイロード自体よりも大きいペイロード長の値を含むハートビート要求
- [ハートビートの最大長（Max Heartbeat Length）] フィールドに格納されている値よりも大きいハートビート応答

（注） ルール内で SSL 状態またはバージョン情報を使用するには、キーワード `ssl_state` および `ssl_version` をルールに追加します。

関連トピック

SSL キーワード, （1186 ページ）

SSL プリプロセッサのオプション

（注） システム付属のネットワーク分析ポリシーは、デフォルトで SSL プリプロセッサを有効にします。暗号化トラフィックがネットワークを通過することを予想している場合、シスコは、カスタム展開で SSL プリプロセッサを無効にしないことを推奨します。

SSLインスペクションを設定しないと、システムは暗号化トラフィックを復号化せずに、マルウェアと侵入について暗号化トラフィックの検査を試行します。SSLプリプロセッサを有効にすると、セッションが暗号化されたときにそのことを検出します。SSLプリプロセッサが有効にされると、ルール エンジンがこのプリプロセッサを呼び出し、SSL の状態およびバージョン情報を取得できるようになります。侵入ポリシーでキーワード `ssl_state` および `ssl_version` を使用してルールを有効にする場合は、そのポリシーで SSL プリプロセッサも有効にする必要があります。

ポート

SSL プリプロセッサは、暗号化されたセッションのトラフィックをモニタする必要があるポートを、カンマで区切って指定します。このフィールドで指定されるポートでのみ、暗号化トラフィックが検査されます。

（注） SSLプリプロセッサは、SSLモニタの対象として指定されたポートでSSL以外のトラフィックを検出すると、そのトラフィックを SSL トラフィックとしてデコードすることを試みた後、破損しているものとしてマークします。

暗号化トラフィックの検査を停止する（Stop inspecting encrypted traffic）

セッションが暗号化されているとしてマークされた後、セッションのトラフィックの検査を有効または無効にします。

暗号化されたセッションの検査を無効化しリアセンブルするには、このオプションを有効にします。SSL プリプロセッサによりセッションの状態が維持されるため、セッションのすべてのトラフィックのインスペクションを無効にできます。システムは、次の両方の場合に、暗号化されたセッションのトラフィックの検査のみを停止します。

- SSL の前処理が有効にされている
- このオプションが選択されている

このオプションをクリアすると、[サーバ側のデータを信頼する（Server side data is trusted）] オプションを変更できません。

サーバ側のデータを信頼する（Server side data is trusted）

[暗号化トラフィックの検査を停止する（Stop inspecting encrypted traffic）] が有効にされてあり、クライアント側のトラフィックにのみ基づいて暗号化されたトラフィックの識別を有効にすると、

ハートビートの最大長（Max Heartbeat Length）

バイト数を指定して、ハートビートバグ悪用の試みに対する SSL ハンドシェイク内のハートビート要求と応答の検査を有効にします。1 ～ 65535 の整数を指定できます。このオプションを無効にする場合は 0 を入力します。

プリプロセッサがハートビート要求を検出し、このペイロード長が実際のペイロード長より大きく、ルール 137:3 が有効にされている場合、または、ルール 137:4 が有効にされている際に、このオプションに設定された値よりハートビート応答のサイズが大きい場合は、プリプロセッサはイベントを生成し、インライン展開では、違反パケットをドロップします。。

SSL プリプロセッサの設定

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

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SSL 設定（SSL Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [SSL 設定（SSL Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 SSL プリプロセッサのオプション, （1354 ページ） に示されている任意の設定を変更します。

- [ポート（Ports）] フィールドに値を入力します。複数の値を指定する場合は、カンマで区切ります。
- [暗号化トラフィックの検査の停止（Stop inspecting encrypted traffic）] チェックボックスをオンまたはオフにします。
- [暗号化トラフィックの検査の停止（Stop inspecting encrypted traffic）] チェックボックスをオンにした場合は、[サーバ側データは信頼済み（Server side data is trusted）] チェックボックスをオンまたはオフにします。
- [最大ハートビート長（Max Heartbeat Length）] フィールドに値を入力します。

  ヒント 値 0 を指定すると、このオプションが無効になります。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次の作業

- 侵入イベントを有効にする場合は、SSL プリプロセッサ ルール（GID 137）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

レイヤの管理, （1023 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

SSL プリプロセッサ ルール

イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、SSL プリプロセッサ ルール（GID 137）を有効にします。

次の表に、有効にできる SSL プリプロセッサ ルールを示します。

表 *179* : *SSL* プリプロセッサ ルール

プリプロセッサルール GID:SID	説明
137:1	ServerHello メッセージの後の ClientHello メッセージを検出します。これは無効であり、異常な動作とみなされます。
137:2	SSL プリプロセッサ オプション [サーバ側のデータを信頼する（Server side data is trusted）] が無効な場合に、ClientHello メッセージのない ServerHello メッセージを検出します。これは無効であり、異常な動作としてみなされます。
137:3	SSL プリプロセッサ オプション [ハートビートの最大長（Max Heartbeat Length）] にゼロ以外の値が含まれている場合に、ペイロード自体よりも大きいペイロード長の値を含むハートビート要求を検出します。このようなハートビート要求は、Heartbleed バグを悪用する試みを示しています。
137:4	SSL プリプロセッサ オプション [ハートビートの最大長（Max Heartbeat Length）] で指定されているゼロ以外の値よりも大きいハートビート応答を検出します。このようなハートビート応答は、Heartbleed バグを悪用する試みを示しています。

第 59 章

SCADA プリプロセッサ

以下のトピックでは、遠隔監視制御・情報取得（SCADA）プロトコルのプリプロセッサとその設定方法について説明します。

SCADA プリプロセッサの概要

Supervisory Control and Data Acquisition（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャ プロセス、および設備プロセスからのデータをモニタ、制御、取得します。Firepower システムは、ネットワーク分析ポリシーの一部として設定できる Modbus および DNP3 SCADA プロトコル用のプリプロセッサを提供します。

対応する侵入ポリシーで Modbus または DNP3 キーワードを含むルールを有効にすると、Modbus または DNP3 プロセッサがその現在の設定で自動的に使用されます。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

Modbus プリプロセッサ

Modbus プロトコルは 1979 年に Modicon が初めて発表した、広く利用されている SCADA プロトコルです。Modbus プリプロセッサは、Modbus トラフィックの異常を検出し、ルール エンジンによる処理のために Modbus プロトコルをデコードします。ルール エンジンは Modbus キーワードを使用して特定のプロトコル フィールドにアクセスします。

1 つの構成オプションで、プリプロセッサが Modbus トラフィックを検査するポートのデフォルト設定を変更できます。

関連トピック

SCADA キーワード，（1212 ページ）

Modbus プリプロセッサ ポート オプション

ポート

プリプロセッサが Modbus トラフィックを検査するポートを指定します。複数のポートを指定する場合は、カンマで区切ります。

Modbus プリプロセッサの設定

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

ネットワークに Modbus 対応デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。または[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [SCADA プリプロセッサ（SCADA Preprocessors）] の下の [Modbus の構成（Modbus Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [Modbus の構成（Modbus Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 [ポート（Ports）] フィールドに値を入力します。
複数の値を指定する場合は、カンマで区切ります。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

次の作業

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、Modbus プリプロセッサ ルール（GID 144）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）およびModbus プリプロセッサ ルール, （1361 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

レイヤの管理, （1023 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

Modbus プリプロセッサ ルール

次の表に示す Modbus プリプロセッサ ルールによって イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、これらのルールを有効にする必要があります。

表 *180* : *Modbus* プリプロセッサ ルール

プリプロセッサルール GID:SID	説明
144:1	Modbus の見出しの長さが、Modbus 機能コードに必要な長さと一致していない場合に、イベントが生成されます。 各 Modbus 機能の要求と応答には期待される形式があります。メッセージの長さが、期待される形式と一致しない場合に、このイベントが生成されます。
144:2	Modbus プロトコル ID がゼロ以外の場合に、イベントが生成されます。プロトコル ID フィールドは、Modbus と共にその他のプロトコルを多重伝送するために使用されます。プリプロセッサはこのような他のプロトコルを処理しないため、代わりにこのイベントが生成されます。
144:3	プリプロセッサが予約済み Modbus 機能コードを検出すると、イベントが生成されます。

DNP3 プリプロセッサ

Distributed Network Protocol（DNP3）は、当初は発電所間で一貫性のある通信を実現する目的で開発されたSCADAプロトコルです。DNP3も、水処理、廃棄物処理、輸送などさまざまな産業分野で幅広く利用されるようになっています。

DNP3 プリプロセッサは、DNP3 トラフィックの異常を検出し、ルール エンジンによる処理のために DNP3 プロトコルをデコードします。ルール エンジンは、DNP3 キーワードを使用して特定のプロトコル フィールドにアクセスします。

関連トピック

DNP3 キーワード, （1214 ページ）

DNP3 プリプロセッサ オプション

ポート

指定された各ポートでの DNP3 トラフィックのインスペクションを有効にします。1 つのポートを指定するか、複数のポートをカンマで区切ったリストを指定できます。

無効な CRC を記録（Log bad CRCs）

DNP3 リンク層フレームに含まれているチェックサムを検証します。無効なチェックサムを含むフレームは無視されます。

ルール 145:1 を有効にすると、無効なチェックサムが検出されたときに イベントを生成し、インライン展開では、違反パケットをドロップします。 できます。

DNP3 プリプロセッサの設定

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

ネットワークにDNP3対応デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。または[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [SCADA プリプロセッサ（SCADA Preprocessors）] の下の [DNP3 の構成（DNP3 Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [DNP3 の構成（DNP3 Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 ポートの値を入力します。
複数の値を指定する場合は、カンマで区切ります。

ステップ 7 [不良 CRC の記録（Log bad CRCs）] チェックボックスをオンまたはオフにします。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

次の作業

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、DNP3 プリプロセッサ ルール（GID 145）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）、DNP3 プリプロセッサ オプション, （1362 ページ）、およびDNP3 プリプロセッサ ルール, （1363 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

レイヤの管理, （1023 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

DNP3 プリプロセッサ ルール

次の表に示す DNP3 プリプロセッサ ルールによってイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、これらのルールを有効にする必要があります。

表 *181* : *DNP3* プリプロセッサ ルール

プリプロセッサルール GID:SID	説明
145:1	[無効な CRC を記録（Log bad CRC）] が有効である場合に、無効なチェックサムを含むリンク層フレームがプリプロセッサにより検出されると、イベントが生成されます。
145:2	無効な長さの DNP3 リンク層フレームがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:3	再構成中に無効なシーケンス番号のトランスポート層セグメントがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:4	完全なフラグメントを再構成する前に DNP3 再構成バッファがクリアされると、イベントが生成されます。このことは、FIR フラグを伝送するセグメントが、他のセグメントがキューに入れられた後で現れる場合に発生します。
145:5	予約済みアドレスを使用する DNP3 リンク層フレームをプリプロセッサが検出すると、イベントが生成されます。
145:6	予約済み機能コードを使用する DNP3 要求または応答をプリプロセッサが検出すると、イベントが生成されます。

第 60 章

トランスポート層およびネットワーク層プリプロセッサ

以下のトピックでは、トランスポート層およびネットワーク層プリプロセッサとそれらの設定方法について説明します。

トランスポート層およびネットワーク層のプリプロセッサの概要

トランスポート層およびネットワーク層のプリプロセッサは、IP フラグメンテーション、チェックサム検証、TCP および UDP セッションの前処理を悪用する攻撃を検出します。パケットがプリプロセッサに送信される前に、パケットデコーダはパケットヘッダーとペイロードを、プリプロセッサおよび侵入ルールエンジンで簡単に使用できるフォーマットに変換し、パケットヘッダー内でさまざまな変則的動作を検出します。インライン正規化プリプロセッサは、パケットをデコードした後、他のプリプロセッサにパケットを送信する前に、インライン型展開を対象にトラフィックを正規化します。

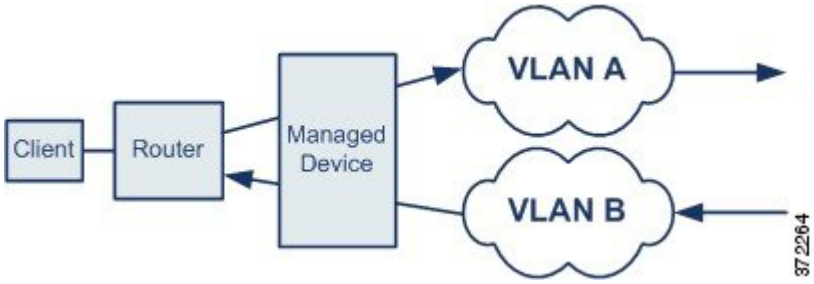
侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。

トランスポート/ネットワーク プリプロセッサの詳細設定

トランスポート/ネットワーク プリプロセッサの詳細設定は、アクセス コントロール ポリシーを展開するすべてのネットワーク、ゾーン、VLAN にグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。

無視される VLAN ヘッダー

同じ接続で異なる方向に流れるトラフィックの VLAN タグが異なると、トラフィックのリアセンブルやルールの処理に影響を与える場合があります。たとえば、以下の図では、同じ接続のトラフィックを VLAN A で送信し、VLAN B で受信できます。



展開でパケットを正しく処理するため、VLAN ヘッダーを無視するようにシステムを設定できます。

（注） このオプションは、ASA FirePOWER ではサポートされません。

侵入廃棄ルールでのアクティブ応答

廃棄ルールは、ルール状態が [ドロップしてイベントを生成する（Drop and Generate Events）] に設定された侵入ルールまたはプリプロセッサ ルールです。インライン展開では、システムは TCP または UDP 廃棄ルールに応答するために、トリガーしたパケットをドロップし、そのパケットが開始されたセッションをブロックします。パッシブ展開の場合、システムがパケットをドロップすることはできません。また、セッションをブロックすることもありませんが、アクティブ応答を使用する場合はその限りではありません。

ヒント UDP データ ストリームは一般にセッションという観点では考慮されないため、ストリーム プリプロセッサはカプセル化 IP データグラム ヘッダーの送信元と宛先の IP アドレス フィールドと UDP ヘッダーのポート フィールドを使用してフローの方向を判別し、UDP セッションを識別します。

問題のあるパケットによってTCPまたはUDP廃棄ルールがトリガーされた時点で、1つ以上のアクティブ応答を開始して、より正確かつ明示的にTCP接続またはUDPセッションを閉じるようにシステムを設定することができます。

インライン展開でアクティブ応答が有効にされている場合、システムはTCP廃棄ルールへの応答として、トリガーしたパケットをドロップし、クライアントとサーバの両方のトラフィックにTCPリセット（RST）パケットを挿入します。システムはパッシブ展開でパケットをドロップできません。アクティブ応答がパッシブ展開で有効になっている場合、システムはTCP接続のクライアント側とサーバ側の両方にTCPリセットを送信することによってTCP廃棄ルールに応答します。インライン展開またはパッシブ展開でアクティブ応答が有効にされていると、システムはセッションの両端にICMP到達不能パケットを送信することによってUDPセッションを閉じます。リセットは接続やセッションに影響を与えるのに間に合うまでに到着する可能性が高いため、アクティブ応答はインライン展開で最も効果を発揮します。

設定内容によっては、接続またはセッションのいずれかの側からさらにトラフィックが発生しているようであれば、システムが追加のアクティブ応答を開始することもできます。システムは、指定された間隔（秒数）で、指定された最大回数まで追加のアクティブ応答を開始します。

トランスポート/ネットワーク プリプロセッサの詳細オプション

接続の追跡時にVLANヘッダーを無視する（Ignore the VLAN header when tracking connections）

トラフィックの識別時にVLANヘッダーを無視するか、それとも考慮するかを指定します。次のようになります。

- このオプションを選択すると、VLANヘッダーが無視されます。この設定は、異なる方向に移動するトラフィックで同じ接続について異なるVLANタグを検出する可能性がある展開済みデバイスに使用します。
- このオプションを無効にすると、VLANヘッダーが考慮されます。この設定は、異なる方向に移動するトラフィックで同じ接続について異なるVLANタグを検出しない展開済みデバイスに使用します。

（注） このオプションは、ASA FirePOWER ではサポートされていません。

アクティブ応答の最大数（Maximum Active Responses）

TCP接続あたりのアクティブ応答の最大数を指定します。アクティブ応答が開始された接続でさらにトラフィックが発生し、前のアクティブ応答を送信してから[最小応答秒数（Minimum Response Seconds）]を超えるトラフィックが発生した場合、システムは指定された最大数に達するまで、別のアクティブ応答を送信します。0を設定すると、廃棄ルールによってトリガーされるアクティブ応答が無効になり、respまたはreactルールによってトリガーされる追加のアクティブ応答も無効になります。

このオプションの設定とは関係なく、respまたはreactルールがトリガーされた場合にも、アクティブ応答が開始されることに注意してください。ただし、このオプションは、ドロップ ルール

でアクティブ応答の最大数を制御するのと同じ方法で、resp および react ルールで追加のアクティブ応答をシステムが開始するかどうかを制御します。

`config response` コマンドを使用して、使用するアクティブ応答インターフェイス、およびパッシブ展開で試行する TCP リセットの回数を設定することもできます。

最小応答時間（秒）（Minimum Response Seconds）

[最大アクティブ応答数（Maximum Active Responses）] に達するまで、システムがアクティブ応答を開始した接続で発生した追加のトラフィックに対して次のアクティブ応答を送信するまで待機する時間を指定します。

トラブルシューティング オプション：セッション終了ロギングしきい値（Troubleshooting Options: Session Termination Logging Threshold）

注意 [セッション終了ロギングしきい値（Session Termination Logging Threshold）] は、サポート担当から指示されない限り変更しないでください。

トラブルシューティングの電話中に、個別の接続が指定したしきい値を超えた場合にメッセージを記録するようにシステムを設定することをサポートから依頼される場合があります。このオプションの設定を変更するとパフォーマンスに影響するので、必ずサポートのガイダンスに従って実行してください。

このオプションは、ログに記録されるメッセージのバイト数を指定します。セッションが終了し、メッセージが指定のバイト数を超えた場合は、ログに記録されます。

（注） 上限は 1 GB ですが、管理対象デバイスでストリーム処理のために割り当てられるメモリの量によっても制限されます。

関連トピック

アクティブ応答のキーワード, （1219 ページ）

トランスポート/ネットワーク プリプロセッサの詳細設定の構成

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

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [トランスポート/ネットワーク レイヤ設定（Transport/Network Layer Settings）] セクションの横にある編集アイコン（  ）をクリックします。

ステップ 3 トラブルシューティング オプション [セッション終了のロギングしきい値（Session Termination Logging Threshold）] を除き、トランスポート/ネットワーク プリプロセッサの詳細オプション，（1367 ページ）の説明に従ってオプションを変更します。

（注） [接続のトラッキング時は VLAN ヘッダーを無視（Ignore the VLAN header when tracking connectons）] オプションは、ASA FirePOWER モジュールでは使用できません。

注意 [セッション終了のロギングしきい値（Session Termination Logging Threshold）] は、サポートからの指示がない限り変更しないでください。

ステップ 4 [OK] をクリックします。

次の作業

- 必要に応じて、アクセス コントロール ポリシーの編集，（789 ページ）の説明に従ってさらにポリシーを設定します。
- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

チェックサム検証

システムは、あらゆるプロトコル レベルのチェックサムを検証することで、IP、TCP、UDP、および ICMP による送信データが完全に受信されていることを確認できます。さらに基本的なレベルで、パケットが転送中に改ざんされたり、誤って変更されたりしていないことも確認できます。チェックサムはアルゴリズムを使用して、パケットでのプロトコルの整合性を検証します。システムが終端のホストでパケットに書き込まれた値を計算し、それがチェックサムと同じであれば、そのパケットは変更されていないと見なされます。

チェックサムの検証を無効にすると、ネットワークが侵入攻撃にさらされる危険があります。システムは、チェックサム検証イベントを生成しないことに注意してください。インライン展開では、パケットのチェックサムが正しくない場合、そのパケットをドロップするようにシステムを設定できます。

チェックサム検証オプション

次のオプションは、いずれも、パッシブ展開またはインライン展開で [有効（Enabled）] または [無効（Disabled）] に設定することができます。インライン展開では [ドロップ（Drop）] に設定することもできます。

- ICMP チェックサム（ICMP Checksums）

- IP チェックサム（IP Checksums）
- TCP チェックサム（TCP Checksums）
- UDP チェックサム（UDP Checksums）

違反パケットをドロップするには、オプションを [ドロップ（Drop）] に設定するだけでなく、関連付けられているネットワーク分析ポリシーの [インライン モード（Inline Mode）] を有効にし、確実にデバイスがインラインで展開されるようにする必要があります。

パッシブ展開またはタップモードでのインライン展開で、これらのオプションを[ドロップ（Drop）] に設定することは、[有効（Enabled）] に設定するのと同じです。

すべてのチェックサム検証オプションは、デフォルトで、[有効（Enabled）] になっています。

関連トピック

インライン導入でのプリプロセッサによるトラフィックの変更, （1274 ページ）

チェックサムの確認

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [トランスポート層/ネットワーク層のプロセッサ（Transport/Network Layer Preprocessors）] の下にある [チェックサムの確認（Checksum Verification）] が無効になっている場合、[有効（Enabled）] をクリックします。

ステップ 5 [チェックサムの確認（Checksum Verification）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 チェックサム検証, （1369 ページ） で説明されているオプションを変更します。

ステップ 7 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

レイヤ管理, （1021 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

インライン正規化プリプロセッサ

インライン正規化プリプロセッサは、インライン展開で攻撃者が検出を免れる可能性を最小限にするために、トラフィックを正規化します。

（注） システムでトラフィックに影響を与えるには、ルーテッド、スイッチド、またはトランスペアレント インターフェイスあるいはインライン インターフェイス ペアを使用して、関連する設定を管理対象デバイスに展開する必要があります。

IPv4、IPv6、ICMPv4、ICMPv6、TCP トラフィックを任意に組み合わせて正規化を指定できます。ほとんどの正規化は、パケット単位で行われ、インライン正規化プリプロセッサによって処理されます。ただし、TCP ストリーム プリプロセッサは、TCP ペイロードの正規化を含む、ほとんどの状態関連パケットおよびストリームの正規化を処理します。

インライン正規化は、パケット デコーダによるデコードの直後に行われます。その後で、別のプリプロセッサによる処理が行われます。正規化は、パケット層の内部から外部への方向で行われます。

インライン正規化プリプロセッサはイベントを生成しません。インライン正規化プリプロセッサの役割は、インライン展開の別のプリプロセッサおよびルール エンジンで使用できるようにパ

ケットを準備することです。また、システムが処理するパケットが、ネットワーク上のホストで受信したパケットと同じであるようにする役割もあります。

（注） インライン展開では、インライン モードを有効にし、[TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にして、インライン正規化プリプロセッサを設定することをお勧めします。パッシブ展開では、アダプティブ プロファイルを使用することをお勧めします。

関連トピック

インライン導入でのプリプロセッサによるトラフィックの変更，（1274 ページ）
アダプティブ プロファイルについて，（1429 ページ）

インライン正規化オプション

最小 TTL（Minimum TTL）

[TTL のリセット（Reset TTL）] がこのオプションに設定する値以上の値に設定されている場合、このオプションは以下を指定します。

- [IPv4 の正規化（Normalize IPv4）] が有効にされている場合は、[IPv4 存続可能時間（TTL）（IPv4 Time to Live (TTL)）] フィールドの最小許容値。TTL のパケット値がこの値を下回る場合、[TTL のリセット（Reset TTL）] に設定された値に正規化されます。
- [IPv6 の正規化（Normalize IPv6）] が有効にされている場合は、[IPv6 ホップ リミット（IPv6 Hop Limit）] フィールドの最小許容値。ホップ リミットの値がこの値を下回る場合、[TTL のリセット（Reset TTL）] に設定された値に正規化されます。

このフィールドが空白の場合、システムは値が 1 であると想定します。

パケット復号化の [プロトコル ヘッダー異常の検出（Detect Protocol Header Anomalies）] オプションが有効になっている場合、デコーダ ルール カテゴリで次のルールを有効にして、このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

- 指定の最小値を下回る TTL が設定された IPv4 パケットが検出された場合にトリガーするには、ルール 116:428 を有効にします。
- 指定の最小値を下回るホップ リミットが設定された IPv6 パケットが検出された場合にトリガーするには、ルール 116:270 を有効にします。

TTL のリセット（Reset TTL）

[最小 TTL（Minimum TTL）] の値以上の値を設定した場合、以下のフィールドが正規化されます。

- [IPv4 の正規化（Normalize IPv4）] が有効にされている場合は、[IPv4 TTL] フィールド

- [IPv6 の正規化（Normalize IPv6）] が有効にされている場合は、[IPv6 ホップ リミット（IPv6 Hop Limit）] フィールド

パケット値が [最小 TTL（Minimum TTL）] を下回る場合、システムはパケットの TTL またはホップ リミットの値をこのオプションに対して設定された値に変更して、パケットを正規化します。このフィールドを空白のままにするか、0 に設定するか、または [最小 TTL（Minimum TTL）] 未満の値に設定すると、このオプションは無効になります。

IPv4 の正規化（Normalize IPv4）

IPv4 トラフィックの正規化を有効にします。システムは、以下の場合にも必要に応じて TTL フィールドを正規化します。

- このオプションが有効になっていて、さらに、
- [TTL のリセット（Reset TTL）] に設定された値によって TTL の正規化が有効になっている。

このオプションを有効にすると、追加の IPv4 オプションを有効にすることもできます。

このオプションを有効にすると、システムは以下の基本の IPv4 正規化を実行します。

- 過剰なペイロードを持つパケットを、IP ヘッダーに指定されたデータグラム長まで切り捨てます。
- [差別化サービス（DS）（Differentiated Services (DS)）] フィールド（旧称 [タイプ オブ サービス（TOS）（Type of Service (TOS)）] フィールド）をクリアします。
- すべてのオプション オクテットを 1（[操作なし（No Operation）]）に設定します。

フラグメント禁止ビットの正規化（Normalize Don't Fragment Bit）

[IPv4 フラグ（IPv4 Flags）] ヘッダー フィールドの単一ビットの [フラグメント禁止（Don't Fragment）] サブフィールドをクリアします。このオプションを有効にすると、ダウンストリームのルータがパケットをドロップする代わりに、必要に応じてパケットをフラグメント化できます。また、このオプションを有効にすることで、ドロップされるパケットを巧妙に作成してポリシーを回避する試みを防ぐこともできます。このオプションを選択するには、[IPv4 の正規化（Normalize IPv4）] を有効にする必要があります。

リザーブド ビットの正規化（Normalize Reserved Bit）

[IPv4 フラグ（IPv4 Flags）] ヘッダー フィールドの単一ビットの [予約済み（Reserved）] サブフィールドをクリアします。通常は、このオプションを有効にします。このオプションを選択するには、[IPv4 の正規化（Normalize IPv4）] を有効にする必要があります。

TOS ビットの正規化（Normalize TOS Bit）

1 バイトの [差別化サービス（Differentiated Services）]（旧称 [タイプ オブ サービス（Type of Service）]）フィールドをクリアします。このオプションを選択するには、[IPv4 の正規化（Normalize IPv4）] を有効にする必要があります。

余剰ペイロードの正規化（Normalize Excess Payload）

過剰なペイロードを持つパケットを、IP ヘッダーに指定されたデータグラム長にレイヤ 2（たとえば、イーサネット）ヘッダーを合計した長さにまで切り捨てます。ただし、最小フレーム長より小さく切り捨てることはしません。このオプションを選択するには、[IPv4 の正規化（Normalize IPv4）] を有効にする必要があります。

IPv6 の正規化（Normalize IPv6）

[ホップバイホップ オプション（Hop-by-Hop Options）] および [宛先オプション（Destination Options）] 拡張ヘッダーに含まれるすべてのオプション タイプ フィールドを 00（スキップして処理を続行）に設定します。このオプションが有効にされていて、[TTL のリセット（Reset TTL）] に設定された値がホップ リミット正規化を有効にしている場合、システムは必要に応じてホップ リミット フィールドも正規化します。

ICMPv4 の正規化（Normalize ICMPv4）

ICMPv4 トラフィックのエコー（要求）およびエコー応答メッセージで 8 ビットのコード フィールドをクリアします。

ICMPv6 の正規化（Normalize ICMPv6）

ICMPv6 トラフィックのエコー（要求）およびエコー応答メッセージで 8 ビットのコード フィールドをクリアします。

予約済みビットの正規化またはクリア（Normalize/Clear Reserved Bits）

TCP ヘッダーの予約ビットをクリアします。

オプション パディング バイトの正規化またはクリア（Normalize/Clear Option Padding Bytes）

TCP オプションのパディング バイトをクリアします。

URG=0 の場合に緊急ポインタをクリア（Clear Urgent Pointer if URG=0）

緊急（URG）制御ビットが設定されていない場合、16 ビットの TCP ヘッダー [緊急ポインタ（Urgent Pointer）] フィールドをクリアします。

空のペイロードに設定された緊急ポインタまたは URG をクリア（Clear Urgent Pointer/URG on Empty Payload）

ペイロードがない場合、TCP ヘッダー [緊急ポインタ（Urgent Pointer）] フィールドおよび URG 制御ビットをクリアします。

緊急ポインタが設定されていない場合 URG をクリア（Clear URG if Urgent Pointer is Not Set）

緊急ポインタが設定されていない場合、TCP ヘッダー URG 制御ビットをクリアします。

緊急ポインタの正規化（Normalize Urgent Pointer）

ポインタがペイロード長を上回る場合、2バイトのTCPヘッダー[緊急ポインタ（Urgent Pointer）]フィールドをペイロード長に設定します。

TCP ペイロードの正規化（Normalize TCP Payload）

再送信されるデータの一貫性が確保されるように[TCPデータ（TCP Data）]フィールドの正規化を有効にします。正しく再構成できないセグメントはすべてドロップされます。

SYN に関するデータを削除（Remove Data on SYN）

TCP オペレーティング システム ポリシーが Mac OS **以外**の場合、同期（SYN）パケットのデータを削除します。

また、このオプションにより、TCP ストリーム プリプロセッサの [ポリシー（Policy）] オプションが [Mac OS] に設定されていない場合にトリガー可能なルール 129:2 もまた無効になります。

RST に関するデータを削除（Remove Data on RST）

TCP リセット（RST）パケットからデータを削除します。

データをウィンドウにトリミング（Trim Data to Window）

[TCPデータ（TCP Data）]フィールドを[ウィンドウ（Window）]フィールドに指定されたサイズにまで切り捨てます。

データを MSS にトリミング（Trim Data to MSS）

ペイロードが MSS より長い場合、[TCP データ（TCP Data）] フィールドを最大セグメント サイズ（MSS）にまで切り捨てます。

解決不可能な TCP ヘッダーの異常をブロック（Block Unresolvable TCP Header Anomalies）

このオプションを有効にすると、システムは無効になり受信ホストによってブロックされる可能性が高い異常なTCPパケット（正規化されている場合）をブロックします。たとえば、システムは確立されたセッションの後に送信されたSYNパケットをブロックします。

また、システムは、ルールが有効にされているかどうかに関係なく、以下に示すTCPストリームプリプロセッサ ルールのいずれかに一致するパケットもドロップします。

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 ～ 129:19

[ブロックされたパケットの合計（Total Blocked Packets）] パフォーマンス グラフには、インライン展開でブロックされたパケットの数が示され、パッシブ展開とタップ モードでのインライン展開の場合は、インライン展開でブロックされる予想数が示されます。

明示的な混雑通知（ECN）（Explicit Congestion Notification）

明示的輻輳通知（ECN）フラグのパケット単位またはストリーム単位の正規化を以下のように有効にします。

- [パケット（Packet）] を選択すると、ネゴシエーションに関係なく、パケット単位で ECN フラグがクリアされます。
- [ストリーム（Stream）] を選択すると、ECN の使用がネゴシエートされていない場合、ストリーム単位で ECN フラグがクリアされます。

[ストリーム（Stream）] を選択した場合、この正規化が実行されるようにするには、TCP ストリーム プリプロセッサの [TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）] オプションも有効にされている必要があります。

既存の TCP オプションをクリア（Clear Existing TCP Options）

[これらの TCP オプションを許可（Allow These TCP Options）] を有効にします。

.

これらの TCP オプションを許可（Allow These TCP Options）

トラフィックで許可する特定の TCP オプションの正規化を無効にします。

明示的に許可されたオプションは、正規化されません。オプションを [操作なし（No Operation）]（TCP オプション 1）に設定して明示的に許可していないオプションは、正規化されます。

[これらの TCP オプションを許可（Allow These TCP Options）] の設定に関係なく、次のオプションは最適な TCP パフォーマンスに一般的に使用されるため、システムは常にこれらのオプションを許可します。

- 最大セグメント サイズ（MSS）（Maximum Segment Size (MSS)）
- ウィンドウ スケール（Window Scale）
- タイム スタンプ TCP（Time Stamp TCP）

他のそれほど一般的に使用されないオプションについては、システムは自動的に許可しません。

特定のオプションを許可するには、オプション キーワード、オプション番号、またはこの両方のカンマ区切りリストを設定します。以下に、一例を示します。

```
sack, echo, 19
```

オプション キーワードを指定するということは、そのキーワードと関連付けられた 1 つ以上の TCP オプションの番号を指定することと同じです。たとえば、`sack` を指定することは、TCP オプション 4（[選択的確認応答を許可（Selective Acknowledgment Permitted）]）および TCP オプショ

ン 5（[選択的確認応答（Selective Acknowledgment）]）を指定することと同じです。オプションキーワードでは、大文字と小文字が区別されません。

また、any を指定すると、すべての TCP オプションが許可されるため、実質的にすべての TCP オプションの正規化が無効にされます。

次の表に、許可する TCP オプションを指定する方法を要約します。フィールドを空のままにすると、システムはMSS、ウィンドウスケール、およびタイムスタンプのオプションのみを許可します。

指定する内容	許可されるオプション
sack	TCP オプション 4（Selective Acknowledgment Permitted）および 5（Selective Acknowledgment）
エコー	TCP オプション 6（Echo Request）および 7（Echo Reply）
partial_order	TCP オプション 9（Partial Order Connection Permitted）および 10（Partial Order Service Profile）
conn_count	TCP 接続数オプション 11（CC）、12（CC.New）、および 13（CC.Echo）
alt_checksum	TCP オプション 14（Alternate Checksum Request）および 15（Alternate Checksum）
md5	TCP オプション 19（MD5 Signature）
オプション番号 2 ～ 255	キーワードのないオプションを含む、特定のオプション
任意	すべての TCP オプション（この設定は、実質的に TCP オプションの正規化を無効にします）

このオプションに any を指定しない場合、正規化には次のものが含まれます。

- MSS、ウィンドウ スケール、タイムスタンプ、およびその他の明示的に許可されたオプションを除き、すべてのオプションのバイトを [操作なし（No Operation）]（TCP オプション 1）に設定します。
- タイムスタンプは存在していても無効な場合、あるいは有効であってもネゴシエートされない場合、タイムスタンプ オクテットを [操作なし（No Operation）] に設定します。
- タイムスタンプがネゴシエートされるものの、存在しない場合、パケットをブロックします。
- 確認応答（ACK）制御ビットが設定されていない場合、[タイムスタンプエコー応答（TSecr）（Time Stamp Echo Reply (TSecr)）] オプション フィールドをクリアします。
- SYN 制御ビットが設定されていない場合、[MSS] および [ウィンドウ スケール（Window Scale）] オプションを [操作なし（No Operation）]（TCP オプション 1）に設定します。

関連トピック

侵入イベントのパフォーマンス統計情報グラフの種類，（2007 ページ）

インライン正規化の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

はじめる前に

- 問題を起こすパケットを正規化またはドロップするには、インライン導入でのプリプロセッサによるトラフィックの変更，（1274 ページ）の説明に従って [インライン モード（Inline Mode）] を有効にします。また、管理対象デバイスは、インラインで展開する必要があります。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [トランスポートまたはネットワーク レイヤプリプロセッサ（Transport/Network Layer Preprocessors）] で [インライン正規化（Inline Normalization）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [インライン正規化（Inline Normalization）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 インライン正規化プリプロセッサ，（1371 ページ）で説明されているオプションを設定します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次の作業

- インライン正規化 [最小 TTL（Minimum TTL）] オプションで侵入イベントを生成する場合は、パケット デコーダ ルール 116:429（IPv4）と 116:270（IPv6）のいずれかまたは両方を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）およびインライン正規化オプション, （1372 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

レイヤ管理, （1021 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

IP 最適化プリプロセッサ

最大伝送ユニット（MTU）より大きいために IP データグラムが複数の小さい IP データグラムに分割されると、その IP データグラムはフラグメント化されたことになります。単一の IP データグラム フラグメントには、隠れた攻撃を識別するのに十分な情報が含まれない場合があります。そのため、攻撃者はエクスプロイトの検出を免れるために、フラグメント化されるパケットで攻撃データを送信する可能性があります。IP 最適化プリプロセッサは、ルール エンジンが IP データグラムに対してルールを実行する前に、パケットに仕込まれた攻撃をルールで識別しやすくするために、フラグメント化された IP データグラムを再構成します。フラグメント化されたデータグラムを再構成できない場合、それらのデータグラムに対しては、ルールが実行されません。

IP フラグメンテーション エクスプロイト

IP 最適化を有効にすると、ネットワーク上のホストに対する攻撃（ティアドロップ攻撃など）や、システム自体に対するリソース消費攻撃（Jolt2 攻撃など）を検出するのに役立ちます。

ティアドロップ攻撃は、特定のオペレーティング システムのバグを悪用して、そのオペレーティング システムがオーバーラップした IP フラグメントを再構成しようとするとクラッシュするように仕掛けます。IP 最適化プリプロセッサを有効にして、オーバーラップしたフラグメントを識別するように設定すれば、該当するフラグメントを識別できます。IP 最適化プリプロセッサは、ティアドロップ攻撃などのオーバーラップ フラグメント攻撃で、最初のパケットを検出するだけで、同じ攻撃での後続のパケットは検出しません。

Jolt2 攻撃では、IP 最適化機能を酷使させるという方法でサービス妨害攻撃を仕掛けるために、フラグメント化された同じ IP パケットのコピーを大量に送信します。IP 最適化プリプロセッサでは、メモリ使用量の上限によって、このような攻撃を阻止し、包括的検査においてシステムを自己防衛状態にします。システムは攻撃によって過負荷にならず、運用可能な状態を維持し、ネットワーク トラフィックの検査を続行します。

フラグメント化されたパケットを再構成する方法は、オペレーティング システムによって異なります。ホストがどのオペレーティング システムで実行されているのかを攻撃者が特定できれば、

その攻撃者はターゲット ホストが特定の方法で再構成するように不正なパケットをフラグメント化することも可能です。モニタ対象のネットワーク上でホストを実行しているオペレーティング システムは、システムには不明です。したがって、プリプロセッサがパケットを誤った方法で再構成して検査し、それによってエクスプロイトが検出されないままパス スルーする可能性があります。このような攻撃を軽減するために、ネットワーク上のホストごとに適切な方法でパケットを最適化するよう、最適化プリプロセッサを設定できるようになっています。

パッシブ展開でアダプティブ プロファイルを使用することで、パケットのターゲット ホストのホスト オペレーティング システム情報に応じて、IP 最適化プリプロセッサに適用するターゲット ベースのポリシーが動的に選択されるようにすることもできます。

ターゲット ベースの最適化ポリシー

ホストのオペレーティング システムは以下の 3 つの基準を使用して、パケットを再構成する際に優先するパケット フラグメントを決定します。

- オペレーティング システムがフラグメントを受信した順序
- フラグメントのオフセット（パケットの先頭からのそのフラグメントの距離（バイト単位））
- オーバーラップしているフラグメントとの相対開始位置と相対終了位置

これらの基準はすべてのオペレーティング システムで使用されているものの、フラグメント化されたパケットを再構成するときに優先するフラグメントは、オペレーティング システムによって異なります。したがって、ネットワーク上で異なるオペレーティング システムを使用する 2 台のホストが、同じオーバーラップ フラグメントをまったく異なる方法で再構成する場合も考えられます。

いずれかのホストのオペレーティング システムを認識している攻撃者が、オーバーラップしたパケット フラグメントに不正なコンテンツを忍ばせて送信することによって、エクスプロイトの検出を免れ、そのホストを悪用する可能性があります。このパケットが他のホストで再構成されて検査されても、パケットに害はないように見えますが、ターゲット ホストで再構成される場合には不正なエクスプロイトが含まれています。ただし、モニタ対象のネットワーク セグメントで稼働するオペレーティング システムを認識するようにIP最適化プリプロセッサを設定すれば、このプリプロセッサがターゲット ホストと同じ方法でフラグメントを再構成することによって、攻撃を識別できます。

IP 最適化オプション

IP 最適化を有効または無効にすることだけを選択することもできますが、シスコでは、それよりも細かいレベルで、有効にする IP 最適化プリプロセッサの動作を指定することを推奨しています。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

次のグローバル オプションを構成できます。

事前に割り当てられたフラグメント（Preallocated Fragments）

プリプロセッサが一度に処理できる個々のフラグメントの最大数。事前割り当てするフラグメント ノードの数を指定すると、静的メモリ割り当てが有効になります。

注意 個々のフラグメントの処理には、約 1550 バイトのメモリが使用されます。プリプロセッサで個々のフラグメントを処理するために必要なメモリが、管理対象デバイスに事前定義された使用可能なメモリ量の制限を上回る場合は、管理対象デバイスのメモリ制限が優先されます。

IP 最適化ポリシーごとに、以下のオプションを設定できます。

ネットワーク

最適化ポリシーを適用するホスト（複数可）の IP アドレス。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを指定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

ポリシー

モニタ対象ネットワーク セグメント上のホスト一式に使用する最適化ポリシー。

ターゲット ホストのオペレーティング システムに応じて、7 つの最適化ポリシーの 1 つを選択できます。以下の表に、7 つのポリシーと、それぞれのポリシーを使用するオペレーティング システムを記載します。First と Last というポリシー名は、これらのポリシーが元のオーバーラップ パケットまたは後続のオーバーラップ パケットのどちらを優先するかを反映しています。

表 *182*：ターゲットベースの最適化ポリシー

ポリシー	オペレーティング システム
BSD	AIX FreeBSD IRIX VAX/VMS
BSD-right	HP JetDirect
ファースト	Mac OS HP-UX
Linux	Linux OpenBSD
Last	Cisco IOS
Solaris	SunOS
Windows	Windows

Timeout

プリプロセッサ エンジンがフラグメント化されたパケットを再構成する際に使用できる最大時間（秒数）を指定します。指定された時間内にパケットを再構成できない場合、プリプロセッサ エンジンはパケットの再構成試行を停止し、受信したフラグメントを破棄します。

最小 TTL（Min TTL）

パケットに許容される最小 TTL 値を指定します。このオプションは、TTL ベースの挿入攻撃を検出します。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 123:11 を有効にします。

異常検知（Detect Anomalies）

オーバーラップ フラグメントのようなフラグメンテーション問題を識別します。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、次のルールを有効にすることができます：

- 123:1 ～ 123:4
- 123:5（BSD ポリシー）
- 123:6 ～ 123:8

オーバーラップ範囲（Overlap Limit）

セッション内で重複しているセグメントの設定された数が検出されると、そのセッションの最適化を停止することを指定します。

このオプションを設定するには、[異常検知（Detect Anomalies）] を有効にする必要があります。値が空白の場合、このオプションは無効になります。値 0 は、無制限の重複セグメント数を指定します。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 123:12 を有効にできます。

最小フラグメント サイズ（Minimum Fragment Size）

設定されたバイト数より小さい最後でないフラグメントが検出された場合、そのパケットは悪意のあるものとみなされることを指定します。

このオプションを設定するには、[異常検知（Detect Anomalies）] を有効にする必要があります。値が空白の場合、このオプションは無効になります。値 0 は、無制限のバイト数を指定します。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 123:13 を有効にできます。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）

IP 最適化の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

はじめる前に

- カスタム ターゲットベース ポリシーで識別するネットワークが、親ネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、およびVLANのサブセットと一致するか、サブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定, （1262 ページ）を参照してください。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [トランスポートまたはネットワーク レイヤプリプロセッサ（Transport/Network Layer Preprocessors）] で [IP 最適化（IP Defragmentation）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [IP 最適化（IP Defragmentation）] の横にある編集アイコン（）をクリックします。

ステップ 6 必要に応じて、[事前割り当て済みフラグメント（Preallocated Fragments）] フィールドに値を入力します。

ステップ 7 次の選択肢があります。

- サーバ プロファイルの追加：ページの左側の [サーバ（Servers）] の横にある追加アイコン（）をクリックし、[ホスト アドレス（Host Address）] フィールドに値を入力して、[OK] をクリックします。単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のターゲットベースのポリシーを作成できます。
- サーバプロファイルの編集：ページの左側の [サーバ（Servers）] で設定済みのアドレスをクリックするか、[デフォルト（default）] をクリックします。
- プロファイルの削除：ポリシーの横にある削除アイコン（）をクリックします。

ステップ 8 IP 最適化オプション, （1380 ページ）の説明に従ってオプションを変更します。

ステップ 9 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

次の作業

- イベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、IP最適化ルール（GID 123）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）およびIP 最適化オプション, （1380 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）
レイヤの基本, （1015 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

パケット デコーダ

キャプチャしたパケットをプリプロセッサに送信する前に、システムはパケットをパケット デコーダに送信します。パケットデコーダは、プリプロセッサやルールエンジンが容易に使用できる形式に、パケット ヘッダーおよびペイロードを変換します。データリンク層から開始して、ネットワーク層、トランスポート層へと、各スタック層が順にデコードされます。

パケット デコーダ オプション

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

GTP データ チャネルのデコード（Decode GTP Data Channel）

カプセル化された GTP（General Packet Radio Service（GPRS）トンネリング プロトコル）データ チャネルをデコードします。デフォルトでは、デコーダはポート 3386 ではバージョン 0 のデータをデコードし、ポート 2152 ではバージョン 1 のデータをデコードします。`GTP_PORTS` デフォルト変数を使用して、カプセル化された GTP トラフィックを識別するポートを変更できます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:297 および 116:298 を有効にします。

[標準外ポートで Teredo を検知（Detect Teredo on Non-Standard Ports）]

ポート 3544 以外の UDP ポートで識別される IPv6 トラフィックの Teredo トンネリングを検査します。

IPv6 トラフィックが存在する場合、システムは常にこのトラフィックを検査します。デフォルトでは、IPv6 インスペクションには 4in6、6in4、6to4、および 6in6 トンネリング方式が含まれます。また、UDP ヘッダーがポート 3544 を指定している場合は、Teredo トンネリングも含まれます。

IPv4 ネットワークでは、IPv4 ホストが Teredo プロトコルを使用して、IPv4 ネットワーク アドレス変換（NAT）デバイスを介して IPv6 トラフィックをトンネリングできます。Teredo は、IPv6 パケットを IPv4 UDP データグラムにカプセル化して、IPv4 NAT デバイスの背後で IPv6 接続を許可

します。システムは通常、UDP ポート 3544 を使用して Teredo トラフィックを識別します。ただし、攻撃者が検出を免れるために標準以外のポートを使用する可能性も考えられます。[非標準ポートでの Teredo の検出（Detect Teredo on Non-Standard Ports）] を有効にすることで、システムに Teredo トンネリングのすべての UDP ペイロードを検査させることができます。

Teredo のデコードは、外側のネットワーク層に IPv4 が使用されている場合に限り、最初の UDP ヘッダーに対してのみ行われます。UDP データが IPv6 データにカプセル化されるため、Teredo IPv6 層の後に 2 つ目の UDP 層が存在する場合、ルール エンジンは UDP 侵入ルールを使用して、内側および外側の両方の UDP 層を分析します。

policy-other ルール カテゴリの侵入ルール 12065、12066、12067、および 12068 は Teredo トラフィックを検出しますが、デコードは行わないので注意してください。（任意）これらのルールを使用してインライン展開で Teredo トラフィックをドロップすることができます。ただし、[非標準ポートでの Teredo の検出（Detect Teredo on Non-Standard Ports）] を有効にする場合は、これらのルールを無効化するか、トラフィックをドロップせずにイベントを生成するように設定する必要があります。

[余長値の検知（Detect Excessive Length Value）]

パケット ヘッダーが実際のパケット長を超えるパケット長を指定しているかどうかを検出します。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 116:6、116:47、116:97、および 116:275 を有効にできます。

[間違いな IP オプションを検知（Detect Invalid IP Options）]

無効な IP オプションを使用したエクスプロイトを識別するために、無効な IP ヘッダー オプションを検出します。たとえば、ファイアウォールに対するサービス妨害攻撃は、システムをフリーズさせる原因になります。ファイアウォールが無効なタイムスタンプおよびIPセキュリティオプションを解析しようとして、ゼロ長のチェックに失敗すると、回復不可能な無限ループが発生します。ルール エンジンはゼロ長のオプションを識別し、ファイアウォールでの攻撃を軽減するために使用できる情報を提供します。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 116:4 および 116:5 を有効にします。

[実験的 TCP オプションを検知（Detect Experimental TCP Options）]

試験的な TCP オプションが設定された TCP ヘッダーを検出します。以下の表は、それらのオプションを示しています。

TCP オプション	説明
9	半順序接続許可（Partial Order Connection Permitted）
10	半順序サービス プロファイル（Partial Order Service Profile）
14	Alternate Checksum Request

TCP オプション	説明
15	Alternate Checksum Data
18	Trailer Checksum
20	Space Communications Protocol Standards（SCPS）
21	Selective Negative Acknowledgements（SCPS）
22	Record Boundaries（SCPS）
23	Corruption（SPCS）
24	SNAP
26	TCP 圧縮フィルタ（TCP Compression Filter）

これらのオプションは試験的なものであるため、一部のシステムでは考慮されず、悪用される恐れがあります。

（注） 上記の表に記載されている試験的オプションに加えて、26 より大きいオプション番号を持つ TCP オプションは、試験的オプションと見なされます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:58 を有効にします。

廃止された TCP オプションを検知

廃止された TCP オプションが設定された TCP ヘッダーを検出します。これらのオプションは廃止されたものであるため、一部のシステムでは考慮されず、悪用される恐れがあります。以下の表は、それらのオプションを示しています。

TCP オプション	説明
[6]	エコー（Echo）
7	エコー応答（Echo Reply）
16	Skeeter
17	Bubba
19	MD5 Signature（MD5 認証）
25	Unassigned（未定義）

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:57 を有効にします。

[T または TCP を検知（Detect T/TCP）]

CC.ECHO オプションが設定された TCP ヘッダーを検出します。CC.ECHO オプションは、TCP for Transactions（T/TCP）が使用されていることを確認します。T/TCP ヘッダー オプションは幅広く使用されていないため、一部のシステムでは考慮されず、悪用される恐れがあります。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:56 を有効にします。

[その他の TCP オプションを検知（Detect Other TCP Options）]

他の TCP デコード イベント オプションでは検出されない無効な TCP オプションが設定された TCP ヘッダーを検出します。たとえば、このオプションは、無効な長さ、またはオプション データが TCP ヘッダーに収まらない長さの TCP オプションを検出します。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 116:54、116:55、および 116:59 を有効にできます。

[プロトコルヘッダの異常を検知（Detect Protocol Header Anomalies）]

より具体的な IP および TCP デコーダ オプションでは検出されない他のデコード エラーを検出します。たとえば、このデコーダは、不正な形式のデータ リンク プロトコル ヘッダーを検出する場合があります。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、次のルールを有効にすることができます。

GID:SID	該当する場合にイベントを生成
116:467	パケットが Cisco FabricPath ヘッダーにカプセル化されるパケットの最小サイズより小さい。
116:468	ヘッダーの Cisco メタデータ（CMD）フィールドに、有効な CMD ヘッダの最小サイズより小さいヘッダー長が含まれている。CMD フィールドは、Cisco TrustSec プロトコルと関連付けられています。
116:469	ヘッダーの CMD フィールドに、無効なフィールド長が含まれている。
116:470	ヘッダーの CMD フィールドに、無効なセキュリティ グループ タグ（SGT）オプションのタイプがあります。

GID:SID	該当する場合にイベントを生成
116:471	ヘッダーの CMD フィールドに、値が予約されている SGT が含まれています。

その他のパケット デコーダ オプションに関連付けられていないパケット デコーダ ルールを有効にすることもできます。

関連トピック

定義済みデフォルト変数, （400 ページ）

パケット復号化の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [トランスポートまたはネットワーク レイヤプリプロセッサ（Transport/Network Layer Preprocessors）] の下の [パケット復号化（Packet Decoding）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [パケット復号化（Packet Decoding）] の横にある編集アイコン（）をクリックします。

ステップ 6 パケット デコーダ オプション, （1385 ページ）で説明されているオプションを有効または無効にします。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

次の作業

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、パケット デコーダ ルール（GID 116）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）およびパケットデコーダ オプション, （1385 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

レイヤの基本, （1015 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

TCP ストリームの前処理

TCP プロトコルは、接続で生じ得るさまざまな状態を定義します。各 TCP 接続は、送信元と宛先の IP アドレス、および送信元と宛先のポートによって識別されます。TCP では、接続パラメータ値が同じ接続は、一度に 1 つしか存在できません。

状態に関連する TCP エクスプロイト

侵入ルールに `established` 引数と組み合わせた `flow` キーワードを追加すると、侵入ルール エンジンはステートフルモードでルールとフローディレクティブに一致するパケットを検査します。ステートフル モードでは、クライアントとサーバの間で正当な 3 ウェイ ハンドシェイクによって確立された TCP セッションの一部となっているトラフィックだけが評価されます。

確立された TCP セッションの一部として識別できない TCP トラフィックをプリプロセッサが検出するようにシステムを設定することは可能です。しかし、このようなイベントは、システムをすぐに過負荷状態に陥らせ、しかも意味のあるデータを提供しないため、通常の使用法では推奨されません。

Stick や Snot などの攻撃では、システムの自身に対する広範なルール セットとパケット インスペクションを悪用します。これらのツールは、Snort ベースの侵入ルールのパターンに基づいてパケットを生成し、ネットワークに送信します。ステートフル インスペクションに対して設定するルールに `flow` または `flowbits` キーワードを含めなければ、パケットのそれぞれがルールをトリガーするため、システムが過負荷状態になります。ステートフル インスペクションを使用することで、確立された TCP セッションに含まれず、意味のある情報を提供しないこれらのパケットを無視できます。ステートフルインスペクションを実行すると、ルールエンジンは確立された TCP セッションに含まれる攻撃のみを検出するため、アナリストが stick や snot によって大量に生成されるイベントに時間を取られることがなくなります。

ターゲット ベースの TCP ポリシー

オペレーティング システムによって、TCP の実装方法は異なります。たとえば、セッションをリセットするために、Windows やその他のオペレーティング システムの一部では TCP リセット セグメントに正確な TCP シーケンス番号を割り当てる必要があるのに対し、Linux や他のオペレーティング システムではシーケンス番号の範囲を使用できます。この例の場合、ストリーム プリプロセッサは、シーケンス番号に基づき、宛先ホストがリセットにどのように応答するかを正確に把握しなければなりません。ストリーム プリプロセッサがセッションの追跡を停止するのは、宛先ホストがリセットが有効であると見なした場合のみです。したがって、プリプロセッサがストリームの検査を停止した後は、パケットを送信することによって攻撃が検出を免れることはできません。TCP の実装方法の違いには、オペレーティング システムで TCP タイムスタンプ オプションを採用しているかどうか、採用している場合にはどのようにタイムスタンプを処理するか、そしてオペレーティング システムで SYN パケットのデータを受け入れるか、無視するかどうかも含まれます。

また、オーバーラップ TCP セグメントを再構成する方法も、オペレーティング システムによって異なります。オーバーラップ TCP セグメントは、確認応答済み TCP トラフィックの通常の再送信を反映する場合があります。あるいは、ホストのオペレーティング システムを認識している攻撃者が、エクスプロイトの検出を免れるためにオーバーラップ セグメントに不正なコンテンツを忍ばせて送信し、そのホストを悪用しようとしている場合もあります。ただし、モニタ対象のネットワーク セグメント上で稼働するオペレーティング システムを認識するようにストリーム プリプロセッサを設定すれば、そのプリプロセッサがターゲット ホストと同じ方法でセグメントを再構成することによって、攻撃を識別できます。

モニタ対象のネットワーク セグメント上のさまざまなオペレーティング システムに合わせて TCP ストリーム インスペクションおよび再構成を調整するために、1 つ以上の TCP ポリシーを作成することができます。ポリシーごとに、13 のオペレーティング システム ポリシーのうちの 1 つを特定します。異なるオペレーティング システムを使用するホストのいずれか、あるいはすべてを識別するために必要な数だけ TCP ポリシーを使用し、各 TCP ポリシーを特定の IP アドレスまたはアドレス ブロックにバインドします。デフォルトの TCP ポリシーは、他の TCP ポリシーで指定されていないモニタ対象ネットワーク上のすべてのホストに適用されます。したがって、デフォルトの TCP ポリシーに IP アドレスまたはアドレス ブロックを指定する必要はありません。

パッシブ展開で アダプティブ プロファイル を使用することで、パケットのターゲット ホストのホスト オペレーティング システム情報に応じて、TCP ストリーム プリプロセッサに適用するターゲットベースのポリシーが動的に選択されるようにすることもできます。

TCP ストリームの再構成

ストリーム プリプロセッサは、TCP セッションでのサーバからクライアントへの通信ストリーム、クライアントからサーバへの通信ストリーム、またはその両方の通信ストリームに含まれるすべてのパケットを収集して再構成します。これにより、ルール エンジンは、特定のストリームに含まれる個々のパケットだけを検査するのではなく、ストリームを再構成された単一のエンティティとして検査できます。

ストリームの再構成により、ルール エンジンは、個々のパケットを検査する場合には検出できない可能性のあるストリームベースの攻撃を識別できます。ルール エンジンの再構成対象とする通

信ストリームは、ネットワークのニーズに応じて指定できます。たとえば、Web サーバ上のトラフィックをモニタする際に、独自の Web サーバから不正なトラフィックを受信する可能性がほとんどないため、クライアント トラフィックだけを検査するという場合もあります。

各 TCP ポリシーに、ストリーム プリプロセッサが再構成するトラフィックを識別するポートのカンマ区切りのリストを指定できます。アダプティブ プロファイルが有効にされている場合、再構成するトラフィックを識別するサービスを、ポートの代わりとして、あるいはポートと組み合わせてリストすることもできます。

ポート、サービス、またはその両方を指定できます。クライアント ポート、サーバ ポート、またはその両方を任意に組み合わせた個別のポート リストを指定できます。また、クライアント サービス、サーバ サービス、またはその両方を任意に組み合わせた個別のサービス リストを指定することもできます。たとえば、以下を再構成する必要があるとします。

- クライアントからの SMTP（ポート 25）トラフィック
- FTP サーバ応答（ポート 21）
- 両方向の Telnet（ポート 23）トラフィック

この場合、以下のように設定できます。

- クライアント ポートとして、`23, 25` を指定
- サーバ ポートとして、`21, 23` を指定

あるいは、以下のように設定することもできます。

- クライアント ポートとして、`25` を指定
- サーバ ポートとして、`21` を指定
- 両方のポートとして、`23` を指定

さらに、ポートとサービスを組み合わせた以下の設定例は、アダプティブ プロファイルが有効にされている場合、有効になります。

- クライアント ポートとして、`23` を指定
- クライアント サービスとして、`smtp` を指定
- サーバ ポートとして、`21` を指定
- サーバ サービスとして、`telnet` を指定

ポートを否定すると（`!80` など）、そのポートのトラフィックが TCP ストリーム プリプロセッサで処理されなくなり、パフォーマンスが向上します。

`all` を引数として指定して、すべてのポートに対して再構成を指定することもできますが、ではポートを `all` に**設定しない**よう推奨しています。この設定では、このプリプロセッサで検査するトラフィックの量が増え、不必要にパフォーマンスが低下するためです。

TCP 再構成には、自動的かつ透過的にその他のプリプロセッサに追加するポートが含まれています。しかし、他のプリプロセッサの設定に追加した TCP 再構成リストにポートを明示的に追加す

る場合は、これらの追加したポートは通常処理されます。これには、次のプリプロセッサのポート リストが含まれています。

- FTP/Telnet（サーバ レベル FTP）
- DCE/RPC
- HTTP Inspect
- SMTP
- Session Initiation Protocol
- POP
- IMAP
- SSL

追加のトラフィック タイプ（クライアント、サーバ、両方）を再構成すると、リソースの需要が増大することに注意してください。

TCP ストリームのプリプロセス オプション

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

次のグローバル TCP オプションを構成できます。

パケット タイプ パフォーマンスの向上（Packet Type Performance Boost）

送信元ポートおよび宛先ポートの両方を `any` に設定した TCP ルールで、`flow` または `flowbits` オプションが使用されている場合を除き、有効化された侵入ルールに指定されていないポートおよびアプリケーション プロトコルのすべてについて、TCP トラフィックを無視するように設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。

TCP ポリシーごとに、以下のオプションを設定できます。

ネットワーク（Network）

TCP ストリーム再構成ポリシーを適用するホストの IP アドレスを指定します。

単一の IP アドレスまたはアドレス ブロックを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを指定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してくださ

い。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、any を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

ポリシー

TCP ポリシーを適用するターゲット ホスト（複数可）のオペレーティング システムを識別します。[Mac OS] 以外のポリシーを選択すると、システムは同期（SYN）パケットからデータを削除し、ルール 129:2 に対するイベントの生成を無効にします。インライン正規化プリプロセッサの [SYN に関するデータを削除（Remove Data on SYN）] オプションを有効にすると、ルール 129:2 も無効になることに注意してください。

以下の表に、オペレーティング システム ポリシーとそれを使用するホスト オペレーティング システムをリストします。

表 *183* : *TCP* オペレーティング システム ポリシー

ポリシー	オペレーティング システム
ファースト	不明な OS
Last	Cisco IOS
BSD	AIX FreeBSD OpenBSD
Linux	Linux 2.4 カーネル Linux 2.6 カーネル
Old Linux	Linux 2.2 以前のカーネル
Windows	Windows 98 Windows NT Windows 2000 Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista
Solaris	Solaris OS SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 以降

ポリシー	オペレーティング システム
HPUX 10	HP-UX 10.2 以前
Mac OS	Mac OS 10（Mac OS X）

ヒント First オペレーティング システム ポリシーは、ホストのオペレーティング システムが不明な場合にはある程度の保護対策になります。ただし、攻撃を見逃す可能性もあります。オペレーティング システムが既知であれば、ポリシーを編集して、その正しいオペレーティング システムを指定してください。

Timeout

侵入ルール エンジンが非アクティブなストリームを状態テーブルで保持する秒数（1 ～ 86400 秒）。指定された期間内にストリームが再構成されない場合、侵入ルール エンジンはそのストリームを状態テーブルから削除します。

（注） ネットワーク トラフィックがデバイスの帯域幅制限に到達しやすいセグメントに、管理対象デバイスが展開されている場合は、処理のオーバーヘッド量を削減するために、この値を大きい値（たとえば、600 秒）に設定することを検討する必要があります。

最大 TCP ウィンドウ（Maximum TCP Window）

受信側ホストで指定されている TCP ウィンドウの最大許容サイズを 1 ～ 1073725440 バイトの範囲で指定します。値を 0 に設定すると、TCP ウィンドウ サイズのチェックが無効になります。

注意 上限は RFC で許可される最大ウィンドウ サイズです。これは、攻撃者が検出を回避できないようにすることを目的としていますが、あまりにも大きな最大ウィンドウ サイズを設定すると、システム自体がサービス妨害を招く可能性があります。

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効になっている場合は、ルール 129:6 を有効にして、このオプションに対しイベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。

オーバーラップ範囲（Overlap Limit）

セッションで許容するオーバーラップセグメントの数を 0（無制限）～255 の範囲で指定します。セッションで、この指定された値に達すると、セグメントの再構成が停止します。[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされていて、それに付随するプリプロセッサ ルールが有効にされている場合、イベントも生成されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:7 を有効にします。

ファクタをフラッシュ（Flush Factor）

インライン展開では、ここで設定するサイズ減少なしのセグメントの数（1 ～ 2048）の後にサイズが減少したセグメントが検出されると、システムは検出用に累積されたセグメント データをフラッシュします。値を 0 に設定すると、要求または応答の終わりを示す可能性のあるこのセグメント パターンの検出が無効になります。このオプションを有効にするには、インライン正規化の [TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にする必要があることに注意してください。

ステートフル インスペクションの異常（Stateful Inspection Anomalies）

TCP スタックの異常な動作を検出します。付随するプリプロセッサ ルールが有効にされている場合、TCP/IP スタックが不完全に作成されていると、多数のイベントが生成される可能性があります。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、次のルールを有効にすることができます：

- 129:1 ～ 129:5
- 129:6（Mac OS のみ）
- 129:8 ～ 129:11
- 129:13 ～ 129:19

次の点に注意してください。

- ルール 129:6 でトリガーするには、さらに [最大 TCP ウィンドウ（Maximum TCP Window）] に 0 より大きい値を設定する必要があります。
- ルール 129:9 および 129:10 でトリガーするには、さらに [TCP セッションのハイジャック（TCP Session Hijacking）] を有効にする必要があります。

TCP セッションのハイジャック（TCP Session Hijacking）

3 ウェイ ハンドシェイク中に TCP 接続の両端から検出されたハードウェア（MAC）アドレスの有効性を、セッションで受信した後続のパケットに照合して検査することにより、TCP セッション ハイジャックを検出します。[ステートフルインスペクションの異常（Stateful Inspection Anomalies）] が有効にされていて、2つの対応するプリプロセッサルールのいずれかが有効にされている場合、接続のどちらかの側の MAC アドレスが一致しないと、システムがイベントを生成します。

このオプションに対し イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、ルール 129:9 および 129:10 を有効にします。これらのルールのいずれかを使用してイベントを生成するには、[ステートフルインスペクションの異常（Stateful Inspection Anomalies）] を有効にする必要があります。

連続した小型セグメント（Consecutive Small Segments）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされている場合、連続する小さな TCP セグメントの許容数を 1 ～ 2048 の範囲で指定します。値を 0 に設定すると、連続する小さなセグメントのチェックが無効になります。

このオプションは、[小さなセグメント サイズ（Small Segment Size）] オプションと同時に設定し、両方とも無効にするか、両方にゼロ以外の値を設定する必要があります。通常は、それぞれのセグメントの長さが 1 バイトであったとしても、ACK が介在することなく 2000 個もの連続するセグメントを受信することはないので注意してください。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:12 を有効にします。

小型セグメントのサイズ（Small Segment Size）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされている場合、小さいと見なされる TCP セグメントのサイズを 1 ～ 2048 バイトの範囲で指定します。値を 0 に設定すると、小さいセグメントのサイズの指定が無効になります。

このオプションは、[連続する小さなセグメント（Consecutive Small Segments）] オプションと同時に設定し、両方とも無効にするか、両方にゼロ以外の値を設定する必要があります。2048 バイトの TCP セグメントは、標準的な 1500 バイトのイーサネット フレームより大きいことに注意してください。

小型セグメントを無視したポート（Ports Ignoring Small Segments）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）]、[連続する小さなセグメント（Consecutive Small Segments）]、および [小さなセグメント サイズ（Small Segment Size）] が有効になっている場合は、小さい TCP セグメントの検出を無視する 1 つ以上のポートのカンマ区切りリストを指定します。このオプションを空白のままにすると、ポートはすべて無視されないように指定されます。

リストには任意のポートを追加できますが、このリストが適用されるのは、TCP ポリシーの [ストリーム再構成を実行（Perform Stream Reassembly on）] ポート リストに指定されているポートのみです。

TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）

TCP スリーウェイ ハンドシェイクの完了時に確立されたセッションだけを処理することを指定します。パフォーマンスを向上させ、SYN フラッド攻撃から保護し、部分的に非同期の環境での運用を可能にするには、このオプションを無効にします。確立された TCP セッションには含まれていない情報を送信して誤検出を発生させようとする攻撃を回避するには、このオプションを有効にします。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:20 を有効にします。

3 ウェイ ハンドシェイク タイムアウト（3-Way Handshake Timeout）

[TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）] が有効にされている場合、ハンドシェイクを完了するまでの時間制限を 0（無制限）～ 86400 秒（24 時間）の範囲で指定します。このオプションの値を変更するには、[TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）] を有効にする必要があります。

パケット サイズ パフォーマンスの向上（Packet Size Performance Boost）

再構成バッファで大きいパケットをキューに入れないようにプリプロセッサを設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。1 ～ 20 バイトの小さなパケットを使用した検出回避の試行から保護するには、このオプションを無効にします。すべてのトラフィックが非常に大きなパケットからなるため、そのような攻撃は起こらないと確信できる場合は、このオプションを有効にします。

レガシー再構成（Legacy Reassembly）

パケットを再構成する際に、廃止されたストリーム 4 プリプロセッサをエミュレートするようにストリームプリプロセッサを設定します。これにより、ストリームプリプロセッサで再構成されたイベントを、ストリーム 4 プリプロセッサで再構成された、同じデータ ストリームに基づくイベントと比較できます。

非同期ネットワーク（Asynchronous Network）

モニタ対象ネットワークが非同期ネットワーク（システムにトラフィックの半分だけが見えるネットワーク）であるかどうかを指定します。このオプションを有効にすると、システムは TCP ストリームを再構成しないため、パフォーマンスが向上します。

クライアント ポートでのストリーム再構成の実行（Perform Stream Reassembly on Client Ports）

接続のクライアント側のポートに基づくストリームの再構成を有効にします。つまり、Web サーバ、メール サーバ、または一般に $HOME_NET で指定された IP アドレスによって定義されたその他の IP アドレスを宛先とするストリームが再構成されます。不正なトラフィックがクライアントから発生する可能性がある場合は、このオプションを使用します。

クライアント サービスでのストリーム再構成の実行（Perform Stream Reassembly on Client Services）

接続のクライアント側のサービスに基づくストリーム再構成を有効にします。不正なトラフィックがクライアントから発生する可能性がある場合は、このオプションを使用します。

選択するクライアント サービスごとに、1 つ以上のクライアント ディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。関連するクライアント アプリケーションに有効にされているディレクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタをアプリケーションに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーションに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

サーバ ポートでのストリーム再構成の実行（Perform Stream Reassembly on Server Ports）

接続のサーバ側のポートに基づくストリーム再構成のみを有効にします。つまり、Web サーバ、メール サーバ、または一般に $EXTERNAL_NET で指定された IP アドレスによって定義されたその他の IP アドレスから発信されたストリームが再構成されます。サーバ側の攻撃を監視する必要がある場合は、このオプションを使用します。ポートを指定しないことによって、このオプションを無効にできます。

サーバ サービスでのストリーム再構成の実行（Perform Stream Reassembly on Server Services）

接続のサーバ側のサービスに基づくストリーム再構成のみを有効にします。サーバ側の攻撃を監視する必要がある場合は、このオプションを使用します。サービスを指定しないことによって、このオプションを無効にできます。

1 つ以上のディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。サービスに有効にされているディレクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタを関連するアプリケーション プロトコルに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーション プロトコルに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

両方のポートでのストリーム再構成の実行（Perform Stream Reassembly on Both Ports）

接続のクライアント側とサーバ側の両方のポートに基づくストリーム再構成を有効にします。同じポートで、不正なトラフィックがクライアントとサーバ間のいずれの方向でも移動する可能性がある場合は、このオプションを使用します。ポートを指定しないことによって、このオプションを無効にできます。

両方のサービスでのストリーム再構成の実行（Perform Stream Reassembly on Both Services）

接続のクライアント側とサーバ側の両方のサービスに基づくストリーム再構成を有効にします。同じサービスで、不正なトラフィックがクライアントとサーバ間のいずれの方向でも移動する可能性がある場合は、このオプションを使用します。サービスを指定しないことによって、このオプションを無効にできます。

1 つ以上のディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。関連するクライアント アプリケーションまたはアプリケーション プロトコルに対して有効になっているディレクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタをアプリケーションまたはアプリケーション プロトコルに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーションまたはアプリケーション プロトコルに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

トラブルシューティング オプション：最大キューイング バイト（Troubleshooting Options: Maximum Queued Bytes）

トラブルシューティングの電話中に、TCP 接続の片側でキューイングできるデータの量を指定するようにサポートから依頼される場合があります。値 0 は、無制限のバイト数を指定します。

注意 このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

トラブルシューティング オプション：最大キューイング セグメント（Troubleshooting Options：Maximum Queued Segments）

トラブルシューティングの電話中に、TCP 接続の片側でキューイングできるデータ セグメントの最大バイト数を指定するようにサポートから依頼される場合があります。値 0 は、無制限のデータ セグメント バイト数を指定します。

注意 このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）
ディテクタのアクティブおよび非アクティブの設定, （1527 ページ）
レイヤ管理, （1021 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

TCP ストリームの前処理の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

はじめる前に

- カスタム ターゲットベースのポリシーで指定するネットワークが一致しているか、または親のネットワーク分析ポリシーで処理されるネットワーク、ゾーン、およびVLANのサブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定, （1262 ページ）を参照してください。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 変更するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 左側のナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [トランスポートまたはネットワーク レイヤプリプロセッサ（Transport/Network Layer Preprocessors）] の下の [TCP ストリームの構成（TCP Stream Configuration）] 設定が無効になっている場合は、[有効化（Enabled）] をクリックして有効にします。

ステップ 5 [TCP ストリームの構成（TCP Stream Configuration）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 [グローバル設定（Global Settings）] セクションの [パケット タイプ パフォーマンス ブースト（Packet Type Performance Boost）] チェックボックスをオンまたはオフにします。

ステップ 7 次の操作を実行できます。

- ターゲットベースのポリシーの追加：[ターゲット（Targets）]セクションの[ホスト（Hosts）] の横にある追加アイコン（  ）をクリックします。[ホストアドレス（Host Address）]フィールドに 1 つまたは複数の IP アドレスを指定します。単一の IP アドレスまたはアドレス ブロックを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のターゲットベースのポリシーを作成できます。作業が完了したら [OK] をクリックします。
- 既存のターゲットベースのポリシーの編集：[ホスト（Hosts）] の下で、編集するポリシーのアドレスをクリックするか、またはデフォルトの構成値を編集します。
- TCP ストリームの前処理オプションの変更：TCP ストリームのプリプロセス オプション，（1393 ページ）を参照してください。

  注意 サポートから指示がない限り、[最大キュー済みバイト（Maximum Queued Bytes）] または [最大キュー済みセグメント（Maximum Queued Segments）] を変更しないでください。

  ヒント クライアント サービス、サーバ サービス、またはその両方に基づくストリーム リアセンブル設定を変更するには、変更するフィールドの内側をクリックするか、そのフィールドの横にある [編集（Edit）] をクリックします。ポップアップ ウィンドウで矢印ボタンを使用して、サービスを [利用可能（Available）] リストと [有効化（Enabled）] リスト間で移動し、[OK] をクリックします。

- 既存のターゲットベースのポリシーの削除：削除するポリシーの横にある削除アイコン（  ）をクリックします。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

次の作業

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、SMTP ストリーム プリプロセッサ ルール（GID 129）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）およびTCP ストリームのプリプロセス オプション, （1393 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

レイヤ管理, （1021 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）
Firepower システムの IP アドレス表記法, （16 ページ）

UDP ストリームの前処理

UDP ストリームの前処理が行われるのは、ルールエンジンがパケットを処理するために使用する UDP ルールに、以下の引数のいずれかを使用した `flow` キーワードが含まれる場合です。

- `Established`
- `To Client`
- `From Client`
- `To Server`
- `From Server`

UDP データ ストリームは一般に、セッションという観点で考慮されません。UDP はコネクションレス型プロトコルであり、2 つのエンドポイントが通信チャネルを確立してデータを交換し、チャネルを終了する手段は提供していません。ただし、ストリーム プリプロセッサは、カプセル化 IP データグラム ヘッダーの送信元および宛先 IP アドレス フィールドと、UDP ヘッダーのポート フィールドを使用して、フローの方向を判断し、セッションを識別します。セッションが終了するのは、設定可能なタイマーの時間を超えた場合、または一方のエンドポイントで、もう一方のエンドポイントが到達不能、あるいは要求されたサービスが利用不可という内容の ICMP メッセージを受け取った場合です。

システムはUDPストリームの前処理に関連するイベントを生成しないことに注意してください。ただし、関連するパケット デコーダ ルールを有効にすることで、UDP プロトコル ヘッダーの異常を検出することができます。

関連トピック

TCP ヘッダー値とストリーム サイズ, （1180 ページ）

UDP ストリームのプリプロセス オプション

Timeout

プリプロセッサが非アクティブなストリームを状態テーブルに保持する秒数を指定します。指定した時間内に追加のデータグラムが現れなかった場合、プリプロセッサはそのストリームを状態テーブルから削除します。

パケット タイプ パフォーマンスの向上（Packet Type Performance Boost）

送信元および宛先ポートの両方を `any` に設定した UDP ルールで `flow` または `flowbits` オプションが使用されている場合を除き、有効化されたルールに指定されていないポートおよびアプリケーションプロトコルのすべてについて、UDP トラフィックを無視するようにプリプロセッサを設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。

UDP ストリームの前処理の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [トランスポートまたはネットワーク レイヤプリプロセッサ（Transport/Network Layer Preprocessors）] の下の [UDP ストリームの構成（UDP Stream Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [UDP ストリームの構成（UDP Stream Configuration）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 UDP ストリームのプリプロセス オプション, （1403 ページ）で説明されているオプションを設定します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

次の作業

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、関連するパケット デコーダ ルール（GID 116）を有効にします。詳細については、侵入ルール状態の設定, （1063 ページ）およびパケット デコーダ, （1385 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

レイヤ管理, （1021 ページ）
競合と変更：ネットワーク分析ポリシーと侵入ポリシー, （1011 ページ）

第 61 章

特定の脅威の検出

次のトピックでは、特定の脅威を検出するためにネットワーク分析ポリシーでプリプロセッサを使用する方法について説明します。

特定の脅威の検出の概要

ネットワーク分析ポリシーでさまざまなプリプロセッサを使用して、モニタ対象ネットワークへの特定の攻撃、たとえば、Back Orifice 攻撃、複数のポートスキャン タイプ、過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレート ベース攻撃などを検出できます。ただし、侵入ルールまたはルールの引数が無効化されたプリプロセッサを必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。

侵入ポリシーで設定する機密データ検出を使用して、センシティブな数値データの保護なし送信を検出することもできます。

Back Orifice の検出

Firepower システムは、Back Orifice プログラムの存在を検出するプリプロセッサを提供しています。Back Orifice プログラムにより Windows ホストに対する管理者アクセス権を取得される可能性があります。

Back Orifice 検出プリプロセッサ

Back Orifice プリプロセッサは、UDP トラフィックを分析し、Back Orifice マジック クッキー「*!*QWTY?」を調べます。このクッキーは、パケットの最初の 8 バイトにあり、XOR で暗号化されています。

Back Orifice プリプロセッサには設定ページがありますが、設定オプションはありません。Back Orifice プリプロセッサが有効になっていても、プリプロセッサ ルールを有効にしなければ、イベントを生成し、インライン展開では、違反パケットをドロップします。。

表 *184* : *Back Orifice GID:SID*

プリプロセッサ ルール GID:SID	説明
105:1	Back Orifice トラフィック検出
105:2	Back Orifice クライアント トラフィック検出
105:3	Back Orifice サーバ トラフィック検出
105:4	Back Orifice Snort バッファ攻撃検出

Back Orifice の検出

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [設定（Settings）] をクリックします。

ステップ 4 [特定の脅威の検出（Specific Threat Detection）] の下の [Back Orifice の検出（Back Orifice Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

（注） Back Orifice にユーザが設定できるオプションはありません。

ステップ 5 最後のポリシーの確定以降にこのポリシーに加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、Back Orifice 検出ルール 105:1、105:2、105:3、または 105:4 を有効にします。詳細については、侵入ルールの状態, （1062 ページ）およびBack Orifice 検出プリプロセッサ, （1406 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ポートスキャン検出

ポートスキャンとは、攻撃者が攻撃の準備段階としてよく使用する、ネットワーク調査の形式です。ポートスキャンでは、攻撃者が特別に細工したパケットをターゲット ホストに送信します。攻撃者は多くの場合、ホストが応答するパケットを調べることで、ホストでどのポートが開かれているか、そして開かれているポートでどのアプリケーション プロトコルが実行されているかを、直接あるいは推論によって判断できます。

ポートスキャンは、それ自体では攻撃の証拠になりません。実際、攻撃者が使用するポートスキャン手法の中には、正当なユーザがネットワークで使用する可能性があるものもあります。Cisco のポートスキャン ディテクタは、アクティビティのパターンを検出するという方法で、悪意のあるポートスキャンの可能性があるポートスキャンを判別できるように設計されています。

ポートスキャン タイプ、プロトコル、フィルタリング感度レベル

攻撃者がネットワークを調査するために複数の手法を使用することはよくあります。通常、攻撃者は異なる複数のプロトコルを使用して、ターゲット ホストからさまざまな応答を引き出します。その目的は、ブロックされた特定タイプのプロトコルを基に、使用できる可能性のあるプロトコルを絞り込んでいくことです。

表 *185*：プロトコル タイプ

プロトコル	説明
[TCP]	TCP プローブを検出します。たとえば、SYN スキャン、ACK スキャン、TCP connect() スキャン、および Xmas tree、FIN、NULL といった異常なフラグを組み合わせたスキャンなどです。
UDP	ゼロ バイト UDP パケットなどの UDP プローブを検出します。
ICMP	ICMP エコー要求（ping）を検出します。
IP	IP プロトコル スキャンを検出します。これらのスキャンは、攻撃者が開いているポートを見つけようとしているのではなく、ターゲット ホストでサポートされている IP プロトコルを発見しようとするためのスキャンであるため、TCP スキャンおよび UDP スキャンとは異なります。

一般に、ターゲット ホストの数、スキャン側ホストの数、およびスキャン対象のポートの数に応じて、ポートスキャンは 4 つのタイプに分けられます。

表 *186*：ポートスキャン タイプ

タイプ（Type）	説明
ポートスキャン検出	攻撃者が少数のホストを使用して、1 つの対象ホスト上で複数のポートをスキャンする 1 対 1 ポートスキャン。 1 対 1 ポートスキャンは次のような特徴があります： • 少数のホストを使用してスキャン • 単一のホストをスキャン • 多数のポートをスキャン このオプションでは、TCP、UDP、および IP ポートスキャンが検出されます。
ポートスイープ	攻撃者が少数のホストを使用して、複数の対象ホスト上で 1 つのポートをスキャンする 1 対複数のポートスイープ。 ポートスイープには次のような特徴があります。 • 少数のホストを使用してスキャン • 多数のホストをスキャン • 少数の固有のポートをスキャン このオプションでは、TCP、UDP、ICMP、および IP ポートスイープが検出されます。

タイプ（Type）	説明
デコイ ポートスキャン	攻撃者がスプーフィングされた送信元 IP アドレスと実際にスキャンされた IP アドレスとを組み合わせた 1 対 1 ポートスキャン。 デコイ ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 少数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン デコイ ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。
分散型ポートスキャン	複数のホストが開いているポストに対して 1 つのホストをクエリする複数対 1 のポートスキャン。 分散型ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 多数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン 分散型ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。

ポートスキャン ディテクタは、主にプローブ対象ホストからの否定応答に基づいて、プローブに関する情報を取得します。たとえば、Web クライアントが Web サーバに接続するときに、クライアントはサーバのポート 80/tcp が開いていることを頼りに、そのポートを使用します。ただし、攻撃者がサーバをプローブする場合、そのサーバがウェブ サービスを提供するかどうかを攻撃者があらかじめ知っていることはありません。ポートスキャン ディテクタは否定応答（つまり、ICMP 到達不能または TCP RST パケット）を見つけると、その応答を潜在的ポートスキャンとして記録します。否定応答をフィルタリングするデバイス（ファイアウォールやルータなど）の向こう側にターゲット ホストがある場合、このプロセスはさらに困難になります。この場合、ポートスキャンディテクタは、選択された機密レベルに基づいてフィルタリングされたポートスキャン イベントを生成することができます。

表 *187*：感度レベル

水準器	説明
低（Low）	ターゲット ホストからの否定応答だけが検出されます。誤検出を抑えるためには、この機密レベルを選択します。ただし、特定のタイプのポートスキャン（時間をかけたスキャン、フィルタリングされたスキャン）が見逃される可能性があることに注意してください。 このレベルを使用すると、ポートスキャン検出の所要時間が最短になります。

水準器	説明
中（Medium）	ホストへの接続数に基づいてポートスキャンが検出されます。したがって、フィルタリングされたポートスキャンを検出できます。ただし、ネットワーク アドレス変換プログラムやプロキシなど、ホストが非常にアクティブな場合は、誤検出が発生する可能性があります。 [スキャン済みの無視（Ignore Scanned）] フィールドに、アクティブなホストの IP アドレスを追加すると、そのような誤検出を軽減できます。 このレベルを使用すると、ポートスキャン検出の所要時間が長くなります。
高（High）	時間帯に基づいてポートスキャンを検出します。つまり、時間を基準としたポートスキャンを検出できます。ただし、このオプションを使用する場合は、[スキャン済みの無視（Ignore Scanned）] および [スキャナの無視（Ignore Scanner）] フィールドに IP アドレスを指定するという方法で、時間をかけて慎重にディテクタを調整してください。 このレベルを使用すると、ポートスキャン検出の所要時間が大幅に長くなります。

ポートスキャン イベント生成

ポートスキャン検出が有効の場合、ジェネレータ ID（GID）122 および SID 1～27 の Snort ID（SID）によりルールを有効にして、それぞれ有効化したポートスキャン タイプのイベントを生成し、インライン展開では、違反パケットをドロップします。する必要があります。

（注） イベントがポートスキャン接続ディテクタによって生成され場合、プロトコル番号は255に設定されます。デフォルトでは、ポートスキャンに特定のプロトコルは関連付けられません。したがって、Internet Assigned Numbers Authority（IANA）にはプロトコル番号が割り当てられません。IANA では 255 を予約番号として指定しているため、ポートスキャン イベントでは、そのイベントに関連付けられている番号がないことを示すために、この番号が使用されます。

表 *188*：ポートスキャン検出 *SID*（*GID 122*）

ポートスキャン タイプ	[プロトコル（**Protocol**）]：	機密レベル	プリプロセッサ ルール **SID**
ポートスキャン検出	[TCP] UDP ICMP IP	低（Low） 中または高 低（Low） 中または高 低（Low） 中または高 低（Low） 中または高	1 5 17 21 イベントを生成しません。 イベントを生成しません。 9 13
ポートスイープ	[TCP] UDP ICMP IP	低（Low） 中または高 低（Low） 中または高 低（Low） 中または高 低（Low） 中または高	3、27 7 19 23 25 26 11 15
デコイ ポートスキャン	[TCP] UDP ICMP IP	低（Low） 中または高 低（Low） 中または高 低（Low） 中または高 低（Low） 中または高	2 [6] 18 22 イベントを生成しません。 イベントを生成しません。 10 18

ポートスキャン タイプ	[プロトコル（Protocol）]：	機密レベル	プリプロセッサ ルール SID
分散型ポートスキャン	[TCP] UDP ICMP IP	低（Low） 中または高 低（Low） 中または高 低（Low） 中または高 低（Low） 中または高	4 8 20 24 イベントを生成しません。 イベントを生成しません。 12 16

ポートスキャン イベント パケット ビュー

関連するプリプロセッサルールを有効にすると、ポートスキャンディテクタによって侵入イベントが生成されるようになります。生成されたイベントは、他のすべての侵入イベントと同じように表示できます。ただし、ポートスキャンイベントのパケットビューに表示される情報は、他のタイプの侵入イベントとは異なります。

侵入イベント ビューを出発点に、ポートスキャン イベントのパケット ビューまでドリルダウンします。各ポートスキャン イベントは複数のパケットに基づくため、単一のポートスキャン パケットをダウンロードすることはできません。ただし、ポートスキャンパケットビューで、使用可能なすべてのパケット情報を確認できます。

任意の IP アドレスをクリックしてコンテキスト メニューを表示し、[whois（whois）] を選択して、その IP アドレスでルックアップを実行するか、[ホスト プロファイルの表示（View Host Profile）] を選択して、そのホストのホスト プロファイルを表示できます。

表 *189*：ポートスキャン パケット ビュー

情報	説明
Device	イベントを検出したデバイス。
時刻（Time）	イベントが発生した時刻。
メッセージ（Message）	プリプロセッサによって生成されたイベント メッセージ。
ソース IP	スキャン側ホストの IP アドレス。
宛先 IP（Destination IP）	スキャンされたホストの IP アドレス。

情報	説明
プライオリティ カウント（Priority Count）	スキャンされたホストからの否定応答（TCP RST、ICMP 到達不能など）の数。否定応答の数が多ければ多いほど、プライオリティ カウントが高くなります。
接続数（Connection Count）	ホスト上でアクティブな接続数。この値は、TCP および IP など接続ベースのスキャンではさらに正確です。
IP カウント（IP Count）	スキャン対象のホストに接続する IP アドレスが変更された回数。たとえば、最初の IP アドレスが 10.1.1.1、2 番目の IP アドレスが 10.1.1.2、3 番目の IP アドレスが 10.1.1.1 の場合、IP カウントは 3 となります。 プロキシや DNS サーバなどのアクティブ ホストでは、この数値はそれほど正確ではありません。
スキャナ/スキャン対象 IP 範囲（Scanner/Scanned IP Range）	スキャン対象ホストまたはスキャン側ホスト（スキャンのタイプに依存）の IP アドレスの範囲。ポートスイープの場合、このフィールドにはスキャン対象ホストの IP アドレス範囲が示されます。ポートスキャンの場合は、スキャン側ホストの IP アドレス範囲が示されます。
ポート/プロトコル カウント（Port/Proto Count）	TCP および UDP ポートスキャンの場合は、スキャン対象のポートが変更された回数です。たとえば、スキャンされた最初のポートが 80、2 番目のポートが 8080、3 番目のポートが再び 80 の場合、ポート カウントは 3 となります。 IP プロトコル ポートスキャンの場合は、スキャン対象ホストに接続するために使用されたプロトコルが変更された回数です。
ポート/プロトコル範囲（Port/Proto Range）	TCP および UDP ポートスキャンの場合は、スキャンされたポートの範囲です。 IP プロトコル ポートスキャンの場合は、スキャン対象ホストへの接続試行で使用された IP プロトコル番号の範囲です。
開いているポート（Open Ports）	スキャン対象ホストで開かれた TCP ポート。このフィールドは、ポートスキャンで 1 つ以上の開かれたポートが検出された場合にのみ表示されます。

関連トピック

侵入イベントについて，（1959 ページ）

ポートスキャン検出の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

ポートスキャン検出の設定オプションを使用して、ポートスキャンディテクタによるスキャンアクティビティのレポート方法を微調整できます。

システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際のIPアドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。または[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [設定（Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [ポートスキャン検出（Portscan Detection）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [ポートスキャン検出（Portscan Detection）] の横にある編集アイコン（）をクリックします。

ステップ 6 [プロトコル（Protocol）] フィールドで、有効にするプロトコルを指定します。

（注） TCP を介してスキャンを検出するには TCP ストリーム処理が有効になっていること、UDP を介してスキャンを検出するには UDP ストリーム処理が有効になっていることを確認する必要があります。

ステップ 7 [スキャン タイプ（Scan Type）] フィールドで、検出するポートスキャン タイプを指定します。

ステップ 8 [重要度レベル（Sensitivity Level）] リストからレベルを選択します。ポートスキャン タイプ、プロトコル、フィルタリング感度レベル，（1407 ページ）を参照してください。

ステップ 9 特定のホストのポートスキャン アクティビティのサインをモニタする場合は、[IP の監視（Watch IP）] フィールドにホストの IP アドレスを入力します。
単一のIPアドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。すべてのネットワーク トラフィックを監視するには、フィールドを空白のままにします。

ステップ 10 ホストをスキャナとして無視するには、[スキャナの無視（Ignore Scanners）] フィールドにホストの IP アドレスを入力します。
単一のIPアドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。

ステップ 11 ホストをスキャンのターゲットとして無視するには、[スキャン対象の無視（Ignore Scanned）] フィールドにホストの IP アドレスを入力します。
単一のIPアドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。

ヒント 特にアクティブなネットワーク上のホストを示すには、[スキャナの無視（Ignore Scanners）] と [スキャン対象の無視（Ignore Scanned）] を使用します。このホスト リストは、時間経過とともに変更しなければならない場合があります。

ステップ 12 ミッドストリームでピックアップされたセッションのモニタリングを中断するには、[ACK スキャンの検出（Detect Ack Scans）] チェックボックスをオフにします。

（注） ミッドストリーム セッションの検出は ACK スキャンの識別に役立ちますが、大量のトラフィックとパケットのドロップが発生するネットワークでは、誤ってイベントが生成される可能性があります。

ステップ 13 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- イベントを生成し、インライン展開では、違反パケットをドロップします。するためにポートスキャン検出を行う場合は、ルール 122:1 ～ 122:27 を有効にします。詳細については、侵入ルールの状態, （1062 ページ）およびポートスキャン イベント生成, （1410 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）

レート ベースの攻撃防御

レート ベース攻撃とは、接続の頻度または攻撃を行うための反復試行に依存する攻撃のことです。レート ベースの検出基準を使用することで、レート ベース攻撃が行われていることを検出し、攻撃が発生するごとに対応できます。また、攻撃が収まった後は、通常の検出設定に戻すことができます。

レートベース フィルタを含めたネットワーク分析ポリシーを設定することで、ネットワーク上のホストを対象とした過剰なアクティビティを検出できます。インライン モードで展開されている管理対象デバイスでこの機能を使用すると、指定の期間だけレートベース攻撃をブロックし、その後イベントだけを生成してトラフィックをドロップしない状態に戻せます。

ネットワークのホストを SYN フラッドから保護するには、SYN 攻撃防止オプションを利用します。一定期間中に認められたパケットの数を基準に、個々のホストまたはネットワーク全体を保

護することができます。パッシブ導入のデバイスでは、イベントを生成できます。インライン導入のデバイスでは、不正なパケットをドロップすることもできます。タイムアウト期間の満了時にレート条件に達しなくなっていれば、イベントの生成およびパケットのドロップが停止します。

たとえば、1 つの IP アドレスからの SYN パケットの最大許容数を設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

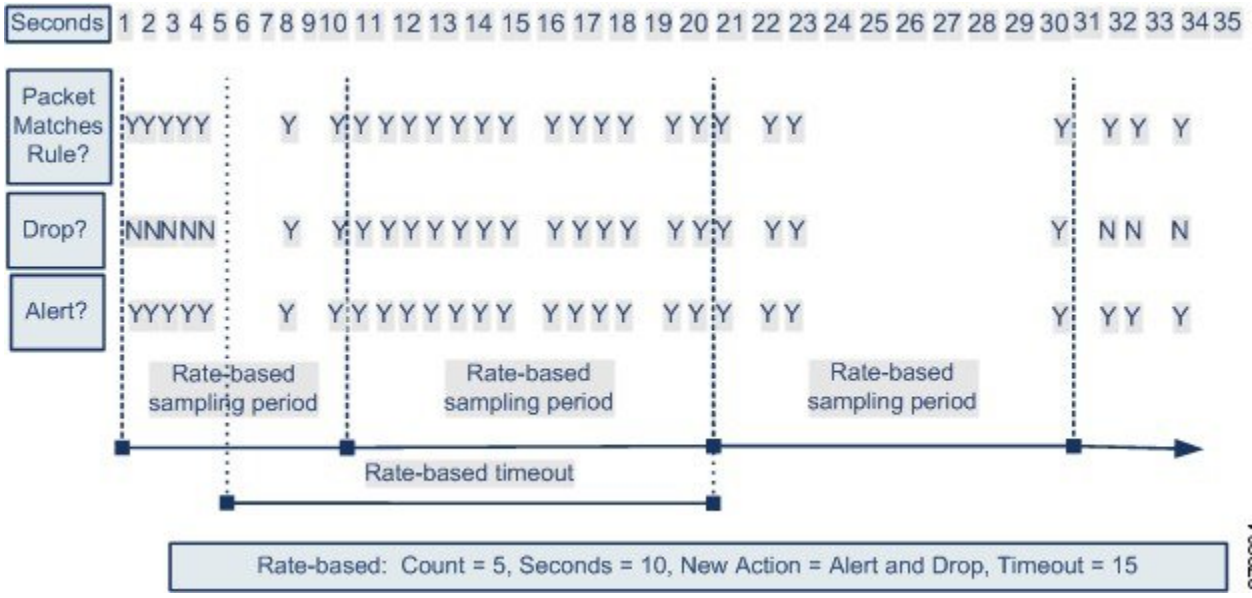
ネットワーク上のホストでの TCP/IP 接続数を制限することで、サービス妨害（DoS）攻撃や、ユーザによる過剰なアクティビティを防止できます。システムが、指定の IP アドレスまたはアドレス範囲で正常に行われている接続が設定された許容数に達したことを検出すると、以降の接続に対してイベントを生成します。タイムアウト期間が満了するまでは、レート条件に達しなくなっても、レート ベースのイベント生成が続行されます。インライン導入では、レート条件がタイムアウトになるまでパケットをドロップするように設定できます。

たとえば、1 つの IP アドレスからの同時接続の最大許容数を 10 に設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

（注） デバイスは内部リソース全体でインスペクションのロード バランスを行います。レート ベースの攻撃の防御を設定すると、デバイスごとではなく、リソースごとのトリガー レートを設定します。レートベースの攻撃の防御が適切に作動しなければ、トリガー レートを低減する必要があります。正しいレートを決定する際に支援が必要な場合は、サポートに連絡してください。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。繰り返しパスワードを特定しようとする試みが、レートベースの攻撃防止が設定されたルールをトリガーします。レートベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [ドロップしてイベントを生成する（Drop and Generate Events）] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または過去のサンプリング期間のしきい値を上回っている場合は、新しいアクションが継続されます。新しいアクションが元の「イベントの生成」アクションに戻されるのは、サンプリング期間の完了時にサンプルリング レートがしきい値を下回っている場合のみです。



関連トピック

動的侵入ルール状態, （1071 ページ）

レート ベースの攻撃防御の例

トラフィック自体またはシステムが生成するイベントをフィルタリングする手段としては、`detection_filter` キーワード、しきい値および抑制機能も使用できます。レート ベースの攻撃防御は、単独で使用することも、しきい値構成、抑制、または `detection_filter` キーワードと任意に組み合わせて使用することもできます。

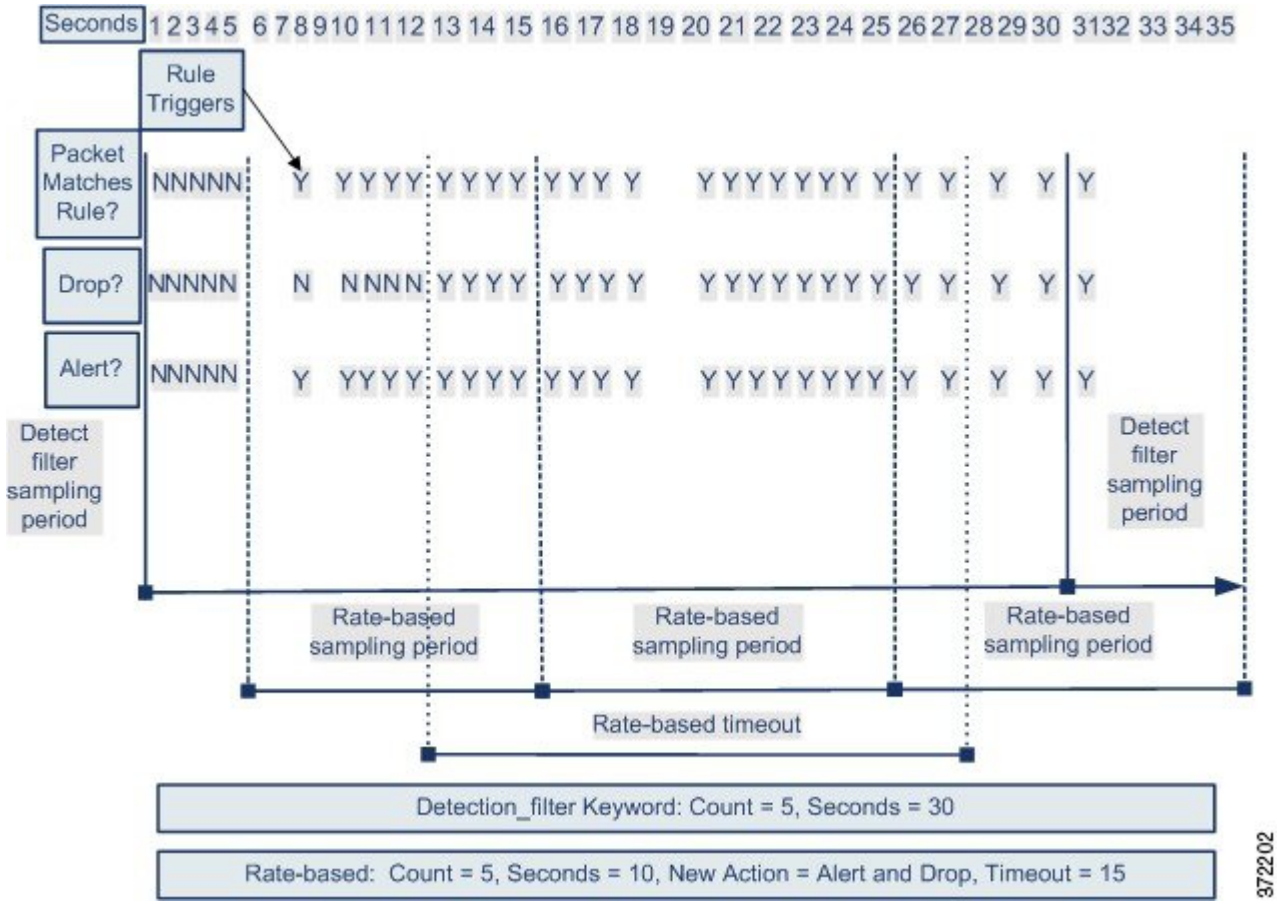
`detection_filter` キーワード、しきい値構成または抑制、およびレート ベースの基準のすべてが同じトラフィックに適用される場合もあります。抑制をルールに適用すると、レート ベースの変更が発生しても、指定の IP アドレスに対するイベントの生成は抑制されます。

detection_filter キーワードの例

以下に、攻撃者がブルートフォース ログインを仕掛ける例を示します。パスワードの検出試行が繰り返されると、カウントが 5 に設定された `detection_filter` キーワードも含むルールがトリガーされます。このルールには、レート ベース攻撃防止が設定されています。10 秒以内にルールに 5 回ヒットすると、レート ベースの設定により、ルール属性が 20 秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。

図に示されているように、最初の 5 個のパケットがルールに一致しても、イベントは生成されません。それは、レートが `detection_filter` キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに 5 個のパケットが通過するまでは、レート ベースの基準によって新しいアクション [ドロップしてイベントを生成する（Drop and Generate Events）] がトリガーされることはありません。

レート ベースの基準に一致すると、イベントが生成されて、パケットがドロップされます。これは、レート ベースのタイムアウト期間が満了し、かつレートがしきい値未満になるまで続きます。20 秒が経過すると、レート ベース アクションがタイムアウトになります。タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。タイムアウトが発生した時点で、サンプリングされたレートは前のサンプリング期間のしきい値レートを超過しているため、レート ベースのアクションは続行されます。



この例には示されていませんが、[ドロップしてイベントを生成する（Drop and Generate Events）] ルール状態を `detection_filter` キーワードと組み合わせて使用することで、ルールのヒット数が指定のレートに達するとトラフィックのドロップが開始されるようにすることができることにも注意してください。ルールにレート ベースの設定を使用するかどうかを決定する際は、ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定した場合の結果と `detection_filter` キーワードを含めた場合の結果が同じであるかどうか、あるいは侵入ポリシーでレートとタイムアウトの設定を管理する必要があるかどうかを検討してください。

関連トピック

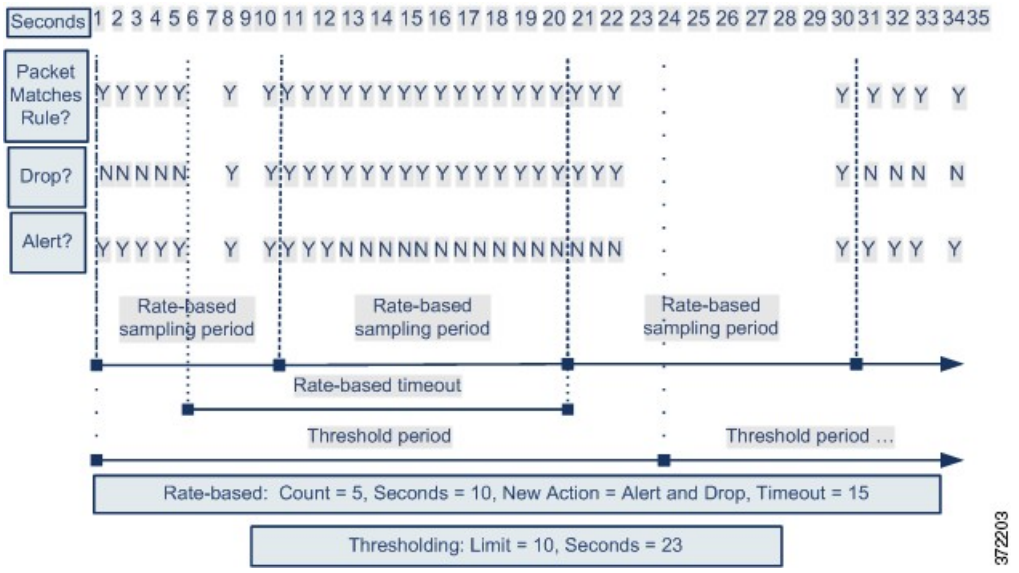
侵入ルールの状態, （1062 ページ）

ダイナミック ルール状態のしきい値構成または抑制の例

以下に、攻撃者がブルートフォースログインを仕掛ける例を示します。パスワードを特定する試みが繰り返されると、レートベースの攻撃防止が設定されているルールがトリガーされます。10秒以内にルールに5回ヒットすると、レートベースの設定により、ルール属性が15秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。さらに、上限しきい値により、ルールで生成可能なイベントの数が 23 秒間で 10 に制限されます。

図に示されているように、最初の5個のパケットが一致すると、ルールはイベントを生成します。5個のパケットがルールに一致した後、レートベースの基準が新しいアクションとして [ドロップしてイベントを生成する（Drop and Generate Events）] をトリガーし、次の 5 個のパケットがルールに一致した時点でイベントが生成され、パケットをドロップします。10 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成することなくドロップします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが続行されます。新しいアクションが元の[イベントを生成する（Generate Events）] アクションに戻されるのは、サンプリング期間の完了時にサンプルリング レートがしきい値を下回っている場合のみです。



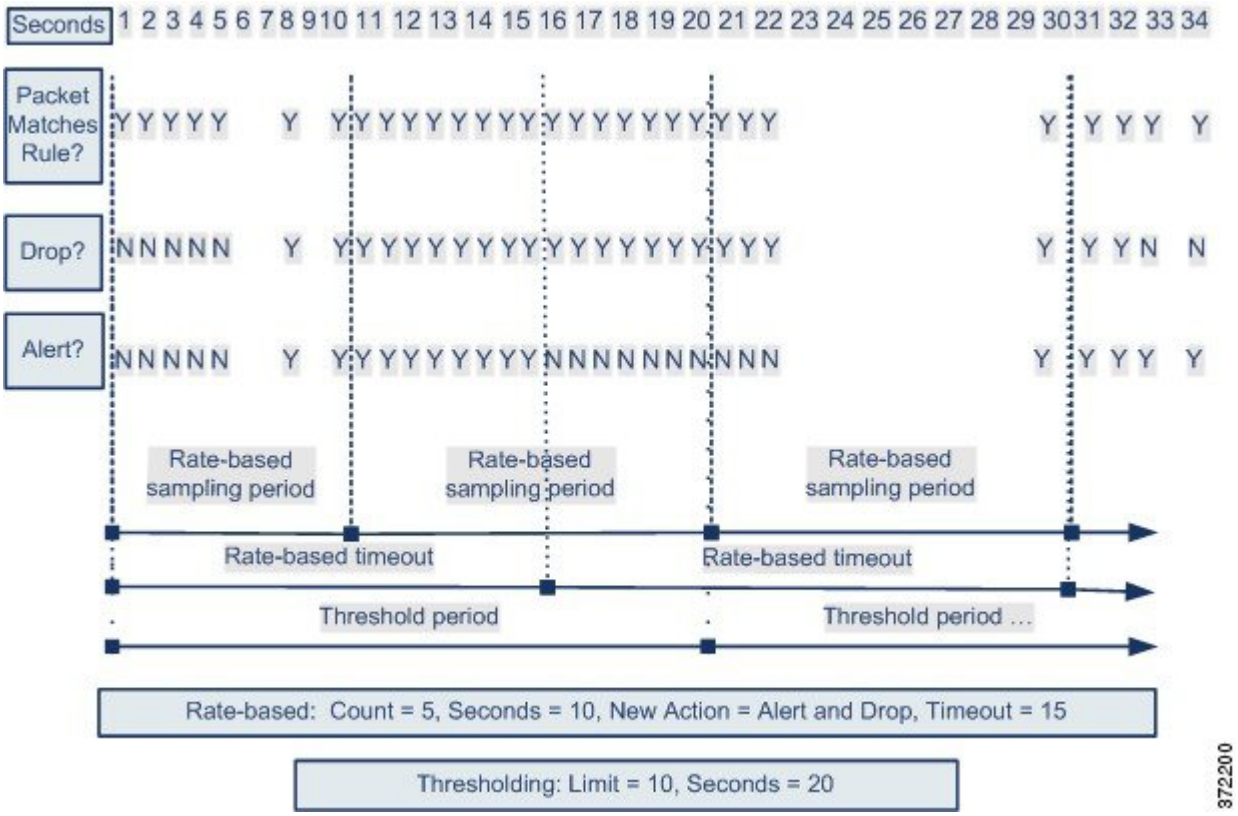
この例には示されていませんが、しきい値に達した後に、レートベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の10に達してシステムがイベントの生成を停止し、14 番目のパケットでアクションが [イベントを生成する（Generate Events）] から [ドロップしてイベントを生成する（Drop and Generate Events）] に変更されると、システムはアクションが変更されたことを示す 11 番目のイベントを生成します。

ポリシー全体のレート ベース検出としきい値構成または抑制の例

以下に、ネットワーク上のホストに対して、攻撃者がサービス妨害（DoS）攻撃を仕掛ける例を示します。同じ送信元から多数のホストに対して同時接続が行われると、ポリシー全体の[同時接続の制御（Control Simultaneous Connections）] 設定がトリガーされます。この設定は、1 つの送信元からの接続数が 10 秒間で 5 つに達すると、イベントを生成して悪意のあるトラフィックをドロップします。さらに、グローバル上限しきい値により、ルールまたは設定で生成可能なイベントの数が 20 秒間で 10 件に制限されます。

この図に示されているように、ポリシー全体の設定により、一致する最初の10個のパケットに対してイベントが生成され、トラフィックがドロップされます。10 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリングされたレートが、現在または前のサンプリング期間のしきい値レートを超過している場合、レート ベースのアクションによるイベントの生成とトラフィックのドロップが続行されます。レートベースアクションが停止するのは、サンプリング期間が完了した時点で、サンプリングされたレートがしきい値レートを下回っている場合のみです。



この例には示されていませんが、しきい値に達した後に、レート ベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の10に達してシステム

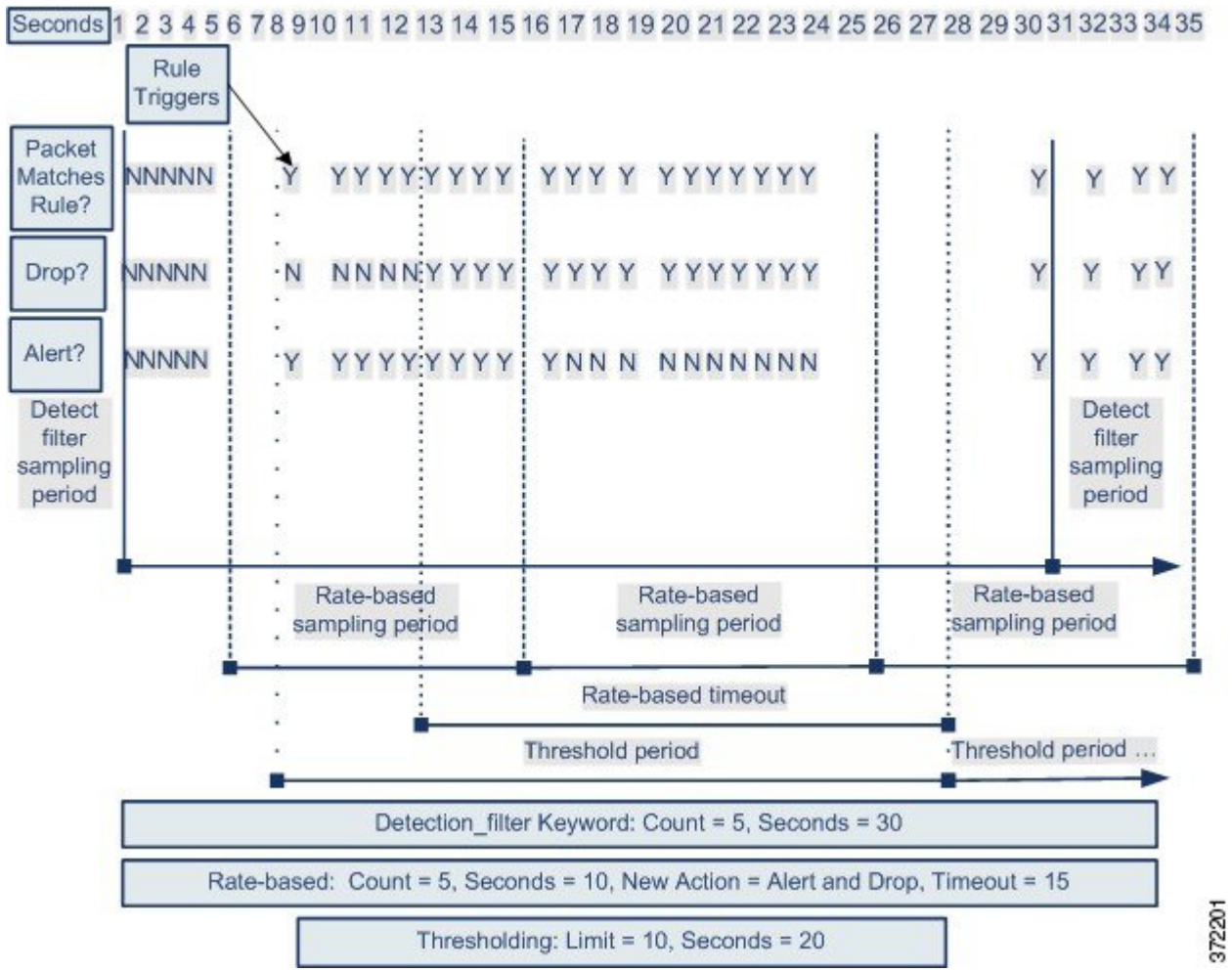
がイベントの生成を停止し、14 番目のパケットでアクションが [ドロップしてイベントを生成する（Drop and Generate Events）] に変更されると、システムはアクションが変更されたことを示す 11 番目のイベントを生成します。

複数のフィルタリング方法によるレート ベース検出の例

以下に、攻撃者がブルートフォース ログインを仕掛ける例で、`detection_filter` キーワード、レート ベースのフィルタリング、およびしきい値が相互作用する場合を説明します。パスワードの検出試行が繰り返されると、カウントが 5 に設定された `detection_filter` キーワードを含むルールがトリガーされます。このルールには、レート ベースの攻撃防御も設定されています。その設定では、15 秒間にルールのヒット数が 5 に達すると、ルール属性が 30 秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。さらに、上限しきい値により、ルールによって生成されるイベントは 30 秒間で 10 件に制限されます。

図に示されているように、最初の 5 個のパケットがルールに一致しても、イベント通知は行われません。それは、`detection_filter` キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに 5 個のパケットが通過するまでは、レート ベースの基準によって新しいルールとして [ドロップしてイベントを生成する（Drop and Generate Events）] がトリガーされることはありません。レート ベースの基準が満たされると、システムは 11 個目から 15 個目のパケットに対してイベントを生成し、パケットをドロップします。15 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

レート ベースのタイムアウトが発生した後は、それに続くレート ベースのサンプリング期間中、パケットが引き続きドロップされることに注意してください。サンプリング レートが前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが続行されます。



レート ベースの攻撃防御オプションと設定

レートベース攻撃の防御では、異常なトラフィック パターンを識別して、そのトラフィックが正当な要求に与える影響を最小限に抑えるようにします。一般に、レート ベース攻撃には次のいずれかの特性があります。

- 任意のトラフィックに、ネットワーク上のホストに対して過剰な未完了接続が含まれています。これは、SYN フラッド攻撃を意味します。
- 任意のトラフィックには、ネットワーク上のホストに対して過剰な接続が含まれています。これは、TCP/IP 接続フラッド攻撃を意味します。
- 1 つ以上の特定の宛先 IP アドレスへのトラフィック、または 1 つ以上の特定の送信元 IP アドレスからのトラフィックで、ルールとの一致が過剰に発生します。
- すべてのトラフィックで、特定のルールとの一致が過剰に発生します。

ネットワーク分析ポリシーでは、ポリシー全体に対して SYN フラッドまたは TCP/IP 接続フラッドのいずれかの検出を設定することができます。または個々の侵入ルールもしくはプリプロセッ

サ ルールに対してレート ベース フィルタを設定できます。GID 135 ルールに手動でレート ベース フィルタを追加すること、またはルールの状態を変更することはできない点に注意してください。GID 135 のルールでは、クライアントを送信元の値、サーバを宛先の値として使用します。

（注） 内部リソースのデバイスの負荷分散試験。レート ベースの攻撃の防御を設定すると、デバイスごとではなく、リソースごとのトリガー レートを設定します。レートベースの攻撃の防御が適切に作動しなければ、トリガー レートを低減する必要があります。正しいレートを決定する場合は、サポート チームにご連絡ください。

[SYN 攻撃の防御（SYN Attack Prevention）] オプションを有効にすると、ルール 135:1 もアクティブになります。このルールを手動でアクティブにしても効果はありません。ルール状態は常に [無効（Disabled）] として表示され、変更されることはありません。このオプションを有効にすると、定義されたレート条件を超過した時点で、ルールによってイベントが生成されます。

[同時接続の制御（Control Simultaneous Connections）] オプションを有効にすると、ルール 135:2 および 135:3 もアクティブになります。このルールを手動でアクティブにしても効果はありません。ルール状態は常に [無効（Disabled）] として表示され、変更されることはありません。定義されたレート条件を超過した時点で、135:2 のルールによってイベントが生成されます。セッションが終了するかタイムアウトすると、ルール 135:3 はイベントを生成します。

各レート ベース フィルタには、以下のコンポーネントが含まれます。

- ポリシー全体またはルール ベースの送信元/宛先の設定の場合、ネットワーク アドレスの指定
- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率
- レートを超過した場合に実行する新しいアクション

  ポリシー全体に対してレート ベースを設定すると、システムはレート ベース攻撃を検出した時点でイベントを生成します。インライン展開では、トラフィックをドロップすることもできます。個々のルールにレート ベース アクションを設定する場合は、[イベントの生成（Generate Events）]、[イベントのドロップと作成（Drop and Generate Events）]、[無効（Disable）] の 3 つの利用可能なアクションから選択できます。
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウト期間が満了し、レートがしきい値を下回っている場合、ルールのアクションはそのルールに最初に設定されたアクションに戻ります。ポリシー全体に適用される設定の場合、アクションは、トラフィックと一致する個々のルールのアクションに戻ります。一致するアクションがなければ、アクションは停止されます。

インライン展開のレート ベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レートベースの設定が使用されていない場合、ルールが [イベントの生成（Generate Events）] に設定されていればイベントが生成されますが、そのルールのパケットがドロップされることはありません。ただし、攻撃トラフィックが、レート ベースの基準が設定されているルールに一致した場合、それらのルールが当初 [イベントのドロップおよび生成（Drop and Generate

Events）]に設定されていないとしても、レートアクションがアクティブである期間は、パケットがドロップされる場合があります。

（注） レート ベース アクションでは、無効にされたルールを有効にすることも、無効にされたルールに一致するトラフィックをドロップすることもできません。ただし、ポリシー レベルでレートベース フィルタを設定すると、指定した期間内の過剰な数のSYNパケットまたはSYN/ACKインタラクションを含むトラフィックに対してイベントを生成するか、イベントを生成してトラフィックをドロップすることができます。

同じルールに複数のレート ベース フィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2つのレートベース フィルタ アクションが競合する場合は、最初のレートベースフィルタのアクションが実行されることに注意してください。同様に、ポリシー全体に対するレート ベース フィルタと個々のルールに設定されたレート ベース フィルタが競合する場合は、ポリシー全体のレート ベース フィルタが優先されます。

関連トピック

[ルール（Rule）] ページからの動的ルール状態の設定, （1073 ページ）

レートベースの攻撃防御、検出フィルタリング、しきい値処理または抑制

キーワード`detection_filter`により、ルールに一致するしきい値が指定の時間内に発生するまで、ルールのトリガーを阻止します。ルールに `detection_filter` キーワードが含まれている場合、システムは指定の期間、ルールのパターンに一致する着信パケットの数を追跡します。システムはそのルールについて、特定の送信元 IP アドレスからのヒット数、または特定の宛先 IP アドレスからのヒット数をカウントできます。レートがルールのレートを超過すると、そのルールに関するイベント通知が開始されます。

しきい値処理と抑制を用いて、ルール、送信元または宛先に関するイベント通知数を制限することまたはそのルールをすべて一緒に通知を抑制することで、過剰なイベントを低減できます。また、オーバーライドする特定のしきい値がない各ルールに適用するグローバル ルールのしきい値を設定できます。

ルールに抑制を提供する場合、ポリシー全体またはルールにより指定されたレート ベースの設定であるため、レート ベースでアクションの変更が発生した場合でも、システムは、すべての適用可能な IP アドレスのそのルールのイベント通知を抑制します。

関連トピック

侵入イベントのしきい値, （1064 ページ）
侵入ポリシーの抑制の設定, （1068 ページ）
グローバル ルールのしきい値の基本, （1099 ページ）

レートベース攻撃防止の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

ポリシー レベルでレートベース攻撃防止を設定することで、SYNフラッド攻撃を阻止できます。特定の送信元からの過剰な接続、または特定の宛先への過剰な接続を阻止することもできます。

手順

ステップ 1 [ポリシー（Policies）]>[アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。または[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [設定（Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [レートベース攻撃防止（Rate-Based Attack Prevention）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [レートベース攻撃防止（Rate-Based Attack Prevention）] の横にある編集アイコン（）をクリックします。

ステップ 6 次の 2 つの選択肢があります。

- ホストのフラッディングを目的とする不完全な接続を防ぐには、[SYN 攻撃の防止（SYN Attack Prevention）] の下にある [追加（Add）] をクリックします。
- 過剰な数の接続を防ぐには、[同時接続の制御（Control Simultaneous Connections）] の下にある [追加（Add）] をクリックします。

ステップ 7 トラフィックを追跡する方法を指定します。

- 特定の送信元または送信元の範囲からのすべてのトラフィックを追跡するには、[追跡対象（Track By）] ドロップダウン リストから [送信元（Source）] を選択し、[ネットワーク（Network）] フィールドに単一の IP アドレスまたはアドレス ブロックを入力します。

- 特定の宛先または宛先の範囲へのすべてのトラフィックを追跡するには、[追跡対象（Track By）] ドロップダウン リストから [宛先（Destination）] を選択し、[ネットワーク（Network）] フィールドに単一の IP アドレスまたはアドレス ブロックを入力します。

  （注） システムは、[ネットワーク（Network）] フィールドに含まれる各 IP アドレスのトラフィックを個別に追跡します。ある特定の IP アドレスからの設定されたレートを超過するトラフィックがある場合、その IP アドレスに関するイベントだけが生成されることになります。例として、ネットワーク設定で `10.1.0.0/16` の送信元 CIDR ブロックを設定し、10 個の同時接続が開始された時点でイベントを生成するようにシステムを設定するとします。10.1.4.21 から 8 つの接続が開始され、10.1.5.10 から 6 つの接続が開始されている場合、いずれの送信元も開始されている接続がトリガーを引き起こす数になっていないため、システムはイベントを生成しません。一方、10.1.4.21 から 11 個の同時接続が開始されている場合、システムは 10.1.4.21 からの接続に対してだけイベントを生成します。

  システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ステップ 8 レート追跡設定をトリガーとして使用するレートを指定します。

- SYN 攻撃に対する構成の場合は、[レート（Rate）] フィールドに、一定の秒数あたりの SYN パケット数を入力します。
- 同時接続に対する構成の場合は、[カウント（Count）] フィールドに、接続数を入力します。

デバイスは、内部リソースにインスペクションの負荷を分散させます。レート ベースの攻撃の防御を設定すると、デバイスごとではなく、リソースごとのトリガー レートを設定します。レート ベースの攻撃の防御が適切に作動しなければ、トリガー レートを低減する必要があります。正しいレートの決定する方法については、サポートに問い合わせてください。

ステップ 9 レートベース攻撃防止設定に一致するパケットをドロップするには、[ドロップ（Drop）] チェックボックスをオンにします。

ステップ 10 [タイムアウト（Timeout）] フィールドに、イベント生成のタイムアウト期間を入力します。この期間を経過すると、SYN または同時接続のパターンに一致するトラフィックに対するイベント生成が（該当する場合はドロップも）停止されます。

注意 インライン展開では、大きいタイムアウト値を指定するとホストへの接続が完全にブロックされる可能性があります。

ステップ 11 [OK] をクリックします。

ステップ 12 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）

第 62 章

適応型プロファイル

ここでは、適応型プロファイルの設定方法について説明します。

アダプティブ プロファイルについて

通常、システムはネットワーク分析ポリシーの静的な設定を使用して、トラフィックの前処理と分析を行います。アダプティブ プロファイルでは、ネットワーク検出で検出したホスト情報またはサードパーティからインポートしたホスト情報に合わせて、システムが処理動作を変更します。

アダプティブプロファイルネットワーク分析ポリシーに手動で設定可能なターゲットベースプロファイルと同様に、ターゲットホストのオペレーティングシステムと同じ方法で、IP パケットの最適化およびストリームのリアセンブルを行うのに役立ちます。その後、侵入ルール エンジンは宛先ホストによって使用されるものと同じ形式でデータを分析します。

手動で設定されたターゲットベース プロファイルは、選択したデフォルト オペレーティング システム プロファイルまたは特定のホストにバインドしたプロファイルのいずれかに適用されます。アダプティブプロファイルでは、ターゲットホストのホストプロファイル内のオペレーティング システムに基づいて、適切なオペレーティング システム プロファイルに切り替えを行います。

10.6.0.0/16 サブネット向けにアダプティブ プロファイルを設定し、Linux にデフォルトの IP 最適化ターゲットベース ポリシーを設定するシナリオを考えてみます。設定を構成する Firepower Management Center には 10.6.0.0/16 サブネットを含むネットワーク マップがあります。

- システムが 10.6.0.0/16 サブネットにないホスト A からのトラフィックを検出すると、Linux ターゲットベース ポリシーを使用して IP フラグメントのリアセンブルを行います。

- システムが 10.6.0.0/16 サブネット上にあるホスト B からのトラフィックを検出すると、ネットワーク マップからホスト B のオペレーティング システム データを取得します。システムは、このオペレーティングシステムに基づいたプロファイルを使用し、ホストBを宛先とするトラフィックを最適化します。

アダプティブプロファイルおよび Firepower 推奨ルール

アダプティブ プロファイル機能は、アクセス コントロール ポリシーの詳細設定で、そのアクセスコントロールポリシーによって呼び出されるすべての侵入ポリシーにグローバルに適用されます。Firepower 推奨ルールの機能は、設定する個々の侵入ポリシーに適用されます。

Firepower推奨ルールと同様に、アダプティブプロファイルはルールのメタデータをホスト情報と比較し、ルールを特定のホストに適用すべきかどうかを判別します。ただし、Firepower推奨ルールがその情報を使用してルールの有効化または無効化を行うための推奨事項を提供するのに対して、アダプティブ プロファイルはその情報を使用して特定のトラフィックに特定のルールを適用します。

Firepower推奨ルールでは、提案された変更をルール状態に実装するために、ユーザの対話が必要になります。一方、アダプティブ プロファイルは侵入ポリシーを変更しません。ルールの適応型処理は、パケット単位で行われます。

さらに、Firepower推奨ルールによって、無効なルールが有効化される可能性があります。アダプティブ プロファイルは、対照的に、侵入ポリシーですでに有効になっているルールの適用にだけ影響します。アダプティブ プロファイルがルール状態を変更することはありません。

アダプティブ プロファイルと Firepower 推奨ルールは組み合わせて使用できます。侵入ポリシーを展開すると、アダプティブ プロファイルはルールの状態を使用して適用の候補に含めるかどうかを判別し、推奨事項の承認または拒否はそのルール状態に反映されます。両方の機能を使用して、監視対象の各ネットワークに最適なルールを有効化または無効化することができ、特定のトラフィックに対する有効化したルールの適用を最も効率的に行うことができます。

適応型プロファイルのオプション

アダプティブ プロファイル - 有効（Adaptive Profiles - Enabled）

アダプティブ プロファイルを有効または無効にします。

アダプティブ プロファイル - 属性の更新間隔（Adaptive Profiles - Attribute Update Interval）

Firepower Management Center から管理対象デバイスに対するネットワーク マップ データの同期の頻度を分単位で制御することができます。システムはデータを使用して、トラフィックを処理する際に使用するプロファイルを判別します。このオプションの値を大きくすると、大規模なネットワークでパフォーマンスを向上させることができます。

アダプティブ プロファイル - ネットワーク（Adaptive Profiles - Networks）

任意で、IP アドレス、アドレス ブロック、およびネットワーク変数のカンマ区切りリストに対する アダプティブ プロファイル を制限して、パフォーマンスを向上させることができます。ネットワーク変数を使用すると、アクセス コントロール ポリシーのデフォルトの侵入ポリシーにリンクされている変数セットの変数の値が使用されるようになります。たとえば、192.168.1.101、192.168.4.0/24、$HOME_NET というように入力することができます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上位ポリシーでアダプティブ プロファイルを有効にして適用する場合、Cisco では、デフォルトのネットワークの制約 0.0.0.0/0 を保持するか、または値 `any` を指定してネットワーク変数を使用することをお勧めしています。この設定により、すべてのサブドメインのすべてのモニタ対象ホストに アダプティブ プロファイル が適用されるようになります。

適応型プロファイルの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

パッシブ展開では、アダプティブ プロファイルを設定することをお勧めします。インライン展開の場合、インライン正規化プリプロセッサの設定で [TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にします。

注意 アクセス制御ルールで AMP を含むアプリケーション/ファイル制御を実行し、侵入ルールでサービス メタデータを使用するためには、この手順の説明に従ってアダプティブ プロファイルを有効にする必要があります。アダプティブ プロファイルを有効化または無効化すると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

手順

ステップ 1 アクセス コントロール ポリシー エディタで [詳細（Advanced）] タブをクリックし、[検出拡張の設定（Detection Enhancement Settings）] セクションの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 2 適応型プロファイルのオプション, （1430 ページ）の説明に従って適応型プロファイルのオプションを設定します。

ステップ 3 [OK] をクリックします。

ステップ 4 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 XVI 部

検出とアイデンティティ

第 63 章

ネットワーク検出とアイデンティティの概要

次のトピックでは、ネットワーク検出およびアイデンティティ ポリシーとデータの概要を示します。

ホスト、アプリケーション、ユーザの検出

Firepower システムは、ネットワーク検出およびアイデンティティ ポリシーを使用して、ネットワーク トラフィックのホスト、アプリケーション、およびユーザのデータを収集します。特定のタイプの検出およびアイデンティティ データを使用すると、ネットワーク アセットの包括的なマップを作成し、フォレンジック分析、動作プロファイリング、アクセス制御を行い、組織が影響を受ける脆弱性およびエクスプロイトに対応して軽減することができます。

ホストおよびアプリケーション データ

ホストやアプリケーション データは、ネットワーク検出ポリシーの設定に従ってホストのアイデンティティ ソースとアプリケーション ディテクタによって収集されます。管理対象デバイスは、指定したネットワーク セグメントのトラフィックを確認します。

詳細については、ホストおよびアプリケーション検出の基礎, （1437ページ）を参照してください。

ユーザ データ（User Data）

ユーザ データはネットワーク検出およびアイデンティティ ポリシーの設定に従ってユーザのアイデンティティ ソースによって収集されます。データはユーザ認識とユーザ制御のために使用できます。

詳細については、ユーザ検出の基本，（1445 ページ）を参照してください。

関連トピック

ホスト ID ソース，（1453 ページ）
アプリケーションの検出，（1507 ページ）
ユーザ アイデンティティ ソース，（1531 ページ）

ホスト、アプリケーション、およびユーザ検出とアイデンティティ データの使用

検出データとアイデンティティ データをロギングすることにより、次のような Firepower システムのさまざまな機能を活用できます。

- ネットワーク アセットとトポロジの詳細を示すネットワーク マップを表示します。その際、ホストとネットワーク デバイス、ホスト属性、アプリケーション プロトコル、または脆弱性をグループ化して表示できます。
- アプリケーション、レルム、ユーザ、ユーザ グループ、およびISE 属性の各条件を使ってアクセス コントロール ルールを作成することにより、アプリケーション制御およびユーザ制御を実行します。
- 検出されたホストで利用可能なすべての情報の完全なビューであるホスト プロファイルを表示します。
- （さまざまな機能の 1 つとして）ネットワーク アセットとユーザ アクティビティの概要を示すダッシュボードを表示します。
- システムによって記録された検出イベントとユーザ アクティビティに関する詳細情報を表示します。
- ホストおよびそこで実行されているサーバ/クライアントと、被害を及ぼす可能性のあるエクスプロイトとを関連付けます。

  これにより、脆弱性を特定して軽減したり、ネットワークに対する侵入イベントの影響を評価したり、ネットワーク アセットを最大限に保護できるように侵入ルール状態を調整したりできます。
- システムで特定の影響フラグ付きの侵入イベントまたは特定のタイプの検出イベントが生成された場合に、電子メール、SNMP トラップ、または syslog によるアラートを発行します。
- 許可されたオペレーティング システム、クライアント、アプリケーション プロトコル、およびプロトコルのホワイト リストを使用して組織のコンプライアンスをモニタします。

- システムが検出イベントを生成するかユーザアクティビティを検出したときにトリガーして相関イベントを生成するルールを使って、相関ポリシーを作成します。
- 該当する場合、NetFlow 接続をロギングして使用します。

ホストおよびアプリケーション検出の基礎

ネットワーク検出ポリシーを設定すると、ホストおよびアプリケーション検出を実行できます。

詳細については、概要：ホストのデータ収集, （1453ページ）および概要：アプリケーション検出, （1507 ページ）を参照してください。

オペレーティング システムおよびホスト データのパッシブ検出

パッシブ検出 は、システムがネットワーク トラフィック（およびエクスポートされた NetFlow データ）を分析してネットワーク マップにデータを取り込む際のデフォルト方式です。パッシブ検出では、ネットワーク アセットに関するコンテキスト情報（オペレーティング システムや実行中のアプリケーションなど）が提供されます。

モニタ対象のホストからのトラフィックが、ホストで実行されているオペレーティング システムを示す決定的証拠とならない場合、使用されている可能性が最も高いオペレーティングがネットワーク マップに表示されます。たとえば、複数のホストが NAT デバイスの「背後」にあることから、NAT デバイスが複数のオペレーティング システムを実行しているように表示される場合があります。この最も可能性の高いオペレーティングを決定するためにシステムが使用するのは、検出された各オペレーティング システムに割り当てられた信頼度の値と、検出されたオペレーティング システムの中でその特定のオペレーティング システムが使用されていることを裏付けるデータの量です。

（注） この決定を行う際、システムは「unknown」として報告されたアプリケーションとオペレーティング システムを考慮しません。

パッシブ検出でネットワーク アセットが正確に識別されない場合は、管理対象デバイスの配置について検討してください。また、システムのパッシブ検出機能をオペレーティング システムのカスタム フィンガープリントとカスタム アプリケーション ディテクタで増補することもできます。あるいは、アクティブ検出 を使用するという方法もあります。アクティブ検出では、トラフィック分析をベースとするのではなく、スキャン結果やその他の情報ソースを使用して直接ネットワーク マップを更新できます。

オペレーティング システムおよびホスト データのアクティブ検出

アクティブ検出では、アクティブ ソースによって収集されたホスト情報をネットワーク マップに追加します。たとえば、Nmap スキャナを使用して、ネットワーク上の対象ホストをアクティブにスキャンできます。Nmap は、ホストでオペレーティング システムおよびアプリケーションを検出します。

さらに、ホスト入力機能によって、ネットワーク マップにホスト入力データをアクティブに追加することができます。ホスト入力データには 2 種類のカテゴリがあります。

- ユーザ入力データ：FirePOWER システム ユーザ インターフェイスで追加されたデータ。このユーザ インターフェイスを使用して、ホストのオペレーティング システムやアプリケーションの ID を変更できます。
- ホスト インポート入力データ：コマンド ライン ユーティリティを使用してインポートされたデータ。

システムは、それぞれのアクティブ ソースに対して 1 個の ID を保持します。たとえば、Nmap スキャン インスタンスを実行すると、以前のスキャンの結果は新しいスキャン結果に置き換えられます。ただし、Nmap スキャンを実行し、それらの結果をクライアントからのデータ（コマンド ラインを使用してインポートした結果）と交換する場合、システムは Nmap の結果の ID とインポート クライアントの ID の両方を保持します。システムは、ネットワーク検出ポリシーで設定された優先順位を使用して、現在の ID として使用するアクティブ ID を判別します。

複数のユーザが入力したとしても、ユーザ入力は1 ソースと見なされることに注意してください。たとえば、UserA がホスト プロファイルを使用してオペレーティング システムを設定し、UserB がホスト プロファイルを使用してその定義を変更した場合、UserB によって設定された定義が保持され、UserA によって設定された定義は破棄されます。また、ユーザ入力によって、他のアクティブ ソースすべてが上書きされ、存在する場合、現在の ID として使用されることに注意してください。

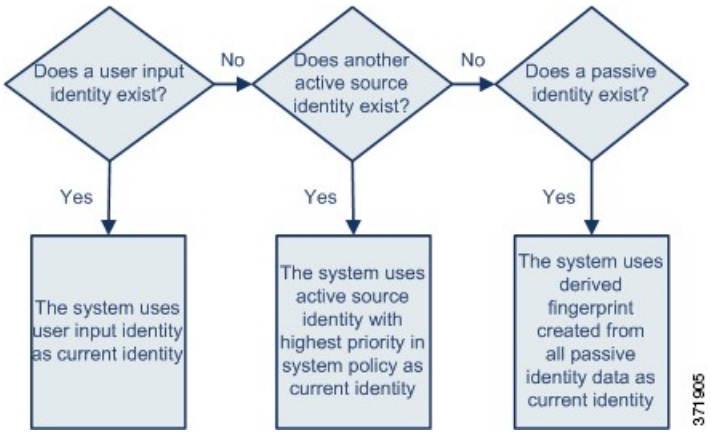
アプリケーションおよびオペレーティング システムの現在の ID

ホストのアプリケーションまたはオペレーティング システムの現在の *ID* は、ホストが最も正しい可能性が高いと認識する ID です。

システムは、以下の目的で、オペレーティング システムまたはアプリケーションの現在の ID を使用します。

- 脆弱性のホストへの割り当て
- 影響評価
- オペレーティング システムの識別、ホスト プロファイルの認定、およびコンプライアンスのホワイトリストに対して記述された相関ルールの評価
- ワークフローのホストおよびサーバのテーブル ビューでの表示
- ホスト プロファイルでの表示
- [検出統計情報（Discovery Statistics）] ページでのオペレーティング システムとアプリケーションの統計の計算

システムは、ソースの優先順位を使用して、アプリケーションまたはオペレーティング システムの現在の ID として使用するアクティブ ID を判別します。



たとえば、ユーザがホストでオペレーティング システムを Windows 2003 Server に設定した場合、Windows 2003 Server が現在の ID になります。そのホストの Windows 2003 Server の脆弱性を狙った攻撃により大きな影響力があると見なされ、ホスト プロファイルのそのホストについてリストされた脆弱性に、Windows 2003 Server の脆弱性が含められます。

データベースは、ホストのオペレーティング システムや特定のアプリケーションに関する複数のソースからの情報を保持する場合があります。

データのソースに最も高いソースの優先順位が付けられている場合に、システムはオペレーティング システムまたはアプリケーションの ID を現在の ID として扱います。使用される可能性のあるソースには、次の優先順位があります。

1：ユーザ

2：スキャナとアプリケーション（ネットワーク検出ポリシーで設定）

3：管理対象デバイス

4：NetFlow レコード

新しい優先順位の高いアプリケーション ID は、現在のアプリケーション ID ほど詳細でない場合、現在の ID を上書きしません。

また、ID の競合が発生した場合、競合の解決はネットワーク検出ポリシーの設定または手動解決によります。

現在のユーザ ID

システムは、同じホストに対して異なるユーザによる複数のログインを検出すると、特定のホストにログインするユーザは一度に 1 人だけであり、ホストの現在のユーザが最後の権限のあるユーザ ログインであると見なします。権限のないユーザ ログインだけがホストにログインしている場合は、最後にログインしたものが現在のユーザと見なされます。複数のユーザがリモート セッション経由でログインしている場合は、サーバによって報告された最後のユーザが Firepower Management Centerに報告されるユーザです。

システムは、同じホストに対して異なるユーザによる複数のログインを検出すると、ユーザが初めて特定のホストにログインした時点を記録し、それ以降のログインを無視します。あるユーザ

が特定のホストにログインしている唯一の人物の場合は、システムが記録する唯一のログインがオリジナルのログインです。

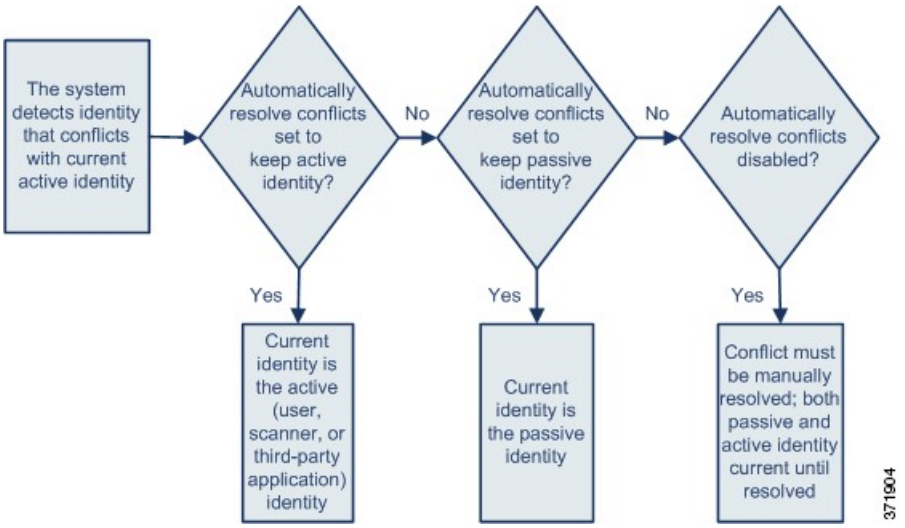
ただし、そのホストに別のユーザがログインした時点で、システムは新しいログインを記録します。その後で、オリジナルのユーザが再度ログインすると、その人物の新しいログインが記録されます。

アプリケーションおよびオペレーティング システムの ID の競合

現在のアクティブ ID および以前に報告されたパッシブ ID と競合する新しいパッシブ ID が報告されると、*ID* の競合が発生します。たとえば、オペレーティング システムの以前のパッシブ ID は Windows 2000 と報告され、Windows XP のアクティブ ID が現在の ID になります。次に、システムが Ubuntu Linux 8.04.1 の新しいパッシブ ID を検出します。Windows XP と Ubuntu Linux の ID が競合状態になります。

ホストのオペレーティング システムまたはホスト上のいずれかのアプリケーションの ID に対して ID の競合が存在する場合、システムは現在の ID として競合する両方の ID をリストし、競合が解決されるまで影響評価に両方の ID を使用します。

管理者特権を持つユーザは、パッシブ ID を常に使用するか、またはアクティブ ID を常に使用するかを選択することによって、自動的に ID の競合を解決できます。ID の競合の自動解決を無効にしない限り、ID の競合は常に自動的に解決されます。



管理者特権を持つユーザは、ID の競合が発生した場合に、イベントを生成するようにシステムを設定することもできます。そのユーザは、相関応答として Nmap スキャンを使用する相関ルールで相関ポリシーを設定できます。イベントが発生すると、Nmap はホストをスキャンして、更新されたホストのオペレーティング システムとアプリケーション データを取得します。

Firepower システムの NetFlow データ

NetFlow は、ルータを通過するパケットの統計情報を提供する、Cisco IOS アプリケーションの 1 つです。NetFlow は Cisco ネットワーキング デバイスで使用できます。また、Juniper、FreeBSD、OpenBSD デバイスに組み込むことも可能です。

NetFlow がネットワーク デバイスで有効にされている場合、そのデバイス上のデータベース（NetFlow キャッシュ）に、ルータを通過するフローのレコードが格納されます。Firepower システムで接続と呼ばれるフローは、特定のポート、プロトコル、およびアプリケーション プロトコルを使用する送信元ホストと宛先ホスト間のセッションを表すパケットのシーケンスです。この NetFlow データをエクスポートするようにネットワーク デバイスを設定できます。本書では、そのように設定されたネットワーク デバイスを NetFlow エクスポータと呼びます。

Firepower システムの管理対象デバイスは、NetFlow エクスポータからレコードを収集して、それらのレコードに含まれるデータに基づいて単方向の接続終了イベントを生成し、それらのイベントを接続イベント データベースに記録するために Firepower Management Center に送信するように設定できます。また、NetFlow 接続内の情報に基づいて、ホストとアプリケーション プロトコルに関する情報をデータベースに追加するためのネットワーク検出ポリシーを設定することもできます。

この検出データと接続データを使用して、管理対象デバイスによって直接収集されたデータを補完できます。これは、管理対象デバイスでモニタできないネットワークを NetFlow エクスポータにモニタさせる場合には特に有効です。

NetFlow データを使用するための要件

NetFlow データを分析するために Firepower System を設定する前に、ルータまたは使用する他の NetFlow が有効なネットワーク デバイス上で NetFlow 機能を有効にし、管理対象デバイスのセンシング インターフェイスを接続する宛先ネットワークへ NetFlow データをブロードキャストするようにデバイスを設定する必要があります。

Firepower System では、NetFlow バージョン 5 レコードと NetFlow バージョン 9 レコードをいずれも解析できます。Firepower System にデータをエクスポートするには、NetFlow エクスポータがいずれかのバージョンを使用する必要があります。さらに、このシステムでは、特定のフィールドがエクスポートされた NetFlow テンプレートとレコードに存在する必要があります。NetFlow エクスポータがカスタマイズ可能なバージョン 9 を使用している場合は、エクスポートされたテンプレートとレコードに次のフィールドが任意の順序で含まれていることを確認する必要があります。

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)

- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

Firepower System は管理対象デバイスを使用して NetFlow データを分析するため、NetFlow エクスポータの監視可能な 1 つ以上の管理対象デバイスを展開に含める必要があります。この管理対象デバイス上の 1 つ以上のセンシング インターフェイスを、エクスポートされた NetFlow データを収集可能なネットワークに接続する必要があります。通常、管理対象デバイス上のセンシング インターフェイスには IP アドレスが割り当てられないため、システムは NetFlow レコードの直接収集をサポートしません。

一部のネットワーク デバイス上で使用可能な Sampled NetFlow 機能は、デバイスを通過するパケットのサブセットだけに基づく NetFlow 統計情報を収集することに注意してください。この機能を有効にすると、ネットワーク デバイス上の CPU 使用率が改善される可能性がありますが、Firepower System で分析するために収集されている NetFlow データに影響する場合があります。

NetFlow データと管理対象デバイス データの違い

Firepower システムは、NetFlow データによって表されるトラフィックを直接分析しません。代わりに、エクスポートした NetFlow レコードを接続ログおよびホストとアプリケーションのプロトコル データに変換します。

その結果、変換された NetFlow データと、管理対象デバイスによって直接収集された検出および接続データにはいくつかの違いがあります。以下のことを必要とする分析を実行する場合に、これらの違いを意識しなければなりません。

- 検出された接続数に基づく統計情報
- オペレーティング システムとその他のホスト関連情報（脆弱性を含む）
- クライアント情報、Web アプリケーション情報、ベンダーおよびバージョン サーバ情報を含むアプリケーション データ
- 接続内の発信側のホストと応答側のホストの認識

ネットワーク検出ポリシーとアクセス コントロール ポリシーの違い

接続ロギングを含む NetFlow データ収集は、ネットワーク検出ポリシー内のルールを使用して設定します。これを、アクセス コントロール ルールごとに設定した FirePOWER システム管理対象デバイスによって検出された接続の接続ロギングと比較してください。

接続イベントのタイプ

NetFlow データ収集はアクセス コントロール ルールではなくネットワークにリンクされているため、システムがログに記録する NetFlow 接続をきめ細かく制御することはできません。

NetFlow データは、セキュリティ インテリジェンス イベントを生成することはできません。

NetFlow ベースの接続イベントは、接続イベント データベースにのみ保存できます。システム ログまたは SNMP トラップ サーバに送信することはできません。

モニタ対象セッションごとに生成される接続イベントの数

管理対象デバイスによって直接検出された接続の場合は、アクセス コントロール ルールを設定して、接続の最初か最後またはその両方で双方向接続イベントをログに記録できます。

それに対し、エクスポートされた NetFlow レコードには単方向接続データが含まれているため、システムは処理する各 NetFlow レコードに対し少なくとも 2 つの接続イベントを生成します。これは、概要の接続数が NetFlow データに基づいた接続ごとに 2 ずつ増加することも意味しており、ネットワーク上で実際に発生している接続数が急増することになります。

接続がまだ実行中であっても、NetFlow エクスポータは固定間隔でレコードを出力するため、長時間実行しているセッションの場合は複数のエクスポートされたレコードが生成される場合があり、その各レコードが接続イベントを生成します。たとえば、NetFlow エクスポータが 5 分ごとにエクスポートする場合に、特定の接続が 12 分間続いている場合、システムはそのセッションに対し 6 つの接続イベントを生成します。

- 最初の 5 分間の 1 つのイベント ペア
- 次の 5 分間の 1 つのペア
- 接続が終了した時点の最後のペア

ホスト データとオペレーティング システム データ

NetFlow データからのネットワーク マップに追加されたホストには、オペレーティング システム、NetBIOS、またはホスト タイプ（ホストまたはネットワーク デバイス）の情報がありません。ただし、ホスト入力機能を使用してホストのオペレーティング システム ID を手動で設定できます。

アプリケーション データ

管理対象デバイスによって直接検出された接続の場合は、接続内のパケットを検査することによって、システムはアプリケーション プロトコル、クライアント、および Web アプリケーションを識別できます。

システムは NetFlow レコードを処理するときに、`/etc/sf/services` 内のポート関連付けを使用して、アプリケーション プロトコル ID を推測します。ただし、これらのアプリケーション プロトコルに関するベンダーまたはバージョン情報が存在しないため、接続ログにはセッションで使用されるクライアントまたは Web アプリケーションに関する情報が含まれません。しかし、ホスト入力機能を使用してこの情報を手動で提供できます。

単純なポート関連付けでは、非標準ポート上で動作しているアプリケーション プロトコルが特定されないまたは誤認される可能性があることに注意してください。加えて、関連付けが存在しない場合は、システムがそのアプリケーション プロトコルを接続ログで `unknown` としてマークします。

脆弱性マッピング

システムは、ホスト入力機能を使用してホストのオペレーティング システム ID またはアプリケーション プロトコル ID を手動で設定しない限り、NetFlow エクスポータによってモニタされるホストに脆弱性をマッピングできません。NetFlow 接続内にクライアント情報が存在しないため、クライアントの脆弱性を NetFlow データから作成されたホストに関連付けることはできないことに注意してください。

接続内の発信側情報と応答側情報

管理対象デバイスによって直接検出された接続の場合、システムは発信側または送信元のホストと応答側または宛先のホストを識別できます。ただし、NetFlow データには発信側または応答側の情報が含まれていません。

Firepower システムは、NetFlow レコードを処理するときに、それぞれのホストが使用しているポートとそれらのポートが既知かどうかに基づいて、この情報を判断するアルゴリズムを使用します。

- 使用されているポートの両方が既知のポートの場合、または、どちらも既知のポートでない場合、システムは番号の小さい方のポートを使用しているホストを応答側と見なします。
- どちらかのホストだけが既知のポートを使用している場合は、システムがそのホストを応答側と見なします。

したがって、既知のポートは、1 ～ 1023 の番号が割り当てられたポートまたは管理対象デバイス上の `/etc/sf/services` にアプリケーション プロトコル情報が保存されているポートです。

さらに、管理対象デバイスによって直接検出された接続の場合、システムは対応する接続イベントの 2 バイト数を記録します。

- [イニシエータ バイト数（Initiator Bytes）] フィールドは送信バイト数を記録します。
- [レスポンダ バイト数（Responder Bytes）] フィールドは受信バイト数を記録します。

単方向 NetFlow レコードに基づく接続イベントには、1 バイト数しか含まれておらず、ポートベース アルゴリズムに応じて、システムが [イニシエータ バイト数（Initiator Bytes）] または [レスポンダ バイト数（Responder Bytes）] に割り当てます。システムによって他のフィールドは 0 に設定されます。NetFlow レコードの接続の概要（集約接続データ）を表示している場合に、両方のフィールドに値が読み込まれる場合があることに注意してください。

NetFlow のみの接続イベント フィールド

いくつかのフィールドは、NetFlow レコードから生成された接続イベントでのみ表示されます（接続イベント フィールドで利用可能な情報, （1945 ページ）を参照）。

関連トピック

接続イベント フィールドで利用可能な情報, （1945 ページ）

ユーザ検出の基本

ネットワーク検出およびアイデンティティ ポリシーを使用してネットワーク上のユーザ アクティビティをモニタできます。これにより、脅威、エンドポイント、およびネットワーク インテリジェンスをユーザ アイデンティティ情報に関連付けることができます。ネットワーク動作、トラフィック、およびイベントを個別のユーザに直接リンクすることによって、ポリシー違反、攻撃、またはネットワークの脆弱性の発生源の特定に役立てることができます。たとえば、以下について決定できます。

- 脆弱（レベル 1：赤）影響レベルの侵入イベントの対象になっているホストの所有者
- 内部攻撃またはポートスキャンを開始した人物
- 重要なホストへの不正アクセスを試みている人物
- 不合理な容量の帯域幅を使用している人物
- 重要なオペレーティング システム更新を適用しなかった人物
- 会社の IT ポリシーに違反してインスタント メッセージング ソフトウェアまたはピアツーピア ファイル共有アプリケーションを使用している人物

この情報を入手すれば、Firepower システムの他の機能を使用して、リスクを低減し、アクセス制御を実行し、他のユーザを破壊行為から保護するためのアクションを実行できます。これらの機能により、監査制御が大幅に改善され、規制の順守が促進されます。

ユーザ アイデンティティ ソースを設定してユーザ データを収集すると、ユーザ認識とユーザ制御を実行できます。

ユーザ認識

ユーザ データを表示および分析するための機能。詳細については、ディスカバリおよびアイデンティティ ワークフローの使用，（2097 ページ）を参照してください。

ユーザ制御

ユーザ認識から得られた結論に基づいて、ネットワーク上のトラフィックでユーザまたはユーザ アクティビティをモニタ、信頼、ブロック、または許可するようにユーザ制御ルール条件を設定するための機能。詳細については、ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御），（363 ページ）を参照してください。

（アイデンティティ ポリシーで設定される）権限のあるアイデンティティ ソースおよび（ネットワーク検出ポリシーで設定される）権限のないアイデンティティ ソースからユーザ データを取得できます。

権限のあるアイデンティティ ソース

ユーザ ログインの検証を行った信頼できるサーバ。権限のあるログインから取得したデータを使用すると、ユーザ認識とユーザ制御を実行できます。権限のあるユーザ ログインは、パッシブ認証とアクティブ認証から得られます。

- パッシブ認証は、ユーザが外部サーバ経由で認証されるときに発生します。ユーザ エージェントおよび ISE は、Firepower システムでサポートされるパッシブ認証方式です。
- アクティブ認証は、ユーザが事前設定済みの管理対象デバイス経由で認証されるときに発生します。Firepower システムでサポートされているアクティブ認証方式は、キャプティブ ポータルだけです。

権限のないアイデンティティ ソース

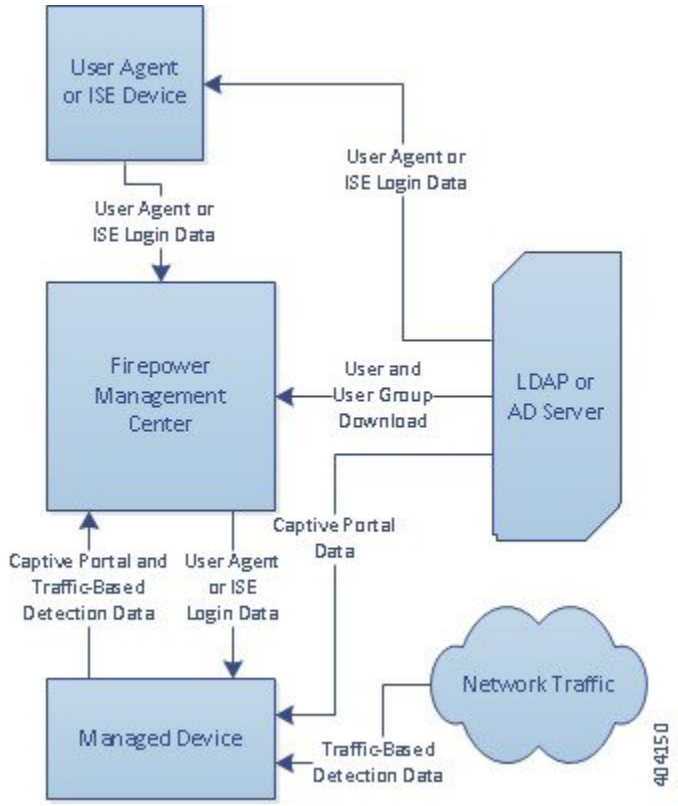
ユーザ ログインの検証を行った不明または信頼できないサーバ。トラフィック ベースの検出は、Firepower システムでサポートされている唯一の権限のないアイデンティティ ソースです。権限のないログインから取得されたデータを使用すると、ユーザ認識を実行できます。

詳細については、ユーザ アイデンティティ ソースについて, （1531 ページ）を参照してください。

ユーザ検出またはユーザ アイデンティティの展開

システムがユーザ ログイン、またはアイデンティティ ソースからのユーザ データを検出すると、そのログインからのユーザは、Firepower Management Center ユーザ データベース内のユーザのリストに照らしてチェックされます。ログイン ユーザが既存のユーザと一致した場合は、ログインからのデータがそのユーザに割り当てられます。ログインが SMTP トラフィック内に存在しない場合は、既存のユーザと一致しないログインによって新しいユーザが作成されます。SMTP トラフィック内の一致しないログインは破棄されます。

次の図は、Firepower システムがユーザ データをどのように収集して保存するかを示しています。



ユーザ アクティビティ データベース

Firepower Management Center のユーザ アクティビティ データベースには、設定されたすべてのアイデンティティ ソースによって検出または報告されたネットワーク上のユーザアクティビティのレコードが含まれています。システムがイベントを記録するのは以下のような状況です。

- 個別のログインまたはログオフを検出したとき。
- 新しいユーザを検出したとき。
- システム管理者が手動でユーザを削除したとき。
- データベース内に存在しないユーザをシステムが検出したものの、ユーザ数の制限に達したためにそのユーザを追加できなかったとき。

システムで検出されたユーザ アクティビティは、Firepower Management Center Web インターフェイスを使用して表示できます。（[分析（Analysis）]>[ユーザ（Users）]>[ユーザ アクティビティ（User Activity）]）。

ユーザ データベース

Firepower Management Center のユーザ データベースには、設定されたすべてのアイデンティティ ソースによって検出または報告されたユーザごとのレコードが含まれています。権限のあるソースから取得したデータをユーザ制御に使用できます。

サポートされている権限のないアイデンティティ ソースと権限のあるアイデンティティ ソースの詳細については、ユーザ アイデンティティ ソースについて, （1531 ページ） を参照してください。

Firepower システムのユーザの制限, （1450 ページ） で説明されているように、Firepower Management Center で保存できるユーザの合計数は、Firepower Management Center のモデルごとに異なります。ユーザ制限に達した後、システムは、アイデンティティ ソースに基づいて未検出ユーザ データを次のように優先順位付けします。

- 新しいユーザが権限のないアイデンティティ ソースからである場合、ユーザはデータベースに追加されません。新規ユーザを追加できるようにするには、手動またはデータベースの消去によってユーザを削除する必要があります。
- 新しいユーザが権限のあるアイデンティティ ソースからである場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザを削除し、データベースに新しいユーザを追加します。

アイデンティティ ソースが特定のユーザ名を除外するように設定されている場合、それらのユーザ名のユーザ アクティビティ データは Firepower Management Center に報告されません。これらの除外されたユーザ名はデータベースに残りますが、IP アドレスに関連付けられません。システムによって保存されるデータのタイプの詳細については、ユーザ データ（User Data）, （2149 ページ） を参照してください。

システムが新しいユーザ セッションを検出すると、そのユーザ セッションのデータは、次のいずれかが発生するまでユーザ データベースに残ります。

- Firepower Management Center のユーザが手動でユーザ セッションを削除した。
- アイデンティティ ソースがそのユーザ セッションのログオフを報告した。
- レルムがレルムの [ユーザ セッションのタイムアウト：認証されたユーザ（User Session Timeout: Authenticated Users）] 設定、[ユーザ セッションのタイムアウト：認証に失敗したユーザ（User Session Timeout: Failed Authentication Users）] 設定、または [ユーザ セッションのタイムアウト：ゲスト ユーザ（User Session Timeout: Guest Users）] 設定で指定されているユーザ セッションを終了した。

Firepower システムのホストとユーザの制限

Firepower Management Center モデルにより、展開でモニタできる個別のホストの数、モニタし、ユーザ制御を実行するために使用できるユーザの数が決定されます。

関連トピック

Management Center データベースからのデータの消去, （219 ページ）

Firepower システムのホスト制限

システムは（ネットワーク検出ポリシーで定義されている）モニタ対象ネットワークでIPアドレスに関連付けられたアクティビティを検出すると、ネットワーク マップにホストを追加します。Firepower Management Center がモニタでき、ネットワーク マップに保存できるホストの数。モデルによって異なります。

表 *190*：*Firepower Management Center* モデル別のホスト制限

Management Center モデル	ホスト
MC750	2,000
MC1500	50,000
FS2000	150,000
MC3500	300,000
MC4000	600,000
仮想	50,000

ネットワークマップに存在しないホストのコンテキストデータは表示できません。ただし、アクセス制御は実行できます。たとえば、コンプライアンス ホワイトリストを使用してホストのネットワーク コンプライアンスをモニタできない場合でも、ネットワークマップに存在しないホストとの間のトラフィックでアプリケーション制御を実行できます。

（注） システムでは、IPアドレスとMACアドレスの両方によって識別されるホストとは別に、MAC専用ホストがカウントされます。1つのホストに関連付けられているすべてのIPアドレスは、まとめて 1 つのホストとしてカウントされます。

ホスト制限への到達とホストの削除

ホスト制限に到達した後に新しいホストを検出すると、ネットワーク検出ポリシーが制御を行います。新しいホストをドロップするか、または非アクティブになっている期間が最も長いホストを置換することができます。また、システムが非アクティブであるためネットワークからホストを削除するまでの期間を設定できます。ホスト、サブネット全体、またはすべてのホストをネットワーク マップから手動で削除できますが、システムは、削除されたホストに関連付けられたアクティビティを検出した場合は、ホストを再追加します。

マルチドメイン展開では、各リーフ ドメインに自身のネットワーク検出ポリシーがあります。したがって、各リーフ ドメインによって、システムが新しいホストを検出したときの独自の動作が決定されます。

関連トピック

ドメインのプロパティ, （312 ページ）
ネットワーク検出のデータ ストレージ設定, （1572 ページ）

Firepower システムのユーザの制限

Firepower Management Center モデルにより、モニタできる個々のユーザ数が決まります。システムが新しいユーザのアクティビティを検出すると、そのユーザは Firepower Management Center の Users データベースに追加されます。任意のアイデンティティ ソースを使用して、ユーザを検出できます。

検討するユーザ制限には 2 つのタイプがあります。

- 権限のあるユーザ数の制限。データベースに保存でき、アクセス制御に使用できる、アクセス制御されたユーザの数です。権限のあるユーザ データは、ユーザ エージェント、ISE、TS エージェント、およびキャプティブ ポータルによって収集されます。
- ユーザ総数の制限。データベースに保存できる、権限のあるユーザと権限のないユーザの数です。この制限には、すべての権限のあるユーザ データとトラフィック ベースの検出を使用して収集された権限のないユーザ データが含まれます。

表 *191*：*Firepower Management Center* モデル別のユーザ制限

Management Center モデル	権限のあるユーザ	ユーザ総数
MC750	2,000	2,000
MC1500	50,000	50,000
FS2000	64,000	150,000
MC3500	64,000	300,000
MC4000	64,000	600,000
仮想	50,000	50,000

制限に達してから、新しい、以前検出されなかったユーザをシステムが検出すると、アイデンティティ ソースに基づいてユーザ データに優先順位が付けられます。

- 新しいユーザが権限のないアイデンティティ ソースからである場合、ユーザはデータベースに追加されません。新規ユーザを追加できるようにするには、手動またはデータベースの消去によってユーザを削除する必要があります。
- 新しいユーザが権限のあるアイデンティティ ソースからである場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザを削除し、データベースに新しいユーザを追加します。

（注） 展開に ASDM によって管理される ASA FirePOWER モジュールが含まれる場合、Firepower Management Center モデルに関係なく、最大 2,000 の権限のあるユーザを保存できます。

ヒント トラフィック ベースの検出を使用している場合、プロトコルによるユーザ ロギングを制限すると、ユーザ名の散乱を最小限に抑え、データベースのスペースを残しておくことができます。たとえば、システムが AIM、POP3、および IMAP トラフィックで検出されたユーザを追加できないようにすることができます（モニタを望んでいない特定の契約業者または訪問者からのトラフィックであることがわかっているため）。

第 64 章

ホスト ID ソース

次のトピックでは、ホスト ID ソースについて説明します。

概要：ホストのデータ収集

Firepower システムはネットワークを通過するトラフィックを受動的に監視するため、ネットワーク トラフィックからの特定のパケット ヘッダー値とその他の固有データを設定された定義と比較して（フィンガープリントと呼ばれる）、ネットワーク上のホストに関する次の情報を判断します。

- ホストの台数と種類（ブリッジ、ルータ、ロードバランサ、NAT デバイスなどのネットワーク デバイスを含む）
- ネットワーク上の検出ポイントからホストまでのホップ数を含む、基本的なネットワーク トポロジ データ
- ホスト上で実行中のオペレーティング システム
- ホスト上のアプリケーションとそのアプリケーションに関連付けられているユーザ

システムがホストのオペレーティング システムを特定できない場合、カスタムのクライアントまたはサーバのフィンガープリントを作成できます。システムはこれらのフィンガープリントを使用して新しいホストを特定します。フィンガープリントを脆弱性データベース（VDB）内のシス

テムにマップすることにより、カスタム フィンガープリントを使用してホストが特定されるたびに適切な脆弱性情報を表示できます。

（注） システムはモニタ対象のネットワーク トラフィックからだけでなく、エクスポートされた NetFlow レコードからもホスト データを収集することができ、また Nmap スキャンやホスト入力機能を使用してアクティブにホスト データを追加することもできます。

システムが検出できるホスト オペレーティング システムの判別

システムがどのオペレーティング システムのフィンガープリントを作成できるかを確認するには、カスタム OS フィンガープリントの作成プロセス中に表示される、使用可能なフィンガープリントの一覧を表示します。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 [カスタム フィンガープリントの作成（Create Custom Fingerprint）] をクリックします。

ステップ 4 [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションにあるドロップダウン リスト内のオプションのリストを表示します。これらのオプションが、システムがフィンガープリントを作成できるオペレーティング システムになります。

次の作業

必要に応じて、ホスト オペレーティング システムの識別, （1454 ページ）を参照してください。

ホスト オペレーティング システムの識別

システムがホストのオペレーティング システムを正しく識別しない場合（たとえばホスト プロファイル「不明」を示したり間違って識別したりする場合）には、下記の方法を試してください。

手順

次のいずれかの方法を試します。

- ネットワーク検出アイデンティティ競合設定を確認します。
- ホストのカスタム フィンガープリントを作成します。
- ホストに対して Nmap スキャンを実行します。
- ホスト入力機能を使用して、ネットワーク マップにデータをインポートします。

- オペレーティング システム情報を手動で入力します。

カスタムフィンガープリント

Firepowerシステムには、検出された各ホストのオペレーティング システムを識別するためにシステムが使用するオペレーティング システムのフィンガープリントが含まれます。しかし、オペレーティング システムに一致するフィンガープリントがないため、システムがホスト オペレーティング システムを識別できない、または誤って識別することがあります。この問題を解決するために、不明または誤認されたオペレーティングシステムに固有のオペレーティングシステム特性のパターンを提供するカスタムフィンガープリントを作成し、識別用のオペレーティングシステムの名前を提供することができます。

システムはオペレーティング システムのフィンガープリントから各ホストの脆弱性リストを取得するため、システムがホストのオペレーティング システムを照合できない場合、ホストの脆弱性を識別することはできません。たとえば、システムがMicrosoft Windowsを実行中のホストを検出した場合、そのシステムには保存されたMicrosoft Windowsの脆弱性リストが存在します。このリストは、検出したWindowsオペレーティング システムに基づいて、そのホストのホストプロファイルに追加されます。

たとえば、ネットワーク上にMicrosoft Windowsの新しいベータ バージョンを実行中の複数のデバイスがある場合、システムはそのオペレーティング システムを識別できず、脆弱性をそれらのホストにマッピングすることもできません。しかし、システムにMicrosoft Windowsに関する脆弱性のリストがあるならば、同じオペレーティング システムを実行中の他のホストを識別できるように、いずれか1台のホストに対してカスタム フィンガープリントを作成できます。フィンガープリントにMicrosoft Windowsの脆弱性リストのマッピングを含め、フィンガープリントに一致する各ホストとそのリストを関連付けることができます。

カスタム フィンガープリントを作成するとFirepower Management Centerは、同じオペレーティング システムを実行中のすべてのホストに関するそのフィンガープリントに関連付けられた脆弱性のセットをリストします。ユーザが作成したカスタム フィンガープリントに脆弱性マッピングが1つも存在しない場合、システムはフィンガープリントを使用して、フィンガープリントで提供するカスタムオペレーティングシステムの情報を割り当てます。以前に検出されたホストからの新しいトラフィックが確認されると、システムはそのホストを新しいフィンガープリント情報で更新します。さらに、そのオペレーティング システムを実行する新しいホストの最初の検出時に、新しいフィンガープリントを使用して識別します。

カスタム フィンガープリントを作成する前に、ホストが正しく識別されない理由を特定して、カスタム フィンガープリントが実行可能なソリューションであるかどうかを判断する必要があります。

以下の2種類のフィンガープリントを作成できます。

- クライアントのフィンガープリント。ネットワーク上の別のホストで実行中のTCPアプリケーションに接続されている場合、ホストが送信するSYNパケットに基づいてオペレーティング システムを識別します。

- サーバのフィンガープリント。実行中のTCPアプリケーションへの着信接続に応答するためにホストが使用するSYN-ACKパケットに基づいてオペレーティング システムを識別します。

（注） クライアントとサーバの両方のフィンガープリントが同じホストに一致する場合、クライアントのフィンガープリントが使用されます。

フィンガープリントを作成した後、システムがフィンガープリントをホストに関連付けるには、その前に、フィンガープリントを有効化する必要があります。

関連トピック

クライアント用のカスタム フィンガープリントの作成, （1460 ページ）
サーバ用のカスタム フィンガープリントの作成, （1463 ページ）

フィンガープリントの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

フィンガープリントを作成してアクティブにした後、フィンガープリントを編集して変更を加えたり、脆弱性マッピングを追加したりできます。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム オペレーティング システム（Custom Operating Systems）] をクリックします。システムがフィンガープリントを作成するデータを待機している場合、フィンガープリントが作成されるまで 10 秒ごとに自動的に更新されます。

ステップ 3 カスタムのフィンガープリントを管理します。

- アクティブ化/非アクティブ化：フィンガープリントをアクティブ化または非アクティブ化します。詳細については、フィンガープリントのアクティブおよび非アクティブの設定, （1457 ページ）を参照してください。
- 作成：フィンガープリントを作成します。詳細については、クライアント用のカスタム フィンガープリントの作成, （1460 ページ）およびサーバ用のカスタム フィンガープリントの作成, （1463 ページ）を参照してください。

- 編集：フィンガープリントを編集します。詳細については、アクティブなフィンガープリントの編集，（1458ページ）および非アクティブなフィンガープリントの編集，（1459ページ）を参照してください。
- 削除：削除するフィンガープリントの横にある削除アイコン（）をクリックして、確認のために [OK] をクリックします。削除できるのは、非アクティブ化したフィンガープリントのみです。

フィンガープリントのアクティブおよび非アクティブの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

ホストを識別するためにシステムがカスタム フィンガープリントを使用できるようにするには、その前に、カスタム フィンガープリントをアクティブにする必要があります。新しいフィンガープリントがアクティブにされた後は、以前に検出したホストを再識別し、新しいホストを検出するために使用されます。

フィンガープリントの使用を停止する場合は、それを非アクティブにすることができます。フィンガープリントを非アクティブにすると、フィンガープリントは使用できなくなりますが、システム上で維持できます。フィンガープリントを非アクティブにすると、オペレーティング システムは、フィンガープリントを使用しているホストに対して不明としてマークされます。ホストが再度検出され、別のアクティブなフィンガープリントに一致すると、ホストはそのアクティブなフィンガープリントによって識別されます。

フィンガープリントを削除すると、システムから完全に削除されます。フィンガープリントを非アクティブにした後に削除できます。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 アクティブまたは非アクティブにするフィンガープリントの横にあるスライダをクリックします。

（注） アクティブ化オプションは、作成したフィンガープリントが有効である場合に限り使用できます。スライダが使用できない場合、フィンガープリントを再作成してください。

アクティブなフィンガープリントの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

フィンガープリントがアクティブである場合、フィンガープリントの名前、説明、オペレーティング システムのカスタム表示の変更、および追加の脆弱性のフィンガープリントへのマッピングを行えます。

フィンガープリントの名前、説明、オペレーティング システムのカスタム表示の変更、および追加の脆弱性のフィンガープリントへのマッピングを行えます。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム オペレーティング システム（Custom Operating Systems）] をクリックします。

ステップ 3 編集するフィンガープリントの横にある編集アイコン（）をクリックします。

ステップ 4 必要に応じて、フィンガープリントの名前、説明、およびカスタム OS 表示を変更します。

ステップ 5 脆弱性マッピングを削除する場合は、ページの [事前定義された OS 製品マップ（Pre-Defined OS Product Maps）] セクションのマッピングの横にある [削除（Delete）] をクリックします。

ステップ 6 脆弱性マッピングにその他のオペレーティング システムを追加する場合は、[製品（Product）] を選択し（該当する場合は [メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[リビジョン バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、および [拡張（Extension）] も選択します）、[OS 定義の追加（Add OS Definition）] をクリックします。
脆弱性マッピングが、[事前定義された OS 製品マップ（Pre-Defined OS Product Maps）] リストに追加されます。

ステップ 7 [保存（Save）] をクリックします。

非アクティブなフィンガープリントの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

フィンガープリントが非アクティブである場合は、フィンガープリントのすべての要素を変更し、それらを Firepower Management Center に再送信できます。これには、フィンガープリントのタイプ、ターゲットの IP アドレスとポート、脆弱性マッピングなど、フィンガープリントの作成時に指定したすべてのプロパティが含まれます。非アクティブのフィンガープリントを編集および送信すると、システムに再送信されます。また、それがクライアントのフィンガープリントである場合、アクティブにする前に、アプライアンスにトラフィックを再送信する必要があります。非アクティブのフィンガープリントに対して選択できる脆弱性マッピングは 1 つだけであることに注意してください。フィンガープリントをアクティブにした後、追加のオペレーティング システムおよびバージョンを脆弱性リストにマッピングすることができます。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム オペレーティング システム（Custom Operating Systems）] をクリックします。

ステップ 3 編集するフィンガープリントの横にある編集アイコン（  ）をクリックします。

ステップ 4 必要に応じてフィンガープリントを変更します。

- クライアントのフィンガープリントを変更している場合は、クライアント用のカスタム フィンガープリントの作成, （1460 ページ）を参照してください。
- サーバのフィンガープリントを変更している場合は、サーバ用のカスタム フィンガープリントの作成, （1463 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

次の作業

- クライアントのフィンガープリントを変更した場合は、ホストからフィンガープリントを収集しているアプライアンスにトラフィックを必ず送信してください。

クライアント用のカスタム フィンガープリントの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

クライアントのフィンガープリントは、クライアントがネットワーク上の別のホストで実行するTCP アプリケーションに接続されている場合、ホストが送信する SYN パケットに基づいてオペレーティング システムを識別します。

Firepower Management Center が監視対象ホストと直接通信することがない場合は、クライアントのフィンガープリントのプロパティを指定するときに、Management Center によって管理され、フィンガープリントを作成するホストに最も近いデバイスを指定することができます。

フィンガープリント作成プロセスを開始する前に、フィンガープリントを作成するホストに関する次の情報を取得します。

- ホストとフィンガープリントを取得するために使用する Firepower Management Center またはデバイスの間のネットワーク ホップの数。（Cisco では、ホストが接続されている同じサブネットに Firepower Management Center またはデバイスを直接接続することを強く推奨します）。
- ホストが存在するネットワークに接続されているネットワーク インターフェイス（Firepower Management Center またはデバイス上）。
- ホストの実際のオペレーティング システム ベンダー、製品、バージョン。
- クライアント トラフィックを生成するためのホストへのアクセス。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 [カスタム フィンガープリントの作成（Create Custom Fingerprint）] をクリックします。

ステップ 4 [デバイス（Device）] ドロップダウンリストから、フィンガープリントを収集するために使用する Firepower Management Center またはデバイスを選択します。

ステップ 5 [フィンガープリント名（Fingerprint Name）] を入力します。

ステップ 6 [フィンガープリントの説明（Fingerprint Description）] を入力します。

ステップ 7 [フィンガープリント タイプ（Fingerprint Type）] リストから、[クライアント（Client）] を選択します。

ステップ 8 [ターゲット IP アドレス（Target IP Address）] フィールドで、フィンガープリントを作成するホストの IP アドレスを入力します。
フィンガープリントは、ホストに他の IP アドレスが存在していても、ユーザが指定したホスト IP アドレスから送受信されるトラフィックにのみ基づくことに注意してください。

ステップ 9 [ターゲット距離（Target Distance）] フィールドで、前の手順で選択したフィンガープリントを収集するデバイスとホストの間のネットワーク ホップ数を入力します。

注意 これは、ホストへの実際の物理ネットワーク ホップ数である必要があります。システムによって検出されるホップ数と同じになる場合も、同じにならない場合もあります。

ステップ 10 [インターフェイス（Interface）] リストから、ホストが存在するネットワーク セグメントに接続されているネットワーク インターフェイスを選択します。

注意 Cisco では、いくつかの理由でフィンガープリントの作成に管理対象デバイスのセンシング インターフェイスを使用**しない**ことを推奨します。まず、フィンガープリントは、センシング インターフェイスが SPAN ポート上にあると機能しません。また、デバイスでセンシング インターフェイスを使用する場合、デバイスはフィンガープリントを収集している間、ネットワークの監視を停止します。ただし、フィンガープリントの収集を実行するために、管理インターフェイスまたはその他の使用可能なネットワーク インターフェイスを使用できます。どのインターフェイスがデバイスのセンシング インターフェイスであるかがわからない場合は、フィンガープリントの作成に使用している特定のモデルのインストレーション ガイドを参照してください。

ステップ 11 フィンガープリントを作成したホストのホスト プロファイルのカスタム情報を表示する場合（またはフィンガープリントを作成するホストが [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションに存在しない場合）、[カスタム OS 表示の使用（Use Custom OS Display）] を選択して、次に示すように表示する値を指定します。

- [ベンダー文字列（Vendor String）] フィールドに、オペレーティング システムのベンダー名を入力します。たとえば、Microsoft Windows のベンダーは「Microsoft」になります。
- [製品文字列（Product String）] フィールドに、オペレーティング システムの製品名を入力します。たとえば、Microsoft Windows 2000 の製品名は「Windows」になります。
- [バージョン文字列（Version String）] フィールドに、オペレーティング システムのバージョン番号を入力します。たとえば、Microsoft Windows 2000 のバージョン番号は「2000」になります。

ステップ 12 [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションで、脆弱性マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します。

フィンガープリントを使用して一致するホストの脆弱性を識別する場合、またはオペレーティング システムのカスタム表示情報を割り当てない場合、このセクションで [ベンダー（Vendor）] と [製品（Product）] の値名を指定する必要があります。

オペレーティング システムのすべてのバージョンの脆弱性をマッピングするには、[ベンダー（Vendor）] および [製品（Product）] の値のみを指定します。

（注） [メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[リビジョン バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、および [拡張（Extension）] ドロップダウンリストのオプションの中には、選択したオペレーティング システムに該当しないものもあります。また、フィンガープリントを作成するオペレーティング システムに一致するリストに表示される定義がない場合は、それらの値を空のままにすることができます。フィンガープリントで OS の脆弱性マッピングを作成しない場合、システムはそのフィンガープリントを使用して、脆弱性リストをフィンガープリントによって識別されるホストに割り当てることはできないことに注意してください。

例：
たとえば、カスタム フィンガープリントで Redhat Linux 9 の脆弱性リストを一致するホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、メジャー バージョンとして [9] を選択します。

例：
Palm OS のすべてのバージョンを追加するには、[ベンダー（Vendor）] リストから [PalmSource, Inc.]、[製品（Product）] リストから [Palm OS] を選択し、その他のすべてのリストはデフォルトの設定のままにします。

ステップ 13 [作成（Create）] をクリックします。
ステータスは一時的に [新規（New）] になってから、[保留中（Pending）] に切り替わります。フィンガープリントのトラフィックが確認されるまで、このステータスが維持されます。トラフィックが確認されると、[使用可（Ready）] に切り替わります。

当該のホストからデータを受信するまで、[カスタム フィンガープリント（Custom Fingerprint）] ステータス ページは 10 秒ごとに更新されます。

ステップ 14 ターゲット IP アドレスとして指定した IP アドレスを使用して、フィンガープリントを作成しようとしているホストにアクセスし、アプライアンスへの TCP 接続を開始します。
正確なフィンガープリントを作成するためには、トラフィックがフィンガープリントを収集するアプライアンスで認識される**必要**があります。スイッチを経由して接続している場合は、アプライアンス以外のシステムへのトラフィックはシステムによって認識されない場合があります。

例：
フィンガープリントを作成しようとしているホストから Firepower Management Center の Web インターフェイスにアクセスするか、ホストから SSH で Management Center にアクセスします。SSH を使用する場合は、次に示すコマンドを使用します。このコマンドの localIPv6address は、現在ホストに割り当てられているステップ 7 で指定した IPv6 アドレスです。DCmanagementIPv6address

は、Management Center の管理 IPv6 アドレスです。[カスタム フィンガープリント（Custom Fingerprint）] ページが [使用可（Ready）] ステータスでリロードされるようになります。

```
ssh -b localIPv6address DCmanagementIPv6address
```

次の作業

- フィンガープリントのアクティブおよび非アクティブの設定, （1457 ページ） で説明するように、フィンガープリントをアクティブにします。

サーバ用のカスタム フィンガープリントの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

サーバのフィンガープリントは、実行中の TCP アプリケーションへの着信接続に応答するためにホストが使用する SYN-ACK パケットに基づいてオペレーティング システムを識別します。開始する前に、フィンガープリントを作成するホストに関する次の情報を取得します。

- ホストとフィンガープリントを取得するために使用するアプライアンスの間のネットワークホップの数。Cisco では、ホストが接続されている同じサブネットにアプライアンスの使用されていないインターフェイスを直接接続することを強く推奨します。
- ホストが存在するネットワークに接続されているネットワーク インターフェイス（アプライアンス上）。
- ホストの実際のオペレーティング システム ベンダー、製品、バージョン。
- 現在未使用の、ホストが存在するネットワーク上で許可されている IP アドレス。

ヒント Firepower Management Center が監視対象ホストと直接通信することがない場合は、サーバのフィンガープリントのプロパティを指定するときに、フィンガープリントを作成するホストに最も近い管理対象デバイスを指定することができます。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 [カスタム フィンガープリントの作成（Create Custom Fingerprint）] をクリックします。

ステップ 4 [デバイス（Device）] リストから、フィンガープリントを収集するために使用する Firepower Management Center または管理対象デバイスを選択します。

ステップ 5 [フィンガープリント名（Fingerprint Name）] を入力します。

ステップ 6 [フィンガープリントの説明（Fingerprint Description）] を入力します。

ステップ 7 [フィンガープリント タイプ（Fingerprint Type）] リストから、サーバのフィンガープリント作成オプションを表示する [サーバ（Server）] を選択します。

ステップ 8 [ターゲット IP アドレス（Target IP Address）] フィールドで、フィンガープリントを作成するホストの IP アドレスを入力します。
フィンガープリントは、ホストに他の IP アドレスが存在していても、ユーザが指定したホスト IP アドレスから送受信されるトラフィックにのみ基づくことに注意してください。

注意 Firepower システムのバージョン 5.2 以降を実行するアプライアンスでのみ IPv6 フィンガープリントをキャプチャできます。

ステップ 9 [ターゲット距離（Target Distance）] フィールドで、前の手順で選択したフィンガープリントを収集するデバイスとホストの間のネットワーク ホップ数を入力します。

注意 これは、ホストへの実際の物理ネットワーク ホップ数である必要があります。システムによって検出されるホップ数と同じになる場合も、同じにならない場合もあります。

ステップ 10 [インターフェイス（Interface）] リストから、ホストが存在するネットワーク セグメントに接続されているネットワーク インターフェイスを選択します。

注意 Cisco では、いくつかの理由でフィンガープリントの作成に管理対象デバイスのセンシング インターフェイスを使用**しない**ことを推奨します。まず、フィンガープリントは、センシング インターフェイスが SPAN ポート上にあると機能しません。また、デバイスでセンシング インターフェイスを使用する場合、デバイスはフィンガープリントを収集している間、ネットワークの監視を停止します。ただし、フィンガープリントの収集を実行するために、管理インターフェイスまたはその他の使用可能なネットワーク インターフェイスを使用できます。どのインターフェイスがデバイスのセンシング インターフェイスであるかがわからない場合は、フィンガープリントの作成に使用している特定のモデルのインストレーション ガイドを参照してください。

ステップ 11 [アクティブ ポートの取得（Get Active Ports）] をクリックします。

ステップ 12 [サーバ ポート（Server Port）] フィールドに、フィンガープリントを収集するように選択したデバイスが通信を開始するポートを入力します。または、[アクティブ ポートの取得（Get Active Ports）] ドロップダウンリストからポートを選択します。
ホストでオープンしていると判明しているすべてのサーバ ポートを使用できます（たとえば、ホストで Web サーバを実行している場合は 80）。

ステップ 13 [送信元 IP アドレス（Source IP Address）] フィールドで、ホストとの通信を試行するために使用する IP アドレスを入力します。
ネットワークでの使用が許可されていて、現在未使用の送信元 IP アドレス（たとえば、現在使用されていない DHCP プール アドレス）を使用する必要があります。これにより、フィンガープリントの作成中に、別のホストを一時的にオフラインにすることを防ぎます。

フィンガープリントを作成している間は、そのIPアドレスをネットワーク検出ポリシーでモニタリングから除外する必要があります。そうしていないと、ネットワーク マップおよびディスカバリ イベント ビューに、その IP アドレスによって表されるホストに関する不正確な情報が混在することになります。

ステップ 14 [送信元サブネット マスク（Source Subnet Mask）] フィールドには、ユーザが使用している IP アドレスのサブネット マスクを入力します。

ステップ 15 [送信元ゲートウェイ（Source Gateway）] フィールドが表示されたら、ホストへのルートを確立するために使用するデフォルトのゲートウェイ IP アドレスを入力します。

ステップ 16 フィンガープリントを作成したホストのホスト プロファイルのカスタム情報を表示する場合、または使用するフィンガープリントの名前が [OS 定義（OS Definition）] セクションに存在しない場合、[カスタム OS 表示（Custom OS Display）] セクションの [カスタム OS 表示の使用（Use Custom OS Display）] を選択します。
以下のように、ホスト プロファイルで表示する値を入力します。

- [ベンダー文字列（Vendor String）] フィールドに、オペレーティング システムのベンダー名を入力します。たとえば、Microsoft Windows のベンダーは「Microsoft」になります。
- [製品文字列（Product String）] フィールドに、オペレーティング システムの製品名を入力します。たとえば、Microsoft Windows 2000 の製品名は「Windows」になります。
- [バージョン文字列（Version String）] フィールドに、オペレーティング システムのバージョン番号を入力します。たとえば、Microsoft Windows 2000 のバージョン番号は「2000」になります。

ステップ 17 [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションで、脆弱性マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します。
フィンガープリントを使用して一致するホストの脆弱性を識別する場合、またはオペレーティング システムのカスタム表示情報を割り当てない場合、このセクションでベンダーと製品名を指定する必要があります。

オペレーティング システムのすべてのバージョンの脆弱性をマッピングするには、ベンダーおよび製品名のみを指定します。

（注） [メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[リビジョン バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、および [拡張（Extension）] ドロップダウンリストのオプションの中には、選択したオペレーティング システムに該当しないものもあります。また、フィンガープリントを作成するオペレーティング システムに一致するリストに表示される定義がない場合は、それらの値を空のままにすることができます。フィンガープリントで OS の脆弱性マッピングを作成しない場合、システムはそのフィンガープリントを使用して、脆弱性リストをフィンガープリントによって識別されるホストに割り当てることはできないことに注意してください。

例：

カスタム フィンガープリントで Redhat Linux 9 の脆弱性リストを一致するホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

例：
Palm OS のすべてのバージョンを追加するには、[ベンダー（Vendor）] リストから [PalmSource, Inc.]、[製品（Product）] リストから [Palm OS] を選択し、その他のすべてのリストはデフォルトの設定のままにします。

ステップ 18 [作成（Create）] をクリックします。
[カスタム フィンガープリント（Custom Fingerprint）] ステータス ページは 10 秒ごとに更新され、[使用可（Ready）] ステータスでリロードされます。

（注） ターゲット システムがフィンガープリント作成プロセス中に応答を停止した場合、ステータスにはメッセージ「エラー：応答がありません（ERROR: No Response）」が示されます。このメッセージが表示された場合は、フィンガープリントを再度送信します。3 ～ 5 分間（時間はターゲット システムによって異なる場合があります）待機して、編集アイコン（  ）をクリックし、[カスタム フィンガープリント（Custom Fingerprint）] ページにアクセスしてから [作成（Create）] をクリックします。

次の作業

- フィンガープリントのアクティブおよび非アクティブの設定, （1457 ページ） で説明するように、フィンガープリントをアクティブにします。

ホスト入力データ

サードパーティからネットワーク マップ データをインポートすることで、ネットワーク マップを増強することができます。また、Web インターフェイスを使用して、オペレーティング システムまたはアプリケーションの ID を変更するか、アプリケーション プロトコル、プロトコル、ホスト属性、クライアントを削除することによって、ホスト入力機能を使用することができます。

システムは複数のソースからのデータを照合して、オペレーティング システムまたはアプリケーションの現行 ID を判別できます。

ネットワーク マップから影響を受けるホストを削除すると、サードパーティの脆弱性を除くすべてのデータは破棄されます。スクリプトまたはインポート ファイルの設定方法の詳細については、『*Firepower System Host Input API Guide*』を参照してください。

影響の関連付けにインポートしたデータを含めるには、データベースのオペレーティング システムおよびアプリケーション定義にデータをマッピングする必要があります。

サードパーティのデータを使用するための要件

ネットワーク上のサードパーティのシステムから検出データをインポートできます。ただし、Firepower の推奨、アダプティブ プロファイル、影響評価などの侵入データおよび検出データを共

に使用する機能を有効にするには、対応する定義に対して、可能な限り多くのエレメントをマッピングする必要があります。サードパーティのデータを使用するには、以下の要件を考慮してください：

- サードパーティのシステムにネットワーク アセット上に特定のデータがある場合、ホスト入力機能によりそのデータをインポートできます。しかし、サードパーティが異なる製品名をつける可能性があることから、対応する Cisco 製品の定義に対して、サードパーティ ベンダー、製品、バージョンをマッピングする必要があります。製品をマッピング後、Firepower Management Center 設定の影響を評価するために脆弱性のマッピングを有効にして、影響相関を可能にします。バージョンまたはベンダーに関係のないアプリケーション プロトコルでは、Firepower Management Center 設定におけるアプリケーション プロトコルの脆弱性をマッピングする必要があります。
- サードパーティからパッチ情報をインポートし、そのパッチで修正されたすべての脆弱性に無効とマークする場合は、サードパーティの修正名をデータベースの修正定義にマッピングする必要があります。修正によって解決された脆弱性はすべて、その修正を加えるホストから排除されます。
- オペレーティング システムやアプリケーション プロトコルの脆弱性をサードパーティからインポートし、これらを影響相関に使用する場合、サードパーティの脆弱性識別文字列をデータベース内の脆弱性にマッピングする必要があります。多くのクライアントは、脆弱性と関連があり、影響評価に使用されますが、サードパーティのクライアントの脆弱性をインポートし、マッピングすることはできない点にご注意ください。脆弱性のマッピング後、Firepower Management Center 設定の影響評価のためにサードパーティの脆弱性のマッピングを有効にします。ベンダー情報やバージョン情報のないアプリケーションプロトコルを脆弱性にマッピングするには、管理ユーザは、Firepower Management Center 設定のアプリケーションの脆弱性もマッピングする必要があります。
- アプリケーションデータをインポートし、そのデータを影響相関に使用する場合、各アプリケーション プロトコルのベンダー文字列を対応する Cisco アプリケーション プロトコルの定義にマッピングする必要があります。

関連トピック

サードパーティの製品のマッピング，（1468 ページ）
サード パーティ製品の修正のマッピング，（1470 ページ）
サードパーティの脆弱性のマッピング，（1471 ページ）
サーバの脆弱性のマッピング，（611 ページ）
カスタム製品マッピングの作成，（1473 ページ）

サードパーティ製品のマッピング

ユーザ入力機能を使用して各サードパーティからのデータをネットワーク マップに追加する場合、サードパーティで使用するベンダー、製品、およびバージョンの各名前を Cisco 製品定義にマッピングする必要があります。各製品を Cisco の定義にマッピングすると、これらの定義に基づいて脆弱性が割り当てられます。

同様に、パッチ管理製品などのサードパーティからのパッチ情報をインポートする場合、その修正の名前をデータベース内の適切なベンダー、製品、および対応する修正にマッピングする必要があります。

サードパーティの製品のマッピング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

サードパーティからデータをインポートする場合、そのデータを使用して脆弱性を指定したり、影響の関連付けを行ったりするために、シスコの製品をサードパーティの名前にマッピングする必要があります。製品をマッピングすることにより、シスコの脆弱性情報をサードパーティ製品の名前に関連付けます。これにより、システムはそのデータを使用して影響の関連付けを行うことができます。

ホスト入力のインポート機能を使用してデータをインポートする場合、AddScanResult機能を使用して、インポート中にサードパーティ製品をオペレーティングシステムとアプリケーションの脆弱性にマップピングすることもできます。

たとえば、Apache Tomcat をアプリケーションとしてリストしているサードパーティのデータをインポートする場合で、それがバージョン 6 の Apache Tomcat であれば、以下のように設定し、サードパーティのマッピングを追加します。

- ベンダー名を [Apache] に設定します。
- プロダクト名に [Tomcat] 設定します。
- ベンダーのドロップダウン リストから [Apache] を選択します。
- 製品のドロップダウン リストから [Tomcat] を選択します。
- バージョンのドロップダウン リストから [6] を選択します。

このマッピングによって、Apache Tomcat 6 のすべての脆弱性が、Apache Tomcat をアプリケーションとしてリストアップするホストに割り当てられます。

バージョン情報やベンダー情報のないのアプリケーションの場合、Firepower Management Center 構成のアプリケーション タイプで脆弱性をマッピングする必要があります。多くのクライアントには関連付けられた脆弱性があり、クライアントが影響アセスメントに使用されますが、サードパーティのクライアントの脆弱性をインポートしてマッピングすることはできないことに注意してください。

ヒント すでに別のFirepower Management Center にサードパーティのマッピングを作成している場合、そのマッピングをエクスポートして、このManagement Center にインポートすることができます。その後、必要に応じてインポートしたマッピングを編集できます。

手順

ステップ 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）]を選択します。

ステップ 2 [ユーザ サードパーティ マッピング（User Third-Party Mappings）] をクリックします。

ステップ 3 次の 2 つの選択肢があります。

- [作成（Creat）]：新しいマップ セットを作成するには、[製品マップ セットの作成（Create Product Map Set）] をクリックします。
- [編集（Edit）]：既存のマップ セットを編集するには、そのマップ セットの横にある編集アイコン（）をクリックします。代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [マッピング セット名（Mapping Set Name）] を入力します。

ステップ 5 [説明（Description）] を入力します。

ステップ 6 次の 2 つの選択肢があります。

- [作成（Creat）]：サードパーティ製品をマッピングするには、[製品マップの追加（Add Product Map）] をクリックします。
- [編集（Edit）]：既存のサードパーティの製品のマッピングを編集するには、そのマッピングの横にある編集アイコン（）をクリックします。代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 7 サードパーティの製品で使用される [ベンダーの文字列（Vendor String）] を入力します。

ステップ 8 サードパーティの製品で使用される [製品の文字列（Product String）] を入力します。

ステップ 9 サードパーティの製品で使用される [バージョン文字列（Version String）] を入力します。

ステップ 10 製品マッピングセクションで、ベンダーの脆弱性のマッピングに使用するオペレーティング システム、製品、製品バージョンを、以下の項目から選択します。[ベンダー（Vendor）]、[製品（Product）]、[メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[改訂バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、[拡張子（Extension）]。

例：
名前がサードパーティの文字列で構成される製品を実行するホストで Red Hat Linux 9 の脆弱性マッピングを使用する場合、ベンダーとして [Redhat, Inc.]、製品として [Red Hat Linux]、バージョンとして [9] を選択します。

ステップ 11 [保存（Save）] をクリックします。

関連トピック

サーバの脆弱性のマッピング, （611 ページ）

サードパーティ製品の修正のマッピング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

修正名をデータベースの特定の修正セットにマッピングする場合、サードパーティのパッチ管理アプリケーションからデータをインポートし、修正を一連のホストに適用することができます。修正名がホストにインポートされると、システムはその修正によって解決されるすべての脆弱性をそのホストに対して無効としてマークします。

手順

ステップ 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）]を選択します。

ステップ 2 [ユーザ サードパーティ マッピング（User Third-Party Mappings）] をクリックします。

ステップ 3 次の 2 つの選択肢があります。

- [作成（Creat）] : 新しいマップ セットを作成するには、[製品マップ セットの作成（Create Product Map Set）] をクリックします。
- [編集（Edit）] : 既存のマップ セットを編集するには、そのマップ セットの横にある編集アイコン（）をクリックします。代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [マッピング セット名（Mapping Set Name）] を入力します。

ステップ 5 [説明（Description）] を入力します。

ステップ 6 次の 2 つの選択肢があります。

- 作成：サードパーティ製品をマッピングするには、[修正マップの追加（Add Fix Map）] をクリックします。
- 編集：既存のサードパーティ製品マップを編集するには、その横にある編集アイコン（）をクリックします。代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 7 [サードパーティの修正名（Third-Party Fix Name）] フィールドにマッピングする修正の名前を入力します。

ステップ 8 [製品マッピング（Product Mappings）] セクションで、次のフィールドから修正マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します。

- ベンダー
- 製品

- メジャー バージョン（Major Version）
- マイナー バージョン（Minor Version）
- リビジョン バージョン（Revision Version）
- ビルド（Build）
- パッチ（Patch）
- 内線番号

例：
Red Hat Linux 9 からパッチが適用されるホストにマッピングで修正を割り当てる場合は、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

ステップ 9 [保存（Save）] をクリックして、修正マップを保存します。

サードパーティの脆弱性のマッピング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

サードパーティからの脆弱性情報を VDB に追加するには、インポートしたそれぞれの脆弱性のサードパーティ識別文字列を、既存の SVID、Bugtraq、または SID にマッピングする必要があります。脆弱性のマッピングを作成したら、マッピングはネットワーク マップのホストにインポートされたすべての脆弱性に対して機能し、それらの脆弱性に対する影響の関連付けを可能にします。

サードパーティの脆弱性に対する影響の関連付けを有効にし、関連付けの実行を可能にする必要があります。バージョンレスまたはベンダーレスのアプリケーションの場合、Firepower Management Center の設定でアプリケーション タイプの脆弱性をマッピングする必要もあります。

多くのクライアントには関連付けられた脆弱性があり、クライアントが影響評価に使用されますが、サードパーティのクライアントの脆弱性は影響評価に使用できません。

ヒント すでに別の Firepower Management Center にサードパーティのマッピングを作成している場合、そのマッピングをエクスポートして、この Management Center にインポートすることができます。その後、必要に応じてインポートしたマッピングを編集できます。

手順

ステップ 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）]を選択します。

ステップ 2 [ユーザ サードパーティ マッピング（User Third-Party Mappings）] をクリックします。

ステップ 3 次の 2 つの選択肢があります。

- 作成：新しい脆弱性セットを作成するには、[脆弱性マップ セットの作成（Create Vulnerability Map Set）] をクリックします。
- 編集：既存の脆弱性セットを編集するには、脆弱性セットの横にある編集アイコン（  ）をクリックします。代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [脆弱性マップの追加（Add Vulnerability Map）] をクリックします。

ステップ 5 [脆弱性 ID（Vulnerability ID）] フィールドに脆弱性のサードパーティ ID を入力します。

ステップ 6 [脆弱性の説明（Vulnerability Description）] を入力します。

ステップ 7 必要に応じて、次の操作を実行します。

- [Snort 脆弱性 ID マッピング（Snort Vulnerability ID Mappings）] フィールドに Snort ID を入力します。
- [SVID マッピング（SVID Mappings）] フィールドに、レガシー脆弱性 ID を入力します。
- [Bugtraq 脆弱性 ID マッピング（Bugtraq Vulnerability ID Mappings）] フィールドに、Bugtraq ID 番号を入力します。

ステップ 8 [追加（Add）] をクリックします。

関連トピック

ネットワーク検出の脆弱性影響評価の有効化, （1569 ページ）
サーバの脆弱性のマッピング, （611 ページ）

カスタム製品マッピング

製品マッピングを使用して、サード パーティによるサーバ入力が適切なシスコ定義に関連付けられていることを確認できます。製品マッピングを定義し有効化した後、マッピングされたベンダー文字列を持つモニタ対象ホスト上のすべてのサーバまたはクライアントが、カスタム製品マッピングを使用します。したがって、サーバのベンダー、製品、バージョンを明示的に設定する代わりに、特定のベンダー文字列でネットワーク マップのすべてのサーバの脆弱性をマップすることをお勧めします。

カスタム製品マッピングの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

システムがVDBのベンダーおよび製品にサーバをマッピングできない場合は、手動でマッピングを作成できます。カスタム製品マッピングをアクティブにすると、システムは指定されたベンダーおよび製品の脆弱性を、そのベンダー文字列が発生するネットワーク マップのすべてのサーバにマッピングします。

（注） カスタム製品マッピングは、アプリケーション データのソース（Nmap、ホスト入力機能、Firepower システム自体など）に関係なく、アプリケーション プロトコルのすべての発生に適用されます。ただし、ホスト入力機能を使用してインポートしたデータのサードパーティの脆弱性マッピングが、カスタム製品マッピングを介して設定したマッピングと競合する場合、サードパーティの脆弱性マッピングはカスタム製品マッピングをオーバーライドし、入力が発生したときにサードパーティの脆弱性マッピング設定を使用します。

製品マッピング リストを作成し、各リストをアクティブ化/非アクティブ化することによって、複数のマッピングの同時使用を有効にするか、無効にします。マッピングするベンダーを指定すると、そのベンダーによって作成された製品のみを含むように製品リストが更新されます。

カスタム製品マッピングを作成した後で、カスタム製品マッピング リストをアクティブにする必要があります。カスタム製品マッピング リストをアクティブにすると、指定されたベンダー文字列が発生するすべてのサーバが更新されます。ホスト入力機能を介してインポートされるデータでは、このサーバの製品マッピングをすでに明示的に設定していない限り、脆弱性が更新されます。

たとえば、組織が Apache Tomcat Web サーバのバナーの文字列を `Internal Web Server` に変更した場合、ベンダー文字列 `Internal Web Server` をベンダー Apache および製品 Tomcat にマッピングできます。その後、そのマッピングを含むリストをアクティブにすると、`Internal Web Server` とラベル付けされたサーバが存在するすべてのホストのデータベースに Apache Tomcat の脆弱性が想定されます。

ヒント この機能を使用して、もう1つの脆弱性にルールのSIDをマッピングすることによって、ローカルの侵入ルールに脆弱性をマッピングすることができます。

手順

ステップ 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）]を選択します。
ステップ 2 [カスタム製品マッピング（Custom Product Mappings）] をクリックします。
ステップ 3 [カスタム製品マッピング リストの作成（Create Custom Product Mapping List）] をクリックします。
ステップ 4 [カスタム製品マッピング リスト名（Custom Product Mapping List Name）] を入力します。
ステップ 5 [ベンダー文字列の追加（Add Vendor String）] をクリックします。
ステップ 6 [ベンダー文字列（Vendor String）] フィールドに、選択したベンダーおよび製品値にマッピングする必要があるアプリケーションを識別するベンダー文字列を入力します。
ステップ 7 [ベンダー（Vendor）] ドロップダウン リストから、マッピングするベンダーを選択します。
ステップ 8 [製品（Product）] ドロップダウン リストから、マッピングする製品を選択します。
ステップ 9 [追加（Add）] をクリックして、マッピングしたベンダー文字列をリストに追加します。
ステップ 10 オプションで、さらにベンダー文字列のマッピングをリストに追加するには、必要に応じて手順 4 ～ 8 を繰り返します。
ステップ 11 [保存（Save）] をクリックします。

次の作業

- カスタム製品マッピング リストをアクティブにします。詳細については、カスタム製品マッピングのアクティブおよび非アクティブの設定, （1475 ページ）を参照してください。

カスタム製品マッピング リストの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

ベンダー文字列を追加または削除したり、リスト名を変更したりして、既存のカスタム製品マッピング リストを変更できます。

手順

ステップ 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）]を選択します。
ステップ 2 [カスタム製品マッピング（Custom Product Mappings）] をクリックします。
ステップ 3 編集する製品マッピング リストの横にある編集アイコン（  ）をクリックします。
代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 カスタム製品マッピングの作成, （1473 ページ）の説明に従って、リストを変更します。

ステップ 5 終了したら、[保存（Save）] をクリックします。

カスタム製品マッピングのアクティブおよび非アクティブの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

カスタム製品マッピング リスト全体の使用を一度に有効または無効にすることができます。カスタム製品マッピング リストをアクティブにすると、そのリストの各マッピングが、管理対象デバイスによって検出されたか、またはホスト入力機能を介してインポートされたかに関わらず、指定したベンダー文字列を持つすべてのアプリケーションに適用されます。

手順

ステップ 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）]を選択します。

ステップ 2 [カスタム製品のマッピング（Custom Product Mappings）] をクリックします。

ステップ 3 アクティブまたは非アクティブにするカスタム製品のマッピング リストの横にあるスライダをクリックします。
コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

eStreamer サーバ ストリーミング

Event Streamer（eStreamer）を使用すると、Firepower Management Center または 7000 または 8000 シリーズ デバイスからの数種類のイベント データを、カスタム開発されたクライアント アプリケーションにストリーム配信できます。詳細については、*Firepower eStreamer Integration Guide*を参照してください。

eStreamer サーバとして使用するアプライアンスで eStreamer イベントの外部クライアントへのストリームを開始するには、その前に、イベントをクライアントに送信するように eStreamer サーバを設定し、クライアントに関する情報を指定して、通信を確立するときに使用する認証クレデンシャルを生成する必要があります。アプライアンスのユーザ インターフェイスからこれらすべてのタスクを実行できます。設定が保存されると、選択したイベントが、要求時に、eStreamer クライアントに転送されます。

要求したクライアントに eStreamer サーバが送信できるイベント タイプを制御できます。

表 *192* : *eStreamer* サーバで送信可能なイベント タイプ

イベント タイプ（Event Type）	説明	Management Center で使用可能	7000 & 8000 シリーズ デバイスで使用可能
侵入イベント	管理対象デバイスによって生成される侵入イベント	Yes	Yes
侵入イベント パケット データ	侵入イベントに関連付けられたパケット	Yes	Yes
侵入イベント追加データ	HTTP プロキシまたはロードバランサ経由で Web サーバに接続しているクライアントの発信元 IP アドレスのような侵入イベントに関連付けられた追加データ	Yes	Yes
検出イベント	検出イベント	Yes	No
相関およびホワイトリスト イベント	相関およびホワイトリストイベント	Yes	No
インパクト フラグ アラート	Management Center によって生成されたインパクト アラート	Yes	No
ユーザ イベント	ユーザ イベント	Yes	No
マルウェア イベント	マルウェア イベント	Yes	No
ファイル イベント	ファイル イベント	Yes	No
接続イベント	モニタ対象のホストとその他のすべてのホスト間のセッショントラフィックに関する情報	Yes	Yes

eStreamer イベントタイプの選択

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	Management Center 7000 & 8000 シリーズ	任意（Any）	Admin

eStreamer サーバで送信可能なイベントの [eStreamer イベント設定（eStreamer Event Configuration）] チェックボックス管理。クライアントは、eStreamer サーバに送信する要求メッセージで受信するイベント タイプを具体的に要求する必要があります。詳細については、*Firepower eStreamer Integration Guide*を参照してください。

マルチドメイン展開では、どのドメインのレベルでも eStreamer のイベント構成を設定できます。ただし、先祖ドメインで特定のイベントタイプが有効になっている場合は、子孫ドメインのそのイベントタイプを無効にすることはできません。

手順

ステップ 1 [システム（System）] > [統合（Integration）]を選択します。

ステップ 2 [eStreamer] タブをクリックします。

ステップ 3 [eStreamer イベント設定（eStreamer Event Configuration）] の下で、eStreamer サーバ ストリーミング, （1475 ページ）の説明に従って要求元のクライアントに転送するイベントタイプの横にあるチェックボックスをオンまたはオフにします。

ステップ 4 [保存（Save）] をクリックします。

eStreamer クライアント通信の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
機能に応じて異なる	機能に応じて異なる	Management Center 7000 & 8000 シリーズ	任意（Any）	Admin/Discovery Admin

eStreamer がクライアントに eStreamer イベントを送信するには、その前に、eStreamer ページから eStreamer サーバのピア データベースにクライアントを追加しておく必要があります。また、eStreamer サーバによって生成された認証証明書をクライアントにコピーする必要もあります。この手順を完了した後、クライアントが eStreamer サーバに接続できるように eStreamer サービスを再起動する必要はありません。

マルチドメイン展開では、任意のドメインで eStreamer クライアントを作成できます。認証証明書では、クライアントはクライアント証明書のドメインと子孫ドメインからのみイベントを要求することが許可されます。eStreamer 設定ページには、現在のドメインに関連付けられているクライアントのみが表示されるため、証明書をダウンロードまたは取り消す場合は、クライアントが作成されたドメインに切り替えます。

手順

ステップ 1 [システム（System）] > [統合（Integration）]を選択します。

ステップ 2 [eStreamer] タブをクリックします。

ステップ 3 [クライアントの作成（Create Client）] をクリックします。

ステップ 4 [ホスト名（Hostname）] フィールドに、eStreamer クライアントを実行しているホストのホスト名または IP アドレスを入力します。

（注） DNS 解決を設定していない場合は、IP アドレスを使用します。

ステップ 5 証明書ファイルを暗号化するには、[パスワード（Password）] フィールドにパスワードを入力します。

ステップ 6 [保存（Save）] をクリックします。
これで、eStreamer サーバは、ホストが eStreamer サーバ上のポート 8302 にアクセスすることを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。

ステップ 7 クライアントのホスト名の横にあるファイルのダウンロードアイコン（）をクリックして、証明書ファイルをダウンロードします。

ステップ 8 SSL 認証のためにクライアントが使用する適切なディレクトリに証明書ファイルを保存します。

ステップ 9 クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン（）をクリックします。
eStreamer サービスを再起動する必要はありません。アクセスはただちに取り消されます。

ホスト入力クライアントの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
機能に応じて異なる	機能に応じて異なる	Management Center	任意（Any）	Admin/Discovery Admin

ホスト入力機能を使用すると、別のアプライアンスで実行されているクライアント プログラムから Firepower Management Center のネットワーク マップを更新できます。たとえば、ネットワークマップからホストを追加または削除したり、ホスト OS およびサービス情報を更新したりできます。詳細については、*Firepower System Host Input API Guide*を参照してください。

リモート クライアントを実行するには、その前に、[ホスト入力クライアント（Host Input Client）] ページから Firepower Management Center のピア データベースにクライアントを追加する必要があります。また、Management Center によって生成された認証証明書をクライアントにコピーする必要もあります。この手順を完了すると、クライアントは Management Center に接続できます。

マルチドメイン展開では、すべてのドメインにクライアントを作成できます。認証証明書を使用すると、クライアントは、クライアント証明書のドメインに関連付けられているリーフ ドメインにネットワークマップアップデートを送信できます。先祖ドメインの証明書を作成した場合（または後で証明書ドメインが子孫ドメインの追加後に先祖ドメインになった場合）、その証明書を使用するクライアントは、*Firepower System Host Input API Guide*で説明するように、すべてのトランザクションのターゲット リーフ ドメインを指定する必要があります。

[ホスト入力クライアント（Host Input Client）] タブには、現在のドメインに関連付けられているクライアントのみが表示されるため、証明書をダウンロードまたは失効させるには、クライアントが作成されたドメインに切り替えます。

手順

ステップ 1 [システム（System）] > [統合（Integration）]を選択します。

ステップ 2 [ホスト入力クライアント（Host Input Client）] タブをクリックします。

ステップ 3 [クライアントの作成（Create Client）] をクリックします。

ステップ 4 [ホスト名（Hostname）] フィールドに、ホスト入力クライアントを実行しているホストのホスト名または IP アドレスを入力します。

（注） DNS 解決を設定していない場合は、IP アドレスを使用します。

ステップ 5 証明書ファイルを暗号化するには、[パスワード（Password）] フィールドにパスワードを入力します。

ステップ 6 [保存（Save）] をクリックします。
ホスト入力サービスは、ホストが Firepower Management Center 上のポート 8307 にアクセスすることを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。

ステップ 7 証明書ファイルの横にあるファイル ダウンロード アイコン（  ）をクリックします。

ステップ 8 SSL 認証のためにクライアントが使用するディレクトリに証明書ファイルを保存します。

ステップ 9 クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン（  ）をクリックします。

Nmap スキャン

Firepowerシステムは、ネットワークのトラフィックをパッシブ分析してネットワーク マップを構築します。このパッシブ分析によって取得される情報は、システムの状態によっては不完全なことがよくあります。ただし、ホストをアクティブにスキャンすることで、完全な情報を取得できます。たとえば、オープン ポート上で実行中のサーバがホストにあり、システムによるネットワークのモニタリング中にそのサーバがトラフィックを送受信しなかった場合、システムではそのサーバに関する情報をネットワークマップに追加しません。しかし、アクティブ スキャナを使用して直接そのホストをスキャンすると、サーバの存在を検出できます。

Firepower システムには、Nmap™ という、ネットワーク調査およびセキュリティ監査を目的としたオープン ソースのアクティブ スキャナが統合されています。

Nmap を使用してホストをスキャンすると、システムは以下のように動作します。

- 前に検出されていないオープン ポート上のサーバを、該当するホストのホスト プロファイルの [サーバ（Servers）] リストに追加します。ホスト プロファイルの [スキャン結果（Scan Results）] セクションには、フィルタ処理されていたり閉じていたりしている TCP ポートや UDP ポート上で検出されたサーバがリストされます。デフォルトでは、Nmap は 1660 を超える TCP ポートをスキャンします。

  Nmap スキャンで識別されたサーバがシステムで認識され、対応するサーバ定義がシステムにある場合、システムは Nmap がそのサーバに使用する名前を、対応する Cisco サーバ定義にマップします。

- スキャン結果と 1500 を超える既知のオペレーティング システムのフィンガープリントを比較して、オペレーティング システムを判別し、それぞれにスコアを割り当てます。最高スコアのオペレーティング システムのフィンガープリントが、ホストに割り当てられるオペレーティング システムになります。

  システムは Nmap のオペレーティング システム名を Cisco のオペレーティング システム定義にマップします。

- 追加されたサーバおよびオペレーティング システムのホストに脆弱性を割り当てます。

（注）

- ホストがネットワーク マップ内になければ、Nmap は結果をホスト プロファイルに追加することはできません。
- ホストがネットワーク マップから削除されると、そのホストに関する Nmap スキャン結果が破棄されます。

ヒント　スキャン オプションによっては（ポートスキャンなど）低帯域幅のネットワークに非常に負荷をかけることがあります。ネットワーク使用率が低い時間帯にこのようなタスクを実行するよう、スケジュールしてください。

スキャンに使用される基礎的な Nmap テクノロジーの詳細については、http://insecure.org/ にある Nmap のマニュアルを参照してください。

関連トピック

Nmap スキャンの自動化, （202 ページ）

Nmap 修復オプション

Nmap 修復を作成して、Nmap スキャンの設定を定義します。Nmap 修復は、相関ポリシー内で応答として使用したり、オン デマンドで実行したり、特定の時間に実行するようにスケジュールしたりできます。

Nmap により提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままであることに注意してください。Nmapを使用してホスト内でオペレーティング システムやサーバのデータをスキャンすることを計画している場合は、定期的なスキャンのスケジュールをセットアップして、Nmap によって提供されるオペレーティング システムやサーバのデータを最新に保つこともできます。

次の表に、Firepower システム上で設定できる Nmap 修復オプションを示します。

表 *193* : *Nmap* 修復オプション

オプション	説明	対応する Nmap オプション
[スキャンの開始元イベント（Scan Which Address(es) From Event?）]	Nmapスキャンを相関ルールに対する応答として使用する場合、イベント内の送信元ホスト、宛先ホスト、またはその両方のどのアドレスをスキャンするのか制御する次のいずれかのオプションを選択します。 • [送信元アドレスと宛先アドレスのスキャン（Scan Source and Destination Addresses）] は、イベントの送信元 IP アドレスと宛先 IP アドレスによって表されるホストをスキャンします。 • [送信元アドレスのみのスキャン（Scan Source Address Only）] は、イベントの送信元IPアドレスによって表されるホストをスキャンします。 • [宛先アドレスのみのスキャン（Scan Destination Address Only）] は、イベントの宛先IPアドレスによって表されるホストをスキャンします。	該当なし

オプション	説明	対応する Nmap オプション
[スキャン タイプ（Scan Types）]	Nmap がポートをスキャンする方法を選択します。 • [TCP Syn（TCP Syn）] スキャンは、完全な TCP ハンドシェイクを使用せずに数千のポートにただちに接続します。このオプションを使用すると、TCP 接続が開始されますが完了はしていない状態で、admin アカウントが raw パケット アクセス権を持つホストや IPv6 が実行されていないホスト上でステルス モードでクイック スキャンできます。ホストが TCP Syn スキャンで送信される Synパケットを確認応答すると、Nmapは接続をリセットします。 • [TCP 接続（TCP Connect）] スキャンは、connect() システム コールを使用して、ホスト上のオペレーティング システムを介して接続を開きます。TCP Connect スキャンは、Firepower Management Center 上の admin ユーザや管理対象デバイスがホストに対する raw パケット特権を持っていない場合や、IPv6 ネットワークをスキャンしている場合に使用できます。つまり、このオプションは TCP Syn スキャンを使用できない状況で使用します。 • [TCP ACK] スキャンは、ACK パケットを送信して、ポートがフィルタ処理されているかいないかを検査します。 • [TCP ウィンドウ（TCP Window）] スキャンは、TCP ACK スキャンと同じ機能に加えて、ポートが開いているか閉じているかも判別します。 • [TCP Maimon] スキャンは、FIN/ACK プローブを使用して BSD 派生システムを識別します。	TCP Syn：-sS TCP Connect：-sT TCP ACK：-sA TCP Window：-sW TCP Maimon：-sM
[UDP ポートのスキャン（Scan for UDP ports）]	TCP ポートに加えて UDP ポートのスキャンも有効にします。UDP ポートのスキャンには時間がかかることがあるので、クイック スキャンする場合はこのオプションを使用しないように注意してください。	-sU

オプション	説明	対応する Nmap オプション
[イベントからのポートの使用（Use Port From Event）]	相関ポリシー内で応答として修復を使用する計画の場合に、修復によるスキャンの対象として、相関応答をトリガーするイベントで指定されたポートのみを有効にします。 • 相関イベント内のポートをスキャンし、Nmap 修復構成中に指定するポートをスキャンしない場合は、[オン（On）] を選択します。相関イベント内のポートをスキャンする場合は、Nmap 修復構成中に指定する IP アドレス上のポートが修復によりスキャンされることに注意してください。これらのポートも修復の動的スキャンのターゲットに追加されます。 • Nmap 修復構成中に指定するポートのみスキャンするには、[オフ（Off）] を選択します。 Nmap がオペレーティング システムやサーバに関する情報を収集するかどうかも制御できます。新しいサーバに関連付けられたポートをスキャンするには、[イベントからのポートの使用（Use Port From Event）] オプションを有効にします。	該当なし
[レポート検出エンジンからのスキャン（Scan from reporting detection engine）]	ホストを報告した検出エンジンがあるアプライアンスからホストへのスキャンを有効にします。 • レポート検出エンジンを実行しているアプライアンスからスキャンするには、[オン（On）] を選択します。 • 修復内で設定されているアプライアンスからスキャンするには、[オフ（Off）] を選択します。	該当なし
[高速ポート スキャン（Fast Port Scan）]	スキャン元デバイス上の `/var/sf/nmap/share/nmap/nmap-services` ディレクトリ内にある `nmap-services` ファイルにリストされている TCP ポートのみに対するスキャンを有効にし、その他のポート設定を無視できるようにします。このオプションと [ポート範囲とスキャンの順序（Port Ranges and Scan Order）] オプションを併用できないことに注意してください。 • スキャン元デバイス上の `/var/sf/nmap/share/nmap/nmap-services` ディレクトリ内の `nmap-services` ファイルにリストされているポートのみスキャンし、その他のポート設定を無視するには、[オン（On）] を選択します。 • すべての TCP ポートをスキャンするには、[オフ（Off）] を選択します。	`-F`

オプション	説明	対応する Nmap オプション
[ポート範囲とスキャンの順序（Port Ranges and Scan Order）]	Nmap ポート仕様シンタックスを使用して、スキャンする特定のポートを設定し、スキャンする順序も設定します。このオプションと [高速ポート スキャン（Fast Port Scan）] オプションを併用できないことに注意してください。	`-p`
[オープン ポートでベンダーとベンダー情報を調査（Probe open ports for vendor and version information）]	サーバ ベンダーとバージョン情報の検出を有効にします。オープン ポートでサーバ ベンダーとバージョン情報を調査する場合、Nmap はサーバの識別に使用するサーバ データを取得します。次に、シスコのサーバ データをそのサーバに置き換えます。 • ホスト上のオープン ポートでサーバ情報をスキャンして、サーバ ベンダーとバージョンを識別するには、[オン（On）] を選択します。 • ホストのシスコのサーバ情報を使用して続行するには、[オフ（Off）] を選択します。	`-sV`
[サービス バージョンの強度（Service Version Intensity）]	サービス バージョンに対する Nmap プローブの強度を選択します。 • 選択する数値が大きいほど使用するプローブの数が増えるので、スキャンは長時間になり精度が上がります。 • 選択する数値が小さいほど、使用するプローブの数が減るので、スキャンは高速になり精度が下がります。	`--version-intensity` <intensity>
[オペレーティング システムの検出（Detect Operating System）]	ホストのオペレーティング システム情報の検出を有効にします。 ホストでのオペレーティング システムの検出を設定した場合、Nmap はホストをスキャンし、その結果を使用してオペレーティング システムごとに評価を作成します。この評価は、ホスト上でそのオペレーティング システムが実行されている可能性を反映します。 • ホストに対してオペレーティング システムを識別する情報をスキャンするには、[オン（On）] を選択します。 • ホストに関するシスコのオペレーティング システム情報を使い続ける場合は、[オフ（Off）] を選択します。	`-o`

オプション	説明	対応する Nmap オプション
[すべてのホストをオンラインとして処理（Treat All Hosts As Online）]	ホストディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポート スキャンを有効にします。このオプションを有効にすると、Nmap は [ホストディスカバリ方式（Host Discovery Method）] と [ホストディスカバリポート リスト（Host Discovery Port List）] の設定を無視するので注意してください。 • ホスト ディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポート スキャンを実行するには、[オン（On）] を選択します。 • [ホスト ディスカバリ方式（Host Discovery Method）] と [ホスト ディスカバリ ポート リスト（Host Discovery Port List）] の設定を使用してホストディスカバリを実行し、使用不能なホスト上でのポート スキャンを省略するには、[オフ（Off）] を選択します。	-PN

オプション	説明	対応する Nmap オプション
[ホストディスカバリ方式（Host Discovery Method）]	ホストディスカバリを、ターゲット範囲内のすべてのホストに対して実行するか、[ホストディスカバリ ポート リスト（Host Discovery Port List）]にリストされているポートを経由して実行するか、または、ポートがリストされていない場合にそのホストディスカバリ方式のデフォルト ポートを経由するかを選択します。 ここで、[すべてのホストをオンラインとして処理（Treat All Hosts As Online）] も有効にすると、[ホストディスカバリ方式（Host Discovery Method）] オプションは無効になり、ホストディスカバリが実行されないことに注意してください。 ホストが存在していて利用可能であるかどうかを Nmap がテストする際に使用する方式を以下から選択します。 • [TCP SYN] オプションは、SYN フラグが設定された空の TCP パケットを送信し、応答を受信するとホストが利用可能であると認識します。デフォルトでは TCP SYN はポート 80 をスキャンします。TCP SYN スキャンは、ステートフル ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。 • [TCP ACK] オプションは、ACK フラグが設定された空の TCP パケットを送信し、応答を受信するとホストが利用可能であると認識します。デフォルトでは TCP ACK もポート 80 をスキャンします。TCP ACK スキャンは、ステートレス ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。 • [UDP] オプションは、UDP パケットを送信し、クローズ ポートからポート到達不能応答が戻されるとホストが利用可能であると想定します。デフォルトでは UDP はポート 40125 をスキャンします。	TCP SYN：`-PS` TCP ACK：`-PA` UDP：`-PU`
[ホストディスカバリ ポート リスト（Host Discovery Port List）]	ホストディスカバリの実行時にスキャンするポートを、カスタマイズしたカンマ区切りリストで指定します。	ホストディスカバリ方式に応じたポート リスト

オプション	説明	対応する Nmap オプション
[デフォルト NSE スクリプト（Default NSE Scripts）]	ホストディスカバリを行い、サーバ、オペレーティング システム、脆弱性を検出する Nmap スクリプトのデフォルト セットを実行できるようにします。デフォルト スクリプトのリストについては、https://nmap.org/nsedoc/categories/default.html を参照してください。 • Nmap スクリプトのデフォルト セットを実行するには、[オン（On）] を選択します。 • Nmap スクリプトのデフォルト セットを省略するには、[オフ（Off）] を選択します。	`-sC`
[タイミング テンプレート（Timing Template）]	スキャン プロセスのタイミングを選択します。選択する数値が大きいほど、スキャンは高速になり包括的ではなくなります。	0：`T0`（paranoid） 1：`T1`（sneaky） 2：`T2`（polite） 3：`T3`（normal） 4：`T4`（aggressive） 5：`T5`（insane）

Nmap スキャンのガイドライン

アクティブ スキャンにより重要な情報が得られることがありますが、Nmap などのツールを多用すると、ネットワーク リソースに負荷がかかり、重要なホストがクラッシュすることさえあります。アクティブ スキャナを使用する際には、以下のガイドラインに従ってスキャン戦略を作成し、スキャンする必要があるホストとポートのみスキャンするようにしてください。

適切なスキャン ターゲットの選択

Nmap を設定する際に、スキャン対象のホストを識別するスキャン ターゲットを作成できます。スキャン ターゲットには 1 つの IP アドレス、IP アドレスの CIDR ブロックまたはオクテット範囲、IP アドレス範囲、スキャンする IP アドレスまたは範囲のリスト、および 1 つ以上のホスト上のポートが含まれます。

次の方法でターゲットを指定できます。

- IPv6 ホストの場合：
  - 厳密な IP アドレス（`192.168.1.101` など）
- IPv4 ホストの場合：

- 厳密な IP アドレス（192.168.1.101 など）またはカンマかスペースで区切った IP アドレスのリスト
- CIDR 表記を使用した IP アドレス ブロック（たとえば、192.168.1.0/24 は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストをスキャンします）
- オクテットの範囲アドレッシングを使用した IP アドレス範囲（たとえば、192.168.0-255.1-254 は、192.168.x.x の範囲内の末尾が .0 と .255 以外のすべてのアドレスをスキャンします）
- ハイフンを使用した IP アドレス範囲（たとえば、192.168.1.1 - 192.168.1.5 は、両端を含めて 192.168.1.1 から 192.168.1.5 の間の 6 つのホストをスキャンします）
- カンマかスペースで区切ったアドレスか範囲のリスト（たとえば、192.168.1.0/24, 194.168.1.0/24 は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストと、両端を含めて 194.168.1.1 から 194.168.1.254 の間の 254 個のホストをスキャンします）

理想的な Nmap スキャンのスキャン ターゲットには、システムで識別できないオペレーティング システムがあるホスト、識別されていないサーバがあるホスト、最近ネットワーク上で検出されたホストが含まれます。ネットワーク マップ内にないホストに関する Nmap 結果は、ネットワーク マップに追加できないことに注意してください。

注意

- Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、定期的にスキャンをスケジュールします。
- ホストがネットワーク マップから削除されると、Nmap スキャン結果が破棄されます。
- ターゲットをスキャンする権限を持っていることを確認してください。Nmap を使用して自分や自社に属さないホストをスキャンすると違法になる場合があります。

スキャン対象にする適切なポートの選択

設定するスキャン ターゲットごとに、スキャン対象のポートを選択できます。各ターゲット上でスキャンする必要があるポートのセットを正確に識別するため、個々のポート番号、ポート範囲、または一連のポート番号やポート範囲を指定できます。

デフォルトでは、Nmap は 1 から 1024 までの TCP ポートをスキャンします。相関ポリシー内で応答として修復を使用する計画の場合は、相関応答をトリガーするイベントで指定されたポートのみを修復でスキャンできます。オン デマンドまたはスケジュール済みタスクとして修復を実行する場合、または Use Port From Event を使用しない場合は、その他のポート オプションを使用して、スキャンするポートを決定できます。nmap-services ファイルにリストされている TCP ポートのみスキャンし、その他のポート設定を無視するよう選択できます。TCP ポートの他に UDP ポートもスキャンできます。UDP ポートに対するスキャンには時間がかかることがあるので、すばやくスキャンする場合はこのオプションを使用しないように注意してください。スキャン対象

として特定のポートかポート範囲を選択するには、Nmapポート仕様シンタックスを使用してポートを識別します。

ホスト ディスカバリ オプションの設定

ホストに対してポート スキャンを始める前にホスト ディスカバリを実行するかどうかを決めるか、またはスキャンを計画しているすべてのホストがオンラインであると想定できます。すべてのホストをオンラインとして扱わないことを選択した場合、使用するホスト ディスカバリ方式を選択でき、必要に応じて、ホスト ディスカバリ時のスキャン対象ポートのリストをカスタマイズできます。ホストディスカバリ時には、リストされているポートでオペレーティング システムやサーバの情報は調査されません。特定のポートを経由する応答を使用して、ホストがアクティブで使用可能かどうかのみを判別します。ホスト ディスカバリを実行して、ホストが利用可能でなかった場合には、そのホスト上のポートは Nmap でスキャンされません。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）
Nmap スキャンの自動化, （202 ページ）

例：Nmap を使用した不明なオペレーティング システムの解決

この例では、不明なオペレーティング システムを解決するように設計された、Nmap 設定について説明します。Nmap設定の詳細については、Nmapスキャンの管理, （1492ページ）を参照してください。

システムでネットワーク上のホストのオペレーティング システムを判別できない場合、Nmap を使用してホストをアクティブ スキャンできます。Nmap は、スキャンから得られた情報を利用して、使用されている可能性のあるオペレーティング システムを評価します。次に、最高の評価のオペレーティング システムを、ホストのオペレーティング システムを識別したものとして使用します。

Nmapを使用して新しいホストにオペレーティング システムやサーバの情報を要求すると、スキャン対象のホストに対するシステムによるそのデータのモニタリングは非アクティブになります。Nmap を使用してホスト検出を実行し、システムにより不明なオペレーティング システムがあるとマークが付けられたホストのサーバオペレーティング システムを検出すると、同種のホストのグループを識別できる場合があります。その場合、それらのホストのうちの 1 つに基づいたカスタム フィンガープリントを作成し、システムでそのフィンガープリントを、Nmap スキャンに基づいてそのホスト上で実行されていると判明したオペレーティング システムと関連付けるようにすることができます。可能な限り、Nmap などのサードパーティ製の静的データを入力するよりも、カスタムフィンガープリントを作成してください。カスタムフィンガープリントを使用すると、システムはホストのオペレーティング システムを継続してモニタし、必要に応じて更新できるからです。

この例では、次のことを実行します。

1. Nmap スキャン インスタンスの追加, （1493 ページ）の説明に従って、スキャン インスタンスを設定します。
2. 次の設定を使用して Nmap 修復を作成します。

- [イベントからのポートの使用（Use Port From Event）] を有効にして、新しいサーバに関連付けられたポートをスキャンします。
- [オペレーティング システムの検出（Detect Operating System）] を有効にして、ホストのオペレーティング システムの情報を検出します。
- [ベンダーおよびバージョン情報のためのポートのプローブ オープン（Probe open ports for vendor and version information）] を有効にして、サーバ ベンダーとバージョン情報を検出します。
- ホストが既存であることが判明しているので、[すべてのホストをオンラインとして扱う（Treat All Hosts as Online）] を有効にします。

3 システムで不明なオペレーティング システムがあるホストが検出されたときにトリガーされる相関ルールを作成します。このルールは、検出イベントが発生し、ホストの OS 情報が変更されており、OS 名が不明という条件が満たされている場合にトリガーされる必要があります。

4 相関ルールを組み込む相関ポリシーを作成します。

5 相関ポリシー内で、ステップ 2 で応答として作成した Nmap 修復をステップ 3 で作成したルールに追加します。

6 相関ポリシーをアクティブにします。

7 ネットワーク マップ上のホストを消去し、強制的にネットワーク検出が再起動されてネットワーク マップが再構築されるようにします。

8 1 日後か2 日後に、相関ポリシーによって生成されたイベントを検索します。Nmap結果から、ホスト上で検出されたオペレーティング システムを分析し、システムで認識されない特定のホスト設定がネットワーク上にあるかどうか調べます。

9 不明なオペレーティング システムがあるホストが複数検出され、Nmap 結果が同一の場合は、それらのホストの 1 つに対してカスタム フィンガープリントを作成し、将来類似のホストを識別する際に使用します。

関連トピック

Nmap 修復の作成, （1498 ページ）
相関ルールの設定, （1638 ページ）
Nmap スキャンの結果, （1503 ページ）
クライアント用のカスタム フィンガープリントの作成, （1460 ページ）
相関ポリシーの設定, （1635 ページ）

例：Nmap を使用した新しいホストへの応答

この例では、新しいホストに応答するように設計された、Nmap 設定について説明します。Nmap 設定の詳細については、Nmap スキャンの管理, （1492 ページ）を参照してください。

システムにより、侵入の可能性があるサブネット内で新しいホストが検出された場合、そのホストをスキャンして、そのホストの脆弱性に関する正確な情報を入手できます。

そのためには、このサブネット内に新しいホストが出現した時点で検出し、そのホスト上でNmapスキャンを実行する修復を起動する相関ポリシーを作成してアクティブにします。

そのためには、次のことを実行します。

1. Nmap スキャン インスタンスの追加, （1493 ページ）の説明に従って、スキャン インスタンスを設定します。
2. 次の設定を使用して Nmap 修復を作成します。
   - [イベントからのポートの使用（Use Port From Event）] を有効にして、新しいサーバに関連付けられたポートをスキャンします。
   - [オペレーティング システムの検出（Detect Operating System）] を有効にして、ホストのオペレーティング システムの情報を検出します。
   - [ベンダーおよびバージョン情報のためのポートのプローブ オープン（Probe open ports for vendor and version information）] を有効にして、サーバ ベンダーとバージョン情報を検出します。
   - ホストが既存であることが判明しているので、[すべてのホストをオンラインとして扱う（Treat All Hosts as Online）] を有効にします。
3. システムが特定のサブネット上で新しいホストを検出したときにトリガーされる相関ルールを作成します。このルールは、検出イベントが発生し、新しいホストが検出されたときにトリガーされる必要があります。
4. 相関ルールを組み込む相関ポリシーを作成します。
5. 相関ポリシー内で、ステップ 2 で応答として作成した Nmap 修復をステップ 3 で作成したルールに追加します。
6. 相関ポリシーをアクティブにします。
7. 新しいホストが通知されたら、ホストプロファイルを調べてNmapスキャンの結果を確認し、ホストに適用されている脆弱性に対処します。

このポリシーをアクティブにした後で、修復状態の表示（[分析（Analysis）]>[相関（Correlation）]>[ステータス（Status）]）を定期的に検査して、修復が起動された時点を調べることができます。修復の動的なスキャンターゲットには、サーバ検出の結果としてスキャンされたホストのIPアドレスを含める必要があります。これらのホストのホスト プロファイルを調べて、Nmap によって検出されたオペレーティング システムとサーバに基づいて、対処する必要がある脆弱性がホストにあるかどうか確認します。

注意 大規模なネットワークや動的なネットワークがある場合、新しいホストの検出は頻繁に発生するので、スキャンを使用して応答するには不向きな場合があります。リソースの過負荷を避けるために、頻繁に発生するイベントへの応答としてNmapスキャンを使用しないでください。また、Nmapを使用して新しいホストのオペレーティングシステムやサーバの情報を要求すると、スキャン対象のホストに対するによるそのデータのシスコ モニタリングが非アクティブになることに注意してください。

関連トピック

Nmap 修復の作成, （1498 ページ）
相関ルールの設定, （1638 ページ）
相関ポリシーの設定, （1635 ページ）

Nmap スキャンの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

Nmap スキャンを使用するには、少なくとも 1 つの Nmap スキャン インスタンスと 1 つの Nmap 修復を設定する必要があります。Nmap スキャン ターゲットの設定はオプションです。

手順

ステップ 1 Nmap スキャンを設定します。

- Nmap スキャン インスタンスを追加します。詳細については、Nmap スキャン インスタンスの追加, （1493 ページ）を参照してください。
- Nmap 修復を作成します。詳細については、Nmap 修復の作成, （1498 ページ）を参照してください。
- 必要に応じて、Nmap スキャン ターゲットを追加します。詳細については、Nmap スキャン ターゲットの追加, （1496 ページ）を参照してください。

ステップ 2 Nmap スキャンを実行します。

- オンデマンド Nmap スキャンを実行します。詳細については、オンデマンド Nmap スキャンの実行, （1502 ページ）を参照してください。
- 自動 Nmap スキャンを設定します。詳細については、Nmap スキャンの自動化, （202 ページ）を参照してください。

- 自動 Nmap スキャンをスケジュールします。詳細については、Nmap スキャンのスケジュール, （202 ページ）を参照してください。

次の作業

- 関連タスクを表示することで、進行中の Nmap スキャンをモニタします。タスク メッセージの表示, （303 ページ）を参照してください。
- 必要に応じて、次に示すようにスキャンを調整します。
  - Nmap スキャン インスタンスを編集します。詳細については、Nmap スキャン インスタンスの編集, （1495 ページ）を参照してください。
  - Nmap スキャン ターゲットを編集します。詳細については、Nmap スキャン ターゲットの編集, （1497 ページ）を参照してください。
  - Nmap 修復を編集します。詳細については、Nmap 修復の編集, （1501 ページ）を参照してください。

Nmap スキャン インスタンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

脆弱性についてネットワークをスキャンするのに使用する Nmap モジュールごとに別々のスキャン インスタンスをセットアップできます。Firepower Management Center 上のローカル Nmap モジュールか、リモートでスキャンを実行するために使用するデバイスに対してスキャン インスタンスをセットアップできます。各スキャンの結果は常に Firepower Management Center に保存されます。リモート デバイスからスキャンを実行する場合でも、この場所でスキャンを設定できます。ミッション クリティカルなホストへの不慮のスキャンや悪意のあるスキャンを防ぐには、インスタンスのブラックリストを作成し、そのインスタンスで決してスキャンしてはならないホストを指示できます。

既存のスキャン インスタンスと同じ名前のスキャン インスタンスは追加できません。

マルチドメイン展開では、現在のドメインで作成されたスキャン インスタンスが表示されます。これは編集できます。先祖ドメインで作成されたスキャン インスタンスも表示されますが、これは編集できません。下位のドメインのスキャン インスタンスを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 次のいずれかの方法を使用して Nmap スキャン インスタンスのリストにアクセスします。

- [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]を選択します。
- [ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]を選択します。

ステップ 2 以下の場合、修復を追加します。

- 上記の最初の方法でリストにアクセスした場合は、[新しいインスタンスの追加（Add a New Instance）] セクションを探し、ドロップダウン リストから Nmap 修復モジュールを選択し、[追加（Add）] をクリックします。
- 上記の 2 番目の方法でリストにアクセスした場合は、[Nmap インスタンスの追加（Add Nmap Instance）] をクリックします。

ステップ 3 [インスタンス名（Instance Name）] を入力します。

ステップ 4 [説明（Description）] を入力します。

ステップ 5 オプションで、[ブラックリスト化されたスキャン ホスト（Black Listed Scan hosts）] フィールドで、このスキャン インスタンスがスキャンしないホストまたはネットワークを指定します。

- IPv6 ホストの場合、厳密な IP アドレス（`2001:DB8::fedd:eeff` など）
- IPv4 ホストの場合、厳密な IP アドレス（`192.168.1.101` など）または CIDR 表記を使用した IP アドレス ブロック（たとえば、`192.168.1.0/24` は、両端を含めて `192.168.1.1` から `192.168.1.254` の間の 254 個のホストをスキャンします）
- 感嘆符（!）を使用してアドレス値の否定はできないことに注意してください。

（注） ブラックリストに含まれるネットワーク内のホストをスキャン対象として特定すると、スキャンは実行されません。

ステップ 6 オプションで、Firepower Management Center の代わりにリモート デバイスからスキャンを実行するには、そのデバイスの IP アドレスか名前を指定します。この情報は、Management Center Web インターフェイス内のそのデバイスに関する [Information] ページの [Remote Device Name] フィールドに表示されます。

ステップ 7 [作成（Create）] をクリックします。
システムがインスタンスの作成を終えると、編集モードでこのインスタンスが表示されます。

ステップ 8 必要に応じて、インスタンスに Nmap の修復を追加します。そのためには、インスタンスの [設定されている修復（Configured Remediations）] を探し、[追加（Add）] をクリックし、Nmap 修復の作成, （1498 ページ）の説明に従って修復を作成します。

ステップ 9 インスタンスのリストに戻るには、[キャンセル（Cancel）] をクリックします。

（注） [スキャナ（Scanners）] オプションにより Nmap スキャンインスタンスのリストにアクセスした場合は、インスタンスの修復も併せて追加しないと追加したインスタンスは表示されません。修復が追加されていないインスタンスをすべて表示するには、[インスタンス（Instances）] メニュー オプションを使ってリストにアクセスします。

Nmap スキャン インスタンスの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

スキャン インスタンスを編集する場合、インスタンスに関連付けられている修復を表示、追加、および削除できます。インスタンス内でプロファイルが作成された Nmap モジュールを使用しなくなった場合には、Nmap スキャン インスタンスを削除します。スキャン インスタンスを削除すると、そのインスタンスを使用する修復も削除されることに注意してください。

マルチドメイン展開では、現在のドメインで作成されたスキャン インスタンスが表示されます。これは編集できます。先祖ドメインで作成されたスキャン インスタンスも表示されますが、これは編集できません。下位のドメインのスキャン インスタンスを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 次のいずれかの方法を使用して Nmap スキャン インスタンスのリストにアクセスします。

- [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]を選択します。
- [ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]を選択します。

ステップ 2 編集するインスタンスの横にある表示アイコン（  ）をクリックします。

ステップ 3 Nmap スキャンインスタンスの追加, （1493 ページ）の説明に従って、スキャンインスタンスの設定を変更します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [完了（Done）] をクリックします。

次の作業

- 必要に応じて、スキャンインスタンスに新しい修復を追加します。次を参照してください。Nmap 修復の作成, （1498 ページ）

- 必要に応じて、インスタンスに関連付けられている修復を編集します。Nmap 修復の編集, （1501 ページ）を参照してください。
- 必要に応じて、インスタンスに関連付けられる修復を削除します。オンデマンド Nmap スキャンの実行, （1502 ページ）を参照してください。
- 必要に応じて、その横にある削除アイコン（）をクリックして、スキャン インスタンスを削除します。

Nmap スキャン ターゲットの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

Nmap モジュールを設定する際にスキャン ターゲットを作成して保存できます。スキャン ターゲットは、オンデマンドまたはスケジュール済みのスキャンの実行時にターゲットにするホストとポートを識別します。これにより、毎回新しいスキャン ターゲットを作成する必要がなくなります。スキャン ターゲットには、スキャンする 1 つの IP アドレスか IP アドレスのブロック、および 1 つ以上のホスト上のポートが含まれます。Nmap ターゲットの場合、オクテット範囲による Nmap のアドレッシングや IP アドレスの範囲も使用できます。Nmap のオクテット範囲によるアドレッシングの詳細については、http://insecure.org にある Nmap のマニュアルを参照してください。

（注）

- スキャン ターゲットに多数のホストが含まれている場合、スキャンに要する時間が延びる場合があります。回避策として、一度にスキャンするホストを減らしてください。
- Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、定期的にスキャンをスケジュールします。ホストがネットワーク マップから削除されると、Nmap スキャン結果はすべて破棄されます。
- マルチドメイン展開では、現在のドメインで作成されたスキャン ターゲットが表示されます。これは編集できます。先祖ドメインで作成されたスキャン ターゲットも表示されますが、これは編集できません。下位のドメインのスキャン ターゲットを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]を選択します。

ステップ 2 ツールバーで、[ターゲット（Targets）] をクリックします。

ステップ 3 [スキャン ターゲットの作成（Create Scan Target）] をクリックします。

ステップ 4 [名前（Name）] フィールドに、このスキャン ターゲットに使用する名前を入力します。

ステップ 5 [IP 範囲（IP Range）] テキスト ボックスで、Nmap スキャンのガイドライン, （1487 ページ）で説明しているシンタックスを使用して、スキャンする 1 つ以上のホストを指定します。

（注） スキャン ターゲット内の IP アドレスか範囲のリストでカンマを使用した場合、ターゲットを保存する際にカンマはスペースに変換されます。

ステップ 6 [ポート（Ports）] フィールドで、スキャンするポートを指定します。
1 から 65535 までの値を使用して、次のいずれかを入力できます。

- ポート番号
- カンマで区切ったポートのリスト
- ハイフンで区切ったポート番号の範囲
- ハイフンで区切ったポート番号の複数の範囲をカンマで区切ったもの

ステップ 7 [保存（Save）] をクリックします。

関連トピック

Nmap スキャンの自動化, （202 ページ）

Nmap スキャン ターゲットの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

ヒント 修復を使用して特定の IP アドレスをスキャンするつもりがないのに、修復を起動した相関ポリシー違反にホストが関係していたためにその IP アドレスがターゲットに追加された場合は、修復の動的スキャン ターゲットを編集できます。

スキャン ターゲットにリストされているホストをスキャンする必要がなくなった場合は、そのスキャン ターゲットを削除します。

マルチドメイン展開では、現在のドメインで作成されたスキャン ターゲットが表示されます。これは編集できます。先祖ドメインで作成されたスキャン ターゲットも表示されますが、これは編集できません。下位のドメインのスキャン ターゲットを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]を選択します。

ステップ 2 ツールバーで、[ターゲット（Targets）] をクリックします。

ステップ 3 編集するスキャン ターゲットの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 必要に応じて変更を加えます。詳細については、Nmap スキャン ターゲットの追加, （1496ページ）を参照してください。

ステップ 5 [Save] をクリックします。

ステップ 6 必要に応じて、その横にある削除アイコン（）をクリックして、スキャン ターゲットを削除します。

Nmap 修復の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

Nmap 修復は、既存の Nmap スキャン インスタンスに修復を追加することによってのみ作成できます。修復では、スキャンの設定を定義します。これは相関ポリシーで応答として使用したり、オンデマンドで実行したり、スケジュール タスクとして特定の時刻に実行したりできます。

Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、定期的にスキャンをスケジュールします。ホストがネットワーク マップから削除されると、Nmap スキャン結果が破棄されます。

Nmap の機能に関する一般情報については、http://insecure.org にある Nmap のマニュアルを参照してください。

マルチドメイン導入では、現在のドメインで作成された Nmap 修復が表示されます。これは編集できます。先祖ドメインで作成された Nmap 修復も表示されますが、これは編集できません。下位ドメインの Nmap 修復を表示および編集するには、そのドメインに切り替えます。

はじめる前に

- Nmap スキャンインスタンスの追加, （1493 ページ）の説明に従って、Nmap スキャンインスタンスを追加します。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（  ）をクリックします。

ステップ 3 [設定済みの修復（Configured Remediations）] セクションで、[追加（Add）] をクリックします。

ステップ 4 [修復名（Remediation Name）] を入力します。

ステップ 5 [説明（Description）] を入力します。

ステップ 6 侵入イベント、接続イベント、ユーザ イベントをトリガーする相関ルールに応じてこの修復を使用する場合は、[スキャンするイベントのアドレス（Scan Which Address(es) From Event?）] オプションを設定します。

ヒント ディスカバリ イベントまたはホスト入力イベントに対してトリガーする相関ルールへの応答としてこの修復を使用する計画の場合は、デフォルトでそのイベントに関連するホストの IP アドレスが修復によってスキャンされます。このオプションを設定する必要はありません。

（注） トラフィック プロファイルの変更に対してトリガーする相関ルールへの応答として Nmap 修復を割り当てないでください。

ステップ 7 [スキャン タイプ（Scan Type）] オプションを設定します。

ステップ 8 オプションで、TCP ポートに加えて UDP ポートをスキャンするには、[UDP ポートのスキャン（Scan for UDP ports）] オプションで [オン（On）] を選択します。

ヒント UDP ポートスキャンは TCP ポートスキャンよりも時間がかかります。スキャン時間を短縮するには、このオプションを無効のままにします。

ステップ 9 相関ポリシー違反への応答としてこの修復を使用する計画の場合は、[イベントからポートを使用（Use Port From Event）] オプションを設定します。

ステップ 10 相関ポリシー違反への応答としてこの修復を使用する計画で、イベントを検出した検出エンジンを実行しているアプライアンスを使用してスキャンを実行するには、[レポート検出エンジンからスキャン（Scan from reporting detection engine）] オプションを設定します。

ステップ 11 [高速ポート スキャン（Fast Port Scan）] オプションを設定します。

ステップ 12 [ポート範囲およびスキャン順序（Port Ranges and Scan Order）] フィールドに、デフォルトでスキャンするポートを入力します。Nmap ポート指定シンタックスを使用し、ポートをスキャンする順序で入力します。
次の形式を使用します。

- 1 から 65535 までの値を指定します。
- ポートを区切るには、カンマかスペースを使用します。
- ポート範囲を示すには、ハイフンを使用します。

- TCP ポートと UDP ポートの両方ともスキャンする場合は、スキャン対象の TCP ポートのリストの先頭に T を挿入し、UDP ポートのリストの先頭に U を挿入します。

（注） 手順 8 で説明されているように、相関ポリシー違反への応答として修復が起動する場合には、[イベントからポートを使用（Use Port From Event）] オプションによりこの設定が上書きされます。

例：
UDP トラフィックのポート 53 と 111 をスキャンしてから、TCP トラフィックのポート 21 から 25 までスキャンするには、`U:53,111,T:21-25` と入力します。

ステップ 13 開いているポートでサーバベンダーおよびバージョン情報をプローブするには、[ベンダーおよびバージョン情報に関するオープン ポートのプローブ（Probe open ports for vendor and version information）] を設定します。

ステップ 14 開いているポートをプローブすることにした場合、[サービス バージョンの強さ（Service Version Intensity）] ドロップダウン リストから数値を選択することにより、使用されるプローブの数を設定します。

ステップ 15 オペレーティング システム情報をスキャンするには、[オペレーティング システムの検出（Detect Operating System）] 設定を行います。

ステップ 16 ホスト ディスカバリが行われるかどうか、およびポートのスキャンが使用可能なホストのみに対して実行されるかどうかを決めるには、[すべてのホストをオンラインとして扱う（Treat All Hosts As Online）] を設定します。

ステップ 17 Nmap でホストの使用可能性をテストする際に使用する方法を設定するには、[ホスト ディスカバリ方式（Host Discovery Method）] ドロップダウン リストから方式を選択します。

ステップ 18 ホスト ディスカバリ時にポートのカスタム リストをスキャンする場合は、選択したホスト ディスカバリ方式に適したポートのリストを、[ホスト ディスカバリ ポート リスト（Host Discovery Port List）] フィールドにカンマで区切って入力します。

ステップ 19 [デフォルト NSE スクリプト（Default NSE Scripts）] オプションを設定して、ホスト ディスカバリおよび、サーバ、オペレーティング システム、脆弱性のディスカバリに Nmap スクリプトのデフォルト セットを使用するかどうかを制御します。

ヒント デフォルト スクリプトのリストについては、http://nmap.org/nsedoc/categories/default.html を参照してください。

ステップ 20 スキャン プロセスのタイミングを設定するには、[タイミング テンプレート（Timing Template）] ドロップダウン リストからタイミング テンプレート番号を選択します。
より高速だが、包括的でないスキャンを実行する場合は大きい番号を選択し、低速で、より包括的なスキャンを実行する場合は小さい番号を選択します。

ステップ 21 [作成（Create）] をクリックします。
修復の作成が完了すると、修復が編集モードで表示されます。

ステップ 22 [完了（Done）] をクリックして、関連インスタンスに戻ります。

ステップ 23 [キャンセル（Cancel）] をクリックすると、インスタンス リストに戻ります。

関連トピック

Nmap スキャンの自動化, （202 ページ）
Nmap 修復オプション, （1480 ページ）

Nmap 修復の編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

Nmap修復に加えた変更は、進行中のスキャンには影響しません。新しい設定は、次回スキャンが開始されたときに有効になります。Nmap 修復が不要になったら削除します。

マルチドメイン導入では、現在のドメインで作成された Nmap 修復が表示されます。これは編集できます。先祖ドメインで作成された Nmap 修復も表示されますが、これは編集できません。下位ドメインの Nmap 修復を表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 以下のいずれかの方法を使用して、Nmap スキャン インスタンスのリストにアクセスします。

- [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]を選択します。
- [ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]を選択します。

ステップ 2 編集する修復にアクセスします。

- 上記の最初の方法でリストにアクセスした場合は、関連するインスタンスの横にある表示アイコン（）をクリックし、次に、[設定済み修復（Configured Remediations）] セクションで、編集する修復の横にある表示アイコンを再度クリックします。
- 上記の 2 番目の方法でリストにアクセスした場合は、編集する修復の横にある表示アイコン（）をクリックします。

ステップ 3 Nmap 修復の作成, （1498 ページ）の説明に従って、必要に応じて変更を加えます。

ステップ 4 変更を保存する場合は [保存（Save）] をクリックし、保存せずに終了する場合は [完了（Done）] をクリックします。

ステップ 5 必要に応じて、その横にある削除アイコン（）をクリックして修復を削除します。

オンデマンド Nmap スキャンの実行

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

オンデマンド Nmap スキャンは、いつでも必要なときに起動できます。スキャンする IP アドレスとポートを入力するか、既存のスキャンターゲットを選択することで、オンデマンドスキャンのターゲットを指定できます。

Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、定期的にスキャンをスケジュールします。ホストがネットワーク マップから削除されると、Nmap スキャンの結果は破棄されます。

はじめる前に

- 必要に応じて、Nmap スキャン ターゲットを追加します。Nmap スキャン ターゲットの追加, （1496 ページ）を参照してください。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]を選択します。

ステップ 2 スキャンの実行時に使用する Nmap 修復の横にあるスキャン アイコン（）をクリックします。

ステップ 3 必要に応じて、保存済みのスキャンターゲットを使用してスキャンする場合は、[保存済ターゲット（Saved Targets）] ドロップダウンリストからターゲットを選択して、[ロード（Load）] をクリックします。

（注） スキャン ターゲットを追加するには、ダイアログの上部にある編集アイコン（）をクリックします。

ステップ 4 [IP 範囲（IP Range(s)）] フィールドで、スキャンするホストの IP アドレスを指定するかロードされたリストを変更します。

（注）

- IPv4 アドレスのホストの場合は、複数の IP アドレスをカンマで区切って指定するか、CIDR 表記を使用できます。感嘆符（!）を前に挿入して IP アドレスを否定することもできます。
- IPv6 アドレスのホストの場合は、厳密な IP アドレスを使用します。範囲はサポートされていません。

ステップ 5 [ポート（Ports）] フィールドで、スキャンするポートを指定するか、ロードされたリストを変更します。

ポート番号、カンマで区切ったポートのリスト、ハイフンで区切ったポート番号の範囲を入力できます。

ステップ 6 マルチドメイン展開では、[ドメイン（Domain）]フィールドを使用して、スキャンを実行するリーフ ドメインを指定します。

ステップ 7 [今すぐスキャン（Scan Now）] をクリックします。

次の作業

- 必要に応じて、タスクのステータスをモニタします（タスク メッセージの表示, （303 ページ） を参照）。

関連トピック

Nmap スキャンの自動化, （202 ページ）
Firepower システムの IP アドレス表記法, （16 ページ）
検索でのポート, （1876 ページ）

Nmap スキャンの結果

進行中の Nmap スキャンをモニタし、Firepower システムによって実行されたスキャンの結果あるいは Firepower システム外部で行われたスキャンの結果をインポートして、スキャン結果を表示および分析することができます。

ローカル Nmap モジュールを使用して作成したスキャン結果を、レンダリングされたページとしてポップアップ ウィンドウで表示できます。Nmap 結果ファイルを raw XML 形式でダウンロードすることもできます。

Nmap によって検出されたオペレーティング システムやサーバの情報を、ホスト プロファイルやネットワーク マップ内で参照することもできます。ホストのスキャンが生成するサーバ情報がフィルタ除去されているかクローズ状態のポートのサーバに関する情報の場合、または、スキャンが収集した情報がオペレーティング システム情報やサーバのセクションに含めることができない情報の場合、それらの結果は、ホストプロファイルの [Nmap スキャン結果（Nmap Scan Results）] セクションに含めることができます。

Nmap スキャン結果の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

Nmap スキャンが完了したら、スキャン結果のテーブルを表示できます。

ユーザは検索する情報に応じて結果のビューを操作することができます。スキャン結果にアクセスすると表示されるページは、使用するワークフローに応じて異なります。定義済みのワークフローを使用できます。このワークフローにはスキャン結果のテーブル ビューが含まれます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

http://insecure.org で使用可能な Nmap バージョン 1.01 DTD を使用して Nmap の結果をダウンロードして表示することができます。

スキャン結果をクリアすることもできます。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]を選択します。

ステップ 2 ツールバーで、[スキャン結果（Scan Results）] をクリックします。

ステップ 3 次の選択肢があります。

- イベント時間の制約, （1855 ページ）の説明に従って、時間範囲を調整します。
- カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [（ワークフローの切り替え）（(switch workflow)）] をクリックします。
- スキャン結果をレンダリングされたページとしてポップアップ ウィンドウで表示するには、スキャン ジョブの横にある [表示（View）] をクリックします。
- テキスト エディタで raw XML コードを表示できるようにスキャン結果ファイルのコピーを保存するには、スキャン ジョブの横の [ダウンロード（Download）] をクリックします。
- スキャン結果をソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- 表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン（✖）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）]をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）]をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効にしたカラムをビューに戻すには、展開の矢印をクリックして検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。
- ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用, （1844 ページ）を参照してください。
- スキャン インスタンスや修復を設定するには、ツールバーの [スキャナ（Scanners）] をクリックしてください（Nmap スキャンの管理, （1492 ページ）を参照）。
- ワークフロー ページ内およびワークフロー ページ間で移動するには、ワークフロー ページのナビゲーション ツール, （1840 ページ）を参照してください。

- その他のイベント ビューに移動して関連するイベントを表示するには、[ジャンプ（Jump to）] ドロップダウン リストから、表示するイベント ビューの名前を選択します。
- スキャン結果を検索するには、該当するフィールドに検索条件を入力します。

関連トピック

Nmap スキャン結果のフィールド, （1505 ページ）

Nmap スキャン結果のフィールド

Nmap スキャンを実行すると、Firepower Management Center でデータベース内のスキャン結果が収集されます。次の表に、表示および検索できるスキャン結果テーブルのフィールドを示します。

表 *194*：スキャン結果のフィールド

フィールド	説明
開始時間（Start Time）	この結果を作成したスキャンの開始日時。
終了時間（End Time）	この結果を作成したスキャンの終了日時。
ターゲット（Target）	この結果を作成したスキャンのスキャン ターゲットの IP アドレス（DNS 解決が有効になっている場合はホスト名）。
Scan Type	この結果を作成したスキャンのタイプを示す、`Nmap` またはサードパーティのスキャナ名。
スキャン モード（Scan Mode）	この結果を作成したスキャンのモード： • [オンデマンド（On Demand）]：オン デマンドで実行されたスキャンからの結果。 • [インポート済み（Imported）]：別のシステムでスキャンされて Firepower Management Center にインポートされた結果。 • [スケジュール済み（Scheduled）]：スケジュール済みタスクとして実行されたスキャンからの結果。
結果	スキャンの結果。
ドメイン	スキャン ターゲットのドメイン。このフィールドは、マルチドメイン展開の場合にのみ存在します。

関連トピック

イベントの検索, （1871 ページ）

Nmap スキャン結果のインポート

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

Firepower システムの外部で実行した Nmap スキャンによって作成された XML 結果ファイルをインポートできます。以前に Firepower システムからダウンロードした XML 結果ファイルもインポートできます。Nmap スキャン結果をインポートする場合、結果ファイルは XML 形式で、Nmap バージョン 1.01 DTD に準拠している必要があります。Nmap 結果の作成と Nmap DTD の詳細については、http://insecure.org にある Nmap のマニュアルを参照してください。

Nmap がホスト プロファイルに結果を追加できるようにするには、その前にホストがネットワーク マップ内に存在している必要があります。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]を選択します。

ステップ 2 ツールバーで、[結果のインポート（Import Results）] をクリックします。

ステップ 3 マルチドメイン展開では、インポートされた結果の保存場所を指定するために、[ドメイン（Domain）] ドロップダウンリストからリーフ ドメインを選択します。

ステップ 4 [参照（Browse）] をクリックして、結果ファイルに移動します。

ステップ 5 [インポートの結果（Import Results）]ページに戻ったら、[インポート（Import）] をクリックして結果をインポートします。

第 65 章

アプリケーションの検出

次のトピックでは、Firepower システム アプリケーション検出について説明します。

概要：アプリケーション検出

Firepower システムは IP トラフィックを分析するときに、ネットワーク上でよく使用されているアプリケーションを特定しようとします。アプリケーション認識は、アプリケーションを制御するために不可欠です。

システムによって検出されるアプリケーションには以下の 3 種類があります。

- HTTP や SSH などのホスト間の通信を表すアプリケーション プロトコル
- Web ブラウザや電子メール クライアントなどのホスト上で動作しているソフトウェアを表すクライアント
- HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの *Web* アプリケーション

システムは、ディテクタに指定されている特性に従って、ネットワーク トラフィック内のアプリケーションを識別します。たとえば、システムはパケット ヘッダーに含まれる ASCII パターンによってアプリケーションを確認できます。加えて、Secure Socket Layer（SSL）プロトコル ディテクタは、セキュアなセッションからの情報を使用して、セッションからアプリケーションを識別します。

Firepower システムのアプリケーション ディテクタには以下の 2 つのソースがあります。

- システム提供ディテクタ。Web アプリケーション、クライアント、およびアプリケーション プロトコルを検出します。

  アプリケーション（およびオペレーティング システム）に対して使用できるシステム提供ディテクタは、インストールされている Firepower システムのバージョンと VDB のバージョンによって異なります。リリース ノートとアドバイザリに、新しいディテクタと更新されたディテクタに関する情報が記載されています。また、プロフェッショナル サービスが作成した個別のディテクタをインポートすることもできます。検出されるアプリケーションの完全なリストについては、サポート サイトを参照してください。

- カスタム アプリケーション プロトコル ディテクタ。Web アプリケーション、クライアント、アプリケーション プロトコルを検出するためにユーザが作成するディテクタです。

また、暗黙的アプリケーション プロトコル検出を通してアプリケーション プロトコルを検出することもできます。これは、クライアントの検出に基づいてアプリケーション プロトコルの存在を推測するものです。

ネットワーク検出ポリシーで定義されているように、システムはモニタ対象ネットワーク内のホスト上で動作しているアプリケーション プロトコルだけを識別します。たとえば、モニタされていないリモート サイト上の FTP サーバに内部ホストがアクセスする場合、システムはアプリケーション プロトコルを FTP として識別しません。一方、モニタされているホスト上の FTP サーバにリモートまたは内部ホストがアクセスする場合、システムはアプリケーション プロトコルを肯定的に識別できます。

モニタ対象ホストが非モニタ対象サーバに接続するために使用するクライアントをシステムで識別できる場合、システムはクライアントの対応するアプリケーション プロトコルを識別することができますが、そのプロトコルをネットワーク マップに追加することはしません。アプリケーション検出が発生するためには、クライアント セッションにサーバからの応答が含まれている必要があることに注意してください。

システムは、検出した各アプリケーションの特徴を把握します（アプリケーションの特性, （353 ページ）を参照）。システムはこれらの特徴を使用して、アプリケーション フィルタと呼ばれるアプリケーションのグループを作成します。アプリケーション フィルタは、アクセス制御するため、およびレポートとダッシュボード ウィジェットで使用する検索結果とデータを制限するために使用されます。

また、エクスポートした NetFlow レコード、Nmap のアクティブ スキャン、ホスト入力機能を使用してアプリケーション ディテクタ データを補完することもできます。

関連トピック

アプリケーション ディテクタの基本, （1509 ページ）

アプリケーション ディテクタの基本

Firepowerシステムは、アプリケーションディテクタを使用して、ネットワーク上で一般的に使用されるアプリケーションを識別します。[ディテクタ（Detectors）]ページ（[ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）]）を使用してディテクタ リストを表示し、検出機能をカスタマイズします。

ディテクタまたはその状態（アクティブ/非アクティブ）を変更できるかどうかは、そのタイプによって異なります。システムは、アクティブなディテクタのみを使用して、アプリケーション トラフィックを分析します。

（注） シスコが提供するディテクタは、FirepowerシステムおよびVDBのアップデートによって変更される可能性があります。更新されたディテクタに関する情報については、リリース ノートおよびアドバイザリを参照してください。

シスコが提供する内部ディテクタ

内部ディテクタは、クライアント、Webアプリケーション、およびアプリケーション プロトコルのトラフィック用の特別なディテクタ カテゴリです。内部ディテクタはシステム アップデートによって配信され、常にオンになっています。

シスコが提供するクライアント ディテクタ

クライアント ディテクタは、クライアント トラフィックを検出し、VDB またはシステム アップデートを介して配信されるか、または Cisco Professional サービスによってインポート用に提供されます。クライアント ディテクタを有効または無効にすることができます。インポートしたクライアント ディテクタのみエクスポートできます。

シスコが提供する **Web** アプリケーション ディテクタ

Web アプリケーション ディテクタは、HTTP トラフィック ペイロード内の Web アプリケーションを検出し、VDBまたはシステム アップデートを介して配信されます。Webアプリケーション ディテクタは常にオンになっています。

シスコが提供するアプリケーション プロトコル（ポート）ディテクタ

ポートベースのアプリケーション プロトコル ディテクタは、ウェルノウン ポートを使用してネットワーク トラフィックを識別します。これらは VDB またはシステム アップデートを介して配信されるか、または Cisco Professional サービスによってインポート用に提供されます。アプリケーション プロトコル ディテクタを有効または無効にしたり、カスタム ディテクタの基礎として使用するためにディテクタ定義を表示することができます。

シスコが提供するアプリケーション プロトコル（**Firepower**）ディテクタ

Firepower ベースのアプリケーション プロトコル ディテクタは、Firepower アプリケーション フィンガープリントを使用してネットワーク トラフィックを分析し、VDB またはシステム アップデー

トを介して配信されます。アプリケーションプロトコルディテクタを有効または無効にすることができます。

カスタム アプリケーション ディテクタ

カスタム アプリケーション ディテクタはパターンベースです。クライアント、Web アプリケーション、またはアプリケーション プロトコルのトラフィックからのパケット内のパターンを検出します。インポートされたカスタム ディテクタを完全に制御できます。

Web インターフェイスでのアプリケーション プロトコルの識別

次の表に、Firepowerシステムが検出されたアプリケーションプロトコルを識別する方法について概略を示します。

表 *195*：*Firepower* システムのアプリケーション プロトコルの識別

ID	説明
アプリケーション プロトコル名	Firepower Management Center は、次のアプリケーション プロトコルの場合に、名前でアプリケーション プロトコルを識別します。 • システムによって肯定的に識別された • NetFlowデータを使用して識別され、`/etc/sf/services`にポートとアプリケーション プロトコルの関連付けが存在する • ホスト入力機能を使用して手動で識別された • Nmap または別のアクティブな発生源によって識別された
`pending`	Firepower Management Centerは、システムが肯定的と否定的のどちらでもアプリケーションを識別できない場合に、アプリケーション プロトコルを `pending` として識別します。 多くの場合、システムが保留中のアプリケーションを識別するには、より多くの接続データを収集して分析する必要があります。 [アプリケーションの詳細（Application Details）]および[サーバ（Servers）]テーブルやホスト プロファイルで `pending` ステータスが表示されるのは、特定のアプリケーション プロトコル トラフィック（検出されたクライアントまたはWebアプリケーショントラフィックから推論されたトラフィック以外）が検出されたアプリケーション プロトコルだけです。
不明	Firepower Management Centerは、以下の場合にアプリケーション プロトコルを `unknown` として識別します。 • アプリケーションがシステムのディテクタのどれとも一致しない • アプリケーション プロトコルが NetFlow データを使用して識別されたものの、`/etc/sf/services` にポートとアプリケーション プロトコルの関連付けが存在しない

ID	説明
空白	使用可能なすべての検出データが検証されましたが、アプリケーション プロトコルが識別されませんでした。[アプリケーションの詳細（Application Details）] および [サーバ（Servers）] テーブルとホスト プロファイルでは、アプリケーション プロトコルが検出されなかった非 HTTP 汎用クライアント トラフィックに対して、アプリケーション プロトコルが空白として表示されます。

クライアント検出からの暗黙的アプリケーション プロトコル検出

非監視対象サーバにアクセスするために監視対象ホストが使用しているクライアントをシステムが識別できる場合、Firepower Management Center はその接続でクライアントに対応するアプリケーション プロトコルが使用されていると推測します（システムは監視対象ネットワーク上のアプリケーションだけを追跡するため、通常、接続ログには監視対象ホストが非監視対象サーバにアクセスしている接続に関するアプリケーション プロトコル情報が含まれていません）。

暗黙的アプリケーション プロトコル検出と呼ばれるこのプロセスの結果は次のようになります。

- システムはこれらのサーバの New TCP Port イベントまたは New UDP Port イベントを生成しないため、サーバが [サーバ（Servers）] テーブルに表示されません。加えて、これらのアプリケーション プロトコルの検出を基準にして、検出イベント アラートまたは相関ルールをトリガーすることはできません。
- アプリケーション プロトコルはホストに関連付けられないため、ホスト プロファイルの詳細を表示したり、サーバ ID を設定したり、トラフィック プロファイルまたは相関ルールに関するホストプロファイル資格内の情報を使用したりできません。加えて、システムはこの種の検出に基づいて脆弱性とホストを関連付けません。

ただし、アプリケーション プロトコル情報が接続内に存在するかどうかに対する相関イベントをトリガーできます。また、接続ログ内のアプリケーション プロトコル情報を使用して、接続トラッカーとトラフィック プロファイルを作成できます。

ホスト制限と検出イベント ロギング

システムがクライアント、サーバ、または Web アプリケーションを検出すると、関連するホストがすでにクライアント、サーバ、または Web アプリケーションの最大数に達していなければ、検出イベントが生成されます。

ホスト プロファイルには、ホストごとに最大 16 のクライアント、100 のサーバ、および 100 の Web アプリケーションが表示されます。

クライアント、サーバ、または Web アプリケーションの検出によって異なるアクションはこの制限の影響を受けないことに注意してください。たとえば、サーバ上でトリガーするように設定されたアクセス コントロール ルールでは、引き続き、接続イベントが記録されます。

アプリケーション検出に関する特殊な考慮事項

Squid

システムは、次のいずれかの場合に Squid サーバ トラフィックを肯定的に識別します。

- モニタ対象ネットワーク上のホストからプロキシ認証が有効になっている Squid サーバへの接続をシステムが検出した場合
- モニタ対象ネットワーク上の Squid プロキシ サーバからターゲット システム（つまり、クライアントが情報または別のリソースを要求する宛先サーバ）への接続をシステムが検出した場合

ただし、システムは次の場合に Squid サービス トラフィックを識別できません。

- モニタ対象ネットワーク上のホストが、プロキシ認証が無効になっている Squid サーバに接続している場合
- Squid プロキシ サーバが HTTP 応答から Via: ヘッダー フィールドを除去するように設定されている場合

SSL アプリケーション検出

システムは、Secure Socket Layer（SSL）セッションからのセッション情報を使用してセッション内のアプリケーション プロトコル、クライアント アプリケーション、または Web アプリケーションを識別するアプリケーション ディテクタを備えています。

システムは暗号化された接続を検出すると、その接続を汎用 HTTPS 接続として、または、該当する場合には SMTPS などのより特殊なセキュア プロトコルとしてマークします。システムは SSL セッションを検出すると、そのセッションに対する接続イベント内の [クライアント（Client）] フィールドに `SSL client` を追加します。セッションの Web アプリケーションが識別されると、システムでトラフィックの検出イベントが生成されます。

SSL アプリケーション トラフィックの場合は、管理対象デバイスも、サーバ証明書から一般名を検出して SSL ホスト パターンからのクライアントまたは Web アプリケーションと照合できます。システムが特定のクライアントを識別すると、`SSL client` をそのクライアントの名前に置き換えます。

SSL アプリケーション トラフィックは暗号化されるため、システムは暗号化されたストリーム内のアプリケーションデータではなく、証明書内の情報しか識別に使用できません。そのため、SSL ホスト パターンではアプリケーションを制作した会社しか識別できない場合があり、同じ会社が作成した SSL アプリケーションは識別情報が同じ可能性があります。

HTTPS セッションが HTTP セッション内から起動される場合などは、管理対象デバイスがクライアント側のパケット内のクライアント証明書からサーバ名を検出します。

SSL アプリケーション識別を有効にするには、応答側のトラフィックをモニタするアクセス コントロール ルールを作成する必要があります。このようなルールには、SSL アプリケーションに関するアプリケーション条件または SSL 証明書からの URL を使用した URL 条件を含める必要があります。ネットワーク検出では、応答側の IP アドレスがネットワーク上に存在しなくても、ネッ

トワーク検出ポリシーでモニタできます。アクセス コントロール ポリシーの設定によって、トラフィックが識別されるかどうかが決まります。SSL アプリケーションの検出を識別するには、アプリケーション ディテクタ リストで、または、アプリケーション条件をアクセス コントロール ルールに追加するときに、`SSL protocol` タグでフィルタ処理します。

参照先 Web アプリケーション

Web サーバがトラフィックを他の Web サイト（通常は、アドバタイズメント サーバ）に参照する場合があります。ネットワーク上で発生するトラフィック参照のコンテキストをわかりやすくするために、システムは、参照セッションに対するイベント内の [Web アプリケーション（Web Application）] フィールドにトラフィックを参照した Web アプリケーションを列挙します。VDB に既知の参照先サイトのリストが含まれています。システムがこのようなサイトのいずれかからのトラフィックを検出すると、参照元サイトがそのトラフィックに対するイベントと一緒に保存されます。たとえば、Facebook 経由でアクセスされるアドバタイズメントが実際は Advertising.com 上でホストされている場合は、検出された Advertising.com トラフィックが Facebook Web アプリケーションに関連付けられます。また、システムは、Web サイトで他のサイトへの単リンクが提供されている場合などは、HTTP トラフィック内の参照元 URL を検出することもできます。この場合、参照元 URL は [HTTP 参照元（HTTP Referrer）] イベント フィールドに表示されます。

イベントでは、参照元アプリケーションが存在する場合に、それがトラフィックの Web アプリケーションとして列挙されますが、URL は参照先サイトの URL です。上の例では、トラフィックに対する接続イベントの Web アプリケーションは Facebook ですが、URL は Advertising.com です。参照元 Web アプリケーションが検出されない場合、ホストが自身を参照している場合、または参照がチェインしている場合は、参照先アプリケーションが Web アプリケーションとして表示される場合もあります。ダッシュボードでは、Web アプリケーションの接続カウントとバイト カウントに、Web アプリケーションが参照先のトラフィックに関連付けられたセッションが含まれます。

参照先トラフィックに対して明示的に機能するルールを作成する場合は、参照元アプリケーションではなく、参照先アプリケーションに関する条件を追加する必要があることに注意してください。Facebook から参照される Advertising.com トラフィックをブロックするには、Advertising.com アプリケーションのアクセス コントロール ルールにアプリケーション条件を追加します。

カスタム アプリケーション ディテクタ

ネットワーク上でカスタム アプリケーションを使用する場合、アプリケーションの識別に必要な情報をシステムに提供するカスタム Web アプリケーション、クライアント、またはアプリケーション プロトコル ディテクタを作成します。アプリケーション ディテクタの種類は、[プロトコル（Protocol）]、[タイプ（Type）]、および [検出方向（Direction）] フィールドで選択した内容によって決まります。

システムがサーバ トラフィックでアプリケーション プロトコルの検出および識別を開始するように、クライアント セッションにサーバからの応答パケットを含める必要があります。UDP トラフィックの場合、応答パケットの送信元がサーバとして指定されることに注意してください。

すでに別の Firepower Management Center にディテクタを作成している場合、そのディテクタをエクスポートして、この Firepower Management Center にインポートすることができます。その後、

必要に応じてインポートしたディテクタを編集できます。カスタム ディテクタおよび Cisco Professional サービスが提供するディテクタをエクスポートおよびインポートすることができます。ただし、シスコが提供するその他の種類のディテクタをエクスポートおよびインポートすることは**できません**。

カスタム アプリケーション ディテクタおよびユーザ定義アプリケーション フィールド

次のフィールドを使用して、カスタムアプリケーションディテクタおよびユーザ定義アプリケーションを設定できます。

カスタム アプリケーション ディテクタ フィールド：概要

基本および高度なカスタムアプリケーションディテクタを設定するには、次のフィールドを使用します。

アプリケーション プロトコル（Application Protocol）

検出するアプリケーション プロトコル。これには、システムが提供するアプリケーションまたはユーザ定義のアプリケーションを指定できます。

アプリケーションを（アイデンティティ ルールで設定された）アクティブな認証から除外できるようにする場合は、User-Agent Exclusion タグを使用してアプリケーション プロトコルを選択するか、作成する必要があります。

説明

アプリケーション ディテクタの説明。

[名前（Name）]

アプリケーション ディテクタの名前。

ディテクタ タイプ（Detector Type）

ディテクタのタイプ（[基本（Basic）] または [高度（Advanced）]）。基本的なアプリケーションディテクタは、一連のフィールドとして Web インターフェイスで作成されます。高度なアプリケーション ディテクタは、外部で作成され、カスタム .lua ファイルとしてアップロードされます。

カスタム アプリケーション ディテクタ（Custom Application Detector）フィールド：検出パターン

基本的なカスタムアプリケーションディテクタの検出パターンを設定するには、次のフィールドを使用します。

方向（Direction）

ディテクタが検出するトラフィックの送信元。[クライアント（Client）] または [サーバ（Server）]。

オフセット（Offset）

システムがパターンの検索を開始する必要がある、パケット ペイロードの先頭からのパケットの場所（バイト単位）。

パケット ペイロードは 0 バイトから始まるため、パケット ペイロードの先頭から数えたバイト数から 1 を減算することでオフセットを計算します。たとえば、パケットの 5 桁目のビット パターンを検索するには、[オフセット（Offset）] フィールドに「4」と入力します。

パターン

パターン文字列は、選択した [タイプ（Type）] に関連付けられます。

ポート

ディテクタが検出するトラフィックのポート。

プロトコル

検出するプロトコル。選択するプロトコルによって、[タイプ（Type）] フィールドが表示されるか [URL（URL）] フィールドが表示されるかが決まります。

プロトコル（および、場合によっては、[タイプ（Type）] フィールドと [方向（Direction）] フィールドの後続の選択）によって、作成するアプリケーション ディテクタのタイプ（Web アプリケーション、クライアント、またはアプリケーション プロトコル）が決まります。

ディテクタ タイプ（Detector Type）	プロトコル	タイプ（Type）または 方向（Direction）
Web アプリケーション（Web Application）	HTTP	[タイプ（Type）] は [コンテンツ タイプ（Content Type）] または [URL（URL）] です。
	RTMP	任意（Any）
	SSL	任意（Any）
クライアント（Client）	HTTP	[タイプ（Type）] は [ユーザ エージェント（User Agent）] です。
	SIP	任意（Any）
	TCP または UDP	[方向（Direction）] は [クライアント（Client）] です。
アプリケーション プロトコル（Application Protocol）	TCP または UDP	[方向（Direction）] は [サーバ（Server）] です。

タイプ（Type）

入力したパターン文字列のタイプ。表示されるオプションは、選択した [プロトコル（Protocol）] によって決まります。プロトコルとして [RTMP（RTMP）] を選択すると、[タイプ（Type）] フィールドの代わりに [URL（URL）] フィールドが表示されます。

（注） [タイプ（Type）] として [ユーザ エージェント（User Agent）] を選択すると、システムはアプリケーションの [タグ（Tag）] を User-Agent Exclusion に自動的に設定します。

タイプの選択	文字列特性
Ascii	文字列は ASCII でエンコードされます。
Common Name	文字列は、サーバ応答メッセージ内の commonName フィールドの値です。
コンテンツ タイプ（Content Type）	文字列は、サーバ応答ヘッダー内のコンテンツ タイプ フィールドの値です。
16 進数	文字列は、16 進表記です。
組織	文字列は、サーバ応答メッセージ内の organizationName フィールドの値です。
SIP サーバ	文字列は、メッセージ ヘッダー内の From フィールドの値です。
SSL ホスト（SSL Host）	文字列は、ClientHello メッセージ内の server_name フィールドの値です。
URL	文字列は URL です。 （注） ディテクタは、ユーザが入力する文字列が URL の完全なセクションであると想定します。たとえば、cisco.com と入力した場合、www.cisco.com/support や www.cisco.com と一致しますが、www.wearecisco.com とは一致しません。
ユーザ エージェント（User Agent）	文字列は、GET リクエスト ヘッダー内の user-agent フィールドの値です。これはSIPプロトコルにも使用可能であり、文字列が SIP メッセージ ヘッダー内の User-Agent フィールドの値であることを示します。

URL

RTMP パケットの C2 メッセージ内の swfURL フィールドの完全な URL または URL のセクション。[プロトコル（Protocol）] として [RTMP（RTMP）] を選択すると、[タイプ（Type）] フィールドの代わりにこのフィールドが表示されます。

（注） ディテクタは、ユーザが入力する文字列が URL の完全なセクションであると想定します。たとえば、cisco.com と入力した場合、www.cisco.com/support や www.cisco.com と一致しますが、www.wearecisco.com とは一致しません。

ユーザ定義のアプリケーション フィールド

基本および高度なカスタムアプリケーションディテクタでユーザ定義のアプリケーションを設定するには、次のフィールドを使用します。

ビジネスとの関連性（Business Relevance）

アプリケーションが娯楽ではなく組織のビジネス活動のコンテキストで使用される可能性。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、または [非常に低い（Very Low）]。アプリケーションを最も的確に説明するオプションを選択します。

カテゴリ（Categories）

アプリケーションの最も重要な機能を説明する一般分類。

説明

アプリケーションの説明。

[名前（Name）]

アプリケーションの名前。

リスク（Risk）

アプリケーションが組織のセキュリティ ポリシーに対抗する目的で使用される可能性。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）] または [非常に低い（Very Low）]。アプリケーションを最も的確に説明するオプションを選択します。

タグ（Tags）

アプリケーションに関する追加情報を提供する 1 つ以上の事前定義されたタグ。アプリケーションを（アイデンティティ ルールで設定された）アクティブな認証から除外できるようにする場合は、User-Agent Exclusion タグをアプリケーションに追加する必要があります。

カスタム アプリケーション ディテクタの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

基本または高度なカスタム アプリケーション ディテクタを設定できます。

手順

ステップ 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）] を選択します。

ステップ 2 [カスタム ディテクタの作成（Create Custom Detector）] をクリックします。

ステップ 3 [名前（Name）] と [説明（Description）] を入力します。

ステップ 4 [アプリケーション プロトコル（Application Protocol）] を選択します。次の選択肢があります。

- 既存のアプリケーションプロトコルのディテクタを作成する場合（たとえば、非標準ポートで特定のアプリケーション プロトコルを検出する場合）、ドロップダウン リストからアプリケーション プロトコルを選択します。
- ユーザ定義アプリケーションのディテクタを作成する場合は、ユーザ定義のアプリケーションの作成，（1519 ページ）に示されている手順に従います。

ステップ 5 [ディテクタ タイプ（Detector Type）] を選択します。

ステップ 6 [OK] をクリックします。

ステップ 7 [検出パターン（Detection Patterns）] または [検出基準（Detection Criteria）] を設定します。

- 基本ディテクタを設定する場合は、基本ディテクタでの検出パターンの指定，（1520ページ）の説明に従って、プリセットした [検出パターン（Detection Patterns）] を指定します。
- 高度なディテクタを設定する場合は、高度なディテクタでの検出条件の指定，（1521 ページ）の説明に従って、カスタム [検出基準（Detection Criteria）] を指定します。

  注意 高度なカスタム ディテクタは複雑で、有効な .lua ファイルを作成すること以外の知識も必要になります。ディテクタを誤って設定すると、パフォーマンスや検出機能にマイナスの影響を与える可能性があります。

ステップ 8 高度なディテクタを設定する場合は、カスタム アプリケーション プロトコル ディテクタのテスト，（1523 ページ）の説明に従って、[パケット キャプチャ（Packet Captures）] を使用して新しいディテクタをテストします。基本ディテクタを設定する場合は、この手順を省略できます。

ステップ 9 [保存（Save）] をクリックします。

（注） アクセス コントロール ルールにアプリケーションを含めると、ディテクタは自動的にアクティブにされ、使用中は非アクティブにできません。

次の作業

- ディテクタのアクティブおよび非アクティブの設定, （1527ページ）の説明に従ってディテクタをアクティブにします。

関連トピック

カスタムアプリケーションディテクタおよびユーザ定義アプリケーション フィールド, （1514ページ）

ユーザ定義のアプリケーションの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

ここで作成するアプリケーション、カテゴリ、およびタグは、アクセス コントロール ルールやアプリケーション フィルタ オブジェクト マネージャで使用できます。

はじめる前に

- カスタムアプリケーションディテクタの設定, （1518ページ）の説明に従って、カスタムアプリケーション プロトコル ディテクタの設定を開始します。

手順

ステップ 1 [ディテクタの作成（Create Detector）] ページで、[追加（Add）] をクリックします。

ステップ 2 [名前（Name）] を入力します。

ステップ 3 [説明（Description）] を入力します。

ステップ 4 [ビジネスとの関連性（Business Relevance）] を選択します。

ステップ 5 [リスク（Risk）] を選択します。

ステップ 6 [カテゴリ（Categories）] の横にある [追加（Add）] をクリックしてカテゴリを追加し、新しいカテゴリの名前を入力するか、または [カテゴリ（Categories）] ドロップダウン リストから既存のカテゴリを選択します。

ステップ 7 オプションで、[タグ（Tags）] の横にある [追加（Add）] をクリックしてタグを追加し、新しいタグの名前を入力するか、または [タグ（Tags）] ドロップダウン リストから既存のタグを選択します。

ステップ 8 [OK] をクリックします。

次の作業

- カスタムアプリケーションディテクタの設定, （1518ページ）の説明に従って、カスタムアプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

関連トピック

カスタムアプリケーションディテクタおよびユーザ定義アプリケーションフィールド, （1514ページ）

基本ディテクタでの検出パターンの指定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

アプリケーションプロトコルのパケットヘッダーで特定のパターン文字列を検索するよう、カスタム アプリケーション プロトコル ディテクタを設定できます。また、複数のパターンを検索するようにディテクタを設定することもできます。この場合は、アプリケーション プロトコルのトラフィックは、アプリケーション プロトコルを確実に識別するため、ディテクタのすべてのパターンとマッチングさせる必要があります。

アプリケーションプロトコルディテクタは、オフセットを使用してASCIIまたは16進数のパターンを検索できます。

はじめる前に

- カスタムアプリケーションディテクタの設定, （1518ページ）の説明に従って、カスタムアプリケーション プロトコル ディテクタの設定を開始します。

手順

ステップ 1 [ディテクタの作成（Create Detector）] ページの [検出パターン（Detection Patterns）] セクションで、[追加（Add）] をクリックします。

ステップ 2 ディテクタの検査対象とするトラフィックの [プロトコル（Protocol）] を選択します。

ステップ 3 ユーザが検出するパターン [タイプ（Type）] を指定します。

ステップ 4 指定した [タイプ（Type）] に一致する [パターン文字列（Pattern String）] を入力します。

ステップ 5 オプションで、[オフセット（Offset）] を入力します（バイト単位）。

ステップ 6 オプションで、使用するポートに基づいてアプリケーション プロトコルのトラフィックを指定するには、1 から 65535 までのポートを [ポート（Port(s)）] フィールドに入力します。複数のポートを使用する場合は、カンマで区切ります。

ステップ 7 オプションで、[クライアント（Client）] または [サーバ（Server）] のいずれかの [方向（Direction）] を選択します。

ステップ 8 [OK] をクリックします。

ヒント パターンを削除する場合、削除するパターンの横の削除アイコン（）をクリックします。

次の作業

- カスタムアプリケーションディテクタの設定, （1518ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

関連トピック

高度なディテクタでの検出条件の指定, （1521 ページ）

高度なディテクタでの検出条件の指定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

注意 高度なカスタム ディテクタは複雑で、有効な .lua ファイルを作成すること以外の知識も必要になります。ディテクタを誤って設定すると、パフォーマンスや検出機能にマイナスの影響を与える可能性があります。

注意 信頼できないソースから .lua ファイルをアップロードしないでください。

カスタム .lua ファイルには、カスタム アプリケーションのディテクタ設定を含めます。カスタム .lua ファイルを作成するには、lua プログラミング言語に関する高度な知識とシスコの C-lua API に関する経験が求められます。以下を使用して、.lua ファイルを準備することを強くお勧めします。

- lua プログラミング言語に関するサードパーティの説明書と参考資料
- オープン ソース ディテクタ開発者ガイド： https://www.snort.org/downloads
- OpenAppID Snort コミュニティ リソース： http://blog.snort.org/search/label/openappid

（注） システムは、システム コールまたはファイル I/O を参照する .lua ファイルをサポートしていません。

はじめる前に

- カスタムアプリケーションディテクタの設定，（1518ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を開始します。
- 該当する .lua ファイルをダウンロードし、内容を調べることによって、有効な .lua ファイルを作成する準備を進めます。ディテクタ ファイルのダウンロードの詳細については、ディテクタ詳細の表示またはダウンロード，（1524 ページ）を参照してください。
- カスタム アプリケーションのディテクタ設定を含む有効な .lua ファイルを作成します。

手順

ステップ 1 高度なカスタム アプリケーション ディテクタの [ディテクタの作成（Create Detector）] ページにある [検出条件（Detection Criteria）] セクションで、[追加（Add）] をクリックします。

ステップ 2 [参照...（Browse...）] をクリックして、.lua ファイルに移動し、アップロードします。

ステップ 3 [OK] をクリックします。

次の作業

- カスタムアプリケーションディテクタの設定，（1518ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

関連トピック

基本ディテクタでの検出パターンの指定, （1520 ページ）

カスタム アプリケーション プロトコル ディテクタのテスト

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

検出するアプリケーション プロトコルからのトラフィックを持つパケットが格納されたパケットキャプチャ（pcap）ファイルが存在する場合、その pcap ファイルに対してカスタム アプリケーションプロトコルディテクタをテストできます。シスコでは、不要なトラフィックのない単純でクリーンな pcap ファイルを使用することをお勧めします。

pcap ファイルは 256 KB 以下でなければなりません。それより大きい pcap ファイルに対してディテクタのテストを試行すると、Firepower Management Center は自動的にファイルを切り捨て、不完全なファイルをテストします。ディテクタをテストするためにファイルを使用する前に、pcap の未解決のチェックサムを修正する必要があります。

はじめる前に

- カスタムアプリケーションディテクタの設定, （1518ページ）の説明に従って、カスタムアプリケーション プロトコル ディテクタを設定します。

手順

ステップ 1 [ディテクタの作成（Create Detector）]ページの [パケット キャプチャ（Packet Captures）] セクションで、[追加（Add）] をクリックします。

ステップ 2 ポップアップ ウィンドウで pcap ファイルを参照し、[OK] をクリックします。

ステップ 3 pcap ファイルの内容に対してディテクタをテストするには、pcap ファイルの横にある評価アイコンをクリックします。メッセージに、テストが成功したかどうかが示されます。

ステップ 4 必要に応じて手順 1 ～ 3 を繰り返し、その他の pcap ファイルに対してディテクタをテストします。

ヒント pcap ファイルを削除するには、削除するファイルの横の削除アイコン（）をクリックします。

次の作業

- カスタムアプリケーションディテクタの設定, （1518ページ）の説明に従って、カスタムアプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するために

システムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

ディテクタ詳細の表示またはダウンロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

ディテクタ リストを使用して、アプリケーション ディテクタの詳細を表示（すべてのディテクタ）したり、ディテクタの詳細をダウンロード（カスタムアプリケーションディテクタのみ）したりできます。

手順

ステップ 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）] を選択します。

ステップ 2 ディテクタの詳細を表示するには、情報アイコン（）をクリックして、概要：アプリケーション検出, （1507 ページ）で説明されているリスク、ビジネスとの関連性、タグ、カテゴリを表示します。

ステップ 3 カスタムアプリケーションディテクタのディテクタ詳細をダウンロードするには、ダウンロードアイコン（）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ディテクタ リストのソート

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

[ディテクタ（Detectors）] ページには、デフォルトで名前のアルファベット順にディテクタがリストされます。列見出しの横にある上または下矢印は、ページがその列でその方向にソートされていることを示します。

手順

ステップ 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）] を選択します。

ステップ 2 該当する列見出しをクリックします。

検出機能リストのフィルタリング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

手順

ステップ 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）] を選択します。

ステップ 2 ディテクタ リストのフィルタ グループ, （1525 ページ）に記載されているフィルタ グループの 1 つを展開し、フィルタの横にあるチェックボックスを選択します。グループ内のすべてのフィルタを選択するには、グループ名を右クリックし、[すべて選択（Check All）] を選択します。

ステップ 3 あるフィルタを削除するには、[フィルタ（Filters）] フィールドにあるフィルタの名前の削除アイコン（✖）をクリックするか、フィルタ リストでフィルタを無効にします。グループ内のすべてのフィルタを削除するには、グループ名を右クリックし、[すべて選択解除（Uncheck All）] を選択します。

ステップ 4 すべてのフィルタを削除するには、検出機能に適用されるフィルタ リストの横の [すべてクリア（Clear all）] をクリックします。

ディテクタ リストのフィルタ グループ

複数のフィルタ グループを別個にまたは組み合わせて使用し、ディテクタのリストをフィルタリングすることができます。

[名前（Name）]

ユーザが入力した文字列を含む名前または説明でディテクタを検索します。文字列には任意の英数字または特殊文字を含めることができます。

カスタム フィルタ（Custom Filter）

オブジェクト管理ページで作成したカスタムアプリケーションフィルタに一致するディテクタを検索します。

作成者（Author）

ディテクタを作成したユーザに照らしてディテクタを検索します。次によってディテクタをフィルタリングできます。

- カスタム ディテクタを作成またはインポートした個々のユーザ
- シスコ。これは、個別にインポートされたアドオンディテクタを除く、シスコが提供するすべてのディテクタを表します（ディテクタをインポートした場合、そのユーザはそのディテクタの作成者になります）。
- 任意のユーザ（Any User）。これは、によって提供されたのではないすべてのディテクタを表します。

状態（State）

状態（つまり、アクティブまたは非アクティブ）に照らしてディテクタを検索します。

タイプ（Type）

アプリケーション ディテクタの基本, （1509 ページ）に示すように、ディテクタ タイプに従ってディテクタを検索します。

プロトコル

ディテクタが検査するトラフィック プロトコルに照らしてディテクタを検索します。

カテゴリ（Category）

検出するアプリケーションに割り当てられたカテゴリに照らしてディテクタを検索します。

タグ

検出するアプリケーションに割り当てられたタグに照らしてディテクタを検索します。

リスク

検出するアプリケーションに割り当てられたリスク（[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、[非常に低い（Very Low）]）に照らしてディテクタを検索します。

ビジネスとの関連性（Business Relevance）

検出するアプリケーションに割り当てられたビジネスとの関連性（[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、[非常に低い（Very Low）]）に照らしてディテクタを検索します。

別のディテクタ ページへの移動

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

手順

ステップ 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）] を選択します。

ステップ 2 次のページを表示するには、右下矢印アイコン（ ）をクリックします。

ステップ 3 前のページを表示するには、左矢印のアイコン（ ）をクリックします。

ステップ 4 別のページを表示するには、ページ番号を入力して、Enter キーを押します。

ステップ 5 最後のページに移動するには、右矢印アイコン（ ）をクリックします。

ステップ 6 最初のページに移動するには、左矢印アイコン（ ）をクリックします。

ディテクタのアクティブおよび非アクティブの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

ネットワーク トラフィックを分析するためにディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があります。デフォルトでは、Ciscoが提供するすべてのディテクタはアクティブにされています。

システムの検出機能を補完するために、ポートごとに複数のアプリケーション ディテクタをアクティブにすることができます。

ポリシーのアクセスコントロールルールにアプリケーションを含め、そのポリシーを導入するときに、そのアプリケーションに対してアクティブなディテクタがない場合、1 つ以上のディテクタが自動的にアクティブになります。同様に、導入されているポリシーのアプリケーションが使用されているときに、そのアプリケーションのアクティブなディテクタをすべて非アクティブにしようとしても、ディテクタを非アクティブにすることはできません。

ヒント パフォーマンスを向上させるために、使用する予定のないアプリケーション プロトコル、クライアント、または Web アプリケーションのディテクタはすべて非アクティブにします。

手順

ステップ 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）] を選択します。

ステップ 2 アクティブまたは非アクティブにするディテクタの横にあるスライダをクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

（注） 一部のアプリケーション ディテクタはその他のディテクタによって必要とされることに注意してください。そのようなディテクタのいずれかを非アクティブにすると、それに依存するディテクタも無効となることを示す警告が表示されます。

カスタム アプリケーション ディテクタの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

カスタム アプリケーション ディテクタを変更するには、次の手順を使用します。

手順

ステップ 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）] を選択します。

ステップ 2 変更するディテクタの横にある編集アイコン（  ）をクリックします。代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 カスタム アプリケーション ディテクタの設定, （1518 ページ）の説明に従って、ディテクタを変更します。

ステップ 4 ディテクタの状態に応じて、次の保存オプションがあります。

- 非アクティブなディテクタを保存するには、[保存（Save）] をクリックします。
- 非アクティブなディテクタを新規の非アクティブなディテクタとして保存するには、[新規保存（Save as New）] をクリックします。
- アクティブなディテクタを保存してすぐに使用を開始するには、[保存して再アクティブ化（Save and Reactivate）] をクリックします。

- アクティブなディテクタを新規の非アクティブなディテクタとして保存するには、[新規保存（Save as New）] をクリックします。

ディテクタの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

カスタム ディテクタおよび Cisco Professional サービスが提供する個別にインポートされたアドオン ディテクタを削除することができます。その他の Cisco が提供するディテクタを削除することはできませんが、その多くを非アクティブにすることはできます。

（注） ディテクタが展開されたポリシーで使用されている間は、そのディテクタを削除できません。

手順

ステップ 1 [ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）] を選択します。

ステップ 2 削除するディテクタの横にある削除アイコン（）をクリックします。代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [OK] をクリックします。

第 66 章

ユーザ アイデンティティ ソース

以下のトピックでは、Firepower システムのユーザ アイデンティティ ソースについて説明します。

ユーザ アイデンティティ ソースについて

次の表に、Firepower システムでサポートされているユーザ アイデンティティ ソースの概要を示します。

ユーザ アイデンティティ ソース	ポリシー	サーバ要件	ソース タイプ	認証タイプ（Authentication Type）	ユーザ認識	ユーザ制御	詳細
ユーザ エージェント	ID	Microsoft Active Directory	権限のあるログイン	パッシブ	Yes	Yes	ユーザ エージェントのアイデンティティ ソース，（1533 ページ）

ユーザ アイデンティティ ソース	ポリシー	サーバ要件	ソース タイプ	認証タイプ（Authentication Type）	ユーザ認識	ユーザ制御	詳細
ISE	ID	Microsoft Active Directory	権限のあるログイン	パッシブ	Yes	Yes	ISE アイデンティティ ソース, （1535 ページ）
キャプティブ ポータル	ID	LDAP または Microsoft Active Directory	権限のあるログイン	active	Yes	Yes	キャプティブ ポータルのアイデンティティ ソース, （1540 ページ）
トラフィック ベースの検出	ネットワーク検出	適用対象外	権限のないログイン	適用対象外	Yes	No	トラフィック ベース検出のアイデンティティ ソース, （1546 ページ）

展開するアイデンティティ ソースを選択する際には、以下を検討してください。

- 非 LDAP ユーザ ログインを検出するにはトラフィック ベースの検出を使用する必要があります。たとえば、ユーザ エージェントのみを使用してユーザ アクティビティを検出している場合は、非 LDAP ログインを制限しても効果はありません。
- 失敗したログインまたは認証アクティビティを記録するには、トラフィック ベースの検出またはキャプティブ ポータルを使用する必要があります。失敗したログインまたは認証試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。
- キャプティブ ポータルを使用するには、センシング インターフェイス（仮想ルータなど）に IP アドレスがあるアプライアンスを展開する必要があります。

これらのアイデンティティ ソースからのデータは、Firepower Management Center のユーザ データベースとユーザ アクティビティ データベースに格納されます。Firepower Management Center サーバ ユーザ ダウンロードを設定して、新しいユーザ データがデータベースに自動的かつ定期的にダウンロードされるようにできます。

Firepower システムでのユーザ検出の詳細については、ユーザ検出の基本, （1445 ページ）を参照してください。

ユーザ エージェントのアイデンティティ ソース

ユーザエージェントは、パッシブ認証方法で、信頼できるアイデンティティ ソース（つまり、信頼された Active Directory サーバでユーザ情報が提供されます）でもあります。ユーザ エージェントは、Firepower システムと統合されると、ユーザが Active Directory クレデンシャルでホストにログインする、またはホストからログアウトするときに、そのユーザをモニタします。ユーザ エージェントから取得されたデータは、ユーザ認識とユーザ制御に使用できます。

ユーザエージェントは、各ユーザを IP アドレスと関連付けます。これにより、ユーザ条件を使用するアクセス コントロール ルールをトリガーすることができます。1 つのユーザ エージェントを使用して、最大 5 つの Active Directory サーバでユーザ アクティビティをモニタでき、最大 5 つの Firepower Management Center に暗号化データを送信できます。

ユーザ エージェントは失敗したログイン試行を報告しません。

ユーザ エージェントは、以下を含む段階的な設定が必要です。

- ユーザ エージェントがインストールされている少なくとも 1 台のコンピュータ 。
- ユーザ エージェントがインストールされたコンピュータまたは Active Directory サーバと Firepower Management Center との間の接続。
- ユーザ エージェントからユーザ データを受け取る各 Firepower Management Center で設定されたアイデンティティ レルム。

段階的なユーザ エージェントの設定とサーバの要件の詳細については、『*Firepower* ユーザ エージェント構成ガイド』を参照してください。

（注） コンピュータまたは Active Directory サーバの時間が Firepower Management Center の時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。

Firepower Management Center接続は、ログインとログオフがユーザ エージェントによって検出されたユーザのメタデータを取得可能にするだけでなく、アクセス コントロール ルール内で使用するユーザとグループを指定するためにも使用されます。ユーザ エージェントが特定のユーザ名を除外するように設定されている場合は、そのようなユーザ名のログイン データは Firepower Management Center に報告されません。ユーザ エージェントのデータは、Firepower Management Center のユーザ データベースとユーザ アクティビティ データベースに保存されます。

（注） ユーザ エージェントは $ 記号で終わる Active Directory ユーザ名を Firepower Management Center に送信できません。これらのユーザをモニタする場合は、最後の $ の文字を削除する必要があります。

複数のユーザがリモート セッションを使用してホストにログインしている場合は、エージェントがそのホストからのログインを正確に検出しない場合があります。これを防ぐ方法の詳細については、『*Firepower* ユーザ エージェント構成ガイド』を参照してください。

ユーザ エージェント接続の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバルだけ	Admin/Access Admin/Network Admin

ユーザ エージェントの詳細については、ユーザ エージェントのアイデンティティ ソース, （1533 ページ） を参照してください。

はじめる前に

- ユーザ エージェント データを使用してユーザ制御を実行する場合は、レルムの作成, （1586 ページ）の説明に従ってユーザ エージェント接続用の Active Directory レルムを設定して有効にします。

手順

ステップ 1 [システム（System）] > [統合（Integration）] をクリックします。

ステップ 2 [アイデンティティの送信元（Identity Sources）] タブをクリックします。

ステップ 3 [サービス タイプ（Service Type）] に [ユーザ エージェント（User Agent）] をクリックし、ユーザ エージェント接続を有効にします。

（注） 接続を無効にするには、[なし（None）] をクリックします。

ステップ 4 [新規エージェント（New Agent）] をクリックして新しいエージェントを追加します。

ステップ 5 エージェントをインストールするコンピュータの [ホスト名（Hostname）] または [アドレス（Address）] を入力します。IPv4 アドレスを使用する必要があります。IPv6 アドレスを使用してユーザ エージェントに接続するように Firepower Management Center を設定することはできません。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 接続を削除するには、削除アイコン（  ）をクリックして、その削除を確認します。

次の作業

- *Firepower* ユーザ エージェント構成ガイド の説明に従って、ユーザ エージェントの設定を続けます。
- アイデンティティ ルールの作成, （1595 ページ）の説明に従ってアイデンティティ ルールを設定します。

- アイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けます（アクセス制御への他のポリシーの関連付け，（798 ページ） を参照）。

関連トピック

ユーザ エージェント アイデンティティ ソースのトラブルシューティング，（1535 ページ）
アクセス コントロール ポリシーの開始，（779 ページ）

ユーザ エージェント アイデンティティ ソースのトラブルシューティング

ユーザエージェント接続に問題が起こった場合は、*Firepower* ユーザ エージェント構成ガイド を確認してください。

このガイドの関連するトラブルシューティング情報については、レルムとユーザのダウンロードのトラブルシューティング，（1583 ページ）とユーザ制御のトラブルシューティング，（367 ページ）を参照してください。

ユーザエージェントによって報告されるユーザデータに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにないユーザ エージェント ユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。ユーザのアクティビティは、システムがユーザのダウンロードでユーザに関する情報の取得に成功するまでルールで処理されず、Web インターフェイスに表示されません。

ISE アイデンティティ ソース

Cisco Identity Services Engine（ISE）の展開を Firepower システムと統合して、ISE をパッシブ認証に使用できます。

ISE は、信頼できるアイデンティティ ソースで、Active Directory（AD）、LDAP、RADIUS、または RSA を使用して認証するユーザに関するユーザ認識データを提供します。さらに、Active Directory ユーザのユーザ制御を行えます。ISE は、ISE ゲスト サービス ユーザの失敗したログイン試行またはアクティビティは報告しません。

（注） Firepower は、マシンの認証をユーザと関連付けないため、AD 認証と同時に 802.1x マシン認証を使用することはできません。802.1x アクティブ ログインを使用する場合は、802.1x アクティブ ログイン（マシンとユーザの両方）だけを報告するように ISE を設定します。このように設定すれば、マシン ログインはシステムに 1 回だけ報告されます。

Cisco ISE の詳細については、*Cisco Identity Services Engine Administrator Guide*を参照してください。

ISE バージョンと設定の互換性

ご使用の ISE バージョンと設定は、次のように Firepower との統合や相互作用に影響を与えます。

- ISE サーバと Firepower Management Center の時刻を同期します。そうしないと、システムが予期しない間隔でユーザのタイムアウトを実行する可能性があります。
- 多数のユーザ グループをモニタするように ISE を設定した場合、システムはメモリ制限のためにグループに基づいてユーザ マッピングをドロップすることがあります。その結果、レルムまたはユーザ条件を使用するルールが想定どおりに実行されない可能性があります。
- ISE のバージョン 1.3 には、IPv6 対応エンドポイントのサポートが含まれていません。ISE のこのバージョンを実行している場合、ユーザ アイデンティティ データを収集したり、IPv6 対応エンドポイント上で修正を実行したりすることはできません。

システムのこのバージョンと互換性がある特定のバージョンの ISE については、『*Cisco Firepower Compatibility Guide*』を参照してください。

ISE 属性

ISE 接続を設定すると、ISE 属性データが Firepower Management Center データベースに入力されます。ユーザ認識とユーザ制御に使用できる ISE 属性は、次のとおりです。

セキュリティ グループ タグ（SGT）（Security Group Tag (SGT)）

セキュリティ グループ タグ（SGT）は、信頼ネットワーク内のトラフィックの送信元の権限を指定します。Cisco ISE および Cisco TrustSec は、ネットワークに入るときに、セキュリティ グループ アクセス（SGA）と呼ばれる機能を使用して、パケットに SGT 属性を適用します。これらの SGT は、ISE または TrustSec 内のユーザの割り当てられたセキュリティ グループに対応します。ID ソースとして ISE を設定すると、Firepower システムは、これらの SGT を使用してトラフィックをフィルタリングできます。

エンドポイント ロケーション（Endpoint Location）（またはロケーション IP（Location IP））

[エンドポイント ロケーション（Endpoint Location）] 属性は、ISE によって識別される、ユーザの認証に ISE を使用したネットワーク デバイスの IP アドレスです。

エンドポイント プロファイル（Endpoint Profile）（またはデバイス タイプ（Device Type））

[エンドポイント プロファイル（Endpoint Profile）] 属性は、ISE によって識別されるユーザのエンドポイント デバイス タイプです。

ISE 接続の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバルだけ	Admin/Access Admin/Network Admin

詳細については、ISE アイデンティティ ソース, （1535 ページ）およびISE 設定フィールド, （1538 ページ）を参照してください。

はじめる前に

- Firepower Management Center のアクセス元となるマシンでPKI オブジェクトするか、証明書データとキーを利用可能にします。
- ISE データを使用してユーザ制御を実装する予定の場合、レルムの作成, （1586 ページ）の説明に従って、pxGrid のペルソナを想定して ISE サーバのレルムを設定し有効にします。

手順

ステップ 1 [システム（System）] > [統合（Integration）] をクリックします。

ステップ 2 [アイデンティティの送信元（Identity Sources）] タブをクリックします。

ステップ 3 [サービス タイプ（Service Type）] で [Identity Services Engine] をクリックし、ISE 接続を有効にします。

（注） 接続を無効にするには、[なし（None）] をクリックします。

ステップ 4 [プライマリ ホスト名/IP アドレス（Primary Host Name/IP Address）]、およびオプションで [セカンダリ ホスト名/IP アドレス（Secondary Host Name/IP Address）] を入力します。

ステップ 5 [pxGrid サーバ CA（pxGrid Server CA）] および [MNT サーバ CA（MNT Server CA）] リストから該当する認証局を、[FMC サーバ証明書（FMC Server Certificate）] リストから適切な証明書をそれぞれクリックします。また、追加アイコン（  ）をクリックして証明書を追加することもできます。

（注） [FMC サーバ証明書（FMC Server Certificate）] には、clientAuth 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。

ステップ 6 （オプション）CIDR ブロック表記を使用して [ISE ネットワーク フィルタ（ISE Network Filter）] を入力します。

ステップ 7 接続をテストするには、[テスト（Test）] をクリックします。

次の作業

- アイデンティティ ルールを作成します（アイデンティティ ルールの作成, （1595 ページ） を参照）。
- アイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けます（アクセス制御への他のポリシーの関連付け, （798 ページ） を参照）。

関連トピック

キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング, （1546 ページ）
信頼できる認証局オブジェクト, （447 ページ）

内部証明書オブジェクト，（452 ページ）

ISE 設定フィールド

次のフィールドを使用して ISE への接続を設定します。

プライマリおよびセカンダリ ホスト名/IP アドレス（Primary and Secondary Host Name/IP Address）

プライマリ（およびオプションでセカンダリ）ISE サーバのホスト名または IP アドレス。

pxGrid サーバ CA（pxGrid Server CA）

pxGrid フレームワークの認証局。展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

MNT サーバ CA（MNT Server CA）

一括ダウンロード実行時の ISE 証明書の認証局。展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

FMC サーバ証明書（FMC Server Certificate）

ISE への接続時、または一括ダウンロードの実行時に Firepower Management Center が ISE に提供する必要がある証明書およびキー。

（注） [FMC サーバ証明書（FMC Server Certificate）] には、clientAuth 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。

ISE ネットワーク フィルタ（ISE Network Filter）

オプションのフィルタで、ISE が Firepower Management Center にレポートするデータを制限するために設定できます。ネットワーク フィルタを指定する場合、ISE はそのフィルタ内のネットワークからデータをレポートします。次の方法でフィルタを指定できます。

- 任意（Any）のフィルタを指定する場合はフィールドを空白のままにします。
- CIDR 表記を使用して単一の IPv4 アドレス ブロックを入力します。
- CIDR 表記を使用して IPv4 アドレス ブロックのリストをカンマで区切って入力します。

（注） このバージョンの FirePOWER システムは、ISE のバージョンに関係なく、IPv6 アドレスを使用したフィルタリングをサポートしません。

関連トピック

信頼できる認証局オブジェクト，（447 ページ）
内部証明書オブジェクト，（452 ページ）

ISE アイデンティティ ソースのトラブルシューティング

関連の他のトラブルシューティングについては、レルムとユーザのダウンロードのトラブルシューティング，（1583 ページ）およびユーザ制御のトラブルシューティング，（367 ページ）を参照してください。

ISE 接続に問題が起こった場合は、次のことを確認してください。

- ISE と Firepower システムを正常に統合するには、ISE 内の pxGrid アイデンティティ マッピング機能を有効にする必要があります。
- [FMC サーバ証明書（FMC Server Certificate）] には、[clientAuth] 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。
- ISE サーバの時刻は、Firepower Management Center の時刻と同期している必要があります。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。
- 展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。
- 展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

ISE によって報告されるユーザ データに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにない ISE ユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。ISE ユーザから見えるアクティビティは、システムがユーザのダウンロードで情報の取得に成功するまでアクセス コントロール ルールで**処理されず**、Web インターフェイスに**表示されません**。
- LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE ユーザに対するユーザ制御は実行できません。
- Firepower Management Center は、ISE ゲスト サービス ユーザのユーザ データを受信できません。
- 使用する ISE バージョンと構成は、Firepower システムでの ISE の使用方法に影響を与えます。詳細については、ISE アイデンティティ ソース，（1535 ページ）を参照してください。
-

サポートされている機能に問題がある場合は、ISE アイデンティティ ソース，（1535 ページ）で詳細を参照してバージョンの互換性を確認してください。

キャプティブ ポータルのアイデンティティ ソース

キャプティブ ポータルは、Firepowerシステムでサポートされる権限のあるアイデンティティ ソースの1つです。これはFirepowerシステムでサポートされる唯一のアクティブな認証方式であり、ユーザは管理対象デバイスを使用してネットワークに対する認証を行うことができます。

通常、キャプティブ ポータルを使用して、インターネットにアクセスするため、または制限されている内部リソースにアクセスするための認証を要求します。必要に応じて、リソースへのゲストアクセスを設定することができます。システムはキャプティブ ポータル ユーザを認証した後、それらのユーザのトラフィックをアクセス制御ルールに従って処理します。キャプティブ ポータルは、HTTP および HTTPS のトラフィックのみで認証を行います。

（注） キャプティブ ポータルが認証を実行する前に、HTTPS トラフィックを復号化する必要があります。

キャプティブ ポータルはまた、失敗した認証の試行を記録します。失敗した試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。キャプティブ ポータルで報告される失敗した認証アクティビティのユーザ アクティビティ タイプは[認証失敗ユーザ（Failed Auth User）] です。

キャプティブ ポータルから取得された認証データはユーザ認識とユーザ制御に使用できます。

アイデンティティ ポリシーでキャプティブ ポータルを設定して展開すると、指定されたレルムのユーザは以下のデバイスを介して認証を行ってからネットワークにアクセスします。

- 7000 および 8000 シリーズ デバイス上の仮想ルータ
- バージョン 9.5(2) 以降で稼働するルーテッド モードの ASA FirePOWER デバイス

アイデンティティ ポリシーのキャプティブ ポータルを設定し、アイデンティティ ルールのアクティブ認証を呼び出します。アイデンティティ ポリシーはアクセス コントロール ポリシーで呼び出されます。詳細については、キャプティブ ポータル アイデンティティ ルールの設定, （1541 ページ）を参照してください。

キャプティブ ポータル アクティブ認証を実行できるのは、ルーテッド インターフェイスが設定されているデバイスのみです。アクセス コントロール ポリシーで参照されているアイデンティティ ポリシーに 1 つ以上のキャプティブ ポータルのアイデンティティ ルールが含まれ、以下を管理する Firepower Management Centerにポリシーを展開する場合、次のようになります。

- ルーテッドインターフェイスが設定されている1つ以上のデバイスの場合、ポリシー導入は成功し、ルーテッド インターフェイスがアクティブ認証を実行します。

  システムは ASA with FirePOWER デバイスでインターフェイス タイプを検証しません。ASA with FirePOWER デバイス上でインライン（タップ モード）インターフェイスにキャプティブ ポータル ポリシーを適用すると、ポリシーは正常に展開されますが、これらのルールに一致するトラフィック内のユーザは「不明」と識別されます。

- 1 つ以上の NGIPSv デバイスの場合、ポリシー導入は失敗します。

以下の要件と制約事項に注意してください。

- システムがサポートするキャプティブ ポータル ログインの数は 1 秒あたり最大 20 です。
- キャプティブ ポータルに使用する予定のデバイスの IP アドレスおよびポートを宛先とするトラフィックを許可する必要があります。アクセス制御で宛先が許可されない場合、キャプティブ ポータルを使用してトラフィックを認証することはできません。
- キャプティブ ポータル アクティブ認証を HTTPS トラフィックで行う場合、SSL ポリシーを使用して、認証対象のユーザからのトラフィックを復号する必要があります。キャプティブ ポータル ユーザの Web ブラウザと管理対象デバイス上のキャプティブ ポータル デーモンとの間の接続では、トラフィックを復号できません。この接続は、キャプティブ ポータル ユーザの認証に使用されます。

関連トピック

キャプティブ ポータル アイデンティティ ルールの設定, （1541 ページ）

キャプティブ ポータル アイデンティティ ルールの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（NGIPSv を除く）	任意（Any）	Administrator/Access Admin/Network Admin

キャプティブ ポータルのいくつかのアイデンティティ ポリシー設定はアクセス コントロール ポリシーの [アクティブ認証（Active Authentication）] タブページで行い、残りの設定はアクセス コントロール ポリシーに関連付けられたアイデンティティ ルールで行います。

アクティブな認証ルールに [アクティブ認証（Active Authentication）] ルール アクションが含まれるか、[パッシブ認証でユーザを識別できない場合にアクティブ認証を使用（Use active authentication if passive authentication cannot identify user）] が選択された [パッシブ認証（Passive Authentication）] ルール アクションが含まれます。それぞれのケースで、システムは SSL 復号を透過的に有効化/無効化し、これにより Snort プロセスが再起動します。

キャプティブ ポータルの詳細については、キャプティブ ポータルのアイデンティティ ソース, （1540 ページ）およびキャプティブ ポータル フィールド, （1544 ページ）を参照してください。

注意 SSL 復号が無効の場合（つまりアクセス コントロール ポリシーに SSL ポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

はじめる前に

- ルーテッド インターフェイスが設定された 1 つ以上のデバイスが、 Firepower Management Center によって管理されていることを確認します。

  Firepower Management Center で ASA with FirePOWER デバイスを管理している場合には、キャプティブ ポータルのアイデンティティ ソース, （1540 ページ） を参照してください。

- Firepower Management Center のアクセス元となるマシンでPKI オブジェクトするか、証明書データとキーを利用可能にします。

- HTTPS トラフィックでキャプティブ ポータルのアクティブ認証を実行するには、キャプティブ ポータルを使用して認証対象のユーザから送信されたトラフィックを復号する SSL ルールを作成する必要があります。

- （ルーテッド モードで ASA バージョン 9.5(2) 以降を実行する）ASA FirePOWER デバイスをキャプティブ ポータルに使用するには、**captive-portal** ASA CLI コマンドを使用してキャプティブ ポータルでのアクティブ認証を有効にし、『*ASA* ファイアウォール設定ガイド（バージョン 9.5(2) 以降）』（http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html [英語]）の説明に従ってポートを定義します。

手順

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

ステップ 2 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [ID（Identity）] をクリックし、アイデンティティ ポリシーを作成または編集します。代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 新しいアクセス コントロール ポリシーを作成する場合は、[保存（Save）] をクリックします。

ステップ 4 [ルールの追加（Add Rule）] をクリックして新しいキャプティブ ポータル アイデンティティ ポリシー ルールを追加するか、編集アイコン（  ）をクリックして既存のルールを編集します。

ステップ 5 [アクティブ認証（Active Authentication）] タブをクリックします。

ステップ 6 リストから適切な [サーバ証明書（Server Certificate）] を選択するか、追加アイコン（  ）をクリックして証明書を追加します。

ステップ 7 [ポート（Port）] を入力して、[最大ログイン試行回数（Maximum login attempts）] を指定します。（デフォルトで、キャプティブ ポータルはポート 885 を使用します。）

ステップ 8 （オプション）キャプティブ ポータル応答ページの設定, （1545 ページ） の説明に従って、[アクティブ認証応答ページ（Active Authentication Response Page）] を選択します。

ステップ 9 [ルール（Rules）] タブをクリックします。

ステップ 10 [レルムおよび設定（Realm & Settings）] タブをクリックします。

ステップ 11 （オプション）[認証でユーザを識別できない場合はゲストとして識別する（Identify as Guest if authentication cannot identify user）] をオンにします。詳細については、キャプティブ ポータル フィールド, （1544 ページ）を参照してください。

ステップ 12 リストから [認証タイプ（Authentication Type）] を 1 つクリックします。

ステップ 13 （オプション）[HTTP ユーザ エージェントの除外（Exclude HTTP User-Agents）] をクリックし、キャプティブ ポータルからのアプリケーションの除外 の説明に従って特定のアプリケーション トラフィックをキャプティブ ポータルから除外します。

ステップ 14 [追加（Add）] をクリックするか、ルールの編集を続けます。

ステップ 15 [保存（Save）] をクリックします。

次の作業

- ユーザ認証のためにキャプティブ ポータルで使用する SSL トラフィックを複合して再署名する SSL アクセス制御ルールを作成します。ルールのターゲットを [不明な（Unknown）] ユーザに設定し、ルールをアクセス コントロール ポリシーに関連付けます。詳細については、SSL ルールの使用を開始するには, （895 ページ）を参照してください。
- キャプティブ ポータル ポート（デフォルトでは TCP ポート 885）経由でトラフィックを許可するアクセス制御ルールを作成します。詳細については、次を参照してください。アクセス コントロール ルールの作成および編集, （807 ページ）

- アイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けます（アクセス制御への他のポリシーの関連付け，（798 ページ） を参照）。

関連トピック

キャプティブ ポータルからのアプリケーションの除外
内部証明書オブジェクト，（452 ページ）
キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング，（1546 ページ）
Snort® の再起動シナリオ，（324 ページ）

キャプティブ ポータル フィールド

次のフィールドを使用して、アイデンティティ ポリシーの[アクティブ認証（Active Authentication）]タブでキャプティブ ポータルを設定します。アイデンティティ ルール フィールド，（1597 ページ）も参照してください。

サーバ証明書（Server Certificate）

キャプティブ ポータル デーモンが示すサーバ証明書。

[ポート（Port）]

キャプティブ ポータル接続のために使用するポート番号。ASA FirePOWER デバイスをキャプティブ ポータルに使用しようとする場合は、このフィールドのポート番号が、**captive-portal** CLI コマンドを使用して ASA FirePOWER デバイスで設定したポート番号と一致していなければなりません。

最大ログイン試行回数（Maximum login attempts）

ユーザのログイン要求がシステムによって拒否されるまでに許容されるログイン試行失敗の最大数。

アクティブ認証回答ページ（Active Authentication Response Page）

キャプティブ ポータル ユーザに対して表示される、システム提供またはカスタムの HTTP 応答ページ。アイデンティティ ポリシーのアクティブ認証設定で[アクティブ認証応答ページ（Active Authentication Response Page）] を選択したら、[HTTP 応答ページ（TTP Response Page）] で 1 つ以上のアイデンティティ ルールを [認証タイプ（Authentication Type）] として設定する必要があります。

関連トピック

内部証明書オブジェクト，（452 ページ）

キャプティブ ポータル応答ページの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（NGIPSv を除く）	任意（Any）	Administrator/Access Admin/Network Admin

キャプティブ ポータル ユーザを表示するために、システム提供またはカスタムのいずれかの HTTP 応答ページを選択できます。

キャプティブ ポータルの詳細については、キャプティブ ポータルのアイデンティティ ソース, （1540 ページ）およびキャプティブ ポータル フィールド, （1544 ページ）を参照してください。

はじめる前に

- キャプティブ ポータル アイデンティティ ルールの設定, （1541 ページ）の説明に従ってキャプティブ ポータルの設定を開始します。

手順

ステップ 1 アイデンティティ ポリシーの [アクティブ認証（Active Authentication）] タブで、ドロップダウン メニューから [アクティブ認証応答ページ（Active Authentication Response Page）] を選択します。

- 汎用的な応答を使用する場合は、[システム提供（System-provided）] を選択します。表示アイコン（  ）をクリックすると、このページの HTML コードが表示されます。
- カスタム応答を作成する場合は、[カスタム...（Custom...）] を選択します。ポップアップ ウィンドウが表示されます。このウィンドウに事前入力されているシステムによって提供されるコードを置換または変更できます。完了したら、変更を保存します。カスタム ページは、編集アイコン（  ）をクリックすると編集できます。

ステップ 2 [保存（Save）] をクリックします。

次の作業

- キャプティブ ポータル アイデンティティ ルールの設定, （1541 ページ）の説明に従ってキャプティブ ポータルの設定を続けます。

キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング

関連の他のトラブルシューティングについては、レルムとユーザのダウンロードのトラブルシューティング, （1583 ページ）およびユーザ制御のトラブルシューティング, （367 ページ）を参照してください。

キャプティブ ポータルに関する問題が発生した場合は、次の点を確認してください。

- キャプティブ ポータル サーバの時刻は、Firepower Management Center の時刻と同期している必要があります。
-
- Firepower Management Center と管理対象デバイスとの間の接続に障害が発生した場合、ユーザが以前に認識され Firepower Management Center にダウンロードされた場合を除き、デバイスによって報告されたすべてのキャプティブ ポータル ログインはダウンタイム中に特定できません。識別されていないユーザは、Firepower Management Center で [不明（Unknown）] のユーザとして記録されます。ダウンタイム後、不明のユーザはアイデンティティ ポリシーのルールに従って再確認され、処理されます。
- キャプティブ ポータルに使用する予定のデバイスにインライン インターフェイスとルーテッド インターフェイスの両方が含まれる場合、キャプティブ ポータル デバイス上でルーテッド インターフェイスだけを対象とするようにキャプティブ ポータル アイデンティティ ルールでゾーン条件を設定する必要があります。
- システムは ASA with FirePOWER デバイスでインターフェイス タイプを検証しません。ASA with FirePOWER デバイス上でインライン（タップ モード）インターフェイスにキャプティブ ポータル ポリシーを適用すると、ポリシーは正常に展開されますが、これらのルールに一致するトラフィック内のユーザは「不明」と識別されます。

トラフィック ベース検出のアイデンティティ ソース

トラフィック ベース検出は、Firepower システムでサポートされている唯一の権限のないアイデンティティ ソースです。トラフィック ベース検出を設定すると、管理対象デバイスは、指定したネットワークでの LDAP、AIM、POP3、IMAP、Oracle、SIP（VoIP）、FTP、HTTP、MDNS、SMTP のログインを検出します。トラフィック ベースの検出から取得されたデータは、ユーザ認識にのみ使用できます。権威のあるアイデンティティ ソースとは異なり、トラフィック ベースの検出はネットワーク検出ポリシーで設定します。トラフィック ベースのユーザ検出の設定, （1563 ページ）を参照してください。

次の制限事項に注意してください。

- トラフィック ベースの検出では、LDAP 接続に対する Kerberos ログインのみを LDAP 認証として解釈します。また、管理対象デバイスは、SSL や TLS などのプロトコルを使用して暗号化された LDAP 認証を検出できません。
- トラフィック ベースの検出では OSCAR プロトコルを使用した AIM ログインだけを検出します。TOC2 を使用する AIM ログインは検出できません。

- トラフィック ベースの検出ではSMTP ロギングを制限することができません。これは、ユーザがSMTP ログインに基づいてデータベースに追加されていないためです。システムがSMTP ログインを検出しても、一致する電子メールアドレスのユーザがデータベース内に存在しなければ、そのログインは記録されません。

トラフィック ベースの検出は、失敗したログイン試行も記録します。失敗ログイン試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。トラフィック ベースの検出により検出された失敗ログイン アクティビティのユーザ アクティビティ タイプは [失敗したユーザ ログイン（Failed User Login）] です。

（注） システムは失敗した HTTP ログインと成功した HTTP ログインを区別できません。HTTP ユーザ情報を表示するには、トラフィック ベースの検出設定で [失敗したログイン試行の取得（Capture Failed Login Attempts）] を有効にする必要があります。

注意 ネットワーク検出ポリシーを使用して、HTTP、FTP、MDNS プロトコルを介した非権限、トラフィック ベースのユーザ検出を有効/無効にすると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

トラフィック ベースの検出データ

デバイスがトラフィック ベースの検出を使用してログインを検出すると、次の情報をユーザアクティビティとして記録するために Firepower Management Centerに送信します。

- ログインで識別されたユーザ名
- ログインの時刻
- ログインに関係するIPアドレス。このアドレスは、ユーザのホスト（LDAP、POP3、IMAP、および AIM ログインの場合）、サーバ（HTTP、MDNS、FTP、SMTP および Oracle ログインの場合）、またはセッション発信元（SIP ログインの場合）の IP アドレスになります。
- ユーザの電子メール アドレス（POP3、IMAP、および SMTP ログインの場合）
- ログインを検出したデバイスの名前

ユーザがすでに検出されている場合、Firepower Management Centerはそのユーザのログイン履歴を更新します。Firepower Management Center は POP3 および IMAP ログイン内の電子メール アドレスを使用して LDAP ユーザに関連付ける場合があることに注意してください。これは、Firepower Management Center が新しい IMAP ログインを検出して、その IMAP ログイン内の電子メール アドレスが既存の LDAP ユーザのアドレスと一致した場合は、IMAP ログインで新しいユーザが作成されるのではなく、LDAP ユーザの履歴が更新されることを意味します。

ユーザが以前に検出されなかった場合、Firepower Management Center はユーザ データベースにユーザを追加します。AIM、SIP、Oracle ログインでは、常に新しいユーザ レコードが作成されます。これは、それらのログイン イベントには Firepower Management Center が他のログイン タイプに関連付けることができるデータが含まれていないためです。

Firepower Management Center は、次の場合に、ユーザ アイデンティティまたはユーザ ID を記録しません。

- そのログイン タイプを無視するようにネットワーク検出ポリシーを設定した場合
- 管理対象デバイスが SMTP ログインを検出したものの、ユーザ データベースに電子メール アドレスが一致する、検出済みの LDAP、POP3、または IMAP ユーザが含まれていない場合

ユーザ データはユーザ テーブルに追加されます。

トラフィック ベースの検出戦略

ユーザ アクティビティを検出するプロトコルを制限して、検出するユーザの総数を削減することにより、ほぼ完全なユーザ情報を提供していると思われるユーザに焦点を絞ることができます。プロトコルの検出を制限すると、ユーザ名の散乱を最小限に抑え、Firepower Management Center 上の記憶域を節約することができます。

トラフィック ベースの検出プロトコルを選択する際には、以下を検討してください。

- AIM、POP3、IMAP などのプロトコル経由でユーザ名を取得すると、契約業者、訪問者、およびその他のゲストからのネットワーク アクセスによって組織に無関係なユーザ名が収集される可能性があります。
- AIM、Oracle、および SIP ログインは、無関係なユーザ レコードを作成する可能性があります。この現象は、このようなログイン タイプが、システムが LDAP サーバから取得するユーザ メタデータのいずれにも関連付けられていないうえ、管理対象デバイスが検出するその他のログイン タイプに含まれている情報のいずれにも関連付けられていないために発生します。そのため、Firepower Management Centerは、これらのユーザとその他のユーザ タイプを関連付けることができません。

関連トピック

トラフィック ベースのユーザ検出の設定, （1563 ページ）

第 67 章

ネットワーク検出ポリシー

以下のトピックでは、ネットワーク検出ポリシーを作成、設定、管理する方法について説明します。

概要：ネットワーク検出ポリシー

Firepower Management Center 上のネットワーク検出ポリシーは、システムが組織のネットワークアセットに関するデータを収集する方法と、どのネットワーク セグメントとポートをモニタ対象とするかを制御します。

マルチドメイン展開では、各リーフ ドメインがそれぞれ独立したネットワーク検出ポリシーを使用します。ネットワーク検出ポリシーのルールやその他の設定をドメイン間で共有、継承、コピーすることはできません。新しいドメインを作成するたびに、システムにより、その新しいドメインに対してデフォルト設定を使用したネットワーク検出ポリシーが作成されます。カスタマイズが必要な場合は、新しいポリシーに明示的に適用する必要があります。

Firepower システムがモニタしてトラフィック内のネットワーク データに基づいて検出データを生成するネットワークおよびポート、ポリシーを適用するゾーンは、ポリシー内の検出ルールで指定します。ルール内では、ホスト、アプリケーション、権限のないユーザを検出するかどうかを設定できます。検出からネットワークとゾーンを除外するルールを作成できます。NetFlow エクスポータからのデータの検出を設定して、ネットワーク上でユーザデータが検出されるトラフィックのプロトコルを制限できます。

ネットワーク検出ポリシーに用意されている単一のデフォルト ルールは、すべてのモニタ対象トラフィックからアプリケーションを検出するように設定されています。このルールが除外するネットワーク、ゾーン、ポートはなく、ホストとユーザの検出も設定されていません。また、このルー

ルは NetFlow エクスポータをモニタするように設定されてはいません。このポリシーは、管理対象デバイスが Firepower Management Center に登録されると、デフォルトでそのデバイスに導入されます。ホストまたはユーザ データの収集を開始するには、検出ルールを追加または変更して、ポリシーをデバイスに再展開する必要があります。

ネットワーク検出の範囲を調整する場合は、追加の検出ルールを作成して、デフォルト ルールを変更または削除できます。

管理対象デバイスごとのアクセス コントロール ポリシーは、そのデバイスに許可されたトラフィック、つまり、ネットワーク検出を使用してモニタ可能なトラフィックを定義することに注意してください。アクセス コントロールを使用して特定のトラフィックをブロックすると、システムでホスト、ユーザ、またはアプリケーションのアクティビティに関するトラフィックを検査できなくなります。たとえば、アクセス コントロール ポリシーでソーシャル ネットワーキング アプリケーションへのアクセスをブロックすると、システムはそれらのアプリケーションに関する検出データを一切提供できなくなります。

検出ルールでトラフィック ベースのユーザ検出を有効にすると、一連のアプリケーション プロトコル全体のトラフィック内のユーザ ログイン アクティビティを通して権限のないユーザを検出できます。必要に応じて、すべてのルールにわたって特定のプロトコル内の検出を無効にできます。一部のプロトコルを無効にすると、Firepower Management Center モデルに関連付けられたユーザ制限に達するのを防ぐのに役立ち、他のプロトコルからのユーザに使用可能なユーザ カウントを確保できます。

詳細ネットワーク検出設定を使用すれば、記録するデータの種類、検出データの保存方法、アクティブにする侵害の兆候（IOC）ルール、影響評価に使用する脆弱性マッピング、送信元からの検出データが競合していた場合の対処を管理できます。また、ホスト入力の送信元や NetFlow エクスポータをモニタ対象として追加することもできます。

ネットワーク検出のカスタマイズ

Firepower システムによって収集されるネットワーク トラフィックに関する情報は、この情報を関連付けて最も脆弱で最も重要なネットワークのホストを識別することができる場合に、最もその価値を発揮します。

たとえば、ネットワーク上に SuSE Linux のカスタマイズ バージョンを実行している複数のデバイスがある場合、システムはそのオペレーティング システムを識別することができません。そのため、脆弱性をそれらのホストにマッピングすることはできません。しかし、システムに SuSE Linux に関する脆弱性のリストがあるならば、同じオペレーティング システムを実行する他のホストを識別するために使用できるカスタム フィンガープリントを、ホストのいずれか 1 台に対して作成することができます。フィンガープリントに SuSE Linux の脆弱性リストのマッピングを含め、フィンガープリントに一致する各ホストとそのリストを関連付けることができます。

また、ホストの入力機能を使用して、ホスト データをサードパーティ システムからネットワーク マップに直接入力することもできます。ただし、サードパーティのオペレーティング システムやアプリケーション データは、脆弱性情報に自動的にマッピングされません。脆弱性を確認し、サードパーティのオペレーティング システム、サーバ、アプリケーション プロトコル データを使用してホストの影響の関連付けを実行する場合、サードパーティ システムからのベンダーとバージョンの情報を、脆弱性データベース（VDB）にリストされているベンダーとバージョンに

マッピングする必要はあります。また、ホストの入力データを継続的に維持する必要がある場合もあります。アプリケーション データを Firepower システムのベンダーおよびバージョン定義にマッピングしたとしても、インポートされたサードパーティの脆弱性はクライアントまたは Web アプリケーションの影響評価に使用されないことに注意してください。

システムがネットワーク上のホストで実行されているアプリケーション プロトコルを識別できない場合は、システムがポートまたはパターンに基づいてアプリケーションを識別できるようにする、ユーザ定義のアプリケーションプロトコルディテクタを作成できます。また、特定のアプリケーション ディテクタをインポートしたり、アクティブ/非アクティブにしたりすることによって、Firepower システムのアプリケーション検出機能をカスタマイズすることができます。

さらに、Nmap アクティブ スキャナのスキャン結果を使用してオペレーティング システムやアプリケーション データの検出を置き換えたり、サードパーティの脆弱性で脆弱性リストを拡張したりすることもできます。システムは複数のソースからのデータを照合して、アプリケーションの ID を判別できます。

ネットワーク検出ポリシーの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

マルチドメイン展開では、各ドメインに個別のネットワーク検出ポリシーがあります。ユーザ アカウントで複数のドメインを管理できる場合は、ポリシーを設定するリーフ ドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 ポリシーの次のコンポーネントを設定します。

- 検出ルール：ネットワーク検出ルールの設定, （1553 ページ）を参照してください。
- ユーザのトラフィックベースの検出：トラフィック ベースのユーザ検出の設定, （1563 ページ）を参照してください。
- 高度なネットワーク検出オプション：高度なネットワーク検出オプションの設定, （1564 ページ）を参照してください。

- カスタム オペレーティング システム定義（フィンガープリント）：クライアント用のカスタム フィンガープリントの作成, （1460 ページ）およびサーバ用のカスタム フィンガープリントの作成, （1463 ページ）を参照してください。

ネットワーク検出ルール

ネットワーク検出ルールを使用すれば、ネットワーク マップに対して検出される情報を調整し、必要な特定のデータだけを含めるようにすることができます。ネットワーク検出ポリシー内のルールは順番に評価されます。モニタリング基準が重複したルールを作成できますが、その場合はシステム パフォーマンスに影響する可能性があります。

モニタリングからホストまたはネットワークを除外すると、そのホストまたはネットワークがネットワーク マップに表示されず、それに対するイベントが報告されません。Cisco では、モニタリングからロード バランサ（またはロード バランサ上の特定のポート）と NAT デバイスを除外することを推奨しています。これらのデバイスは紛らわしいイベントを過剰に生成するため、データベースがいっぱいになったり、Firepower Management Center が過負荷になったりする可能性があります。たとえば、モニタ対象 NAT デバイスが短期間にオペレーティング システムの複数の更新を表示する場合があります。ロード バランサと NAT デバイスの IP アドレスがわかっている場合は、モニタリングからそれらを除外できます。

ヒント システムは、ネットワーク トラフィックを検査することにより、複数のロード バランサと NAT デバイスを識別できます。

加えて、カスタム サーバ フィンガープリントを作成する必要がある場合は、フィンガープリントを行っているホストとの通信に使用されている IP アドレスをモニタリングから一時的に除外する必要があります。そうしないと、ネットワーク マップおよびディスカバリ イベント ビューに、その IP アドレスによって表されるホストに関する不正確な情報が混在することになります。フィンガープリントを作成したら、その IP アドレスをモニタするようにポリシーを設定し直すことができます。

Cisco では、NetFlow エクスポータと Firepower システム管理対象デバイスを使用して、同じネットワーク セグメントをモニタ**しない**ことも推奨しています。重複しないルールを使用してネットワーク検出ポリシーを設定するのが理想です。管理対象デバイスによって生成された重複接続ログはシステムによって破棄されます。ただし、管理対象デバイスと NetFlow エクスポータの両方で検出された接続に関する重複接続ログを破棄することは**できません**。

ネットワーク検出ルールの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

検出ルールを設定し、ニーズに合わせてホストデータとアプリケーションデータの検出を調整できます。

はじめる前に

- ネットワークデータを検出するトラフィックの接続を記録していることを確認します。接続ロギング ストラテジー，（1908 ページ）を参照してください。
- エクスポートされたNetFlowレコードを収集する場合は、NetFlowエクスポータのネットワーク検出ポリシーへの追加，（1571 ページ）の説明に従ってNetFlowエクスポータを追加します。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [ルールの追加（Add Rule）] をクリックします。

ステップ 3 アクションと検出されるアセット，（1554ページ）の説明に従って、ルールの[アクション（Action）]を設定します。

ステップ 4 オプションの検出パラメータを設定します。

- ルールアクションを特定のネットワークに制限します。監視対象ネットワークの制限，（1555 ページ）を参照してください。
- ルールアクションを特定のゾーン内のトラフィックに制限します。ネットワーク検出ルールでのゾーンの設定，（1561 ページ）を参照してください。
- ポートをモニタリングから除外します。ネットワーク検出ルールでのポートの除外，（1558 ページ）を参照してください。
- NetFlowデータ検出のルールの設定します。NetFlowデータ検出のルールの設定，（1556ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

アクションと検出されるアセット

検出ルールを設定する場合は、ルールのアクションを選択する必要があります。アクションの効果は、管理対象デバイスと NetFlow エクスポータのどちらからデータを検出するルールを使用しているかによって異なります。

次の表に、これら 2 つのシナリオで指定されたアクション設定を使用したルールで検出されるアセットの説明を示します。

表 *196*：検出ルールのアクション

	管理対象デバイス（Managed Device）	NetFlow エクスポータ
除外（Exclude）	指定されたネットワークをモニタリング対象から除外します。接続の発信元ホストまたは宛先ホストを検出から除外すると、接続は記録されますが、除外したホストの検出イベントは作成されません。	指定されたネットワークをモニタリング対象から除外します。接続の発信元ホストまたは宛先ホストを検出から除外すると、接続は記録されますが、除外したホストの検出イベントは作成されません。
検出：ホスト（Discover: Hosts）	検出イベントに基づいて、ネットワーク マップにホストを追加します。（任意。ユーザ検出が有効になっていない場合は必須）。	NetFlow レコードに基づいて、ネットワーク マップにホストを追加し、接続をログに記録します。（必須）
検出：アプリケーション（Discover: Applications）	アプリケーション検出に基づいて、ネットワーク マップにアプリケーションを追加します。アプリケーションも検出しないルールでは、ホストまたはユーザを検出できないことに注意してください。（必須）	NetFlow レコードと `/etc/sf/services` 内のポートとアプリケーション プロトコルの関連付けに基づいて、ネットワーク マップにアプリケーション プロトコルを追加します。（オプション）
検出：ユーザ（Discover: Users）	ネットワーク検出ポリシーで設定されたユーザ プロトコルに関するトラフィック ベースの検出に基づいてユーザをユーザ テーブルに追加し、ユーザ アクティビティをログに記録します。（オプション）	適用対象外
NetFlow 接続のロギング（Log NetFlow Connections）	適用対象外	NetFlow 接続のみをログに記録します。ホストまたはアプリケーションは検出しません。

ルールを使用して管理対象デバイスのトラフィックをモニタする場合は、アプリケーション ロギングが必要です。ルールを使用してユーザをモニタする場合は、ホスト ロギングが必要です。

ルールを使用して、エクスポートされた NetFlow レコードをモニタする場合は、ユーザをログに記録するように設定することはできず、アプリケーション ロギングは任意です。

（注） ネットワーク検出ポリシーの[アクション（Action）]の設定に基づいて、エクスポートされた NetFlow レコードで接続が検出されます。アクセス コントロール ポリシーの設定に基づいて、管理対象デバイス ラフィックで接続が検出されます。

モニタ対象ネットワーク

検出ルールは、モニタ対象アセットの検出を、指定されたネットワーク上のホストとの間のトラフィックだけを対象にして行います。検出ルールでは、指定されたネットワーク内の 1 つ以上の IP アドレスが割り当てられた接続に対して検出が行われ、モニタ対象ネットワーク内の IP アドレスに対してのみイベントが生成されます。デフォルトの検出ルールでは、モニタされているすべてのトラフィックのアプリケーションを検出します（すべての IPv4 トラフィックについては `0.0.0.0/0`、すべての IPv6 トラフィックについては `::/0`）。

NetFlow 検出を処理し、接続データだけを記録するルールを設定すると、システムは、指定のネットワークの接続元と接続先の IP アドレスを記録します。ネットワーク検出ルールが NetFlow ネットワーク接続を記録する唯一の方法を提供することに注意してください。

また、ネットワーク オブジェクトまたはオブジェクト グループを使用してモニタ対象ネットワークを指定することもできます。

監視対象ネットワークの制限

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

すべての検出ルールに 1 つ以上のネットワークを含める必要があります。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [ルールの追加（Add Rule）] をクリックします。

ステップ 3 [ネットワーク（Networks）] タブが表示されていない場合は、そのタブをクリックします。

ステップ 4 必要に応じて、[使用可能なネットワーク（Available Networks）] リストにネットワーク オブジェクトを追加します。詳細については、検出ルール設定時のネットワーク オブジェクトの作成, （1557 ページ）を参照してください。

（注） ネットワーク検出ポリシーで使用されるネットワーク オブジェクトを変更した場合、その変更は設定の変更を展開するまで反映されません。

ステップ 5 ネットワークを指定します。

- [使用可能なネットワーク（Available Networks）] リストからネットワークを選択します。

  ヒント ネットワークがすぐにリストに表示されない場合は、リロード アイコン（）をクリックします。

- [使用可能なネットワーク（Available Networks）] ラベルの下にあるテキスト ボックスに IP アドレスを入力します。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 必要に応じて、別のネットワークを追加するために、前の 2 つの手順を繰り返します。

ステップ 8 [保存（Save）] をクリックして、変更を保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

NetFlow データ検出のルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

Firepower システムでは、NetFlow エクスポータからのデータを使用して、接続および検出イベントを生成したり、ネットワーク マップにホストとアプリケーションのデータを追加したりできます。

検出ルール内でNetFlowエクスポータを選択する場合、ルールは指定されたネットワークのNetFlowデータの検出に制限されます。NetFlow デバイスを選択すると使用可能なルール アクションが変更されるため、モニタするNetFlowデバイスを選択してからルール動作の他の側面を設定します。NetFlow エクスポータをモニタするためのポートの除外を設定することはできません。

はじめる前に

- NetFlow-enabled デバイスをネットワーク検出ポリシーに追加します。NetFlow エクスポータのネットワーク検出ポリシーへの追加, （1571 ページ）を参照してください。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [ルールの追加（Add Rule）] をクリックします。

ステップ 3 [NetFlow デバイス（NetFlow Device）] タブを選択します。

ステップ 4 [NetFlow デバイス（NetFlow Device）] ドロップダウン リストから、モニタする NetFlow エクスポータの IP アドレスを選択します。

ステップ 5 Firepower システムの管理対象デバイスで収集する NetFlow データのタイプを指定します。

- 接続のみ：[アクション（Action）] ドロップダウン リストから `Log NetFlow Connections` を選択します。
- ホスト、アプリケーション、および接続：[アクション（Action）] ドロップダウン リストから `Discover` を選択します。[ホスト（Hosts）] チェックボックスが自動的にオンになり、接続データの収集が有効になります。オプションで、[アプリケーション] チェックボックスをオンにして、アプリケーション データを収集できます。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

検出ルール設定時のネットワーク オブジェクトの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

新規ネットワーク オブジェクトを再使用可能なネットワーク オブジェクトおよびグループのリストに追加することで、検出ルールに表示される使用可能なネットワークのリストにそれらのオブジェクトを追加できます。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [ネットワーク（Networks）] タブで、[ルールの追加（Add Rule）] をクリックします。

ステップ 3 [利用可能なネットワーク（Available Networks）] の隣にある追加アイコン（  ）をクリックします。

ステップ 4 ネットワーク オブジェクトの作成, （389 ページ）の説明に従って、ネットワーク オブジェクトを作成します。

ステップ 5 ネットワーク検出ルールの設定, （1553 ページ）の説明に従って、ネットワーク検出ルールの追加を完了します。

ポート除外

モニタリングからホストを除外できるのと同様に、モニタリングから特定のポートを除外できます。次に例を示します。

- ロードバランサは短期間に同じポート上の複数のアプリケーションを報告する可能性があります。モニタリングからそのポートを除外する（Web ファームを処理するロードバランサ上のポート 80 を除外するなど）ようにネットワーク検出ルールを設定できます。
- 組織で特定の範囲のポートを使用するカスタム クライアントを使用しているとします。このクライアントからのトラフィックが紛らわしいイベントを過剰に生成する場合は、モニタリングからそれらのポートを除外できます。同様に、DNS トラフィックをモニタしないように設定することもできます。この場合は、検出ポリシーがポート 53 をモニタしないように、ルールを設定します。

除外するポートを追加するときには、[利用可能なポート（Available Ports）] リストから再利用可能なポート オブジェクトを選択するのか、送信元または宛先除外リストにポートを直接追加するのか、新しい再利用可能なポートを作成してからそれを除外リストに移動するのかを決定できます。

（注） NetFlow データの検出を処理するルールでポートを除外することはできません。

ネットワーク検出ルールでのポートの除外

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

NetFlow データ検出を処理するルールにあるポートを除外することはできません。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [ルールの追加（Add Rule）] をクリックします。

ステップ 3 [ポートの除外（Port Exclusions）] タブをクリックします。

ステップ 4 必要に応じて、検出ルール設定時のポート オブジェクトの作成, （1559 ページ）で説明されているように、使用可能なポート リストにポート オブジェクトを追加します。

ステップ 5 次のいずれかの方法を使用して、モニタリング対象から特定の送信元ポートを除外します。

- [使用可能なポート（Available Ports）] リストから 1 つまたは複数のポートを選択して、[送信元に追加（Add to Source）] をクリックします。
- ポート オブジェクトを追加せずに特定の送信元ポートからのトラフィックを除外するには、[選択済の送信元ポート リスト（Selected Source Ports）] で、[プロトコル（Protocol）] を選択し、[ポート（Port）] 番号（1 から 65535 の数値）を入力して、[追加（Add）] をクリックします。

ステップ 6 次のいずれかの方法を使用して、モニタリング対象から特定の宛先ポートを除外します。

- [使用可能なポート（Available Ports）] リストから 1 つまたは複数のポートを選択して、[宛先に追加（Add to Destination）] をクリックします。
- ポート オブジェクトを追加せずに特定の宛先ポートからのトラフィックを除外するには、[選択済の宛先ポート リスト（Selected Destination Ports）] で、[プロトコル（Protocol）] を選択し、[ポート（Port）] 番号を入力して、[追加（Add）] をクリックします。

ステップ 7 [保存（Save）] をクリックして、変更内容を保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

検出ルール設定時のポート オブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

新規ポートオブジェクトを、Firepowerシステム内の任意の場所で使用できる再使用可能なポートオブジェクトおよびグループのリストに追加することで、検出ルールに表示される使用可能なポートのリストにそれらのオブジェクトを追加できます。

手順

ステップ1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ2 [ネットワーク（Networks）] タブで、[ルールの追加（Add Rule）] をクリックします。

ステップ3 [ポートの除外（Port Exclusions）] をクリックします。

ステップ4 [利用可能なポート（Available Ports）] リストにポートを追加するには、オブジェクトの追加アイコン（）をクリックします。

ステップ5 [名前（Name）] を入力します。

ステップ6 [プロトコル（Protocol）] フィールドで、除外するトラフィックのプロトコルを指定します。

ステップ7 [ポート（Port）] フィールドに、モニタリングから除外するポートを入力します。
単一のポート、ダッシュ（-）を使用したポートの範囲、またはポートとポート範囲のカンマ区切りのリストを指定できます。許容されるポート値は 1 ～ 65535 です。

ステップ8 [保存（Save）] をクリックします。

ステップ9 ポートがすぐにリストに表示されない場合は、更新アイコン（）をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ネットワーク検出ルールのゾーン

パフォーマンスを向上させるために、ルール内の監視対象ネットワークに物理的に接続されている管理対象デバイス上のセンシング インターフェイスがルール内のゾーンに含まれるように、検出ルールを設定することができます。

残念ながら、ネットワーク設定の変更は通知されないことがあります。ネットワーク管理者が通知せずにルーティングやホストの変更によりネットワーク設定を変更した場合、正しいネットワーク検出ポリシー設定を完全に把握するのが難しくなります。管理対象デバイス上のセンシング インターフェイスがどのようにネットワークに物理的に接続されているかが不明な場合は、ゾーンの設定はデフォルト値のままにしておいてください。このデフォルト値によって、システムは展開環境内のすべてのゾーンに検出ルールを展開します（ゾーンが除外されない場合、システムではすべてのゾーンに検出ポリシーを展開します。）。

ネットワーク検出ルールでのゾーンの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [ルールの追加（Add Rule）] をクリックします。

ステップ 3 [ゾーン（Zones）] タブをクリックします。

ステップ 4 [使用可能なゾーン（Available Zones）] リストでゾーンを選択します。

ステップ 5 [保存（Save）] をクリックして、加えた変更を保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

トラフィック ベース検出のアイデンティティ ソース

トラフィック ベース検出は、Firepowerシステムでサポートされている唯一の権限のないアイデンティティ ソースです。トラフィック ベース検出を設定すると、管理対象デバイスは、指定したネットワークでの LDAP、AIM、POP3、IMAP、Oracle、SIP（VoIP）、FTP、HTTP、MDNS、SMTP のログインを検出します。トラフィック ベースの検出から取得されたデータは、ユーザ認識にのみ使用できます。権威のあるアイデンティティ ソースとは異なり、トラフィック ベースの検出はネットワーク検出ポリシーで設定します。トラフィック ベースのユーザ検出の設定, （1563 ページ）を参照してください。

次の制限事項に注意してください。

- トラフィック ベースの検出では、LDAP 接続に対する Kerberos ログインのみを LDAP 認証として解釈します。また、管理対象デバイスは、SSL や TLS などのプロトコルを使用して暗号化された LDAP 認証を検出できません。
- トラフィック ベースの検出では OSCAR プロトコルを使用した AIM ログインだけを検出します。TOC2 を使用する AIM ログインは検出できません。
- トラフィック ベースの検出ではSMTP ロギングを制限することができません。これは、ユーザがSMTP ログインに基づいてデータベースに追加されていないためです。システムがSMTP

ログインを検出しても、一致する電子メールアドレスのユーザがデータベース内に存在しなければ、そのログインは記録されません。

トラフィック ベースの検出は、失敗したログイン試行も記録します。失敗ログイン試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。トラフィック ベースの検出により検出された失敗ログイン アクティビティのユーザ アクティビティ タイプは [失敗したユーザ ログイン（Failed User Login）] です。

（注） システムは失敗した HTTP ログインと成功した HTTP ログインを区別できません。HTTP ユーザ情報を表示するには、トラフィック ベースの検出設定で [失敗したログイン試行の取得（Capture Failed Login Attempts）] を有効にする必要があります。

注意 ネットワーク検出ポリシーを使用して、HTTP、FTP、MDNS プロトコルを介した非権限、トラフィック ベースのユーザ検出を有効/無効にすると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

トラフィック ベースの検出データ

デバイスがトラフィック ベースの検出を使用してログインを検出すると、次の情報をユーザアクティビティとして記録するために Firepower Management Centerに送信します。

- ログインで識別されたユーザ名
- ログインの時刻
- ログインに関係する IP アドレス。このアドレスは、ユーザのホスト（LDAP、POP3、IMAP、および AIM ログインの場合）、サーバ（HTTP、MDNS、FTP、SMTP および Oracle ログインの場合）、またはセッション発信元（SIP ログインの場合）の IP アドレスになります。
- ユーザの電子メール アドレス（POP3、IMAP、および SMTP ログインの場合）
- ログインを検出したデバイスの名前

ユーザがすでに検出されている場合、Firepower Management Centerはそのユーザのログイン履歴を更新します。Firepower Management Center は POP3 および IMAP ログイン内の電子メール アドレスを使用して LDAP ユーザに関連付ける場合があることに注意してください。これは、Firepower Management Center が新しい IMAP ログインを検出して、その IMAP ログイン内の電子メール アドレスが既存の LDAP ユーザのアドレスと一致した場合は、IMAP ログインで新しいユーザが作成されるのではなく、LDAP ユーザの履歴が更新されることを意味します。

ユーザが以前に検出されなかった場合、Firepower Management Center はユーザ データベースにユーザを追加します。AIM、SIP、Oracle ログインでは、常に新しいユーザ レコードが作成されます。

これは、それらのログイン イベントには Firepower Management Center が他のログイン タイプに関連付けることができるデータが含まれていないためです。

Firepower Management Center は、次の場合に、ユーザ アイデンティティまたはユーザ ID を記録しません。

- そのログイン タイプを無視するようにネットワーク検出ポリシーを設定した場合
- 管理対象デバイスが SMTP ログインを検出したものの、ユーザ データベースに電子メール アドレスが一致する、検出済みの LDAP、POP3、または IMAP ユーザが含まれていない場合

ユーザ データはユーザ テーブルに追加されます。

トラフィック ベースの検出戦略

ユーザ アクティビティを検出するプロトコルを制限して、検出するユーザの総数を削減することにより、ほぼ完全なユーザ情報を提供していると思われるユーザに焦点を絞ることができます。プロトコルの検出を制限すると、ユーザ名の散乱を最小限に抑え、Firepower Management Center 上の記憶域を節約することができます。

トラフィック ベースの検出プロトコルを選択する際には、以下を検討してください。

- AIM、POP3、IMAP などのプロトコル経由でユーザ名を取得すると、契約業者、訪問者、およびその他のゲストからのネットワーク アクセスによって組織に無関係なユーザ名が収集される可能性があります。
- AIM、Oracle、および SIP ログインは、無関係なユーザ レコードを作成する可能性があります。この現象は、このようなログイン タイプが、システムが LDAP サーバから取得するユーザ メタデータのいずれにも関連付けられていないうえ、管理対象デバイスが検出するその他のログイン タイプに含まれている情報のいずれにも関連付けられていないために発生します。そのため、Firepower Management Centerは、これらのユーザとその他のユーザ タイプを関連付けることができません。

関連トピック

トラフィック ベースのユーザ検出の設定, （1563 ページ）

トラフィック ベースのユーザ検出の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

ネットワーク検出ルールでトラフィック ベースのユーザ検出を有効にすると、ホスト検出が自動で有効になります。トラフィック ベースの検出の詳細については、トラフィック ベース検出のアイデンティティ ソース, （1546 ページ）を参照してください。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [ユーザ（Users）] をクリックします。

ステップ 3 編集アイコン（  ）をクリックします。

ステップ 4 ログインを検出するプロトコルのチェック ボックスをオンにするか、ログインを検出しないプロトコルのチェック ボックスをオフにします。

ステップ 5 オプションで、LDAP、POP3、FTP、IMAP トラフィックで検出されたログイン試行の失敗を記録したり、HTTP ログインのユーザ情報を取得するには、[失敗したログイン試行のキャプチャ（Capture Failed Login Attempts）] を有効にします。

ステップ 6 [保存（Save）] をクリックします。

次の作業

注意 ネットワーク検出ポリシーを使用して、HTTP、FTP、MDNS プロトコルを介した非権限、トラフィック ベースのユーザ検出を有効/無効にすると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

- ネットワーク検出ルールの設定, （1553 ページ）の説明に従って、ユーザを検出するようにネットワーク検出ルールを設定します。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

高度なネットワーク検出オプションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

ネットワーク検出ポリシーの [詳細（Advanced）] タブを使用すれば、検出するイベント、検出データの保存期間と更新頻度、影響相関に使用する脆弱性マッピング、およびオペレーティング

システム ID とサーバ ID の競合の解決方法に関するポリシー全体の設定を構成できます。加えて、ホスト入力ソースと NetFlow エクスポータを追加して、他のソースからのデータのインポートを許可できます。

（注） 検出イベントとユーザ活動イベントのデータベース イベント制限はシステム構成で設定されます。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 変更する設定の横にある編集アイコン（）または追加アイコン（）をクリックします。

- [データ ストレージ設定（Data Storage Settings）]：ネットワーク検出データ ストレージの設定, （1574 ページ）の説明に従って、設定を更新します。
- [イベント ロギング設定（Event Logging Settings）]：ネットワーク検出イベント ロギングの設定, （1574 ページ）の説明に従って、設定を更新します。
- [全般設定（General Settings）]：ネットワーク検出全般設定, （1566 ページ）の説明に従って、設定を更新します。
- [ID 競合設定（Identity Conflict Settings）]：ネットワーク検出アイデンティティ競合の解決の設定, （1568 ページ）の説明に従って、設定を更新します。
- [侵害の兆候設定（General Settings）]：侵害の兆候ルールの有効化, （1570 ページ）の説明に従って、設定を更新します。
- [NetFlow エクスポータ（NetFlow Exporters）]：NetFlow エクスポータのネットワーク検出ポリシーへの追加, （1571 ページ）の説明に従って、設定を更新します。
- [OS およびサーバの ID ソース（OS and Server Identity Sources）]：ネットワーク検出 OS およびサーバ アイデンティティ ソースの追加, （1575 ページ）の説明に従って、設定を更新します。
- [影響評価に使用する脆弱性（Vulnerabilities to use for Impact Assessment）]：ネットワーク検出の脆弱性影響評価の有効化, （1569 ページ）の説明に従って、設定を更新します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

関連トピック

データベース イベント数の制限, （563 ページ）

ネットワーク検出の一般設定

一般設定は、システムがネットワークマップを更新する頻度と、検出中にサーババナーをキャプチャするかどうかを制御します。

[バナーのキャプチャ（Capture Banners）]

サーバベンダーとバージョン（「バナー」）をアドバタイズするネットワークトラフィックからの見出し情報をシステムで保存させる場合、このチェックボックスをオンにします。この情報は、収集された情報に追加のコンテキストを提供できます。サーバ詳細にアクセスすることによって、ホストに関して収集されたサーバ バナーにアクセスできます。

[アップデート間隔（Update Interval）]

システムが情報を更新する時間間隔（ホストの IP アドレスのいずれかが最後に検出された時点、アプリケーションが使用された時点、アプリケーションのヒット数など）。デフォルト設定は 3600 秒（1 時間）です。

更新タイムアウトの時間間隔を短く設定すると、より正確な情報がホスト画面に表示されますが、より多くのネットワーク イベントが生成されることに注意してください。

ネットワーク検出全般設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [全般設定（General Settings）] の横にある編集アイコン（  ）をクリックします。

ステップ 4 ネットワーク検出の一般設定, （1566 ページ）の説明に従って設定を更新します。

ステップ 5 [保存（Save）] をクリックして、全般設定を保存します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

ネットワーク検出アイデンティティ競合の設定

システムは、オペレーティング システムとサーバのフィンガープリントをトラフィック内のパターンに照合することで、どのオペレーティング システムおよびアプリケーションがホストで実行されているかを判別します。最も信頼できるオペレーティング システムとサーバの ID 情報を提供するために、システムは複数のソースからのフィンガープリント情報を照合します。

システムは、すべてのパッシブ データを使用して、オペレーティング システム ID を抽出し、信頼値を割り当てます。

デフォルトでは、ID 競合が存在しなければ、スキャナまたはサード パーティ アプリケーションによって追加された ID データで、Firepower System によって検出された ID データが上書きされます。[アイデンティティ ソース（Identity Sources）] 設定を使用して、スキャナとサードパーティ アプリケーションのフィンガープリント ソースをプライオリティでランク付けできます。システムはソースごとに 1 つずつの ID を保持しますが、プライオリティが最も高いサードパーティ アプリケーションまたはスキャナ ソースからのデータのみが最新の ID として使用されます。ただし、プライオリティに関係なく、ユーザ入力データによって、スキャナまたはサードパーティ アプリケーションのデータが上書きされることに注意してください。

ID 競合は、[アイデンティティ ソース（Identity Sources）] 設定に列挙されたアクティブ スキャナ ソースまたはサードパーティ アプリケーション ソースと Firepower システム ユーザのどちらかから取得された既存の ID と競合する ID をシステムが検出した場合に発生します。デフォルトでは、ID 競合は自動的に解決されないため、ホスト プロファイルを通して、または、ホストをスキャンし直すか新しい ID データを追加し直してパッシブ ID を上書きすることにより、解決する必要があります。ただし、パッシブ ID またはアクティブな ID のいずれかを維持することで、競合を自動的に解決するようにシステムを設定できます。

[ID 競合イベントを生成する（Generate Identity Conflict Event）]

ID 競合が発生したときにシステムがイベントを生成するかどうかを指定します。

[自動的に競合を解決する（Automatically Resolve Conflicts）]

[自動的に競合を解決する（Automatically Resolve Conflicts）] ドロップダウン リストから、次のいずれかを選択します。

- ID 競合の手動での競合解決を強制する場合は、[無効（Disabled）]
- ID 競合が発生したときにシステムがパッシブ フィンガープリントを使用するようにする場合は、[アイデンティティ（Identity）]
- ID 競合が発生したときにシステムが優先度が最も高いアクティブなソースの現在の ID を使用するようにする場合は、[キープアクティブ（Keep Active）]

ネットワーク検出アイデンティティ競合の解決の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [ID 競合設定（Identity Conflict Settings）] の横にある編集アイコン（  ）をクリックします。

ステップ 4 ネットワーク検出アイデンティティ競合の設定, （1567 ページ）の説明に従って、[ID 競合設定の編集（Edit Identity Conflict Settings）] ポップアップ ウィンドウの設定を更新します。

ステップ 5 [保存（Save）] をクリックして、ID 競合設定を保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ネットワーク検出の脆弱性の影響の評価オプション

Firepower システムで侵入イベントとの影響相関を実行する方法を設定できます。有効な選択肢は次のとおりです。

- システム ベースの脆弱性情報を使用して影響相関を実行する場合は、[ネットワーク検出の脆弱性マッピングを使用（Use Network Discovery Vulnerability Mappings）] チェックボックスをオンにします。
- サードパーティの脆弱性参照を使用して影響相関を実行する場合は、[サードパーティの脆弱性マッピングを使用（Use Third-Party Vulnerability Mappings）] チェックボックスをオンにします。詳細については、*Firepower System Host Input API Guide*を参照してください。

チェックボックスのどちらかまたは両方を選択できます。システムが侵入イベントを生成し、選択された脆弱性マッピングセット内の脆弱性のあるサーバまたはオペレーティング システムがそのイベントに関係するホストに含まれている場合、侵入イベントは脆弱（レベル 1：赤）影響アイコンでマークされます。ベンダーまたはバージョン情報のないサーバの場合は、Firepower Management Center 構成で脆弱性マッピングを有効にする必要があることに注意してください。

両方のチェックボックスをオフにした場合は、侵入イベントが脆弱（レベル 1：赤）影響アイコンでマークされません。

関連トピック

サードパーティの脆弱性のマッピング，（1471 ページ）
サーバの脆弱性のマッピング，（611 ページ）

ネットワーク検出の脆弱性影響評価の有効化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [影響評価に使用する脆弱性（Vulnerabilities to use for Impact Assessment）] の横にある編集アイコン（  ）をクリックします。

ステップ 4 ネットワーク検出の脆弱性の影響の評価オプション，（1568ページ）説明に従って、[脆弱性設定の編集（Edit Vulnerability Settings）] ポップアップ ウィンドウで設定を更新します。

ステップ 5 [保存（Save）] をクリックして、脆弱性設定を保存します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

侵害の兆候

Firepowerシステムでは、ネットワーク検出ポリシー内のIOCルールを使用して悪意のある手段によって侵害されている可能性があるホストを特定します。ホストがこれらのシステム提供のルールで指定されている条件を満たしている場合、そのホストはシステムによって侵害の兆候（IOC）でタグ付けされます。関連のルールは*IOC*ルールと呼ばれます。各IOCルールは1種類のIOCタグに対応しています。*IOC*タグは可能性のある侵害の性質を指定します。

次のうちいずれかの事態が発生すると、関与しているホストにFirepower Management Centerがタグを付けます。

- システムは、侵入、接続、セキュリティインテリジェンス、およびファイルまたはマルウェア イベントを使用してモニタ対象のネットワークとそのトラフィックについて集められたデータを関連付け、潜在的な IOC が発生したと判断します。
- Firepower Management Center は AMP クラウドを経由してエンドポイント向け AMP の展開から IOC データをインポートすることができます。このデータがホスト自体の活動（個別のプログラムによってまたはプログラム上で実行されるアクションなど）を検査するため、ネットワーク専用データでは理解するのが難しい可能性がある脅威に対する理解が促されます。便宜上、Firepower Management Center はシスコが開発した新しい IOC タグを AMP クラウドから自動的に取得します。

この機能を設定するには、侵害の兆候ルールの有効化, （1570 ページ）を参照してください。

また、ホストの IOC データに対する相関ルールと、IOC でタグ付けされたホストから成るコンプライアンス ホワイトリストも記述することができます。

タグ付けされた IOC の調査や操作を行うには、侵害の兆候データ, （2119 ページ）とそのサブトピック参照してください。

侵害の兆候ルールの有効化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

システムで侵害の兆候（IOC）を検出してタグを付けるには、まず、ネットワーク検出ポリシーで 1 つ以上の IOC ルールを有効化する必要があります。IOC ルールのそれぞれが IOC タグの 1 つのタイプに対応します。すべての IOC ルールはシスコが事前定義しています。オリジナル ルールを作成することはできません。ネットワークや組織のニーズに合わせて、一部またはすべてのルールを有効にすることができます。たとえば、Microsoft Excel などのソフトウェアを使用しているホストが絶対に監視対象ネットワーク上に出現しない場合は、Excelベースの脅威に関係する IOC タグを有効にしないようにできます。

ヒント　個別のホストの IOC ルールを無効にするには、単一ホストにおける侵害の兆候のルール状態の編集, （2122 ページ）を参照してください。

はじめる前に

IOC ルールは Firepower システムの他のコンポーネントと、AMP for Endpoints によって提供されるデータに基づいてトリガーされるため、これらのコンポーネントが正しくライセンス付与され、IOC タグを設定できるように設定されている必要があります。侵入検知および防御（IPS）および Advanced Malware Protection（AMP）など、有効にする予定の IOC ルールに関連付けられている Firepower システムの機能を有効にします。IOC ルールの関連機能が有効になっていないと、関連データが収集されず、ルールをトリガーできません。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [侵害の兆候設定（Indications of Compromise Settings）] の横にある編集アイコン（  ）をクリックします。

ステップ 4 IOC 機能全体のオンとオフを切り替えるには、[IOC の有効化（Enable IOC）] の横にあるスライダをクリックします。

ステップ 5 個別の IOC ルールをグローバルに有効または無効にするには、ルールの [有効（Enabled）] 列のスライダをクリックします。

ステップ 6 [保存（Save）] をクリックして IOC ルール設定を保存します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

NetFlow エクスポータのネットワーク検出ポリシーへの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

はじめる前に

- Firepower システムの NetFlow データ，（1441 ページ） の説明に従い、使用する NetFlow エクスポータを設定します。
- NetFlow の他の要件については、NetFlow データを使用するための要件，（1441 ページ）の説明を参照してください。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [NetFlow デバイス（NetFlow Devices）] の横にある追加アイコン（  ）をクリックします。

ステップ 4 [IP アドレス（IP Address）] フィールドに、NetFlow データを収集する対象デバイスの管理を行うネットワークデバイスの IP アドレスを入力します。

ステップ 5 必要に応じて、以下を行います。

- NetFlow エクスポータをさらに追加するには、上記の 2 つのステップを繰り返します。
- 削除アイコン（  ）をクリックして、NetFlow エクスポータを削除します。検出ルールで NetFlow エクスポータを使用する場合は、先にルールを削除しないと、[詳細（Advanced）] ページからデバイスを削除できないことに注意してください。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- ネットワーク検出ルールの設定, （1553 ページ） の説明に従い、NetFlow トラフィックをモニタリングするネットワーク検出ルールを設定します。
- 設定変更を展開します。設定変更の導入, （320 ページ） を参照してください。

ネットワーク検出のデータ ストレージ設定

ディスカバリのデータ ストレージ設定では、ホスト制限とタイムアウトの設定が行われます。

ホスト制限の到達時（When Host Limit Reached）

Firepower Management Center がモニタでき、ネットワーク マップに保存できるホストの数。モデルによって異なります。ホスト制限に到達した後に新しいホストを検出すると、[ホスト制限の到達時（When Host Limit Reached）] オプションが制御を行います。次の操作を実行できます。

ホストをドロップ（Drop hosts）

システムは、長期間非アクティブになっているホストをドロップして、新しいホストを追加します。これがデフォルトの設定です。

新しいホストを挿入しない（Don't insert new hosts）

システムは、新たに検出されたホストを追跡しません。システムが新しいホストを追跡するのは、管理者がドメインのホスト制限を増加させた後などに、ホスト カウントが制限を下回る場合、ネットワーク マップからホストを手動で削除する場合、またはホストが非アクティブであることからタイムアウトと見なされる場合のみです。

マルチドメイン展開では、リーフ ドメインは使用可能なモニタされたホストのプールを共有します。各リーフ ドメインがネットワーク マップに値を入力できるように、ホスト制限をサブドメイン レベルのドメイン プロパティで設定できます。各リーフ ドメインには独自のネットワーク検

出ポリシーがあるため、次の表で説明するように各リーフ ドメインは、システムが新しいホストを検出すると、独自の動作を制御します。

表 *197*：マルチテナンシーによるホスト制限への到達

設定	ドメインのホスト制限の有無	ドメインのホスト制限に到達した場合	先祖ドメインのホスト制限に到達した場合
ホストをドロップ	Yes	制限付きドメインの最も古いホストをドロップします。	ホストをドロップするように設定されているすべての子孫リーフ ドメインで最も古いホストをドロップします。 ドロップされるホストがなければ、ホストの追加は行われません。
	No	適用対象外	ホストをドロップし、一般プールを共有するように設定されているすべての子孫リーフ ドメインで最も古いホストをドロップします。
新しいホストを挿入しない	「Yes」または「No」で答えてください。	ホストの追加は行われません。	ホストの追加は行われません。

ホスト タイムアウト（Host Timeout）

システムが、非アクティブであるという理由でネットワーク マップからホストを除外するまでの分単位の時間。デフォルト設定は 10080 分（1 週間）です。ホスト IP アドレスと MAC アドレスは個別にタイムアウトすることができますが、関連するアドレスのすべてがタイムアウトするまで、ホストはネットワーク マップから削除されません。

ホストの早期タイムアウトを避けるために、ホストのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

サーバ タイムアウト（Server timeout）

システムが、非アクティブであるという理由でネットワーク マップからサーバを除外するまでの分単位の時間。デフォルト設定は 10080 分（1 週間）です。

サーバの早期タイムアウトを避けるために、サービスのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

クライアント アプリケーションのタイムアウト（Client Application Timeout）

システムが、非アクティブであるという理由でネットワーク マップからクライアントを除外するまでの分単位の時間。デフォルト設定は 10080 分（1 週間）です。

クライアントのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

関連トピック

Firepower システムのホスト制限, （1449 ページ）
ドメインのプロパティ, （312 ページ）

ネットワーク検出データ ストレージの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [データ ストレージ設定（Data Storage Settings）] の横にある編集アイコン（  ）をクリックします。

ステップ 4 ネットワーク検出のデータ ストレージ設定, （1572 ページ）の説明に従って、[データ ストレージ設定（Data Storage Settings）] ダイアログの設定を更新します。

ステップ 5 [保存（Save）] をクリックして、データ ストレージ設定を保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ネットワーク検出イベント ロギングの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

イベント ロギング設定は、検出イベントとホスト入力イベントを記録するかどうかを制御します。イベントを記録しない場合は、イベント ビューで検索することも、相関ルールをトリガーするために使用することもできません。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [イベント ロギング設定（Event Logging Settings）] の横にある編集アイコン（  ）をクリックします。

ステップ 4 ディスカバリ イベント タイプ, （2100 ページ）およびホスト入力イベント タイプ, （2104 ページ）の説明に従って、データベースに記録する検出イベントタイプとホスト入力イベントタイプの横にあるチェックボックスをオンまたはオフにします。

ステップ 5 [保存（Save）] をクリックして、イベント ロギング設定を保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

ネットワーク検出 OS およびサーバ アイデンティティ ソースの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

ネットワーク検出ポリシーの [詳細（Advanced）] タブで、新しいアクティブ ソースを追加し、また、既存の送信元の優先度やタイムアウトの設定を変更できます。

このページにスキャナを追加しても、Nmap スキャナ用の完全な統合機能は追加されませんが、インポートされたサードパーティ アプリケーションまたはスキャン結果の統合が可能になります。

サードパーティ アプリケーションまたはスキャナからデータをインポートする場合は、ソースからの脆弱性がネットワークで検出された脆弱性にマップされていることを確認してください。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [OS とサーバ ID ソース（OS and Server Identity Sources）] の横にある編集アイコン（  ）をクリックします。

ステップ 4 新しいソースを追加するには、[ソースの追加（Add Sources）] をクリックします。

ステップ 5 名前を入力します。

ステップ 6 ドロップダウン リストからインプット ソースの [タイプ（Type）] を選択します。

- AddScanResult 機能を使用してスキャン結果をインポートする場合は、[スキャナ（Scanner）] を選択します。
- スキャン結果をインポートしない場合は、[アプリケーション（Application）] を選択します。

ステップ 7 このソースによるネットワーク マップへの ID の追加からその ID の削除までの期間を指定するには、[タイムアウト（Timeout）] ドロップダウンリストから、[時間（Hours）]、[日（Days）]、または [週（Weeks）] を選択し、該当する期間を入力します。

ステップ 8 必要に応じて、以下を行います。

- ソースを昇格させて、オペレーティング システム ID とアプリケーション ID よりもリストでは下にあるソースを優先的に使用するには、そのソースを選択して上矢印をクリックします。
- ソースを降格させて、リストで上にあるソースから提供される ID が存在しない場合にのみオペレーティング システム ID とアプリケーション ID を使用するには、そのソースを選択して下矢印をクリックします。
- ソースを削除するには、ソースの横にある削除アイコン（  ）をクリックします。

ステップ 9 [保存（Save）] をクリックして、ID ソース設定を保存します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

関連トピック

サードパーティの脆弱性のマッピング，（1471 ページ）

ネットワーク検出戦略のトラブルシューティング

システムのデフォルトの検出機能に変更を加える前に、実装すべきソリューションを決定できるように、どのホストが正しく識別されていないかと、その原因を分析してください。

管理対象デバイスは正しく配置されていますか

ロード バランサ、プロキシ サーバ、NAT デバイスなどのネットワーク デバイスが、識別されないホストまたは誤って識別されたホストと管理対象デバイスとの間に存在する場合は、カスタム フィンガープリントを使用するのではなく、誤って識別されたホストのより近くに管理対象デバイスを配置します。このシナリオでは、カスタム フィンガープリントの使用は推奨しません。

識別されないオペレーティング システムに一意の TCP スタックがありますか

システムがホストを誤って識別した場合、カスタム フィンガープリントを作成してアクティブにするか、検出（ディスカバリ）データの代わりに Nmap またはホストの入力データを使用するかを決定するために、ホストが誤って識別された理由を調べる必要があります。

注意 ホストの誤認が発生した場合は、カスタム フィンガープリントを作成する前にサポート担当者にお問い合わせください。

ホストがデフォルトではシステムに検出されないオペレーティング システムを実行していて、識別用の TCP スタックの特性を既存の検出されているオペレーティング システムと共有していない場合、カスタム フィンガープリントを作成する必要があります。

たとえば、システムで識別できない一意の TCP スタックを保持する Linux のカスタマイズ バージョンが存在する場合、継続的に自分でデータを更新する必要のあるスキャン結果またはサードパーティのデータを使用するのではなく、システムがそのホストを識別してそのホストを監視し続けることができるカスタム フィンガープリントを作成する方が便利です。

オープン ソースの Linux ディストリビューションの多くで同じカーネルを使用しているため、システムでは Linux のカーネル名を使用してそれらを識別することに注意してください。Red Hat Linux システム用のカスタム フィンガープリントを作成する場合、同じフィンガープリントが複数の Linux ディストリビューションに一致するために、その他のオペレーティング システム（Debian Linux、Mandrake Linux、Knoppix など）が Red Hat Linux として識別されることがあります。

フィンガープリントをあらゆる状況で使用することは避けてください。たとえば、ホストの TCP スタックが別のオペレーティング システムと類似するか、または同一になるように、すでに変更済みの場合があります。たとえば、Apple Mac OS X ホストのフィンガープリントが Linux 2.4 ホストと同じフィンガープリントになるように変更されると、システムはそのホストを Mac OS X ではなく Linux 2.4 として識別します。その Mac OS X ホストにカスタム フィンガープリントを作成すると、すべての正規の Linux 2.4 ホストが誤って Mac OS X ホストとして識別される場合があります。この場合、Nmap が正しくホストを識別するならば、そのホストに対して定期的な Nmap スキャンをスケジュールできます。

ホスト入力を使用して、サードパーティ製のシステムからデータをインポートする場合、サーバおよびアプリケーション プロトコルを説明するためにサードパーティが使用するベンダー、製品、およびバージョンの文字列を、それらの製品の Cisco の定義にマッピングする必要があります。アプリケーション データを Firepower システムのベンダーとバージョンの定義にマッピングした場合でも、インポートされたサードパーティ製の脆弱性はクライアントまたは Web アプリケーションの影響評価には使用されないことに注意してください。

システムは複数のソースからのデータを照合して、オペレーティング システムまたはアプリケーションの現在の ID を判別することがあります。

Nmap データの場合、定期的な Nmap スキャンをスケジュールできます。ホスト入力データの場合、インポート用の Perl スクリプト、またはコマンドライン ユーティリティを定期的に実行できます。ただし、アクティブのスキャン データとホスト入力データは、検出（ディスカバリ）データの頻度で更新されないことがあるので注意してください。

Firepower システムがすべてのアプリケーションを識別できますか

ホストがシステムによって正しく識別されるものの、識別されないアプリケーションがホストにある場合、ユーザ定義のディテクタを作成して、アプリケーションを識別するために役立つポートおよびパターン マッチング情報をシステムに提供することができます。

脆弱性を修正するパッチを適用しましたか

システムがホストを正しく識別するものの、適用した修正が反映されない場合、ホスト入力機能を使用してパッチ情報をインポートすることができます。パッチ情報をインポートする場合、修正名をデータベース内の修正にマッピングする必要があります。

サードパーティ製の脆弱性を追跡しますか

影響の関連付け（相関）に使用したいサードパーティ製システムからの脆弱性情報がある場合、サーバおよびアプリケーション プロトコル用のサードパーティの脆弱性 ID を Cisco のデータベース内の脆弱性 ID にマッピングしてから、ホスト入力機能を使用してそれらの脆弱性をインポートすることができます。ホスト入力機能の使用の詳細については、『*Firepower System Host Input API Guide*』を参照してください。アプリケーション データを Firepower システムのベンダーとバージョンの定義にマッピングした場合でも、インポートされたサードパーティ製の脆弱性はクライアントまたは Web アプリケーションの影響評価には使用されないことに注意してください。

第 68 章

レルムとアイデンティティ ポリシー

次のトピックでは、レルムとアイデンティティ ポリシーについて説明します。

レルムとアイデンティティ ポリシーについて

レルムは、同じディレクトリ クレデンシャルを共有する 1 つ以上の LDAP または Microsoft Active Directory サーバで構成されます。ユーザおよびユーザ グループ クエリやユーザ制御を実行したり、権限のあるアイデンティティ ソースを設定したりするには、レルムを設定する必要があります。1 つ以上のレルムを設定すると、アイデンティティ ポリシーを設定できます。

アイデンティティ ポリシーは、ネットワーク上のトラフィックを権限のあるアイデンティティ ソースおよびレルムと関連付けます。1 つ以上のアイデンティティ ポリシーを設定した後、1 つをアクセス コントロール ポリシーに関連付け、そのアクセス コントロール ポリシーを管理対象デバイスに展開できます。

レルムについて

レルムは、Firepower Management Center とモニタするサーバのユーザ アカウントとの間の接続です。レルムはサーバの接続設定と認証フィルタ設定を指定します。レルムでは次のことを実行できます。

- アクティビティをモニタするユーザとユーザ グループを指定する。

- 権限のあるユーザ、および権限のあるユーザ以外の一部のユーザ（トラフィック ベースの検出で検出された POP3 および IMAP ユーザ、およびトラフィック ベースの検出、ユーザ エージェント、ISE によって検出されたユーザ）のユーザ メタデータについてユーザ リポジトリに照会する。

レルム内のディレクトリとして複数のドメイン コントローラを追加できますが、同じ基本レルム情報を共有する必要があります。レルム内のディレクトリは、LDAP サーバのみ、または Active Directory（AD）サーバのみである必要があります。レルムを有効にすると、保存された変更は次回 Firepower Management Centerがサーバに照会するときに適用されます。

ユーザ認識を行うには、サポートされるすべてのサーバ タイプのレルムを設定する必要があります。システムは、これらの接続を使用して、POP3 および IMAP ユーザに関連するデータについてサーバにクエリし、トラフィック ベースの検出で検出された LDAP ユーザに関するデータを収集します。

システムは、POP3 および IMAP ログイン内の電子メール アドレスを使用して、Active Directory、OpenLDAP、または Oracle Directory Server Enterprise Edition サーバ上の LDAP ユーザに関連付けます。たとえば、LDAP ユーザと電子メール アドレスが同じユーザの POP3 ログインを管理対象デバイスが検出すると、システムは LDAP ユーザのメタデータをそのユーザに関連付けます。

ユーザ制御を実行するために以下のいずれかを設定できます。

- ユーザ エージェントまたは ISE をサポートするように設定された AD サーバのレルム。
- キャプティブ ポータルをサポートするように設定された AD、Oracle Directory、OpenLDAP サーバのレルム

。

ユーザ ダウンロードについて

特定の検出されたユーザの、次のユーザとユーザ グループのメタデータを取得するために、Firepower Management Center と LDAP サーバまたは AD サーバとの間の接続を確立するためのレルムを設定することができます。

- キャプティブ ポータルで認証された、あるいはユーザ エージェントまたは ISE で報告された LDAP および AD ユーザ。このメタデータは、ユーザ認識とユーザ制御に使用できます。
- トラフィック ベースの検出で検出された POP3 と IMAP ユーザ ログイン（ユーザが LDAP または AD ユーザと同じ電子メール アドレスを持つ場合）。このメタデータは、ユーザ認識に使用できます。

レルム内の 1 つのディレクトリとして、個々のサーバ接続を設定します。ユーザ認識とユーザ制御のためにレルムのユーザおよびユーザ グループ データをダウンロードするには、[アクセス コントロールのためのユーザおよびユーザ グループのダウンロード（Download users and user groups for access control）] をオンにする必要があります。

Firepower Management Centerは、ユーザごとに次の情報とメタデータを取得します。

- LDAP ユーザ名
- 姓と名

- 電子メール アドレス（Email address）
- 部署名（Department）
- 電話番号（Telephone number）

ユーザ アクティビティ データについて

ユーザ アクティビティ データはユーザ アクティビティ データベースに保存され、ユーザのアイデンティティデータはユーザデータベースに保存されます。アクセス制御で保存できる使用可能なユーザの最大数は Firepower Management Center モデルによって異なります。含めるユーザとグループを選択するときは、ユーザの総数がモデルの上限より少ないことを確認してください。アクセス制御パラメータの範囲が広すぎる場合、Firepower Management Center はできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザの数をメッセージ センターの [タスク（Tasks）] タブ ページで報告します。

（注） ユーザ リポジトリからシステムによって検出されたユーザを削除しても、Firepower Management Center はユーザデータベースからそのユーザを削除しません。そのため、手動で削除する必要があります。ただし、LDAP に対する変更は、Firepower Management Center が次に権限のあるユーザのリストを更新したときにアクセス コントロール ルールに反映されます。

レルムおよび信頼できるドメイン

Firepower Management Center でレルムを設定すると、そのレルムは Active Directory または LDAP ドメインに関連付けられます。

互いに信頼する Microsoft Active Directory（AD）ドメインのグループ化は、一般的にフォレストと呼ばれます。この信頼関係により、ドメインは異なる方法で互いのリソースにアクセスできます。たとえば、ドメイン A で定義されたユーザ アカウントに、ドメイン B で定義されたグループのメンバーとしてマークを付けることができます。

Firepower システムは、信頼できる AD ドメインをサポートしていません。つまり、Firepower システムは、どのドメインが互いに信頼しているかを追跡せず、どのドメインが互いの親ドメインまたは子ドメインかを認識しません。また、Firepower システムでは、信頼関係が Firepower システム外で実施される場合でも、クロスドメイン信頼を使用する環境のサポートを保証するテストがまだ行われていません。

詳細については、レルムとユーザのダウンロードのトラブルシューティング，（1583 ページ）を参照してください。

レルムがサポートされているサーバ

レルムを設定して次のサーバ タイプに接続すると、Firepower Management Centerからの TCP/IP アクセスを提供できます。

サーバ タイプ（Server Type）	ユーザ認識によるデータ取得のサポート	ユーザエージェントによるデータ取得のサポート	ISE によるデータ取得のサポート	キャプティブポータルによるデータ取得のサポート
Windows Server 2008 と Windows Server 2012 上の Microsoft Active Directory	○	○	○	○
Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0	[はい（Yes）]	[いいえ（No）]	○	○
Linux 上の OpenLDAP	[はい（Yes）]	[いいえ（No）]	[いいえ（No）]	○

サーバ グループの設定に関して次の点に注意してください。

- ユーザ グループまたはグループ内のユーザに対してユーザ制御を実行するには、サーバでユーザ グループを設定する必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、Firepower Management Centerはユーザ グループ制御を実行できません。
- グループ名は LDAP で内部的に使用されているため、S- で開始することはできません。

  グループ名または組織単位名には、アスタリスク（*）、イコール（=）、バックスラッシュ（\）などの特殊文字は使用できません。使用すると、それらのグループまたは組織単位内のユーザはダウンロードされず、アイデンティティ ポリシーでは使用できません。
- サーバのサブグループのメンバーであるユーザを選別できる Active Directory レルムを設定する際は、Active Directory サーバが報告するユーザの数を以下に制限することに注意します。
  - Windows サーバ 2008 または 2012 上の Microsoft Active Directory では、グループごとに 5000 ユーザまで。

  必要に応じて、より多くのユーザをサポートするため、このデフォルトの制限を引き上げるよう Active Directory サーバの設定を変更できます。

サポートされるサーバ フィールド名

レルムのサーバは、Firepower Management Center がサーバからユーザ メタデータを取得できるように、次の表に記載されているフィールド名を使用する**必要があります**。サーバ上のフィールド名が正しくない場合、Firepower Management Centerはそのフィールドの情報を使ってデータベースに入力できなくなります。

表 *198*：*Firepower Management Center* フィールドへのサーバ フィールドのマッピング

メタデータ	Management Center のフィールド	Active Directory フィールド	Oracle Directory Server フィールド	OpenLDAP フィールド
LDAP ユーザ名	[ユーザ名（Username）]	samaccountname	cn uid	cn uid
first name	名	givenname	givenname	givenname
last name	姓	sn	sn	sn
メールアドレス	E メール	メール アドレス userprincipalname（mail に値が設定されていない場合）	メール アドレス	メール アドレス
部署	部署名（Department）	部署 distinguishedname（department に値が設定されていない場合）	部署	ou
電話番号	電話	telephonenumber	適用対象外	telephonenumber

レルムとユーザのダウンロードのトラブルシューティング

予期しないサーバ接続の動作に気付いたら、レルム設定、デバイス設定、またはサーバ設定の調整を検討してください。関連の他のトラブルシューティングについては、次を参照してください。

- ユーザ エージェント アイデンティティ ソースのトラブルシューティング，（1535 ページ）
- ISE アイデンティティ ソースのトラブルシューティング，（1539 ページ）
- キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング，（1546 ページ）
- ユーザ制御のトラブルシューティング，（367 ページ）

症状：アクセス コントロール ポリシーがグループのメンバーシップと一致しない

この解決策は、他の AD ドメインとの信頼関係にある AD ドメインに適用されます。以下の説明で、外部ドメイン ドメインは、ユーザがログインするドメイン以外のドメインを指します。

ユーザが信頼されている外部ドメインで定義されたグループに属している場合、Firepower は外部ドメインのメンバーシップを追跡しません。たとえば、次のシナリオを考えてください。

- ドメイン コントローラ 1 と 2 は相互に信頼している
- グループ A はドメイン コントローラ 2 で定義されている
- コントローラ 1 のユーザ mparvinder はグループ A のメンバーである

ユーザ mparvinder はグループ A に属しているが、メンバーシップ グループ A を指定する Firepower のアクセス コントロール ポリシー ルールが一致しません。

解決策：グループ A に属する、すべてのドメイン 1 のアカウントを含むドメイン コントローラ 1 に同様のグループを作成します。グループ A またはグループ B のすべてのメンバーに一致するように、アクセス コントロール ポリシー ルールを変更します。

症状：アクセス コントロール ポリシーが子ドメインのメンバーシップと一致しない

ユーザが親ドメインの子であるドメインに属している場合、Firepowerはドメイン間の親/子関係を追跡しません。たとえば、次のシナリオを考えてください。

- ドメイン child.parent.com はドメイン parent.com の子である
- ユーザ mparvinder は child.parent.com で定義されている

ユーザ mparvinder が子ドメインに属しているが、parent.com と一致する Firepower アクセス コントロール ポリシーが child.parent.com ドメインの mparvinder と一致しません。

解決策：parent.com または child.parent.com のいずれかのメンバーシップに一致するようにアクセス コントロール ポリシー ルールを変更します。

予期しない時間にユーザ タイムアウトが発生する

予期しない間隔でユーザタイムアウトが実行されていることに気付いたら、ユーザエージェントまたは ISE サーバの時間が Firepower Management Centerの時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。

レルム設定で指定したようにユーザが含まれない、または除外されない

サーバのサブグループのメンバーであるユーザを選別できる Active Directory レルムを設定する際は、Microsoft Windows サーバが報告するユーザの数を以下に制限することに注意します。

- Windows サーバ 2008 または 2012 では、グループごとに 5000 ユーザまで。Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0

必要に応じて、より多くのユーザをサポートするため、このデフォルトの制限を引き上げるようサーバの設定を変更できます。

ユーザがダウンロードされない

グループ名または組織単位名に特殊文字が使用されている Active Directory グループのユーザは、アイデンティティ ポリシー ルールで使用できない可能性があります。たとえば、グループ名または組織単位名にアスタリスク（*）、イコール（=）、バックスラッシュ（\）などの特殊文字が含

まれている場合、これらのグループ内のユーザはダウンロードされず、アイデンティティ ポリシーで使用できません。

解決策：グループ名または組織単位名から特殊文字を削除します。

未知の ISE とユーザエージェントのユーザのユーザデータが Web インターフェイスで表示されない

システムはデータがまだデータベースにない ISE またはユーザエージェントユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。状況によっては、システムが Active Directory サーバからこの情報を正常に取得するためにさらに時間がかかることもあります。データ取得が成功するまで、ISE またはユーザエージェントユーザから見えるアクティビティは Web インターフェイスに表示**されません**。

これにより、アクセス制御ルールを使ったユーザトラフィックの処理も妨げられることがある点に注意します。

イベントのユーザデータが想定外の内容になる

ユーザやユーザアクティビティイベントに想定外の IP アドレスが含まれる場合は、レルムを確認します。複数のレルムに同一の [AD プライマリ ドメイン（AD Primary Domain）] の値を設定することはできません。

アイデンティティ ポリシーについて

アイデンティティ ポリシーには、アイデンティティ ルールが含まれます。アイデンティティ ルールでは、トラフィックのセットを、レルムおよび認証方式（パッシブ認証、アクティブ認証、または認証なし）と関連付けます。

アイデンティティ ルールで呼び出す前に、使用するレルムおよび認証方式を完全に設定しておく必要があります。

- [システム（System）] > [統合（Integration）] > [レルム（Realms）] でアイデンティティ ポリシー外のレルムを設定します。詳細については、レルムの作成, （1586 ページ）を参照してください。
- パッシブ認証のアイデンティティ ソースであるユーザ エージェントと ISE は、[システム（System）] > [統合（Integration）] > [アイデンティティ ソース（Identity Sources）] で設定します。詳細については、ユーザ エージェント接続の設定, （1534 ページ）およびISE 接続の設定, （1536 ページ）を参照してください。
- アクティブ認証のアイデンティティ ソースであるキャプティブ ポータルについては、アイデンティティ ポリシー内で設定します。詳細については、キャプティブ ポータル アイデンティティ ルールの設定, （1541 ページ）を参照してください。

単一のアイデンティティ ポリシーに複数のアイデンティティ ルールを追加した後、ルールの順番を決めます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールがそのトラフィックを処理するルールです。

1 つ以上のアイデンティティ ポリシーを設定した後、アクセス コントロール ポリシーの 1 つのアイデンティティ ポリシーを呼び出す必要があります。ネットワークのトラフィックがアイデンティティ ルールの条件と一致する場合、システムはトラフィックを指定されたレルムと関連付け、指定されたアイデンティティ ソースを使用してトラフィックのユーザを認証します。

アイデンティティ ポリシーを設定しない場合、システムはユーザ認証を実行しません。

関連トピック

ユーザ アイデンティティ ソース, （1531 ページ）

レルムの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator、Access Admin、Network Admin

レルム設定フィールドの詳細については、レルム フィールド, （1587 ページ）を参照してください。

手順

ステップ 1 Firepower Management Center にログインします。

ステップ 2 [システム（System）] > [統合（Integration）] をクリックします。

ステップ 3 [レルム（Realms）] をクリックします。

ステップ 4 新しいレルムを作成するには、[新規レルム（New Realm）] をクリックします。

ステップ 5 その他のタスク（レルムの有効化、無効化、削除など）を実行する場合は、レルムの管理, （1604 ページ）を参照してください。

ステップ 6 レルム フィールド, （1587 ページ）で説明したように、レルム情報を入力します。

ステップ 7 （オプション）レルムへの接続をテストするには、[テスト（Test）] をクリックします。

（注） レルム テストが成功するには、[AD 結合ユーザ名（AD Join Username）] と [AD 結合パスワード（AD Join Password）] の両方のフィールドに値を入力する必要があります。

ステップ 8 [OK] をクリック

ステップ 9 レルム ディレクトリの設定, （1591 ページ）で説明したように、少なくとも 1 つのディレクトリを設定します。

ステップ 10 ユーザとグループのダウンロード, （1592 ページ）の説明に従ってユーザとユーザ グループのダウンロード（アクセス コントロールに必要）を設定します。

ステップ 11 [レルム設定（Realm Configuration）] タブをクリックします。

ステップ 12 [認証済みユーザ（Authenticated Users）]、[認証に失敗したユーザ（Failed Authentication Users）]、および [ゲスト ユーザ（Guest Users）] にユーザ セッション タイムアウト値（分単位）を入力します。

次の作業

- レルム ディレクトリの設定, （1591 ページ）
- レルムの編集、削除、有効化、または無効化を行います。レルムの管理, （1604 ページ）を参照してください
- レルムの比較, （1605 ページ）。
- 必要に応じて、タスクのステータスをモニタします（タスク メッセージの表示, （303 ページ） を参照）。

レルム フィールド

次のフィールドを使用してレルムを設定します。

レルムの設定（Realm Configuration）フィールド

これらの設定は、レルム内のすべてのサーバまたはコントローラ（別名ディレクトリ）に適用されます。

[名前（Name）]

レルムの一意の名前。英数字や特殊文字に対応しています。

説明

（オプション）レルムの説明を入力します。

AD プライマリ ドメイン（AD Primary Domain）

Active Directory レルムのみの場合に、ユーザを認証する必要があるアクティブ ディレクトリ サーバのドメイン。同じ [AD プライマリ ドメイン（AD Primary Domain）] 値を持つ複数のレルムを作成することはできません。

（注） [AD プライマリ ドメイン（AD Primary Domain）] 値のすべてのレルムが一意である必要があります。

[ディレクトリ ユーザ名（Directory Username）] と [ディレクトリ パスワード（Directory Password）]

取得するユーザ情報に適切な権限を持っているユーザの識別用のユーザ名とパスワード。

ベース DN（Base DN）

Firepower Management Center がユーザ データの検索を開始するサーバのディレクトリ ツリー。

通常、ベース DN は企業ドメイン名および部門を示す基本構造があります。たとえば、Example 社のセキュリティ部門のベース DN は、ou=security,dc=example,dc=com となります。

グループ DN（Group DN）

Firepower Management Centerがグループ属性を持つユーザを検索するサーバのディレクトリツリー。

（注） グループ名または組織単位名には、アスタリスク（*）、イコール（=）、バックスラッシュ（\）などの特殊文字は使用できません。使用した場合、それらのグループのユーザはダウンロードされず、アイデンティティ ポリシーで使用できないためです。

グループ属性（Group Attribute）

（オプション）サーバのグループ属性：メンバー、または一意のメンバー。

タイプ（Type）

レルム、AD、LDAP のタイプ。

（注） キャプティブ ポータルのみ、LDAP レルムをサポートします。

レルムの設定（Realm Configuration）フィールド

Active Directory 情報

Active Directory 情報のフィールドについては、このセクションの前半で説明しました。

[ユーザ セッション タイムアウト（User Session Timeout）]

ユーザ セッションがタイムアウトするまでの分数を入力します。デフォルトは 1440 分（24 時間）です。

（注） ユーザ セッションのタイムアウト値は、アクティブ認証（キャプティブ ポータル）とパッシブ認証（TS エージェント、ISE、ISE-PIC）の両方に適用されます。大きな値を設定すると、ユーザ セッションが終了しない可能性があり、他のユーザによってこれらのセッションが要求される場合があります。

レルムのディレクトリ フィールド（Realm Directory Fields）

これらの設定は、レルム内の個々のサーバ（ディレクトリ）に適用されます。

暗号化（Encryption）

Firepower Management Center サーバ接続に使用する暗号化方式。

- STARTTLS：暗号化 LDAP 接続
- LDAPS：暗号化 LDAP 接続
- なし：非暗号化 LDAP 接続（保護されていないトラフィック）

ホスト名/IP アドレス（Hostname/IP Address）

サーバのホスト名または IP アドレス。[暗号化（Encryption）] 方式を指定する場合は、このフィールドでホスト名を指定します。

[ポート（Port）]

Firepower Management Center サーバ接続に使用するポート。

SSL 証明書（SSL Certificate）

サーバへの認証に使用する SSL 証明書。SSL 証明書を使用するにために、STARTTLS または LDAPS を [暗号化（Encryption）] タイプとして設定できます。

認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IP アドレス（Hostname/IP Address）] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用し、証明書内で computer1.example.com を使用した場合は、接続が失敗します。

ユーザのダウンロード（User Download）フィールド

[使用可能なグループ（Available Groups）]、[含むに追加する（Add to Include）]、[除外するに追加する（Add to Exclude）]

ダウンロードし、ユーザ認識やユーザ制御に使用できるグループを特定します。

- [使用可能グループ ボックス（Available Groups）] にグループが残っている場合、グループのダウンロードは行われません。
- グループを [含むに追加する（Add to Include）] ボックスに移動させた場合、そのグループはダウンロードされ、ユーザ データはユーザ認識やユーザ制御に利用できます。
- [除外に追加する（Add to Exclude）] ボックスにグループを移動させると、グループがダウンロードされ、ユーザ データはユーザ認識に利用できますが、ユーザ制御には利用できません。

自動ダウンロードの開始、繰り返し設定（Begin automatic download at, Repeat every）

自動ダウンロードの回数を指定します。

ユーザおよびグループのダウンロード（ユーザアクセス制御に必須）

ユーザ データの自動ダウンロードができます。

基本的なレルム情報の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

レルム設定フィールドの詳細については、レルム フィールド, （1587 ページ）を参照してください。

手順

ステップ 1 [新しいレルムの追加（Add New Realm）] ページで、[名前（Name）] とオプションで [説明（Description）] を入力します。

ステップ 2 ドロップダウン リストから [タイプ（Type）] を選択します。

ステップ 3 AD レルムを設定する場合は、[AD プライマリ ドメイン（AD Primary Domain）] を入力します。

（注） 同じ [AD プライマリ ドメイン（AD Primary Domain）] 値を持つ複数のレルムを作成することはできません。

ステップ 4 取得するユーザ情報に適切な権限を持っているユーザの識別用の[ディレクトリ ユーザ名（Directory Username）] と [ディレクトリ パスワード（Directory Password）] を入力します。

ステップ 5 ディレクトリの [ベース DN（Base DN）] を入力します。

ステップ 6 ディレクトリの [グループ DN（Group DN）] を入力します。

ステップ 7 オプションで、ドロップダウン リストから [グループ属性（Group Attribute）] を選択します。

ステップ 8 [OK] をクリックします。

ステップ 9 オプションで、レルムへの接続をテストするには、[テスト（Test）] をクリックします。

（注） レルム テストが成功するには、[AD 結合ユーザ名（AD Join Username）] と [AD 結合パスワード（AD Join Password）] の両方のフィールドに値を入力する必要があります。

次の作業

- レルム ディレクトリの設定, （1591 ページ）の説明に従ってレルム ディレクトリを設定します。

レルム ディレクトリの設定

この手順により、レルムを作成できます。レルムは Firepower Management Center と LDAP リポジトリ（Microsoft Active Directory など）の間の接続です。この接続を作成した後、ユーザとグループをダウンロードする必要があります。ユーザ制御ではこれらのユーザとグループのみを使用できます。

ユーザやグループが変更された場合、将来の任意の時点でそれをダウンロードできます。または、ユーザとグループのダウンロード, （1592 ページ）の説明に従って自動ダウンロードを設定することもできます。

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator、Access Admin、Network Admin

レルム設定フィールドの詳細については、レルム フィールド, （1587 ページ）を参照してください。

はじめる前に

オプションで SSL 証明書を使用してディレクトリで認証するには、Firepower Management Center のアクセス元となるマシンでPKI オブジェクトするか、証明書データとキーを利用可能にします。

手順

ステップ 1 まだ実行していない場合は、Firepower Management Center にログインし、[統合（Integration）] > [レルム（Realms）] をクリックします。

ステップ 2 [レルム（Realms）] タブ ページで、ディレクトリの設定対象となるレルムの名前をクリックします。

ステップ 3 [ディレクトリ（Directory）] タブ ページで、[ディレクトリの追加（Add Directory）] をクリックします。

ステップ 4 [サーバのホスト名/IP アドレス（Hostname / IP Address）] と [ポート（Port）] を入力します。

ステップ 5 [暗号化モード（Encryption Mode）] を選択します。

ステップ 6 （オプション）リストから [SSL 証明書（SSL Certificate）] を 1 つ選択するか、追加アイコン（  ）をクリックして証明書を追加します。

ステップ 7 接続をテストするには、[テスト（Test）] をクリックします。

ステップ 8 [OK] をクリックします。

ステップ 9 [保存（Save）] をクリックします。[レルム（Realms）] タブ ページに戻ります。

ステップ 10 レルムをまだ有効にしていない場合は、[レルム（Realms）] タブ ページで、[状態（State）] を有効にします。

次の作業

- ユーザとグループのダウンロード, （1592 ページ）.

ユーザとグループのダウンロード

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

このセクションでは、Active Directory サーバから Firepower Management Center にユーザとグループをダウンロードする方法について説明します。含めるグループを指定しなかった場合、システムは指定されたパラメータと一致するすべてのグループのユーザ データを取得します。パフォーマンス上の理由から、アクセス コントロールに使用するユーザを表すグループだけを明示的に含めることをお勧めします。

Firepower Management Center がサーバから取得可能なユーザの最大数は Firepower Management Center モデルによって異なります。レルムのダウンロード パラメータの範囲が広すぎる場合、Firepower

Management Center はできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数を Message Center の [タスク（Task）] タブで報告します。

レルム設定フィールドの詳細については、レルム フィールド, （1587 ページ）を参照してください。

手順

ステップ 1 Firepower Management Center にログインします。

ステップ 2 [統合（Integration）] > [レルム（Realms）] をクリックします。

ステップ 3 ユーザとグループを手動でダウンロードするには、ユーザやユーザ グループをダウンロードするレルムの横にあるダウンロードアイコン（  ）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。残りの手順をスキップできます。

ステップ 4 自動でユーザとグループをダウンロードするようにレルムを設定するには、自動でユーザやグループをダウンロードするように設定するレルムの横にある編集アイコン（  ）をクリックします。

ステップ 5 [ユーザ アクセス制御（User Access Control）] タブ ページで、[（ユーザのアクセス コントロールに必要な）ユーザとグループをダウンロードする（Download users and groups (required for user access control)）] チェックボックスをオンにします。

ステップ 6 ドロップダウン リストから [自動ダウンロードの開始時間（Begin automatic download at）] の時間を選択します。

ステップ 7 [繰り返し設定（Repeat Every）] ドロップダウン リストからダウンロード間隔を選択します。

ステップ 8 ダウンロードからユーザ グループを含めるか除外するには、[選択可能なグループ（Available Groups）] 列からユーザ グループを選択し、[含めるに追加（Add to Include）] または [除外に追加（Add to Exclude）] をクリックします。
複数のユーザはカンマで区切ります。このフィールドでは、アスタリスク（*）をワイルドカード文字として使用できます。

（注） そのグループのユーザに対してユーザ制御を実行する場合は、[含めるに追加（Add to Include）] をクリックする必要があります。

関連トピック

オンデマンドでのユーザとユーザ グループのダウンロード, （1605 ページ）

レルム ユーザ セッション タイムアウトの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator、Access Admin、Network Admin

レルム設定フィールドの詳細については、レルム フィールド, （1587 ページ）を参照してください。

（注） 予期しない間隔でシステムがユーザ タイムアウトを実行していることに気付いたら、ユーザ エージェントまたは ISE サーバの時間が Firepower Management Centerの時間と同期されていることを確認します。

手順

ステップ 1 [レルム設定（Realm Configuration）] タブを選択します。

ステップ 2 [認証済みユーザ（Authenticated Users）]、[認証に失敗したユーザ（Failed Authentication Users）]、および [ゲスト ユーザ（Guest Users）] にユーザ セッション タイムアウト値を入力します。

ステップ 3 [保存（Save）] をクリックするか、レルムの編集を続けます。

アイデンティティ ポリシーの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

はじめる前に

- レルムの作成, （1586 ページ）の説明に従って 1 つ以上のレルムを作成し、有効にします。

手順

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

ステップ 2 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [ID（Identity）] を選択し、[新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] を入力し、必要に応じて [説明（Description）] を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 ポリシーにルールを追加するには、アイデンティティ ルールの作成, （1595 ページ）で説明されているように、[ルールの追加（Add Rule）] をクリックします。

ステップ 6 ルール カテゴリを作成するには、アイデンティティ ルール カテゴリの追加, （1609 ページ）で説明されているように、[カテゴリの追加（Add Category）] をクリックします。

ステップ 7 キャプティブ ポータルのアクティブ認証を設定するには、キャプティブ ポータル アイデンティティ ルールの設定, （1541 ページ）で説明されているように、[アクティブ認証（Active Authentication）] タブをクリックします。

ステップ 8 [保存（Save）] をクリックして、アイデンティティ ポリシーを保存します。

次の作業

- アクセス コントロール ポリシーとアイデンティティ ポリシーを関連付けます（アクセス制御への他のポリシーの関連付け, （798 ページ）を参照）。
- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

アイデンティティ ルールの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

詳細については、アイデンティティ ルール フィールド, （1597 ページ）を参照してください。

はじめる前に

- アイデンティティ ポリシーの作成, （1594 ページ） の説明に従って、アイデンティティ ポリシーの設定を開始します。

手順

ステップ 1 まだ実行していない場合は、Firepower Management Center にログインし、[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [ID（Identity）] を選択します。

ステップ 2 編集するポリシーの横にある編集（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 名前を入力します。

ステップ 5 ルールを有効にするかどうかを指定します。

ステップ 6 ルール カテゴリにルールを追加するには、ルールを挿入する場所を指定します。カテゴリ作成に関する詳細については、アイデンティティ ルール カテゴリの追加, （1609 ページ） を参照してください。

ステップ 7 リストからルール [アクション（Action）] を選択します。

ステップ 8 オプションで、アイデンティティ ルールへのゾーン条件の追加, （1602 ページ）の説明に従ってゾーン条件を追加します。

（注） キャプティブ ポータルにルールを設定していて、キャプティブ ポータル デバイスにインライン インターフェイスとルーテッド インターフェイスが含まれている場合は、デバイス上のルーテッド インターフェイスのみを対象とするゾーン条件を設定する必要があります。

ステップ 9 オプションで、アイデンティティ ルールへのネットワークまたは位置情報条件の追加, （1599 ページ）の説明に従ってネットワークまたは位置情報の条件を追加します。

ステップ 10 アイデンティティ ルールへの VLAN タグ条件の追加, （1601 ページ）の説明に従って、オプションで VLAN タグの条件を追加します。

ステップ 11 オプションで、アイデンティティ ルールへのポート条件の追加, （1600 ページ）の説明に従ってポート条件を追加します。

システムは、非 TCP トラフィックでキャプティブ ポータル アクティブ認証を実施できません。アイデンティティ ルール アクションが [アクティブ認証（Active Authentication）] である（キャプティブ ポータルを使用している）か、[パッシブ認証でユーザを識別できない場合にアクティブ認証を使用（Use active authentication if passive authentication cannot identify user）] チェックボックスをオンにしている場合は、TCP ポートの制約のみを使用します。アイデンティティ ルール アクションが [パッシブ認証（Passive Authentication）] または [認証なし（No Authentication）] である場合、非 TCP トラフィックに基づいてポート条件を作成できます。

ステップ 12 アイデンティティ ルールとレルムの関連付け, （1603 ページ）の説明に従ってルールをレルムに関連付けます。

ステップ 13 キャプティブ ポータル アイデンティティ ルールの設定, （1541 ページ） の説明に従って、オプションでキャプティブ ポータル設定を構成します。

ステップ 14 [追加（Add）] をクリックします。

ステップ 15 [保存（Save）] をクリックします。

次の作業

- アイデンティティ ポリシーの作成, （1594 ページ） の説明に従って、アイデンティティ ポリシーの設定を続行します。

関連トピック

Snort® の再起動シナリオ , （324 ページ）

アイデンティティ ルール フィールド

次のフィールドを使用して、アイデンティティ ルールを設定します。

[有効（Enabled）]

このオプションを選択すると、アイデンティティ ポリシーのアイデンティティ ルールが有効になります。このオプションの選択を解除すると、アイデンティティ ルールが無効になります。

アクション（Action）

指定されたレルムでユーザに実行する認証のタイプを指定します。[パッシブ認証（Passive Authentication）]（デフォルト）、[アクティブ認証（Active Authentication）]、または [認証なし（No Authentication）] を選択します。アイデンティティ ルールのアクションとして選択する前に、認証方式、またはアイデンティティ ソースを完全に設定する必要があります。

注意 SSL復号が無効の場合（つまりアクセスコントロールポリシーにSSLポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると設定の変更を展開するとSnortプロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作, （326 ページ）を参照してください。

Firepower システムのバージョンでサポートされるパッシブおよびアクティブ認証方式の詳細については、ユーザ アイデンティティ ソースについて, （1531 ページ）を参照してください。

レルム

指定されたアクションを実行するユーザが含まれるレルム。アイデンティティ ルールのレルムとして選択する前に、レルムを完全に設定する必要があります。

認証でユーザを識別できない場合は特別 ID/ゲストとして識別する（Identify as Special Identities/Guest if authentication cannot identify user）

ルール アクションとして [アクティブ認証（Active Authentication）]（つまり、キャプティブ ポータル認証）を設定する場合にのみ、このフィールドが表示されます。

認証タイプ

キャプティブ ポータル アクティブ認証を実行するために使用する方法です。選択は、レルム、LDAP、または AD のタイプによって異なります。

- 暗号化されていない HTTP 基本認証（BA）接続を使用してユーザを認証するには、[HTTP 基本（HTTP Basic）] を選択します。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。

  ほとんどの Web ブラウザは、HTTP 基本ログインからクレデンシャルをキャッシュし、古いセッションがタイムアウトした後にシームレスに新しいセッションを開始するためにそのクレデンシャルを使用します。

- NT LAN Manager（NTLM）接続を使用してユーザを認証するには NTLM を選択します。この選択は AD レルムを選択するときにのみ使用できます。透過的な認証がユーザのブラウザで設定されている場合、ユーザは自動的にログインします。透過的な認証が設定されていない場合、ユーザは各自のブラウザでデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。

- キャプティブ ポータル サーバが認証接続に HTTP 基本認証または NTLM を選択できるようにするには、[HTTP ネゴシエート（HTTP Negotiate）] を選択します。この選択は AD レルムを選択するときにのみ使用できます。

  （注） HTTP ネゴシエート キャプティブ ポータルを実行するアイデンティティ ルールを作成しようとしており、DNS 解決は設定済みである場合は、キャプティブ ポータル デバイスの完全修飾ドメイン名（FQDN）を解決する DNS サーバを設定する必要があります。FQDN は、DNS 設定時に指定したホスト名と一致する必要があります。

  ASA with FirePOWER Services および Firepower Threat Defense デバイスの場合、FQDN は、キャプティブ ポータルに使用されるルーテッド インターフェイスの IP アドレスに解決される必要があります。

- システムで提供されている、またはカスタムの HTTP 応答ページを使用してユーザを認証する場合は、[HTTP 応答ページ（HTTP Response Page）] を選択します。ユーザは設定された応答ページを使用してネットワークにログインします。

アイデンティティ ルールへのネットワークまたは位置情報条件の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 アイデンティティ ルール エディタ ページで、[ネットワーク（Networks）] タブを選択します。

ステップ 2 [利用可能なネットワーク（Available Networks）] から、次のように追加するネットワークを見つけます。

- ネットワーク オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[利用可能なネットワーク（Available Networks）] リストの上にある追加アイコン（  ）をクリックします。
- 追加するネットワークまたは地理位置情報オブジェクトを検索するには、[利用可能なネットワーク（Available Networks）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ 4 [送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。

ステップ 5 手動で指定する送信元または宛先 IP アドレスまたはアドレスブロックを追加します。[送信元ネットワーク（Source Networks）] リストまたは [宛先ネットワーク（Destination Networks）] リストの下にある [IP アドレスの入力（Enter an IP address）] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [追加（Add）] をクリックします。

ステップ 6 [追加（Add）] をクリックするか、ルールの編集を続けます。

次の作業

- アイデンティティ ルールの作成, （1595 ページ）の説明に従ってアイデンティティ ルールの作成を続けます。

アイデンティティ ルールへのポート条件の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Admin Access Admin Network Admin

（注） システムは、非 TCP トラフィックでキャプティブ ポータル アクティブ認証を実施できません。アイデンティティ ルール アクションが [アクティブ認証（Active Authentication）] である（キャプティブ ポータルを使用している）か、[パッシブ認証でユーザを識別できない場合にアクティブ認証を使用（Use active authentication if passive authentication cannot identify user）] チェックボックスをオンにしている場合は、TCP ポートの制約のみを使用します。アイデンティティ ルール アクションが [パッシブ認証（Passive Authentication）] または [認証なし（No Authentication）] である場合、非 TCP トラフィックに基づいてポート条件を作成できます。

手順

ステップ 1 アイデンティティ ルール エディタで、[ポート（Ports）] タブをクリックします。

ステップ 2 [使用可能なポート（Available Ports）] リストで、追加する事前定義されたポートを見つけて選択します。

- ポート オブジェクトをここで追加するには（後で条件に追加できます）、追加アイコン（  ）をクリックします。
- 追加するポート オブジェクトおよびグループを検索するには、[名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトのポートの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。たとえば、「443」と入力すると、システム提供の HTTPS ポート オブジェクトがルール エディタに表示されます。

ステップ 3 [送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 4 手動で指定する送信元ポートまたは宛先ポートを追加します。

- [送信元（Source）]：プロトコルを選択し、0 から 65535 までのポートを 1 つ入力して [追加（Add）] をクリックします。
- [宛先（ICMP 以外）（Destination (non-ICMP)）]：プロトコルを選択または入力します。プロトコルを指定しない場合、または [TCP] か [UDP] を選択した場合は、0 から 65535 までのポートを 1 つ入力します。[追加（Add）] をクリックします。

- [宛先（ICMP）（Destination (ICMP)）]：[プロトコル（Protocol）] ドロップダウン リストから [ICMP] または [IPv6-ICMP] を選択し、表示されるポップアップ ウィンドウでタイプおよび関連するコードを選択します。ICMP タイプとコードの詳細については、Internet Assigned Numbers Authority（IANA）の Web サイトを参照してください。.

ステップ 5 ルールを保存するか、編集を続けます。

次の作業

- アイデンティティ ルールの作成, （1595 ページ）の説明に従ってアイデンティティ ルールの作成を続けます。

アイデンティティ ルールへの VLAN タグ条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator、Access Admin、Network Admin

手順

ステップ 1 アイデンティティ ルール エディタ ページで、[VLAN タグ（VLAN Tags）] タブを選択します。

ステップ 2 [利用可能な VLAN タグ（Available VLAN Tags）] で、次のように追加する VLAN を見つけます。

- VLAN タグ オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[利用可能な VLAN タグ（Available VLAN Tags）] リストの上にある追加アイコン（）をクリックします。
- 追加する VLAN タグ オブジェクトおよびグループを検索するには、[利用可能な VLAN タグ（Available VLAN Tags）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクト名またはオブジェクトの VLAN タグの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ 4 [ルールに追加（Add to Rule）] をクリックします。

ステップ 5 手動で指定する VLAN タグを追加します。[選択した VLAN タグ（Selected VLAN Tags）] リストの下にある [VLAN タグの入力（Enter a VLAN Tag）] プロンプトをクリックし、VLAN タグまた

はその範囲を入力して、[追加（Add）] をクリックします。1 から 4094 までの任意の VLAN タグを指定できます。VLAN タグの範囲を指定するにはハイフンを使用します。

ステップ 6 [追加（Add）] をクリックするか、ルールの編集を続けます。

次の作業

- アイデンティティ ルールの作成, （1595 ページ）の説明に従ってアイデンティティ ルールの作成を続けます。

アイデンティティ ルールへのゾーン条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

（注） キャプティブ ポータルに使用する予定のデバイスにインライン インターフェイスとルーテッド インターフェイスの両方が含まれる場合、キャプティブ ポータル デバイス上でルーテッド インターフェイスだけを対象とするようにキャプティブ ポータル アイデンティティ ルールでゾーン条件を設定する必要があります。

セキュリティ ゾーンの詳細については、セキュリティ ゾーン, （392 ページ）を参照してください。

はじめる前に

- セキュリティ ゾーン オブジェクトの作成, （392 ページ） の説明に従って、セキュリティ ゾーンを設定します。

手順

ステップ 1 アイデンティティ ルール エディタ ページで、[ゾーン（Zones）] タブを選択します。

ステップ 2 [利用可能なゾーン（Available Zones）] から追加するゾーンを見つけます。追加するゾーンを検索するには、[利用可能なゾーン（Available Zones）] リストの上にある [名前で検索（Search by name）]

プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

ステップ 3 クリックすると、ゾーンを選択できます。すべてのゾーンを選択するには、右クリックして[すべて選択（Select All）] を選択します。

ステップ 4 [送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。

ステップ 5 [追加（Add）] をクリックするか、ルールの編集を続けます。

次の作業

- アイデンティティ ルールの作成, （1595 ページ）の説明に従ってアイデンティティ ルールの作成を続けます。

アイデンティティ ルールとレルムの関連付け

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

レルムを各アイデンティティ ルールに関連付けて、指定したアイデンティティ ルールの [アクション（Action）] を使用して認証するユーザを識別する必要があります。

はじめる前に

- レルムの作成, （1586 ページ） の説明に従って 1 つ以上のレルムを作成します。

手順

ステップ 1 まだ実行していない場合は、アイデンティティ ルールの作成, （1595 ページ） を参照してください。

ステップ 2 アイデンティティ ルール エディタ ページで、[レルムおよび設定（Realm & Settings）] タブを選択します。

ステップ 3 リストから [レルム（Realm）] を選択します。

ステップ 4 [追加（Add）] をクリックするか、ルールの編集を続けます。

次の作業

- アイデンティティ ルールの作成, （1595 ページ）の説明に従ってアイデンティティ ルールの作成を続けます。

レルムの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

このセクションでは、[レルム（Realms）] ページ上のコントロールを使用して、レルムに関するさまざまなメンテナンス タスクを実行する方法について説明します。次の点に注意してください。

- コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

手順

ステップ 1 Firepower Management Center にログインします。

ステップ 2 [システム（System）] > [統合（Integration）] をクリックします。

ステップ 3 [レルム（Realms）] をクリックします。

ステップ 4 レルムを削除するには、削除アイコン（）をクリックします。

ステップ 5 レルムを編集するには、レルムの横にある編集アイコン（）をクリックし、レルムの作成, （1586 ページ）の説明に従って変更を行います。

ステップ 6 レルムを有効にするには、[状態（State）] を右にスライドします。レルムを無効にするには、左にスライドします。

ステップ 7 ユーザおよびユーザ グループをダウンロードするには、ダウンロードアイコン（）をクリックします。

ステップ 8 レルムをコピーするには、コピー アイコン（）をクリックします。

ステップ 9 レルムを比較する方法については、レルムの比較, （1605 ページ）を参照してください。

レルムの比較

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator、Security Approver、Access Admin、Network Admin

手順

ステップ 1 Firepower Management Center にログインします。
ステップ 2 [システム（System）] > [統合（Integration）] をクリックします。
ステップ 3 [レルム（Realms）] をクリックします。
ステップ 4 [システム（System）] > [統合（Integration）] をクリックします。
ステップ 5 [レルム（Realms）] をクリックします。
ステップ 6 [レルムの比較（Compare Realms）] をクリックします。
ステップ 7 [比較対象（Compare Against）] リストから [レルムの比較（Compare Realm）] を選択します。
ステップ 8 [レルム A（Realm A）] および [レルム B（Realm B）] リストから比較するレルムを選択します。
ステップ 9 [OK] をクリック
ステップ 10 個々の変更を選択するには、タイトル バーの上の [前へ（Previous）] または [次へ（Next）] をクリックします。
ステップ 11 （オプション）[比較レポート（Comparison Report）] をクリックして、レルム比較レポートを生成します。
ステップ 12 （オプション）[新しい比較（New Comparison）] をクリックして、新しいレルム比較ビューを生成します。

オンデマンドでのユーザとユーザ グループのダウンロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator、Access Admin、Network Admin

レルムのユーザ ダウンロード パラメータまたはグループ ダウンロード パラメータを変更する場合、またはサーバでユーザまたはグループを変更して変更をユーザ制御にすぐに反映させる場合は、サーバからのオンデマンド ユーザ ダウンロードの実行を Firepower Management Centerに強制できます。

Firepower Management Center がサーバから取得可能なユーザの最大数は Firepower Management Center モデルによって異なります。レルムのダウンロードパラメータの範囲が広すぎる場合、Firepower Management Center はできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数を Message Center の [タスク（Task）] タブで報告します。

はじめる前に

- 次の説明に従い、レルムを有効にします。 レルムの有効化または無効化, （1606 ページ）

手順

ステップ 1 [システム（System）] > [統合（Integration）] を選択します。

ステップ 2 [レルム（Realms）] をクリックします。

ステップ 3 ユーザとユーザ グループをダウンロードするレルムの横のダウンロードアイコン（）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

次の作業

- 必要に応じて、タスクのステータスをモニタします（タスク メッセージの表示, （303 ページ） を参照）。

レルムの有効化または無効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

レルムを無効にすると、システムはユーザ ダウンロードのサーバへのクエリを停止し、アイデンティティ ルールでレルムを使用できないようにします。

手順

ステップ 1 [システム（System）] > [統合（Integration）] を選択します。

ステップ 2 [レルム（Realms）] をクリックします。

ステップ 3 有効または無効にするレルムの横にある [状態（State）] をスライドします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

次の作業

- 必要に応じて、タスクのステータスをモニタします（タスク メッセージの表示, （303 ページ） を参照）。

アイデンティティ ポリシーの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

ステップ 2 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [ID（Identity）] を選択します。

ステップ 3 ポリシーを削除するには、削除（）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ポリシーを編集するには、ポリシーの横にある編集（）をクリックし、アイデンティティ ポリシーの作成, （1594 ページ） の説明に従って変更を行います。代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 5 ポリシーをコピーする場合は、コピー アイコン（）をクリックします。

ステップ 6 ポリシーのレポートを生成する場合は、現在のポリシー レポートの生成, （333 ページ） の説明に従って、レポート アイコン（）をクリックします。

ステップ 7 ポリシーを比較する場合は、ポリシーの比較, （331 ページ） を参照してください。

アイデンティティ ルールの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [ID（Identity）] を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 アイデンティティ ルールを編集する場合は、編集アイコン（  ）をクリックし、アイデンティティ ポリシーの作成, （1594 ページ）の説明に従って変更を行います。

ステップ 4 アイデンティティ ルールを削除する場合は、削除アイコン（  ）をクリックします。

ステップ 5 ルール カテゴリを作成する場合は、アイデンティティ ルール カテゴリの追加, （1609 ページ） を参照してください。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

アイデンティティ ルール カテゴリの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

手順

ステップ 1 アイデンティティ ポリシーの編集時に、[カテゴリの追加（Add Category）] をクリックします。

ステップ 2 カテゴリの [名前（Name）] を入力します。

ステップ 3 新しいカテゴリを [挿入（Insert）] する場所を次のように指定します。

- [カテゴリの上（above Category）] を選択した後、2 番目のドロップダウン リストからカテゴリを選択します（この上にルールが配置されます）。
- ドロップダウン リストから [ルールの下（below rule）] を選択し、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

- ドロップダウン リストから [ルールの上（above rule）] を選択し、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

ステップ 4 [OK] をクリックします。

ステップ 5 ポリシーの編集を続けます。

第 XVII 部

相関とコンプライアンス

第 69 章

コンプライアンス ホワイトリスト

次のトピックでは、相関ポリシーに追加する前にコンプライアンス ホワイトリストを設定する方法について説明します。

コンプライアンス ホワイトリストの概要

コンプライアンス ホワイトリスト（ホワイトリストと省略されることもある）は、どのオペレーティング システム、アプリケーション（Web とクライアント）、およびプロトコルがネットワーク上のホストで許可されるかを指定する一連の条件です。システムはホストがホワイトリストに違反するとイベントを生成します。

コンプライアンス ホワイトリストには 2 つの主要な構成要素があります。

- ターゲットは、ホワイトリスト評価の対象として選択するホストです。サブネット、VLAN、およびホスト属性で制約して、全部または一部のモニタ対象ホストを評価できます。マルチドメイン展開では、ドメインと、ドメイン内またはドメインをまたいだサブネットを対象にすることができます。
- ホスト プロファイルは、ターゲットのコンプライアンス基準を指定します。グローバル ホスト プロファイルはオペレーティング システムに依存しません。1 つのホワイトリスト固有として、またはホワイト リスト間で共有される、オペレーティング システム固有のホスト プロファイルを設定することもできます。

Cisco Talos Security Intelligence and Research Group（Talos）は、推奨設定が指定されたデフォルトのホワイトリストを提供しています。カスタム ホワイトリストを作成することも可能です。単純なカスタム ホワイトリストでは、特定のオペレーティング システムを実行するホストのみを許可できます。より複雑なホワイトリストでは、すべてのオペレーティング システムを許可するとと

もに、特定のポートで特定のアプリケーション プロトコルを実行する際にホストが使用する必要のあるオペレーティング システムを指定できます。

（注） システムは、ホストをエクスポートされた NetFlow レコードからネットワーク マップに追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違い，（1442 ページ） を参照）。この制限は、コンプライアンス ホワイトリストの作成方法に影響する場合があります。

コンプライアンス ホワイトリストの実装

ホワイトリストを実装するには、アクティブな相関ポリシーにホワイトリストを追加します。システムはターゲットを評価し、対応する属性を各ホストに割り当てます。

- 準拠（Compliant）：ホストはホワイトリストに違反していません。
- 非準拠（Non-Compliant）：ホストはホワイトリストに違反しています。
- 評価されていない（Not Evaluated）：ホストがホワイトリストのターゲットではないか、現在評価中であるか、またはシステムに十分な情報がないためホストが準拠しているかどうかを判断できません。

（注） ホスト属性を削除するには、対応するホワイトリストを削除します。1 つのホワイトリストを非アクティブ化、削除、または相関ポリシーから削除しても、各ホストのホスト属性は削除**されず**、属性の値が変更されることもありません。

最初の評価後、モニタ対象ホストがアクティブなホワイトリストに違反するたびにホワイトリスト イベントが生成されます。また、ホワイトリスト違反が記録されます。

ワークフロー、ダッシュボード、およびネットワーク マップを使用して、システム全体のコンプライアンス アクティビティをモニタし、個々のホストがホワイトリストにいつどのように違反したのかを判断できます。修復およびアラートでホワイトリスト違反に自動的に応答することもできます。

例：Web サーバへの HTTP の制限

セキュリティ ポリシーは、Web サーバのみが HTTP を実行できることを指定しています。HTTP を実行しているホストを特定するために Web ファーム以外のネットワーク全体を評価するホワイトリストを作成します。

ネットワーク マップとダッシュボードを使用して、ネットワークのコンプライアンスの概要を一目で把握できます。数秒で、ポリシーに違反して HTTP を実行している組織内のホストを正確に特定して適切に対処できます。

その後で、相関機能を使用して、Web ファーム内に存在しないホストが HTTP の実行を開始するたびに警告するようにシステムを設定できます。

コンプライアンス ホワイトリストのターゲット ネットワーク

ターゲットネットワークは、ホワイトリストコンプライアンス評価の対象となるホストを指定します。ホワイトリストには、複数のターゲット ネットワークを含めることができ、いずれかのターゲットの基準を満たすホストが評価されます。

最初は、ターゲットネットワークはIPアドレスまたはアドレス範囲で制約されています。マルチドメイン展開では、初期の制約にドメインも含まれます。

システム提供のデフォルトのホワイトリストでは、すべての監視対象ホスト 0.0.0.0/0 および ::/0 がターゲット設定されています。マルチドメイン展開では、デフォルトのホワイトリストはグローバル ドメインに制約されています（グローバル ドメインでのみ使用可能です）。

ホストがホワイトリストに対して有効ではなくなるようにターゲット ネットワークまたはホストを変更すると、ホストはホワイトリストで評価されなくなり、準拠と非準拠のいずれとしてもみなされなくなります。

ターゲット ネットワークの調査と改善

ホワイトリストにターゲット ネットワークを追加すると、システムにより、準拠ホストの特徴を確認できるようにネットワーク マップを調査するよう求められます。調査により、ターゲットは、調査済みのホストを表すホワイトリストに追加されます。

サブネットまたは個別のホストを調査できます。マルチドメイン展開では、ドメイン全体を調査することも、ドメインをまたいで調査することもできます。先祖ドメインを調査すると、システムによってこのドメインの子孫が調査されます。

追加されたターゲットに加えて、調査では、調査で検出されたオペレーティング システムごとに 1 つのホスト プロファイルがホワイトリストに入力されます。デフォルトで、これらのホスト プロファイルは、システムが該当するオペレーティング システム上で検出したクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルのすべてを許可します。

ターゲット ネットワークを調査（または調査をスキップ）した後、対象を絞り込みます。IP アドレスを使用してホストを除外するか、ホスト属性またはVLANによりターゲット ネットワークを制約します。

コンプライアンス ホワイトリストを使用したドメインの対象化

マルチドメイン展開では、ドメインとターゲット ネットワークは密接にリンクされています。

- リーフ ドメインの管理者は、自分のリーフ ドメイン内のホストを評価するホワイトリストを作成できます。
- 上位ドメインの管理者は、ドメインをまたいでホストを評価するホワイトリストを作成できます。同じホワイトリストで、ドメインの異なるさまざまなサブネットを対象にすることができます。

グローバル ドメインの管理者であり、展開全体の Web サーバに同じコンプライアンス基準を導入する必要があるというシナリオを考えてみます。コンプライアンス基準を定義するグローバル ドメインに 1 つのホワイトリストを作成できます。次に、各リーフ ドメイン内の Web サーバの IP

スペース（または個別のIPアドレス）を指定するターゲットネットワークを使用して、ホワイトリストを制約します。

（注） リーフ ドメインの IP アドレスと範囲を対象にすることに加えて、上位のドメインを使用してターゲット ネットワークを制約することもできます。より高いレベルのドメインのサブネットをターゲットにすると、各子孫リーフ ドメイン内の同じサブネットがターゲットになります。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

コンプライアンス ホワイト リストのホスト プロファイル

コンプライアンス ホワイト リストにおいて、ホスト プロファイルは、ターゲット ホスト上で実行を許可するオペレーティング システム、クライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを指定します。コンプライアンス ホワイト リストで使用できるホスト プロファイルは 3 種類あります。3 種類のホスト プロファイルはそれぞれ、エディタ上での表示が異なります。

表 *199* : コンプライアンス ホワイト リストのホスト プロファイル タイプ

ホスト プロファイル タイプ	表示	説明
グローバル	すべてのオペレーティング システム	オペレーティング システムに関係なく、ターゲット ホスト上で実行が許可されている内容を指定します。
オペレーティング システム別	プレーン テキストで表示	特定のオペレーティング システムを使用するターゲット ホスト上で実行が許可されている内容を指定します。
共有	イタリックで表示	複数のホワイトリストで使用可能なオペレーティング システム条件を指定します。

オペレーティング システム固有のホスト プロファイル

コンプライアンス ホワイト リストでは、オペレーティング システム固有のホスト プロファイルで、ネットワーク上での実行を許可するオペレーティング システムだけでなく、それらのオペレーティング システム上での実行を許可するアプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルも指定します。

たとえば、準拠ホストではMicrosoft Windowsの特定のバージョンを実行することを要件にすることができます。別の例として、SSHの実行をLinuxホストのポート22で許可した上で、SSHクライアントのベンダーとバージョンをさらに制限することもできます。

ネットワーク上での実行を許可するオペレーティング システムごとに1つのホスト プロファイルを作成します。ネットワーク上でオペレーティング システムを禁止する場合は、そのオペレーティングシステム用のホストプロファイルを作成しないでください。たとえば、ネットワーク上のすべてのホストでWindowsが実行されるようにするには、そのオペレーティング システム用のホスト プロファイルのみを含めるようにホワイト リストを設定します。

（注） 未確認ホストは、確認されるまで、すべてのホワイトリストに準拠していると見なされます。ただし、不明ホストのホワイト リスト ホスト プロファイルを作成することはできます。未確認ホストとは、オペレーティング システムを識別するために十分な情報が収集されていないホストのことです。不明ホストとは、既知のフィンガープリントと一致しないオペレーティング システムを使用しているホストのことです。

共有ホスト プロファイル

コンプライアンス ホワイトリストでは、共有ホスト プロファイルが特定のオペレーティング システムに関連付けられますが、それぞれの共有ホスト プロファイルを複数のホワイトリスト内で使用できます。

たとえば、世界中にオフィスがあり、拠点ごとに別々のホワイトリストを使用する一方、Apple Mac OS Xを実行しているすべてのホストに対しては常に同じプロファイルを使用するとします。その場合、該当するオペレーティング システム用の共有プロファイルを作成し、そのプロファイルをすべてのホワイトリストで使用するという方法があります。

デフォルトホワイトリストでは、組み込みホストプロファイルと呼ばれる特殊なカテゴリの共有ホストプロファイルが使用されます。これらのプロファイルは、組み込みのアプリケーションプロトコル、Webアプリケーション、プロトコル、クライアントを使用します。コンプライアンスホワイトリストエディタでは、システムはこれらのプロファイルを組み込みホストプロファイルアイコン（  ）で示します。

マルチドメイン展開では、現在のドメインで作成された共有ホスト プロファイルが表示されます。このプロファイルは編集できます。また、先祖ドメインからの共有ホスト プロファイルも表示されますが、これは編集できません。下位のドメインで作成された共有ホスト プロファイルを表示および編集するには、そのドメインに切り替えます。

（注） 共有ホスト プロファイル（組み込みを含む）を変更した場合や、組み込みアプリケーション プロトコル、プロトコル、またはクライアントを変更した場合、それを使用するすべてのホワイト リストに変更が影響します。意図しない変更を加えた場合や、該当する組み込みの要素を削除した場合は、工場出荷時の初期状態にリセットできます。

ホワイト リスト違反のトリガー

ホストのホワイトリストコンプライアンスは、システムで次のことが発生すると変化する場合があります。

- ホストのオペレーティング システムの変更を検出
- ホストのオペレーティング システムまたはホスト上のアプリケーション プロトコルに関するアイデンティティの競合を検出
- ホスト上でアクティブになっている新しい TCP サーバ ポート（SMTP または Web サーバによって使用されるポートなど）、または、ホスト上で実行中の新しい UDP サーバを検出
- ホスト上で実行中の検出された TCP サーバまたは UDP サーバで、アップグレードのためのバージョン変更などの変更を検出
- ホスト上で実行中の新しいクライアント アプリケーションまたは Web アプリケーションを検出
- クライアント アプリケーションまたは Web アプリケーションを非アクティブを理由にそのデータベースからドロップ
- ホストが新しいネットワークまたはトランスポート プロトコルと通信していることを検出
- 新しいジェイルブレイクされたモバイル デバイスを検出
- ホスト上で TCP ポートまたは UDP ポートが閉じられたか、タイムアウトしたことを検出

さらに、ホスト入力機能またはホスト プロファイルを使用して次の操作を実行することによって、ホストのコンプライアンスの変化をトリガーできます。

- ホストにクライアント、プロトコル、またはサーバを追加する
- ホストからクライアント、プロトコル、またはサーバを削除する
- ホストにオペレーティング システム定義を設定する
- ホストが有効なターゲットでなくなるようにホストのホスト属性を変更する

（注） 非常に多数のイベントが発生しないように、システムでは、その最初の評価に基づいて非準拠のホストにホワイト リスト イベントを生成せず、またユーザがアクティブなホワイト リストまたは共有ホスト プロファイルを変更した結果としてホストを非準拠にしません。ただし、違反は記録されます。すべての非準拠ターゲットに対してホワイト リスト イベントを生成する場合は、検出データを消去してください。ネットワーク アセットを再検出すると、ホワイト リスト イベントをトリガーすることがあります。

例：オペレーティング システムのコンプライアンス

ホワイト リストで Microsoft Windows ホストのみがネットワーク上で許可されるように指定されている場合、システムでは、Mac OS X を実行中のホストを検出するとホワイト リスト イベントを生成します。さらに、ホワイト リストに関連付けられているホスト属性が、そのホストに関して [準拠（Compliant）] から [非準拠（Non-Compliant）] に変更されます。

この例のホストが [準拠（Compliant）] に復帰するには、次のいずれかが行われる必要があります。

- Mac OS X オペレーティング システムを許可するようにホワイト リストを編集する
- ホストのオペレーティング システム定義を手動で Microsoft Windows に変更する
- オペレーティング システムが変更されて Microsoft Windows に戻ったことをシステムが検出する

例：非準拠のアセットをネットワーク マップから削除する

ホワイト リストで FTP の使用が許可されていない場合に、アプリケーション プロトコルのネットワーク マップ、またはイベント ビューから FTP を削除すると、FTP を実行中のホストは準拠になります。ただし、システムがこのアプリケーション プロトコルを再度検出すると、システムによってホワイト リスト イベントが生成され、そのホストは非準拠になります。

例：完全な情報に基づいてのみトリガーを実行

ホワイト リストでポート 21 で TCP FTP トラフィックだけを許可していた場合、システムでポート 21/TCP で不明なアクティビティを検出すると、ホワイト リストはトリガーを実行しません。ホワイト リストがトリガーを実行するのは、システムがトラフィックを FTP 以外のトラフィックとして識別するか、またはユーザがホスト入力機能を使用してトラフィックを非 FTP トラフィックとして指定した場合だけです。システムは、部分的な情報のみを使用して違反を記録することはありません。

コンプライアンス ホワイト リストの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

ホワイト リストを作成する際には、ネットワークを調べて最初のターゲットを作成するよう求めるプロンプトが表示されます。これは、コンプライアンスに準拠するホストの特徴を指定するのに役立ちます。

手順

ステップ 1 [ポリシー（Policies）] > [相関（Correlation）] を選択し、[ホワイト リスト（White List）] タブをクリックします。

ステップ 2 [新規ホワイト リスト（New White List）] をクリックします。

ステップ 3 必要に応じて、最初のターゲット ネットワークの [IP アドレス（IP Address）] および [ネットマスク（Netmask）] を入力します。マルチドメイン導入では、ターゲット ネットワークが存在する [ドメイン（Domain）] を選択します。

ヒント モニタリング対象のネットワーク全体を調査するには、デフォルト値の 0.0.0.0/0 と ::/0 を使用します。

（注） ターゲット ネットワークのドメインを選択した後は、ドメインを変更できません。より高いレベルのドメインのサブネットをターゲットにすると、**各**子孫リーフ ドメイン内の**同じ**サブネットがターゲットになります。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 4 ターゲット ネットワークを追加します。

- [追加（Add）]：調査せずにターゲット ネットワークを追加する場合は、[追加（Add）] をクリックします。
- [ネットワークの追加および調査（Add and Survey Network）]：ターゲット ネットワークを追加して調査する場合は、[ネットワークの追加および調査（Add and Survey Network）] をクリックします。
- [スキップ（Skip）]：ネットワークを調査せずにホワイトリストを作成する場合は、[スキップ（Skip）] をクリックします。

ステップ 5 必要に応じて、ホワイトリストの新しい [名前（Name）] および [説明（Description）] を入力します。

ステップ 6 必要に応じて、[脱獄モバイル デバイスを許可（Allow Jailbroken Mobile Devices）] を選択して、ネットワークで脱獄モバイル デバイスを許可します。このオプションを無効にすると、ジェイルブレイクされたデバイスによってホワイトリスト違反が生成されます。

ステップ 7 コンプライアンス ホワイトリストのターゲット ネットワークの設定, （1621 ページ）の説明に従って、1 つ以上の [ターゲット ネットワーク（Target Network）] をホワイト リストに追加します。

ステップ 8 [許可されるホスト プロファイル（Allowed Host Profiles）] を使用して、準拠ホストの特徴を指定します。

- グローバル ホスト プロファイル：ホワイト リストのグローバル ホスト プロファイルを編集するには、[任意のオペレーティング システム（Any Operating System）] をクリックし、ホワイト リスト ホスト プロファイルの作成, （1622 ページ）の説明に従います。
- 調査済みプロファイルの編集：ネットワーク調査によって作成された既存のオペレーティング システム固有のホスト プロファイルを編集するには、その名前をクリックし、ホワイト リスト ホスト プロファイルの作成, （1622 ページ）の説明に従います。

- 新規プロファイルの作成：このホワイト リストに新しいオペレーティング システム固有のホスト プロファイルを作成するには、[許可されるホスト プロファイル（Allowed Host Profiles）] の隣にある追加アイコン（  ）をクリックし、ホワイト リスト ホスト プロファイルの作成, （1622 ページ）の説明に従います。
- 共有ホスト プロファイルの追加：ホワイト リストに既存の共有ホスト プロファイルを追加するには、[共有ホスト プロファイルの追加（Add Shared Host Profile）] をクリックし、追加する共有ホスト プロファイルを選択して、[OK] をクリックします。共有ホスト プロファイルは斜体で表示されます。

ステップ 9 [ホワイト リストの保存（Save White List）] をクリックします。

次の作業

- 相関ポリシーの設定, （1635 ページ）の説明に従って、アクティブな相関ポリシーにホワイト リストを追加します。システムはすぐにホワイト リストの評価および違反の生成を開始します。

コンプライアンス ホワイト リストのターゲット ネットワークの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

ターゲット ネットワークを追加するときには、ターゲット ネットワークを調査して、準拠しているホストを特定することができます。この調査によって、調査で検出された各オペレーティング システムの 1 つのホスト プロファイルがホワイトリストに追加されます。これらのホスト プロファイルは、システムが該当するオペレーティング システム上で検出したクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルのすべてを許可します。

手順

ステップ 1 コンプライアンス ホワイト リスト エディタで、[ターゲット ネットワークの追加（Add Target Network）] をクリックします。

ステップ 2 ターゲット ネットワークの [IP アドレス（IP Address）] と [ネットマスク（Netmask）] を入力します。

ステップ 3 マルチドメイン展開では、ターゲット ネットワークが存在する [ドメイン（Domain）] を選択します。

（注） ターゲット ネットワークのドメインを選択した後は、ドメインを変更できません。より高いレベルのドメインのサブネットをターゲットにすると、**各**子孫リーフ ドメイン内の**同じ**サブネットがターゲットになります。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 4 ターゲット ネットワークを追加します。

- 追加（Add）：調査なしでターゲット ネットワークを追加するには、[追加（Add）] をクリックします。
- ネットワークの追加と調査（Add and Survey Network）：ターゲット ネットワークを追加および調査するには、[ネットワークの追加と調査（Add and Survey Network）] をクリックします。

ステップ 5 必要に応じて、新しいターゲットをクリックしてさらに構成します。

- 名前（Name）：新しい [名前（Name）] を入力します。
- ネットワークの追加（Add Networks）：追加のホストをターゲットにするには、追加アイコン（  ）をクリックして、[IP アドレス（IP Address）] と [ネットマスク（Netmask）] を入力します。ネットワークをホワイト リスト コンプライアンスから除外するには、[除外（Exclude）] を選択します。
- ホスト属性の追加（Add Host Attributes）：特定のホスト属性を持つホストをターゲットにするには、追加アイコン（）をクリックして、[属性（Attribute）] とその [値（Value）] を指定します。
- VLAN の追加（Add VLANs）：VLAN をターゲットにするには、追加アイコン（）をクリックして VLAN 番号を入力します（802.1q VLAN の場合）。
- 削除（Delete）：ターゲット制限を削除するには、削除アイコン（）をクリックします。

ステップ 6 最後に保存した後で行ったすべての変更をすぐに実装するには、[ホワイト リストの保存（Save White List）] をクリックします。

ホワイト リスト ホスト プロファイルの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

ホスト プロファイルは、ターゲット ホスト上での実行を許可するオペレーティング システム、クライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルといった、ホワイトリストの適合基準を指定します。

すべてのホワイト リストには、オペレーティング システムに依存しないグローバル ホスト プロファイルがあります。たとえば、Mozilla Firefox を許可するように複数の Microsoft Windows ホスト プロファイルと Linux ホスト プロファイルを編集する代わりに、検出されたオペレーティング システムに関係なく、Firefox を許可するようにグローバル ホスト プロファイルを設定できます。

また、各オペレーティング システム専用のホスト プロファイルを設定できます。これは、単一のホワイトリスト専用としても、複数のホワイトリストの共有プロファイルとしても設定できます。

（注） 共有ホスト プロファイル（ビルトインを含む）を変更した場合、またはビルトイン アプリケーション プロトコル、プロトコル、クライアントを変更した場合、これらのプロファイルを使用するすべてのホワイトリストに影響します。これらのビルトイン要素に意図しない変更や削除を行った場合は、出荷時のデフォルトにリセットできます。

はじめる前に

- コンプライアンス ホワイトリストの編集, （1628 ページ）の説明に従い、ホワイトリスト内でホスト プロファイルを作成または編集します。または、共有ホスト プロファイルの管理, （1630 ページ）の説明に従い、共有ホスト プロファイルを作成または編集します。

手順

ステップ 1 ホワイトリスト適合ホスト プロファイル エディタで、以下のホスト プロファイルを設定します。

- 名前：[名前（Name）] を入力します。
- オペレーティング システム：ホスト プロファイルを特定のオペレーティング システム専用にするには、[OS ベンダ（OS Vendor）]、[OS 名（OS Name）]、[バージョン（Version）] ドロップダウン リストを使用します。グローバル ホスト プロファイルはすべてのオペレーティング システムを実行するホストへ適用されることを目的としたプロファイルであるため、これに制限を設定することはできません。
- アプリケーション プロトコル：アプリケーション プロトコルを許可するには、追加アイコン（  ）をクリックし、アプリケーション プロトコルのホワイトリスト, （1624 ページ）の説明に従います。
- クライアント：クライアントを許可するには、追加アイコン（  ）をクリックし、クライアントのホワイトリスト, （1625 ページ）の説明に従います。
- Web アプリケーション：Web アプリケーションを許可するには、追加アイコン（  ）をクリックし、Web アプリケーションのホワイトリスト, （1626 ページ）の説明に従います。
- プロトコル：プロトコルを許可するには、追加アイコン（  ）をクリックし、プロトコルのホワイトリスト, （1626 ページ）の説明に従います。

- 削除：一度許可した項目への許可を解除するには、削除アイコン（）をクリックします。
- プロパティの編集：許可されているアプリケーションプロトコルのプロパティ、クライアント、プロトコルを編集するには、その名前をクリックします。変更は、変更した要素を使用する各ホストプロファイルに反映されます。

ヒント プロファイルに一致するホストにすべてのアプリケーションプロトコル、クライアント、webアプリケーションを許可するには、該当する [すべて許可（Allow all...）] チェックボックスを選択します。

ステップ 2 最後の保存以降に施した変更をすぐに適用するには、[ホワイトリストを保存（Save White List）]（または、共有ホストプロファイルを編集している場合は [すべてのプロファイルを保存（Save All Profiles）]）をクリックします。

アプリケーション プロトコルのホワイトリスト

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティングシステムに対して、アプリケーション プロトコルのホワイトリストを作成できます。オプションで、ポート、ベンダー、バージョンによって、アプリケーション プロトコルを制限できます。たとえば、ポート 22/TCP で、Linux ホスト上で実行する OpenSSH の特定のバージョンを許可することができます。

手順

ステップ 1 ホワイトリスト ホスト プロファイルを作成または変更しているときに、[許可されるアプリケーション プロトコル（Allowed Application Protocols）]（またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可されるアプリケーション プロトコル（Globally Allowed Application Protocols）]）の横にある追加アイコン（）をクリックします。

ステップ 2 次の 2 つの対処法があります。

- 許可するアプリケーションプロトコルが表示されたら、これらを選択します。Webインターフェイスには、ホワイトリストによって、過去に許可されたアプリケーションプロトコル、または今許可しようとしているアプリケーション プロトコルが表示されます。
- リストにないアプリケーションプロトコルを許可するには、[<新規アプリケーションプロトコル>（<New Application Protocol>）] を選択し、[OK] をクリックしてアプリケーション プロトコル エディタを表示します。許可するアプリケーション プロトコル [タイプ（Type）] と [プロトコル（Protocol）] を選択します。オプションで、[ポート（port）]、[ベンダー

（Vendor）]、[バージョン（Version）] によって、アプリケーション プロトコルを制限します。

（注） アプリケーションのテーブル ビューに表示されているとおり正確にベンダーやバージョンを入力する必要があります。ベンダーまたはバージョンを指定しなかった場合は、タイプとプロトコルが一致している限り、ホワイトリストではすべてのベンダーとバージョンが許可されます。

ステップ 3 [OK] をクリックします。

ステップ 4 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存（Save White List）] をクリックします。

クライアントのホワイトリスト

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティング システムに対して、クライアントのホワイトリストを作成できます。オプションで、クライアントを特定のバージョンに限定することができます。たとえば、Microsoft Windows ホスト上での実行を Microsoft Internet Explorer 10 のみに許可することができます。

手順

ステップ 1 ホワイトリスト ホスト プロファイルを作成または変更しているときに、[許可されるクライアント（Allowed Clients）]（またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可されるクライアント（Globally Allowed Clients）]）の横にある追加アイコン（  ）をクリックします。

ステップ 2 次の 2 つの対処法があります。

- 許可するクライアントが表示されたら、これらを選択します。Web インターフェイスには、ホワイトリストによって、過去に許可されたクライアント、または今許可しようとしているクライアントが表示されます。
- リストにないクライアントを許可するには、[<新規クライアント>（<New Client>）] を選択し、[OK] をクリックしてクライアント エディタを表示します。ドロップダウン リストから許可する [クライアント（Client）] を選択し、オプションで許可するクライアントの [バージョン（Version）] を制限します。

（注） クライアントのテーブル ビューに表示されているとおり正確にバージョンを入力する必要があります。バージョンを指定しない場合、ホワイトリストはすべてのバージョンを許可します。

ステップ 3 [OK] をクリックします。

ステップ 4 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存（Save White List）] をクリックします。

Web アプリケーションのホワイトリスト

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティング システムに対して、Web アプリケーションのホワイトリストを作成できます。

手順

ステップ 1 ホワイト リスト ホスト プロファイルを作成または変更しているときに、[許可される Web アプリケーション（Allowed Web Applications）]（またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可される Web アプリケーション（Globally Allowed Web Applications）]）の横にある追加アイコン（  ）をクリックします。

ステップ 2 許可する Web アプリケーションを選択します。

ステップ 3 [OK] をクリックして、

ステップ 4 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存（Save White List）] をクリックします。

プロトコルのホワイトリスト

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティング システムに対して、プロトコルのホワイトリストを作成できます。ARP、IP、TCP、UDP は、常にすべてのホスト上での実行が許可されます。これらを禁止することはできません。

手順

ステップ 1 ホワイトリスト ホスト プロファイルを作成または変更しているときに、[許可されるプロトコル（Allowed Protocols）]（またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可されるプロトコル（Globally Allowed Protocols）]）の横にある追加アイコン（  ）をクリックします。

ステップ 2 次の 2 つの対処法があります。

- 許可するプロトコルが表示されたら、これらを選択します。Web インターフェイスには、ホワイトリストによって、過去に許可されたプロトコル、または今許可しようとしているプロトコルが表示されます。
- リストにないプロトコルを許可するには、[<新規プロトコル>（<New Protocol>）] を選択し、[OK] をクリックしてプロトコル エディタを表示します。[タイプ（Type）] ドロップダウン リストから、プロトコル タイプ（[ネットワーク（Network）] や [トランスポート（Transport）]）を選択し、ドロップダウン リストから [プロトコル（Protocol）] を選択します。

  ヒント リスト内に存在しないプロトコルを指定するには、[その他(手動入力)（Other(manual entry)）] を選択します。ネットワーク プロトコルの場合は、http://www.iana.org/assignments/ethernet-numbers/ に記載されている適切な番号を入力します。トランスポート プロトコルの場合は、http://www.iana.org/assignments/protocol-numbers/ に記載されている適切な番号を入力します。

ステップ 3 [OK] をクリックします。

ステップ 4 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存（Save White List）] をクリックします。

コンプライアンス ホワイト リストの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

[ホワイト リスト（White List）] ページは、コンプライアンス ホワイト リストと共有ホスト プロファイルの管理に使用できます。デフォルト ホワイトリストは、推奨設定を表すものであり、組み込みホストプロファイルと呼ばれる特殊なカテゴリの共有ホストプロファイルを使用します。

マルチドメイン展開では、現在のドメインで作成されたコンプライアンスホワイトリストが表示されます。これは、編集が可能なリストです。また、先祖ドメインからの選択したホワイト リストも表示されますが、これは編集できません。下位のドメインで作成されたホワイト リストを表示および編集するには、そのドメインに切り替えます。

（注） 設定に無関係なドメイン（名前、管理対象デバイスなど）に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。 デフォルト ホワイト リストは、グローバル ドメインでのみ使用できます。

手順

ステップ 1 [ポリシー（Policies）] > [相関（Correlation）] を選択して、[ホワイト リスト（White List）] タブをクリックします。

ステップ 2 コンプライアンス ホワイト リストを管理します。

- 作成：新しいホワイト リストを作成するには、[新規ホワイト リスト（New White List）] をクリックして、コンプライアンス ホワイト リストの作成, （1619 ページ）で説明する手順を実行します。
- 削除：使用していないホワイト リストを削除するには、削除アイコン（）をクリックして、ホワイトリストの削除を確認します。また、ホワイトリストを削除すると、ネットワーク上のすべてのホストから、そのリストに関連付けられたホスト属性も削除されます。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 編集：既存のホワイトリストを変更するには、編集アイコン（）をクリックし、コンプライアンス ホワイトリストの編集, （1628 ページ）で説明する手順を実行します。代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 共有ホスト プロファイル：ホワイト リストの共有ホスト プロファイルを管理するには、[共有プロファイルの編集（Edit Shared Profiles）] をクリックして、共有ホスト プロファイルの管理, （1630 ページ）で説明する手順を実行します。

コンプライアンス ホワイトリストの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

アクティブな相関ポリシーに含まれるコンプライアンス ホワイトリストを修正して保存すると、システムは、ホワイトリストのターゲット ネットワークのホストのコンプライアンスを再評価します。この再評価で一部のホストがコンプライアンス準拠または違反とされた場合でも、ホワイトリスト イベントは生成されません。

手順

ステップ 1 [ポリシー（Policies）]>[相関（Correlation）] を選択し、[ホワイトリスト（White List）] タブをクリックします。

ステップ 2 変更するホワイトリストの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 コンプライアンス ホワイト リストを編集します。

- 名前と説明：名前または説明を変更するには、左側のパネルでホワイトリストの名前をクリックしてホワイトリストの基本情報を表示し、新しい情報を入力します。
- ジェイルブレイクされたデバイスの許可：ネットワーク上でジェイルブレイクされたモバイルデバイスを許可するには、左側のパネルでホワイトリストの名前をクリックしてホワイトリストの基本情報を表示し、[ジェイルブレイクされたモバイル デバイスを許可（Allow Jailbroken Mobile Devices）] を有効にします。このオプションを無効にすると、ジェイルブレイクされたデバイスによってホワイトリスト違反が生成されます。
- 許可されるホスト プロファイルの追加：このホワイトリストに対してオペレーティング システム固有のホスト プロファイルを作成するには、[許可されているホスト プロファイル（Allowed Host Profiles）] の横にある追加アイコン（）をクリックし、ホワイト リスト ホスト プロファイルの作成, （1622 ページ）の説明に従って続行します。
- 共有ホスト プロファイルの追加：ホワイトリストに既存の共有ホスト プロファイルを追加するには、[共有ホスト プロファイルの追加（Add Shared Host Profile）] をクリックし、追加する共有ホスト プロファイルを選択して [OK] をクリックします。共有ホスト プロファイルは斜体で表示されます。
- ターゲット ネットワークの追加：ホストを調査することなく新しいターゲット ネットワークを追加するには、ターゲットネットワークの横にある追加アイコン（）をクリックし、コンプライアンス ホワイトリストのターゲット ネットワークの設定, （1621 ページ）の説明に従って続行します。
- ホスト プロファイルの削除：ホワイトリストから共有またはオペレーティング システム固有のホスト プロファイルを削除するには、ホスト プロファイルの横にある削除アイコン（）をクリックし、選択内容を確認します。共有ホストプロファイルを削除すると、それがホワイトリストから除外されますが、プロファイルは削除されず、それを使用する他のホワイトリストからも除外されません。ホワイトリストのグローバル ホスト プロファイルは削除できません。

- ターゲット ネットワークの削除：ホワイトリストからターゲット ネットワークを削除するには、ネットワークの横にある削除アイコン（）をクリックし、選択内容を確認します。
- グローバル ホスト プロファイルの編集：ホワイトリストのグローバル ホスト プロファイルを編集するには、[任意のオペレーティング システム（Any Operating System）] をクリックし、ホワイトリスト ホスト プロファイルの作成, （1622ページ）の説明に従って続行します。
- 他のホスト プロファイルの編集：共有またはオペレーティング システム固有のホスト プロファイルを編集するには、ホスト プロファイルの名前をクリックし、ホワイト リスト ホスト プロファイルの作成, （1622 ページ）の説明に従って続行します。
- ターゲット ネットワークの編集：ターゲット ネットワークを編集するには、ネットワークの名前をクリックし、コンプライアンス ホワイト リストのターゲット ネットワークの設定, （1621 ページ）の指示に従って続行します。

ステップ 4 前回の保存以降に行ったすべての変更をすぐに実装するには、[ホワイトリストの保存（Save White List）] をクリックします。

共有ホスト プロファイルの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

コンプライアンス ホワイト リストでは、共有ホストプロファイルは特定のオペレーティング システムに関連付けられますが、それぞれの共有ホストプロファイルを複数のホワイトリスト内で使用できます。複数のホワイトリストを作成するが、同じホストプロファイルを使用して複数のホワイトリストで特定のオペレーティングシステムを実行するホストを評価する場合は、共有のホスト プロファイルを使用します。

マルチドメイン展開では、現在のドメインで作成された共有ホスト プロファイルが表示されます。これは、編集が可能なプロファイルです。また、先祖ドメインからの共有ホスト プロファイルも表示されますが、これは編集できません。下位のドメインで作成された共有ホスト プロファイルを表示および編集するには、そのドメインに切り替えます。

（注） 共有ホスト プロファイル（組み込みを含む）を変更した場合や、組み込みアプリケーション プロトコル、プロトコル、またはクライアントを変更した場合、それを使用するすべてのホワイト リストに変更が影響します。意図しない変更を加えた場合や、該当する組み込みの要素を削除した場合は、工場出荷時の初期状態にリセットできます。

手順

ステップ 1 [ポリシー（Policies）] > [相関（Correlation）] を選択して、[ホワイト リスト（White List）] タブをクリックします。

ステップ 2 [共有プロファイルの編集（Edit Shared Profiles）] をクリックします。

ステップ 3 共有ホスト プロファイルを管理します。

- 共有ホスト プロファイルの作成：ホストの調査なしで新しい共有ホスト プロファイルを作成するには、[共有ホストプロファイル（Shared Host Profiles）] の横にある追加アイコン（  ）をクリックし、ホワイト リスト ホスト プロファイルの作成, （1622 ページ）で説明する手順を実行します。
- 調査によるホストプロファイルの作成：ネットワークの調査によって複数の新しい共有ホスト プロファイルを作成するには、[ターゲット ネットワークの追加（Add Target Network）] をクリックして、コンプライアンス ホワイト リストのターゲット ネットワークの設定, （1621 ページ）で説明する手順を実行します。
- 削除：共有ホストプロファイルを削除するには、削除アイコン（  ）をクリックして、選択内容を確認します。
- 編集：既存の共有ホスト プロファイル（組み込み共有ホスト プロファイルを含む）を変更するには、そのプロファイルの名前をクリックして、ホワイト リスト ホスト プロファイルの作成, （1622 ページ）で説明する手順を実行します。
- 組み込みのホスト プロファイルのリセット：すべての組み込みホスト プロファイルを工場出荷時の初期状態にリセットするには、[組み込みホストプロファイル（Built-in Host Profiles）] をクリックして、[工場出荷時の初期状態にリセット（Reset to Factory Defaults）] をクリックしてから、選択内容を確認します。

ステップ 4 最後の保存以降に行われたすべての変更をすぐに実装するには、[すべてのプロファイルの保存（Save All Profiles）] をクリックします。

第 70 章

相関ポリシー

次のトピックでは、相関ポリシーおよびルールの設定方法について説明します。

相関ポリシーとルールの概要

相関機能を使用することで、ネットワークへの脅威に対して相関ポリシーを使用してリアルタイムで応答することができます。

ネットワーク上のアクティビティによって、アクティブな相関ポリシー内の相関ルールまたはコンプライアンス ホワイトリストのいずれかがトリガーされると、相関ポリシー違反が発生します。

相関ルール

アクティブな相関ポリシー内の相関ルールがトリガーされると、システムによって相関イベントが生成されます。相関ルールは、以下の場合にトリガーされます。

- 特定のタイプのイベント（接続、侵入、マルウェア、ディスカバリ、ユーザアクティビティなど）がシステムによって生成された。
- ネットワーク トラフィックが通常のプロファイルから逸脱している。

以下の方法で相関ルールを制約することもできます。

- ホスト プロファイル限定を追加すると、トリガー イベントに関連するホストのプロファイルからの情報に基づいてルールを制約できます。

- 接続トラッカーを相関ルールに追加すると、ルールの初期基準に一致した場合、システムは特定の接続を追跡し始めます。その後、追跡対象の接続がさらに追加の基準を満たす場合にのみ、相関イベントが生成されます。
- ユーザ限定を相関ルールに追加すると、特定のユーザまたはユーザ グループを追跡します。たとえば、特定のユーザのトラフィックや特定の部門からのトラフィックに対してのみトリガーされるように相関ルールを制約することができます。
- スヌーズ期間の追加。相関ルールがトリガーされた後、スヌーズ期間により指定したインターバルの間、そのルールは再びトリガーされません。スヌーズ期間が経過すると、ルールは再びトリガー可能になり、新しいスヌーズ期間が始まります。
- 非アクティブ期間の追加。非アクティブ期間中は、相関ルールはトリガーされません。

展開のライセンスなしでも相関ルールを設定できますが、ライセンス許可のないコンポーネントを使用するルールはトリガーされません。

コンプライアンス ホワイトリスト

コンプライアンス ホワイト リストは、ネットワーク上のホストでどのオペレーティング システム、アプリケーション（Web およびクライアント）、プロトコルが許可されるかを指定します。アクティブな相関ポリシーで使用されているホワイト リストにホストが違反した場合、ホワイト リスト イベントがシステムによって生成されます。

相関応答

相関ポリシー違反への応答には、シンプルなアラートや、さまざまな修復（ホストのスキャンなど）が含まれます。それぞれの相関ルールまたはホワイトリストを、単一の応答または応答グループに関連付けることができます。

ネットワーク トラフィックが複数のルールまたはホワイトリストをトリガーとして使用した場合、システムはそれぞれのルールとホワイトリストに関連付けられているすべての応答を起動します。

相関およびマルチテナンシー

マルチドメイン展開では、ドメイン レベルで利用可能な任意のルール、ホワイトリスト、応答を使って、任意のドメイン レベルで相関ポリシーを作成できます。高位レベル ドメインの管理者はドメイン内、および複数ドメインで関連付けを実行できます。

- ドメインによって相関ルールを制約すると、そのドメインの子孫で報告されるイベントが照合されます。
- 高位レベル ドメインの管理者は複数ドメインでホストを評価するコンプライアンス ホワイトリストを作成できます。同じホワイトリストで、異なるドメイン内の異なるサブネットを対象にすることができます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。リテラルの設定（IP アドレス、VLAN タグ、ユーザ名など）を使用してドメイン間の相関ルールを制約すると、予期しない結果になる可能性があります。

相関ポリシーの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

相関ルール、コンプライアンスのホワイトリスト、アラート応答、および修復を使用して相関ポリシーを作成します。

マルチドメイン展開では、任意のドメイン レベルで、そのレベルで使用可能な構成設定を使用して相関ポリシーを作成できます。

各相関ポリシーと、そのポリシーで使用される各ルールとホワイトリストにプライオリティを割り当てることができます。ルールとホワイトリストのプラオリティは、相関ポリシーのプライオリティをオーバーライドします。ネットワーク トラフィックが相関ポリシーに違反した場合、違反があったルールまたはホワイトリストに独自のプライオリティがない限り、結果の相関イベントでポリシーのプライオリティ値が表示されます。

手順

ステップ 1 [ポリシー（Policies）] > [相関（Correlation）]を選択します。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] と [ポリシーの説明（Policy Desription）] を入力します。

ステップ 4 [デフォルト プライオリティ（Default Priority）] ドロップダウン リストから、ポリシーのプライオリティを選択します。ルールのプライオリティのみを使用するには、[なし（None）] を選択します。

ステップ 5 [ルールの追加（Add Rules）] をクリックし、ポリシーで使用するルールとホワイトリストを選択して、[追加（Add）] をクリックします。

ステップ 6 各ルールまたはホワイトリストの [優先順位（Priority）] リストから、プライオリティを選択します。

- 1 ～ 5 のプライオリティ値
- なし

- デフォルト（Default）（ポリシーのデフォルト プライオリティを使用）

ステップ 7 ルールとホワイトリストに応答を追加する，（1636 ページ）の説明に従ってルールとホワイトリストに応答を追加します。

ステップ 8 [保存（Save）] をクリックします。

次の作業

- スライダをクリックして、ポリシーをアクティブにします。

ルールとホワイトリストに応答を追加する

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

それぞれの相関ルールまたはホワイトリストを、単一の応答または応答グループに関連付けることができます。ネットワーク トラフィックが複数のルールまたはホワイトリストをトリガーとして使用した場合、システムはそれぞれのルールとホワイトリストに関連付けられているすべての応答を起動します。トラフィック プロファイルの変更への応答として使用された場合は、Nmap 修復が開始されないことに注意してください。

マルチドメイン展開では、現在のドメインまたは先祖ドメインで作成された応答を使用できます。

手順

ステップ 1 相関ポリシー エディタで、応答を追加するルールまたはホワイトリストの横にある応答アイコン（  ）をクリックします。

ステップ 2 [未割り当ての応答（Unassigned Responses）] の下で、ルールまたはホワイトリストがトリガーとして使用された場合に起動する応答を選択して、上矢印（^）をクリックします。

ステップ 3 [更新（Update）]をクリックします。

相関ポリシーの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

アクティブな相関ポリシーへの変更は、即座に反映されます。

相関ポリシーを有効化すると、システムは即座にイベントの処理を開始して、応答をトリガーします。システムは、最初の有効化後の評価時に、非準拠ホストのホワイトリストイベントを生成しない点に注意してください。

マルチドメイン展開では、現在のドメインで作成された相関ポリシーが表示されます。このポリシーは編集可能です。また、先祖ドメインからの選択した相関ポリシーも表示されますが、これは編集できません。下位のドメインで作成された相関ポリシーを表示および編集するには、そのドメインに切り替えます。

（注） 設定に無関係なドメイン（名前、管理対象デバイスなど）に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。

手順

ステップ 1 [ポリシー（Policies）] > [相関（Correlation）]を選択します。

ステップ 2 相関ポリシーを管理します。

- アクティブ化または非アクティブ化：スライダをクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 作成：[ポリシーの作成（Create Policy）]をクリックします。相関ポリシーの設定, （1635 ページ）を参照してください。
- 編集：編集アイコン（）をクリックします。相関ポリシーの設定, （1635 ページ）を参照してください。代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 削除：削除アイコン（）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

相関ルールの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

単純な相関ルールでは、特定のタイプのイベントが発生することのみが必要です。より具体的な条件を指定する必要はありません。たとえば、トラフィック プロファイル変化に基づく相関ルールでは、条件を指定する必要はありません。また、複数の条件と追加した制約を使用して複雑な相関ルールを作成することもできます。

相関ルール トリガー基準、ホスト プロファイル限定、ユーザ限定、または接続トラッカーを作成するときの構文はそれぞれに異なりますが、メカニズムはすべて同じです。

（注） マルチドメイン展開では、相関ルールを先祖ドメインで制約すると、そのドメインの子孫によってレポートされるイベントと一致します。

はじめる前に

- 相関イベントをトリガーするために使用するタイプの情報が展開で収集されていることを確認します。たとえば、個々の接続イベントまたは接続サマリー イベントで使用可能な情報は、検出方法、ロギング方法、イベント タイプなど、いくつかの要因により異なります。システムは、ホストをエクスポートされた NetFlow レコードからネットワーク マップに追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違い, （1442 ページ） を参照）。

手順

ステップ 1 [ポリシー（Policies）]>[相関（Correlation）] を選択し、[ルール管理（Rule Management）] タブをクリックします。

ステップ 2 [Create Rule] をクリックします。

ステップ 3 [ルール名（Rule Name）] と [ルールの説明（Rule Description）] を入力します。

ステップ 4 必要に応じて、ルールの [ルール グループ（Rule Group）] を選択します。

ステップ 5 基本イベント タイプを選択し、必要に応じて、相関ルールの追加のトリガー条件を指定します。次の基本イベント タイプを選択できます。

- 侵入イベントが発生：侵入イベント トリガー条件の構文, （1640 ページ）を参照してください。

- マルウェアイベントが発生：マルウェアイベントトリガー条件の構文，（1643ページ）を参照してください。
- 検出イベントが発生：ディスカバリイベントトリガー条件の構文，（1645ページ）を参照してください。
- ユーザ アクティビティが検出された：ユーザ アクティビティのイベント トリガー条件の構文，（1649ページ）を参照してください。
- ホスト入力イベントが発生：ホスト入力イベントトリガー条件の構文，（1649ページ）を参照してください。
- 接続イベントが発生：接続イベントトリガー条件の構文，（1651ページ）を参照してください。
- トラフィック プロファイルの変更：トラフィック プロファイル変化の構文，（1655ページ）を参照してください。

ステップ 6 必要に応じて、次のいずれかまたはすべてを追加することによって相関ルールをさらに制約します。

- ホストプロファイル限定：[ホストプロファイル限定の追加（Add Host Profile Qualification）]をクリックします。相関ホストプロファイル限定の構文，（1657ページ）を参照してください。
- 接続トラッカー：[接続トラッカーの追加（Add Connection Tracker）]をクリックします。接続トラッカー，（1662ページ）を参照してください。
- ユーザ限定：[ユーザ限定の追加（Add User Qualification）]をクリックします。ユーザ限定の構文，（1661ページ）を参照してください。
- スヌーズ期間：ルールオプションで、[スヌーズ（Snooze）]テキストフィールドとドロップダウンリストを使用して、相関ルールのトリガー後、次に相関ルールをトリガーするまで待機する間隔を指定します。
- 非アクティブ期間：ルール オプションで、[非アクティブ期間の追加（Add Inactive Period）]をクリックします。テキスト フィールドとドロップダウン リストを使用して、相関ルールに基づくネットワーク トラフィック評価をシステムに停止させる時点および頻度を指定します。

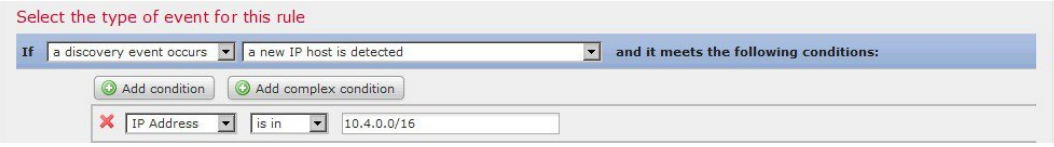
ヒント スヌーズ期間を削除するには、間隔を 0（秒、分、または時間）に指定します。

ステップ 7 [Save Rule] をクリックします。

相関ルールの単純な例

新しいホストが特定のサブネットで検出されると、次の単純な相関ルールがトリガーされます。カテゴリが IP アドレスを表す場合、演算子として [is in] または [is not in] を選択すると、CIDR な

どの特殊な表記で表される IP アドレス ブロックにその IP アドレスが含まれるのか、含まれないのかを指定できます。



次の作業

- 相関ポリシーの設定, （1635 ページ）の説明に従って、相関ポリシーでルールを使用します。

侵入イベント トリガー条件の構文

侵入イベントを基本イベントとして選択した場合、次の表で説明する方法に従って相関ルールの条件を作成します。

表 *200*：侵入イベントの構文

指定する項目	選択する演算子と内容
アクセス コントロール ポリシー	侵入イベントを生成した侵入ポリシーを使用するアクセス コントロール ポリシーを 1 つ以上選択します。
アクセス コントロール ルール名	侵入イベントを生成した侵入ポリシーを使用するアクセス コントロール ルールの名前の全体またはその一部を入力します。
アプリケーション プロトコル	侵入イベントに関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
分類	分類を 1 つ以上を選択します。
クライアント	侵入イベントに関連付けられたクライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアントのカテゴリを 1 つ以上選択します。
接続先（国）または送信元（国）	侵入イベントの送信元または宛先 IP アドレスに関連付けられた国を 1 つ以上選択します。
宛先 IP、送信元 IP、送信元 IP と宛先 IP の両方、または、送信元 IP か宛先 IP のいずれか	単一の IP アドレスまたはアドレス ブロックを入力します。

指定する項目	選択する演算子と内容
宛先ポート/ICMP コードまたは送信元ポート/ICMP タイプ	送信元トラフィックのポート番号またはICMPタイプ、または宛先トラフィックのポート番号または ICMP コードを入力します。
Device	イベントを生成した可能性があるデバイスを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
出力インターフェイスまたは入力インターフェイス	インターフェイスを 1 つ以上選択します。
出力セキュリティ ゾーンまたは入力セキュリティ ゾーン	1 つ以上のセキュリティ ゾーンまたはを選択します。
ジェネレータ ID	プリプロセッサを 1 つ以上選択します。
影響フラグ	侵入イベントに割り当てられた影響レベルを選択します。 NetFlowデータからネットワーク マップに追加されたホストに使用可能なオペレーティング システムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクト レベル 1：赤）インパクト レベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティング システム ID を手動で設定します。
インライン結果	システムは、侵入ポリシーの結果としてパケットを [ドロップした（dropped）] か [ドロップしたと想定（would have dropped）] したのかを選択します。 システムは、インライン展開、スイッチド展開、またはルーテッド展開のパケットをドロップできます。侵入ポリシーのドロップ動作や侵入ルール状態とは無関係に、パッシブ展開（インライン セットがタップ モードである場合を含む）ではシステムがパケットをドロップしません。
侵入ポリシー	侵入イベントを生成した侵入ポリシーを 1 つ以上選択します。
IOC タグ	侵入イベントの結果として侵害の兆候タグが設定されているかどうかを選択します。
[プライオリティ（Priority）]	ルールの優先順位を選択します。 ルールベースの侵入イベントの場合、優先順位は`priority`キーワードまたは`classtype`キーワードのいずれかの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。

指定する項目	選択する演算子と内容
プロトコル	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポート プロトコルの名前または番号を入力します。
ルール メッセージ	ルール メッセージの全体またはその一部を入力します。
ルール SID	単一の Snort ID（SID）またはカンマ区切りの複数の SID を入力します。 演算子として [に含まれる（is in）] または [に含まれない（is not in）] を選択する場合、複数選択ポップアップ ウィンドウを使用することはできません。SID のカンマ区切りリストを入力する必要があります。
ルール タイプ	ルールをローカルにするかどうかを指定します。 ローカル ルールには、カスタマイズされた標準テキスト侵入ルール、ユーザが変更した標準テキスト ルール、見出し情報を変更してルールを保存するときに作成される共有オブジェクト ルールの新規インスタンスが含まれます。
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを選択します。
SSL 証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL 証明書のサブジェクトの共通名（CN）	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの国（C）	セッションの暗号化に使用された証明書のサブジェクトの国番号を 1 つ以上選択します。
SSL 証明書のサブジェクトの組織（O）	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの部門（OU）	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを1つ以上選択します。
[ユーザ名（Username）]	侵入イベントで送信元ホストにログインしたユーザを示すユーザ名を入力します。
VLAN ID（Admin. VLAN ID）	侵入イベントをトリガーとして使用したパケットに関連付けられた最も内側の VLAN ID を入力します。
Web アプリケーション	侵入イベントに関連付けられた Web アプリケーションを 1 つ以上選択します。

指定する項目	選択する演算子と内容
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

マルウェア イベント トリガー条件の構文

マルウェアイベントで相関ルールをベースとして使用するには、まず、使用するマルウェアイベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次のオプションを選択できます。

- [エンドポイントベースのマルウェアの検出（by endpoint-based malware detection）]（エンドポイント向け AMP）
- [ネットワークベースのマルウェアの検出（by network-based malware detection）]（ネットワーク向け AMP）
- [レトロスペクティブ ネットワークベースのマルウェアの検出（by retrospective network-based malware detection）]（ネットワーク向け AMP）

マルウェア イベントを基本イベントとして選択する場合、次の表で説明する方法に従って相関ルールの条件を作成します。

表 *201*：マルウェア イベントの構文

指定する項目	選択する演算子と内容
アプリケーション プロトコル	マルウェア イベントに関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
クライアント	マルウェア イベントに関連付けられたクライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアントのカテゴリを 1 つ以上選択します。
接続先（国）または送信元（国）	マルウェア イベントの送信元または宛先 IP アドレスに関連付けられた国を 1 つ以上選択します。
宛先 IP、ホスト IP、または送信元 IP	単一の IP アドレスまたはアドレス ブロックを入力します。
送信先ポート/ICMP コード	宛先トラフィックのポート番号または ICMP コードを入力します。

指定する項目	選択する演算子と内容
傾向	[マルウェア（Malware）] または [カスタム検出（Custom Detection）]、あるいはその両方を選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
イベント タイプ（Event Type）	エンドポイントベースのマルウェア イベントに関連付けられたイベント タイプを 1 つ以上選択します。
ファイル名	ファイルの名前を入力します。
ファイル タイプ	ファイル タイプを選択します。
ファイル タイプ カテゴリ	ファイル タイプ カテゴリを 1 つ以上選択します。
IOC タグ	マルウェア イベントの結果として侵害の兆候タグが設定 [される（is）] か、設定 [されない（is not）] かを選択します。
SHA-256	ファイルの SHA-256 ハッシュ値を入力するか貼り付けます。
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを選択します。
SSL 証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL 証明書のサブジェクトの共通名（CN）	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの国（C）	セッションの暗号化に使用された証明書のサブジェクトの国番号を1つ以上選択します。
SSL 証明書のサブジェクトの組織（O）	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの部門（OU）	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを 1 つ以上選択します。

指定する項目	選択する演算子と内容
送信元ポート/ICMP タイプ	送信元トラフィックのポート番号または ICMP タイプを入力します。
Web アプリケーション	マルウェア イベントに関連付けられた Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

ディスカバリ イベント トリガー条件の構文

ディスカバリ イベントで相関ルールをベースとして使用するには、まず、使用するディスカバリ イベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次の表は、選択可能なディスカバリ イベントのタイプを示しています。

ホップ変更によって相関ルールをトリガーとして使用したり、ホスト制限到達のためにシステムが新しいホストをドロップした時点で相関ルールをトリガーとして使用したりすることはできません。ただし、[任意のタイプのイベントがある（there is any type of event）] を選択することで、任意のタイプのディスカバリ イベントの発生時にルールをトリガーできます。

表 *202*：相関ルールのトリガー条件とディスカバリ イベント タイプ

選択するオプション	選択内容
クライアントが変更された	クライアント更新
クライアントがタイムアウトになった	クライアント タイムアウト
ホスト IP アドレスが再使用されている	DHCP：IP アドレスの再割り当て
ホスト制限に達したためホストが削除された	ホスト削除：ホスト制限に到達
ホストがネットワーク デバイスとして識別されている	ネットワーク デバイスへのホスト タイプの変更
ホストがタイムアウトになった	ホスト タイムアウト
ホストの IP アドレスが変更された	DHCP：IP アドレスの変更
NETBIOS 名の変更が検出された	NETBIOS 名の変更
新しいクライアントが検出された	新しいクライアント
新しい IP ホストが検出された	新しいホスト
新しい MAC アドレスが検出された	ホストの追加 MAC の検出

選択するオプション	選択内容
新しい MAC ホストが検出された	新しいホスト
新しいネットワーク プロトコルが検出された	新しいネットワーク プロトコル
新しいトランスポート プロトコルが検出された	新しいトランスポート プロトコル
TCP ポートが閉じた	TCP ポート クローズ
TCP ポートがタイムアウトした	TCP ポート タイムアウト
UDP ポートが閉じた	UDP ポート クローズ
UDP ポートがタイムアウトした	UDP ポート タイムアウト
VLAN タグが更新された	VLAN タグ情報の更新
IOC が設定された	侵害の兆候
オープン TCP ポートが検出された	新しい TCP ポート
オープン UDP ポートが検出された	新しい UDP ポート
ホストの OS 情報が変更された	新しい OS
ホストの OS またはサーバ ID でコンフリクトが発生した	アイデンティティ競合
ホストの OS またはサーバ ID がタイムアウトした	アイデンティティ タイムアウト
任意のタイプのイベントがある	任意のイベント タイプ
MAC アドレスに関する新しい情報がある	MAC 情報の変更
TCP サーバに関する新しい情報がある	TCP サーバ情報の更新
UDP サーバに関する新しい情報がある	UDP サーバ情報の更新

次の表では、ディスカバリ イベントを基本イベントとして選択するときに、相関ルールの条件を作成する方法を説明します。

表 *203*：ディスカバリ イベントの構文

指定する項目	選択する演算子と内容
アプリケーション プロトコル	アプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
アプリケーション ポート	アプリケーション プロトコルのポート番号を入力します。
クライアント	クライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアントのカテゴリを 1 つ以上選択します。
クライアント バージョン	クライアントのバージョン番号を入力します。
Device	ディスカバリ イベントを生成した可能性があるデバイスを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
ハードウェア	モバイルデバイスのハードウェア モデルを入力します。たとえば、すべての Apple iPhone に一致させるには iPhone と入力します。
ホスト タイプ	ホスト タイプを 1 つ以上選択します。ホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
IP アドレスまたは新しい IP アドレス	単一の IP アドレスまたはアドレス ブロックを入力します。
ジェイルブロークン	イベントのホストがジェイルブレイクされたモバイル デバイスであることを示すには [はいい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
MAC アドレス	ホストの MAC アドレス全体またはその一部を入力します。 たとえば、特定のハードウェア製造元のデバイスの MAC アドレスが 0A:12:34 で始まることがわかっている場合、演算子として [開始（begins with）] を選択し、値として 0A:12:34 を入力できます。

指定する項目	選択する演算子と内容
MAC タイプ	MAC アドレスが [ARP/DHCP で検出（ARP/DHCP Detected）] されたかどうかを選択します。 つまり、MAC アドレスがホストに属していることをシステムがポジティブに識別したのか（[ARP/DHCP で検出（is ARP/DHCP Detected）]）、または、管理対象デバイスとホストの間にルータがあるなどの理由で、その MAC アドレスを持つ多数のホストをシステムが認識しているのか（[ARP/DHCP で検出されない（is not ARP/DHCP Detected）]）を選択します。
MAC ベンダー	ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックで使われている NIC の MAC ハードウェア ベンダーの名前全体またはその一部を入力します。
Mobile	イベントのホストがモバイル デバイスであることを示すには [はいい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
[NETBIOS 名（NETBIOS Name）]	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
OS 名	オペレーティング システムの名前を 1 つ以上選択します。
OS ベンダー	オペレーティング システムのベンダーを 1 つ以上選択します。
OS バージョン	オペレーティング システムのバージョンを 1 つ以上選択します。
プロトコルまたは トランスポート プロトコル	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポート プロトコルの名前または番号を入力します。
ソース（Source）	ホスト入力データのソースを選択します（オペレーティング システムとサーバのアイデンティティ変更およびタイムアウトの場合）。
ソース タイプ	ホスト入力データのソースのタイプを選択します（オペレーティング システムとサーバのアイデンティティ変更およびタイムアウトの場合）。
VLAN ID（Admin. VLAN ID）	イベントに関連しているホストの VLAN ID を入力します。
Web アプリケーション	Web アプリケーションを選択します。

ユーザ アクティビティのイベント トリガー条件の構文

ユーザ アクティビティで相関ルールをベースとして使用するには、まず、使用するユーザ アクティビティのタイプを選択します。選択肢が使用可能なトリガー条件の設定を決定します。次のオプションを選択できます。

- a new user identity was detected（新しいユーザ ID の検出）
- a user logs into a host（ユーザがホストにログイン）

ユーザ アクティビティを基本イベントとして選択する場合、次の表で説明する方法に従って相関ルールの条件を作成します。

表 *204*：ユーザ アクティビティの構文

指定する項目	選択する演算子と内容
Device	ユーザ アクティビティを検出した可能性のあるデバイスを 1 つ以上選択します。
ドメイン（Domain）	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
[IPアドレス（IP Address）]	単一の IP アドレスまたはアドレス ブロックを入力します。
[ユーザ名（Username）]	ユーザ名を入力します。

ホスト入力イベント トリガー条件の構文

ホスト入力イベントで相関ルールをベースとして使用するには、まず、使用するホスト入力イベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次の表では、選択可能なホスト入力イベントのタイプを示しています。

ユーザ定義によるホスト属性定義を追加/削除/変更するとき、あるいは脆弱性の影響限定を設定するときに、相関ルールをトリガーとして使用することはできません。

表 *205*：相関ルールのトリガー条件とホスト入力イベント タイプ

選択するオプション	ルールをトリガーとして使用するイベント タイプ
クライアントが追加された	クライアントの追加（Add Client）
クライアントが削除された	クライアントの削除（Delete Client）
ホストが追加された	ホストの追加（Add Host）

選択するオプション	ルールをトリガーとして使用するイベント タイプ
プロトコルが追加された	プロトコルの追加（Add Protocol）
プロトコルが削除された	プロトコルの削除（Delete Protocol）
スキャン結果が追加された	スキャン結果の追加（Add Scan Result）
サーバ定義が設定された	サーバ定義の設定（Set Server Definition）
サーバが追加された	ポートの追加（Add Port）
サーバが削除された	ポートの削除（Delete Port）
脆弱性が無効とマークされた	脆弱性を無効に設定（Vulnerability Set Invalid）
脆弱性が有効とマークされた	脆弱性を有効に設定（Vulnerability Set Valid）
アドレスが削除された	ホスト/ネットワークの削除（Delete Host/Network）
属性値が削除された	ホスト属性値の削除（Host Attribute Delete Value）
属性値が設定された	ホスト属性値の設定（Host Attribute Set Value）
OS 定義が設定された	オペレーティング システム定義の設定（Set Operating System Definition）
ホストの重要度が設定された	ホスト重要度の設定（Set Host Criticality）

次の表では、ホスト入力イベントを基本イベントとして選択するときに、相関ルールの条件を作成する方法を説明します。

表 *206*：ホスト入力イベントの構文

指定する項目	選択する演算子と内容
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
[IPアドレス（IP Address）]	単一の IP アドレスまたはアドレス ブロックを入力します。
ソース（Source）	ホスト入力データのソースを選択します。

指定する項目	選択する演算子と内容
ソース タイプ（Source Type）	ホスト入力データのソースのタイプを選択します。

接続イベント トリガー条件の構文

接続イベントで相関ルールをベースとして使用するには、まず、使用する接続イベントのタイプを指定します。接続イベントで利用可能な情報は、システムが接続をログに記録した方法、理由、および時によって変わることに注意してください。次のオプションを選択できます。

- 接続の開始または終了時のいずれか
- 接続の開始時
- 接続の終了時

次の表では、接続イベントを基本イベントとして選択するときに、相関ルールの条件を作成する方法を説明します。

表 *207*：接続イベントの構文

指定する項目	選択する演算子と内容
アクセス コントロール ポリシー	接続をログに記録したアクセス コントロール ポリシーを 1 つ以上選択します。
アクセス コントロール ルールのアクション	接続をログに記録したアクセス コントロール ルールに関連付けられたアクションを 1 つ以上選択します。 あとで接続を処理するルールまたはデフォルト アクションとは無関係に、ネットワーク トラフィックがいずれかのモニタ ルールの条件に一致した場合に相関イベントをトリガーとして使用するには、[モニタ（Monitor）] を選択します。
アクセス コントロール ルール（	接続をログに記録したアクセス コントロール ルールの名前のすべてまたは一部を入力します。 あとで接続を処理したルールまたはデフォルト アクションとは無関係に、接続と一致した条件を持つモニタ ルールの名前を入力できます。
アプリケーション プロトコル	接続に関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
クライアント	クライアントを 1 つ以上選択します。

指定する項目	選択する演算子と内容
クライアント カテゴリ	クライアントのカテゴリを 1 つ以上選択します。
クライアント バージョン	クライアントのバージョン番号を入力します。
接続時間	接続イベントの時間（秒数）を入力します。
接続タイプ	接続情報がどのように取得されたかに基づいて、相関ルールをトリガーするかどうかを指定します。 • エクスポートされた NetFlow データから生成された接続イベントに、[生成元（is）] および [Netflow] を選択します。 • Firepower システムの管理対象デバイスによって検出された接続イベントに、[生成元でない（is not）] および [Netflow] を選択します。
接続先（国）または送信元（国）	接続イベントの送信元または宛先 IP アドレスに関連付けられた国を 1 つ以上選択します。
Device	接続を検出したデバイスを 1 つ以上選択します。または（エクスポートされた NetFlow レコードからの接続データの場合）接続を処理したデバイスを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
出力インターフェイスまたは入力インターフェイス	インターフェイスを 1 つ以上選択します。
出力セキュリティ ゾーンまたは入力セキュリティ ゾーン	1 つ以上のセキュリティ ゾーンまたはを選択します。
イニシエータ バイト数、レスポンダ バイト数、または合計バイト数	次のいずれかを入力します。 • 送信されたバイト数（[イニシエータ バイト数（Initiator Bytes）]）。 • 受信されたバイト数（[レスポンダ バイト数（Responder Bytes）]）。 • 送受信されたバイト数（[合計バイト数（Total Bytes）]）。

指定する項目	選択する演算子と内容
イニシエータ IP、レスポンダ IP、イニシエータおよびレスポンダ IP の両方、あるいはイニシエータ IP またはレスポンダ IP	単一の IP アドレスまたはアドレス ブロックを指定します。
イニシエータ パケット数、レスポンダ パケット数、または合計パケット数	次のいずれかを入力します。 • 送信されたパケット数（[イニシエータ パケット（Initiator Packets）]）。 • 受信されたパケット数（[レスポンダ パケット数（Responder Packets）]）。 • 送受信されたパケット数（[合計パケット数（Total Packets）]）
イニシエータ ポート/ICMP タイプまたはレスポンダ ポート/ICMP コード	イニシエータ トラフィックのポート番号または ICMP タイプ、あるいはレスポンダ トラフィックのポート番号または ICMP コードを入力します。
IOC タグ	接続イベントにより侵害の兆候タグが設定[される（is）]または設定[されない（is not）]かどうかを指定します。
NetBIOS 名	接続におけるモニタ対象ホストの NetBIOS 名を入力します。
NetFlow デバイス	相関ルールをトリガーするために使用する NetFlow エクスポータの IP アドレスを選択します。ネットワーク検出ポリシーに NetFlow エクスポータを追加していない場合、[NetFlow デバイス（NetFlow Device）] ドロップダウン リストは空白になります。
理由（Reason）	接続イベントに関連付けられた理由を 1 つ以上選択します。
セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）	接続イベントに関連付けられたセキュリティ インテリジェンスのカテゴリを 1 つ以上選択します。 接続終了イベントの条件としてセキュリティ インテリジェンス カテゴリを使用するには、アクセス コントロール ポリシーでカテゴリを [ブロック（Block）] ではなく [モニタ（Monitor）] に設定します。
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを指定します。
SSL 証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL 証明書ステータス（SSL Certificate Status）	セッションの暗号化に使用された証明書に関連付けられたステータスを 1 つ以上選択します。

指定する項目	選択する演算子と内容
SSL 証明書のサブジェクトの共通名（CN）	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの国（C）	セッションの暗号化に使用された証明書のサブジェクトの国番号を 1 つ以上選択します。
SSL 証明書のサブジェクトの組織（O）	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの部門（OU）	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL 暗号スイート（SSL Cipher Suite）	セッションの暗号化に使用された暗号スイートを 1 つ以上選択します。
SSL暗号化セッション（SSL Encrypted Session）	[正常に復号（Successfully Decrypted）] を選択します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを1つ以上選択します。
SSL ポリシー	暗号化された接続をログに記録した SSL ポリシーを 1 つ以上選択します。
SSL ルール名	暗号化された接続をログに記録した SSL ルールの名前のすべてまたは一部を入力します。
SSL サーバ名	クライアントが暗号化された接続を確立したサーバの名前のすべてまたは一部を入力します。
SSL URL カテゴリ	暗号化された接続でアクセスされた URL のカテゴリを 1 つ以上選択します。
SSL バージョン	セッションの暗号化に使用された SSL または TLS バージョンを 1 つ以上選択します。
TCP フラグ	相関ルールをトリガーとして使用するために接続イベントに含まれていなければならない TCP フラグを選択します。NetFlow レコードから生成された接続データにのみ TCP フラグが含まれます。
トランスポート プロトコル	接続で使用されたトランスポート プロトコル：TCP または UDP を入力します。
URL	接続でアクセスされた URL 全体またはその一部を入力します。
URL カテゴリ	接続でアクセスされた URL のカテゴリを 1 つ以上選択します。
URLレピュテーション	接続でアクセスされた URL のレピュテーション値を 1 つ以上選択します。

指定する項目	選択する演算子と内容
[ユーザ名（Username）]	接続でいずれかのホストにログインしたユーザのユーザ名を入力します。
Web アプリケーション	接続に関連付けられた Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

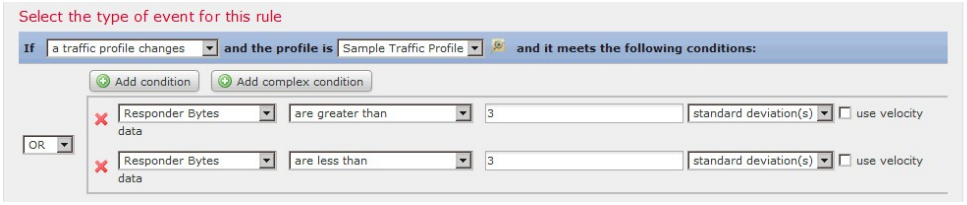
トラフィック プロファイル変化の構文

トラフィック プロファイル変化で相関ルールをベースとして使用するには、まず、使用するトラフィック プロファイルを選択します。ルールは、選択するプロファイルによって特徴付けられるパターンからネットワーク トラフィックが逸脱するときにトリガーされます。

raw データ、またはデータから計算された統計情報のいずれかに基づいてルールをトリガーできます。たとえば、ネットワーク内を移動するデータ量（バイト数で測定）が急激に変化した場合、攻撃または他のセキュリティー ポリシー違反が発生した可能性がありますが、そのような変動時にトリガーとして使用されるルールを作成できます。以下のいずかの場合にトリガーとして使用されるよう、ルールを指定できます。

- ネットワーク内を移動するバイト数が特定のバイト数を上回る場合
- ネットワーク内を移動するバイト数が、平均トラフィック量より上または下の特定数の標準偏差を超えて急激に変化した場合

  ネットワーク内を移動するバイト数が、特定数の標準偏差からなる範囲を（上または下に）超えたときにトリガーとして使用されるルールを作成するには、次の図に示すように、上限と下限を指定する必要があります。



  移動するバイト数が、平均を基準とした特定数の標準偏差の上側を超えた場合にトリガーとして使用されるルールを作成するには、以下の図に示されている最初の条件だけを使用します。

  移動するバイト数が、平均を基準とした特定数の標準偏差の下側を超えた場合にトリガーとして使用されるルールを作成するには、2 番目の条件だけを使用します。

[速度データを使用する（use velocity data）] チェックボックスを選択すると、データ ポイント間の変化率に基づいて相関ルールをトリガーできます。上記の例で仮に速度データを使用する場合は、次のいずれかの時点でルールがトリガーとして使用されるように指定できます。

- ネットワーク内を移動するバイト数の変化が、平均変化率より上または下の特定数の標準偏差を超えた場合
- ネットワーク内を移動するバイト数の変化が、特定のバイト数を上回った場合

トラフィック プロファイル変化を基準イベントとして選択した場合、以下の表で説明する方法に従って相関ルールの条件を作成します。

表 *208*：トラフィック プロファイル変化の構文

指定する項目	選択する演算子と入力内容	いずれかを選択
接続数	検出された接続の合計数 **または** 平均より上または下の標準偏差の数（検出された接続数がこれを超えるとルールがトリガーとして使用されます）	接続 standard deviation(s)：標準偏差の数
合計バイト数、イニシエータ バイト数、またはレスポンダ バイト数	次のいずれかになります。 • 送信された合計バイト数（[合計バイト数（Total Bytes）]） • 送信されたバイト数（[イニシエータ バイト数（Initiator Bytes）]） • 受信されたバイト数（[レスポンダ バイト数（Responder Bytes）]） **または** 平均より上または下の標準偏差の数（上の条件のいずれかはルールがトリガーとして使用される必要があります）	bytes standard deviation(s)：標準偏差の数
合計パケット数、イニシエータ パケット数、またはレスポンダ パケット数	次のいずれかになります。 • 送信された合計パケット数（[合計パケット数（Total Packets）]） • 送信されたパケット数（[イニシエータ パケット数（Initiator Packets）]） • 受信されたパケット数（[レスポンダ パケット数（Responder Packets）]） **または** 平均より上または下の標準偏差の数（上の条件のいずれかはルールがトリガーとして使用される必要があります）	packets standard deviation(s)：標準偏差の数

指定する項目	選択する演算子と入力内容	いずれかを選択
一意のイニシエータ	セッションを開始した個別のホストの数 **または** 平均より上または下の標準偏差の数（検出された一意のイニシエータ数はルールがトリガーとして使用される必要があります）	initiators：イニシエータ数 standard deviation(s)：標準偏差の数
一意のレスポンダ	セッションに応答した個別のホストの数 **または** 平均より上または下の標準偏差の数（検出された一意のレスポンダ数はルールがトリガーとして使用される必要があります）	responders：レスポンダ数 standard deviation(s)：標準偏差の数

相関ホスト プロファイル限定の構文

イベントに関連するホストのホストプロファイルに基づいて相関ルールを制約するには、[ホストプロファイル限定（host profile qualification）] を追加します。マルウェア イベント、トラフィック プロファイル変化、または新しいIPホスト検出によってトリガーとして使用される相関ルールには、ホスト プロファイル限定を追加することはできません。

ホスト プロファイル限定を作成するときには、まず、相関ルールを制約するために使用するホストを指定します。選択可能なホストは、ルールの基盤となるイベントのタイプによって異なります。

- 接続イベント：[レスポンダ ホスト（Responder Host）] または [イニシエータ ホスト（Initiator Host）] を選択します。
- 侵入イベント：[宛先ホスト（Destination Host）] または [送信元ホスト（Source Host）] を選択します。
- ディスカバリ イベント、ホスト入力イベントは、またはユーザ アクティビティ：[ホスト（Host）] を選択します。

次の表では、相関ルールのホスト プロファイル限定を作成する方法について説明します。

表 *209*：ホスト プロファイル限定の構文

指定する項目	選択する演算子と内容
[アプリケーションプロトコル（Application Protocol）] >[アプリケーションプロトコル（Application Protocol）]	アプリケーション プロトコルを選択します。

指定する項目	選択する演算子と内容
[アプリケーションプロトコル（Application Protocol）] >[アプリケーション ポート（Application Port）]	アプリケーション プロトコルのポート番号を入力します。
[アプリケーションプロトコル（Application Protocol）] > [プロトコル（Protocol）]	プロトコルを選択します。
[アプリケーションプロトコル カテゴリ（Application Protocol Category）]	カテゴリを選択します。
[クライアント（Client）] > [クライアント（Client）]	クライアントを選択します。
[クライアント（Client）] > [クライアント バージョン（Client Version）]	クライアント バージョンを入力します。
[クライアント カテゴリ（Client Category）]	カテゴリを選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
ハードウェア	モバイルデバイスのハードウェア モデルを入力します。たとえば、すべての Apple iPhone に一致させるには iPhone と入力します。
[ホストの重要度（Host Criticality）]	ホストの重要度を選択します。
ホスト タイプ	ホスト タイプを 1 つ以上選択します。通常のホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
[IOC タグ（IOC Tag）]	侵害の兆候タグを 1 つ以上選択します。
ジェイルブロークン	イベントのホストがジェイルブレイクされたモバイル デバイスであることを示すには [はいい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。

指定する項目	選択する演算子と内容
[MAC アドレス（MAC Address）]>[MAC アドレス（MAC Address）]	ホストの MAC アドレス全体またはその一部を入力します。
[MAC アドレス（MAC Address）]>[MAC タイプ（MAC Type）]	MAC タイプが ARP/DHCP で検出されるかどうかを選択します。 • システムは MAC アドレスがホストに属していることをポジティブに識別した（[ARP/DHCP で検出（is ARP/DHCP Detected）]） • たとえば、デバイスとホスト間にはルータがあるため、システムはその MAC アドレスを持つ多くのホストを認識している（[ARP/DHCP で検出されない（is not ARP/DHCP Detected）]） • MAC タイプが無関係（[どれでもない（is any）]）
[MAC ベンダー（MAC Vendor）]	ホストが使用するハードウェアの MAC ベンダー全体またはその一部を入力します。
Mobile	イベントのホストがモバイル デバイスであることを示すには [はいい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
[NetBIOS 名（NetBIOS Name）]	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
[オペレーティング システム（Operating System）]>[OS ベンダー（OS Vendor）]	オペレーティング システムのベンダー名を 1 つ以上選択します。
[オペレーティング システム（Operating System）]>[OS 名（OS Name）]	オペレーティング システムの名前を 1 つ以上選択します。
[オペレーティング システム（Operating System）]>[OS バージョン（OS Version）]	オペレーティング システムのバージョンを 1 つ以上選択します。
[トランスポート プロトコル（Transport Protocol）]	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポート プロトコルの名前または番号を入力します。
VLAN ID（Admin. VLAN ID）	ホストの VLAN ID 番号を入力します。

指定する項目	選択する演算子と内容
Web アプリケーション	Web アプリケーションを選択します。
[Webアプリケーションのカテゴリ（Web Application Category）]	カテゴリを選択します。
使用可能な任意のホスト属性（デフォルトコンプライアンスホワイトリストホスト属性を含む）	ホスト属性タイプに応じて適切な値を入力または選択します。

暗黙的または汎用のクライアントを使用したホスト プロファイル限定の作成

システムが `client` が続くアプリケーションプロトコルの名前（たとえば、`HTTPS client`）を使用して検出されたクライアントをレポートする場合、このクライアントは暗黙的または汎用のクライアントです。これらの場合、システムは特定のクライアントを検出していませんが、サーバ応答トラフィックに基づいてクライアントの存在を推測しています。

暗黙的または汎用のクライアントを使用してホストプロファイル限定を作成するには、クライアントではなく、レスポンダホストで実行されているアプリケーションプロトコルを使用して制約します。

イベント データを使用したホスト プロファイル限定の作成

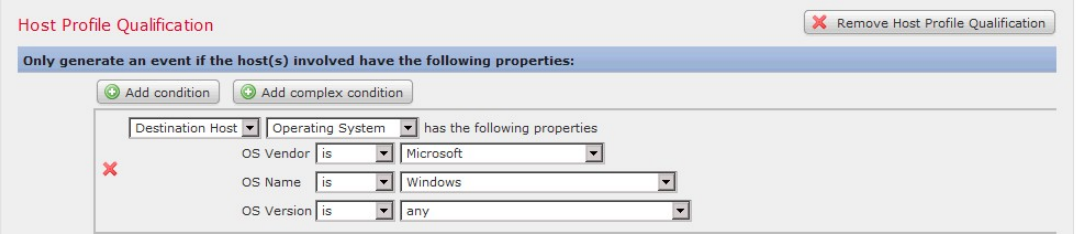
ホストプロファイル限定の制約時に、多くの場合、相関ルールの基本イベントからデータを使用できます。

たとえば、モニタ対象のいずれかのホストで特定のブラウザが使用されていることをシステムが検出した場合に、相関ルールがトリガーとして使用されるとします。さらに、この使用を検出するときに、ブラウザのバージョンが最新でない場合はイベントを生成すると仮定します。

この場合、[クライアント（Client）] は [イベント クライアント（Event Client）] ですが、[クライアントバージョン（Client Version）]が最新のバージョンでない場合にのみルールがトリガーされるように、この相関ルールをホスト プロファイル限定に追加できます。

ホスト プロファイル限定の例

次のホストプロファイル限定は、ルールの基礎となるディスカバリイベントに関連するホストが Microsoft Windows のバージョンを実行している場合にのみ、ルールがトリガーとして使用されるように相関ルールを制約します。



ユーザ限定の構文

接続、侵入、ディスカバリ、またはホスト入力のいずれかのイベントを使用して相関ルールをトリガーとして使用する場合、イベントに関連するユーザのアイデンティティに基づいてルールを制約することができます。この制約は、ユーザ限定と呼ばれます。たとえば、送信元または宛先ユーザのアイデンティティが販売部門所属である場合にのみトリガーとして使用するよう、相関ルールを制約できます。

トラフィックプロファイル変化やユーザアクティビティ検出によってトリガーとして使用される相関ルールに、ユーザ限定を追加することはできません。また、システムは、アイデンティティレルムで確立された Firepower Management Center サーバの接続を介してユーザの詳細を取得します。この情報は、データベース内のすべてのユーザに関して入手可能とは限りません。

ユーザ限定を作成するときには、まず、相関ルールを制約するために使用するアイデンティティを指定します。選択可能なアイデンティティは、ルールの基本イベントのタイプによって異なります。

- 接続イベント：[イニシエータのアイデンティティ（Identity on Initiator）] または [レスポンダのアイデンティティ（Identity on Responder）] を選択します。
- 侵入イベント：[宛先のアイデンティティ（Identity on Destination）] または [送信元のアイデンティティ（Identity on Source）] を選択します。
- ディスカバリ イベント：[ホストのアイデンティティ（Identity on Host）] を選択します。
- ホスト入力イベント：[ホストのアイデンティティ（Identity on Host）] を選択します。

次の表では、相関ルールのユーザ限定を作成する方法について説明します。

表 *210*：ユーザ限定の構文

指定する項目	選択する演算子と内容
認証プロトコル（Authentication Protocol）	ユーザを検出するために使用される認証プロトコル（またはユーザ タイプ）プロトコルを選択します。
部署名（Department）	部署を入力します。

指定する項目	選択する演算子と内容
ドメイン（Domain）	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
E メール	電子メール アドレスを入力します。
名	名を入力します。
姓	姓を入力します。
電話	電話番号を入力します。
[ユーザ名（Username）]	ユーザ名を入力します。

接続トラッカー

接続トラッカーは、ルールの最初の基準（ホストプロファイルおよびユーザ認定を含む）に一致した後にシステムが特定の接続のトラッキングを始めるよう、相関ルールを制約します。追跡される接続が、指定した期間にわたって収集された追加の基準を満たす場合には、システムがルールの相関イベントを生成します。

ヒント　通常、接続トラッカーは特定のトラフィックだけをモニタし、トリガーとして使用された場合には指定された一定期間だけ実行されます。接続トラッカーは、広範なネットワーク トラフィックをモニタして持続的に実行されるトラフィック プロファイルとは対照的です。

接続トラッカーがイベントを生成する方法は 2 つあります。

条件に一致するとただちに起動する接続トラッカー

ネットワーク トラフィックが接続トラッカーの条件に一致すると即座に相関ルールが起動するよう、接続トラッカーを設定できます。この場合、タイムアウト期間が満了していなくても、システムはその接続トラッカー インスタンスでの接続のトラッキングを停止します。相関ルールをトリガーとして使用したのと同じタイプのポリシー違反が再び発生した場合、システムは新しい接続トラッカーを作成します。

ただし、ネットワーク トラフィックが接続トラッカーの条件に一致する前にタイムアウト期間が満了した場合、システムは相関イベントを生成せず、そのルール インスタンスの接続のトラッキングを停止します。

たとえば、特定のタイプの接続が特定の期間中に特定回数を超えて発生した場合にのみ相関イベントを生成させることで、接続トラッカーをある種のイベントしきい値として機能させることが

できます。あるいは、初回接続後に過剰なデータ転送量をシステムが検出した場合にのみ、相関イベントを生成させることもできます。

タイムアウト期間の満了時に起動する接続トラッカー

タイムアウト期間全体にわたって収集されるデータに依存するよう、接続トラッカーを設定できます。この場合、タイムアウト期間が満了するまでは起動しません。

たとえば、特定の期間内に検出された転送量が特定のバイト数を下回った場合に接続トラッカーを起動するよう設定すると、システムはその期間が経過するまで待って、ネットワーク トラフィックがその条件に一致した場合はイベントを生成します。

接続トラッカーの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

はじめる前に

- 接続、侵入、検出、ユーザID、ホスト入力イベントに基づいて相関ルールを作成します。マルウェア イベントやトラフィック プロファイルの変更に基づいたルールに接続トラッカーを追加することはできません。

手順

ステップ 1 相関ルールエディタで、[接続トラッカーの追加（Add Connection Tracker）] をクリックします。

ステップ 2 追跡する接続を指定します。接続トラッカーの構文, （1663 ページ） を参照してください。

ステップ 3 追跡する接続に応じて、いつ相関イベントを生成するかを指定します。接続トラッカー イベントの構文, （1667 ページ） を参照してください。

ステップ 4 トラッカーの条件が満たされなければならない時間の間隔（秒、分または時）を指定します。

接続トラッカーの構文

次の表は、どのような接続を追跡するかを指定する接続トラッカー条件の作成方法を説明しています。

表 *211*：接続トラッカーの構文

指定する項目	選択する演算子と内容
アクセス コントロール ポリシー	追跡対象の接続を処理したアクセス コントロール ポリシーを 1 つ以上選択します。
アクセス コントロール ルールのアクション	追跡対象の接続をログに記録したアクセス コントロール ルールに関連付けられたアクセス コントロール ルール アクションを 1 つ以上選択します。 あとで接続を処理するルールまたはデフォルト アクションとは無関係に、任意のモニタ ルールの条件に一致する接続を追跡するには、[モニタ（Monitor）] を選択します。
アクセス コントロール ルール名	追跡対象の接続をログに記録したアクセス コントロール ルールの名前のすべてまたはその一部を入力します。 モニタ ルールに一致する接続を追跡するには、モニタ ルールの名前を入力します。あとで接続を処理するルールまたはデフォルト アクションとは無関係に、システムは該当する接続を追跡します。
アプリケーション プロトコル	アプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコル カテゴリを 1 つ以上選択します。
クライアント	クライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアント カテゴリを 1 つ以上選択します。
クライアント バージョン	クライアントのバージョンを入力します。
接続時間	接続時間（秒数）を入力します。
接続タイプ	接続情報がどのように取得されたかに基づいて、相関ルールをトリガーするかどうかを指定します。 • エクスポートされた NetFlow レコードから生成された接続イベントに、[生成元（is）] および [Netflow] を選択します。 • Firepower システムの管理対象デバイスによって検出された接続イベントに、[生成元でない（is not）] および [Netflow] を選択します。
接続先（国）または送信元（国）	国を 1 つ以上選択します。

指定する項目	選択する演算子と内容
Device	追跡対象の接続を検出したデバイスを 1 つ以上選択します。NetFlow 接続を追跡する場合は、エクスポートされた NetFlow レコードからの接続データを処理するデバイスを選択します。
入力インターフェイスまたは出力インターフェイス	インターフェイスを 1 つ以上選択します。
入力セキュリティ ゾーンまたは出力セキュリティ ゾーン	1 つ以上のセキュリティ ゾーンまたはを選択します。
イニシエータ IP、レスポンダ IP、またはイニシエータ/レスポンダ IP	単一の IP アドレスまたはアドレス ブロックを入力します。
イニシエータ バイト数、レスポンダ バイト数、または合計バイト数	次のいずれかを入力します。 • 送信されたバイト数（[イニシエータ バイト数（Initiator Bytes）]） • 受信されたバイト数（[レスポンダ バイト数（Responder Bytes）]） • 送受信されたバイト数（[合計バイト数（Total Bytes）]）
イニシエータ パケット数、レスポンダ パケット数、または合計パケット数	次のいずれかを入力します。 • 送信されたパケット数（[イニシエータ パケット数（Initiator Packets）]） • 受信されたパケット数（[レスポンダ パケット数（Responder Packets）]） • 送受信されたパケット数（[合計パケット数（Total Packets）]）
イニシエータ ポート/ICMP タイプまたはレスポンダ ポート/ICMP コード	イニシエータ トラフィックのポート番号または ICMP タイプ、あるいはレスポンダ トラフィックのポート番号または ICMP コードを入力します。
IOC タグ	侵害の兆候タグが設定されて [いる（is）] または設定されて [いない（is not）] かどうかを選択します。
NETBIOS 名	接続におけるモニタ対象ホストの NetBIOS 名を入力します。
NetFlow デバイス	追跡する NetFlow エクスポータの IP アドレスを選択します。ネットワーク検出ポリシーに NetFlow エクスポータを追加していない場合、[NetFlow デバイス（NetFlow Device）] ドロップダウン リストは空白になります。
理由（Reason）	追跡対象の接続に関連付けられている理由を 1 つ以上選択します。

指定する項目	選択する演算子と内容
セキュリティ インテリジェンス カテゴリ	追跡対象の接続に関連付けられているセキュリティ インテリジェンスのカテゴリを 1 つ以上選択します。
TCP フラグ	接続を追跡するために接続に含まれている必要のある TCP フラグを選択します。TCP フラグ データは、エクスポートされた NetFlow レコードから生成された接続にのみ含まれます。
トランスポート プロトコル	接続に使用されるトランスポート プロトコルを選択します。
URL	追跡対象の接続でアクセスされた URL のすべてまたはその一部を入力します。
URL Category	追跡対象の接続でアクセスされた URL のカテゴリを 1 つ以上選択します。
URL レピュテーション	追跡対象の接続でアクセスされた URL のレピュテーション値を 1 つ以上選択します。
[ユーザ名（Username）]	追跡対象の接続でいずれかのホストにログインしたユーザのユーザ名を入力します。
Web アプリケーション	Web アプリケーションを 1 つ以上選択します。
[Web アプリケーションのカテゴリ（Web Application Category）]	Web アプリケーションのカテゴリを 1 つ以上選択します。

イベント データを使用した接続トラッカーの作成

接続トラッカーを作成するときに、多くの場合、相関ルールの基本イベントからデータを使用できます。

たとえば、システムが新しいクライアントを検出するときに、相関ルールがトリガーされると想定します。接続トラッカーをこのタイプの相関ルールに追加すると、システムは次の基本イベントを参照する制約のあるトラッカーを自動的に入力します。

- [イニシエータ/レスポンダ IP（Initiator/Responder IP）] が [イベント IP アドレス（Event IP Address）] に設定される。
- [クライアント（Client）] が [イベント クライアント（Event Client）] に設定される。

ヒント 特定の IP アドレスまたは IP アドレス ブロックに関連する接続を追跡するには、[手動エントリにスイッチ（switch to manual entry）] をクリックして、手動で IP を指定します。[イベント フィールドにスイッチ（switch to event fields）] をクリックすると、イベントの IP アドレスを使用する設定に戻ります。

接続トラッカー イベントの構文

追跡対象の接続に基づいてどのようなときに相関イベントを生成するかを指定する接続トラッカー条件を作成するには、次の表の説明に従います。

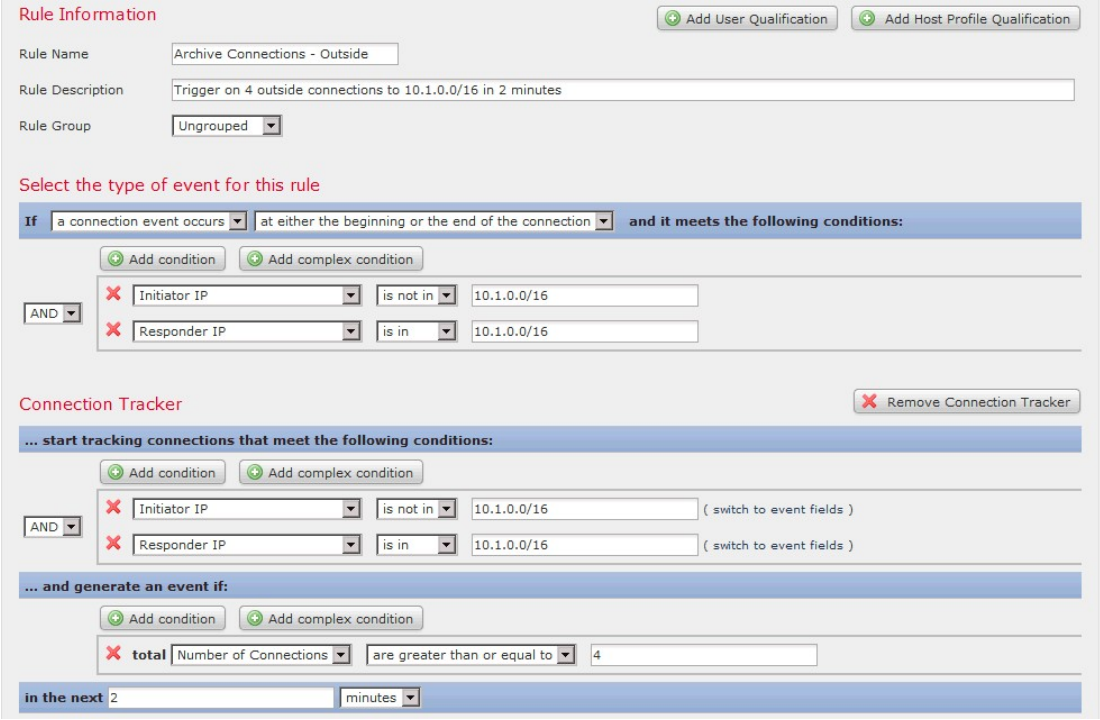
表 *212*：接続トラッカー イベントの構文

指定する項目	選択する演算子と入力内容
接続数	検出された接続の合計数
SSL 暗号化セッションの数	検出された SSL または TLS 暗号化セッションの合計数
合計バイト数、イニシエータ バイト数、またはレスポンダ バイト数	次のいずれかになります。 • 送信された合計バイト数（[合計バイト数（Total Bytes）]） • 送信されたバイト数（[イニシエータ バイト数（Initiator Bytes）]） • 受信されたバイト数（[レスポンダ バイト数（Responder Bytes）]）
合計パケット数、イニシエータ パケット数、またはレスポンダ パケット数	次のいずれかになります。 • 送信された合計パケット数（[合計パケット数（Total Packets）]） • 送信されたパケット数（[イニシエータ パケット数（Initiator Packets）]） • 受信されたパケット数（[レスポンダ パケット数（Responder Packets）]）
一意のイニシエータまたは一意のレスポンダ	次のいずれかになります。 • 検出されたセッションを開始した個別のホスト数（[一意のイニシエータ（Unique Initiators）]） • 検出された接続に応答した個別のホスト数（[一意のレスポンダ（Unique Responders）]）

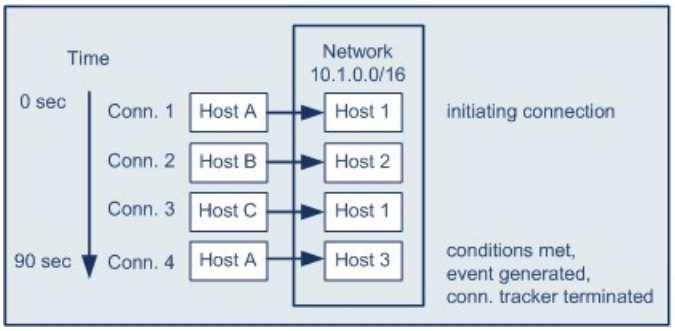
外部ホストからの過剰な接続の設定例

ネットワーク 10.1.0.0/16 のセンシティブ ファイルをアーカイブし、通常、ネットワーク外のホストはネットワーク内のホストへの接続を開始することはないシナリオを考慮します。ネットワーク外から接続が開始される場合もありますが、2 分以内に 4 つ以上の接続が開始されたときに、これが懸念材料であると判断します。

次の図に示すルールでは、接続が 10.1.0.0/16 ネットワーク外からネットワーク内に発生したときに、基準に適合するトラッキング接続を開始するように指定します。その後、2 分以内に署名に一致する 4 つの接続（発信側の接続を含む）が検出されても相関イベントを生成します。



以下の図は、ネットワーク トラフィックが上記の相関ルールをトリガーとして使用できる方法を示します。



この例では、相関ルールの基本的条件に適合する接続が検出されました。つまり、接続が10.1.0.0/16ネットワーク外のホストからネットワーク内のホストへの接続が検出されました。これにより、接続トラッカーが生成されました。

接続トラッカーは、次のステージで処理します。

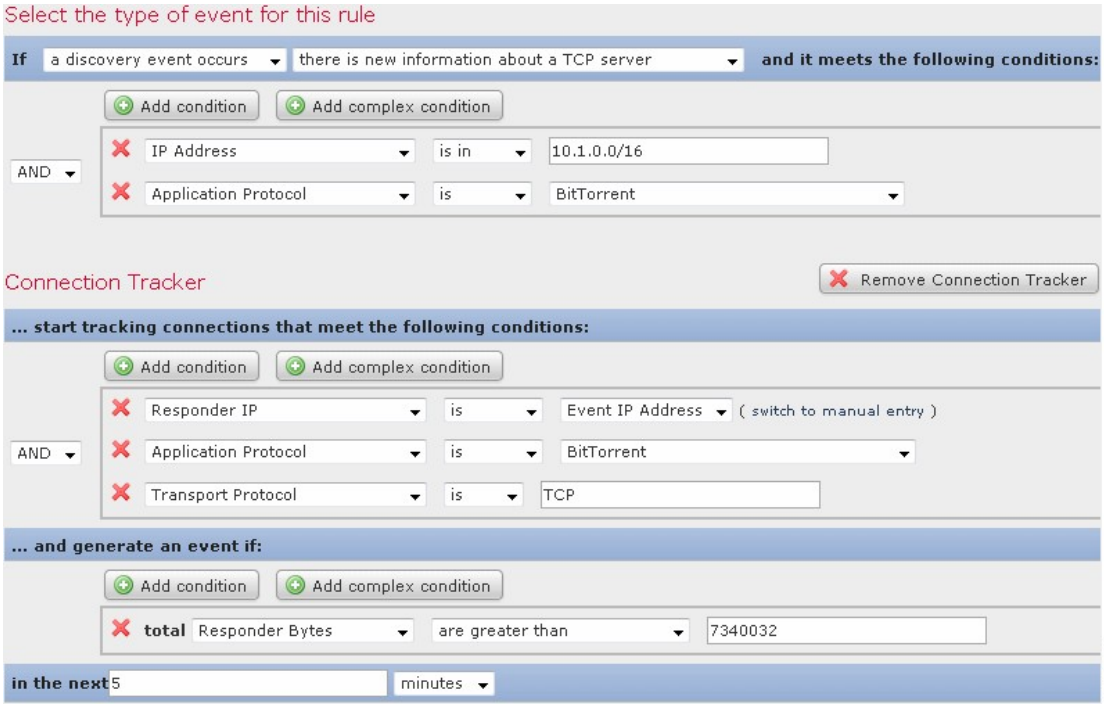
- ネットワーク外のホストAからネットワーク内のホスト1への接続が検出されると、トラッキング接続を開始します。
- 接続トラッカーの署名に一致する2つ以上の接続（ホストB～ホスト2、ホストC～ホスト1）を検出します。
- 2分の時間制限内でホストAがホスト3に接続すると、4つの認定されている接続を検出します。ルール条件が適合します。

- 最後に、相関イベントを生成し、トラッキング接続を停止します。

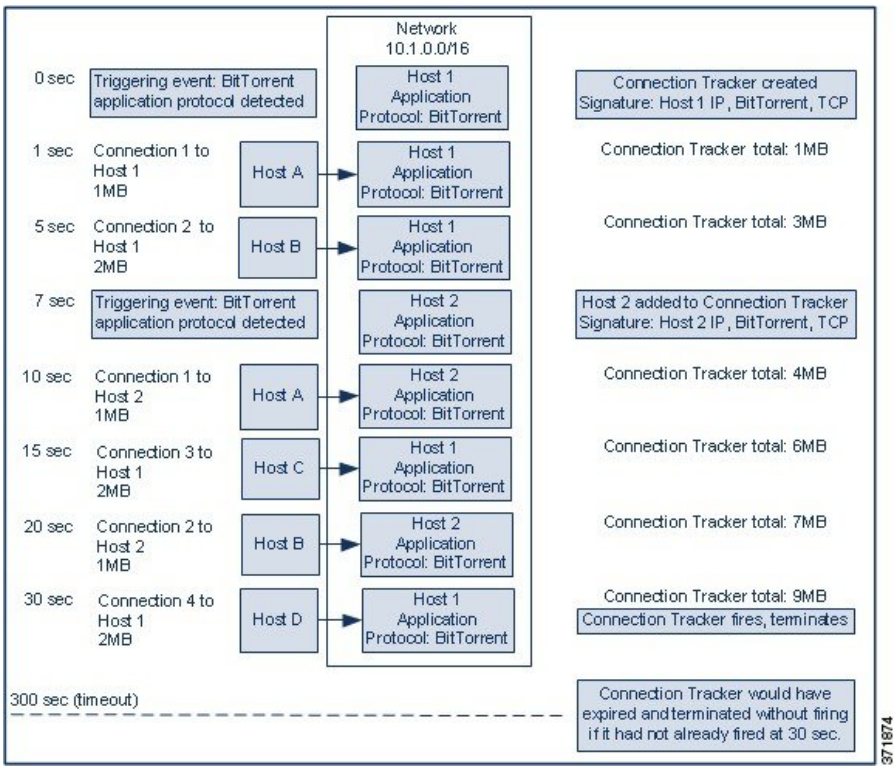
BitTorrent の過剰なデータ転送の設定例

最初に監視対象のネットワークのホストに接続後、過剰な BitTorrent データの転送が検出された場合は相関イベントを生成するシナリオを考慮します。

次の図は、監視対象ネットワーク上に BitTorrent アプリケーション プロトコルを検出した場合にトリガーとして使用される相関ルールを示します。このルールには、監視対象ネットワークのホスト（この例では 10.1.0.0/16）が、最初のポリシー違反後の 5 分間に 7 MB を超えるデータ（7340032 バイト）を BitTorrent を介してまとめて転送する場合にのみルールがトリガーとして使用されるように制約する接続トラッカーがあります。



以下の図は、ネットワーク トラフィックが上記の相関ルールをトリガーとして使用できる方法を示します。



この例では、2 つのホスト（ホスト 1、ホスト 2）に BitTorrent TCP アプリケーション プロトコルが検出されました。この 2 つのホストは、BitTorrent を介して 4 つの他のホスト（ホスト A、ホスト B、ホスト C、ホスト D）にデータを転送しました。

接続トラッカーは、次の工程で処理しました。

- まず、ホスト 1 で BitTorrent アプリケーション プロトコルが検出されると、0 秒マーカーで接続のトラッキングを開始します。次の 5 分の間に 7MB の BitTorrent TCP データの転送が検出されない場合（300 秒マーカーにより）、接続トラッカーは無効になる点にご注意ください。
- 5 秒で、ホスト 1 は、署名に一致する 3MB データを転送します。
  - 1 秒マーカーでは、ホスト 1 からホスト A へ 1 MB（供給した接続トラッカーに対して数えた全 BitTorrent トラフィック 1 MB）
  - 5 秒マーカーでホスト 1 からホストへ B 2 MB（合計 3 MB）
- 7 秒では、ホスト 2 で BitTorrent アプリケーション プロトコルを検出し、ホスト 2 に対しても BitTorrent 接続のトラッキングを開始します。
- 20 秒では、ホスト 1 とホスト 2 の両方から転送される署名に一致する追加のデータを検出します。
  - 10 秒マーカーでホスト 2 からホスト A へ 1 MB（合計 4 MB）
  - 15 秒マーカーでホスト 1 からホスト C へ 2 MB（合計 6 MB）

- 20 秒マーカーでホスト 2 からホスト B へ 1MB（合計 7MB）

- ホスト 1 とホスト 2 では、現在合わせて 7 MB の BitTorrent データが転送されていますが、ルールはトリガーとして使用されていません。これは、転送された合計バイト数が 7 MB を超えている（[レスポンダのバイトは 7340032 を超えています（Responder Bytes are greater than 7340032）]）必要があるためです。この時点で、トラッカーのタイムアウト期間内の残りの 280 秒の間、追加の BitTorrent 転送が検出されない場合に、トラッカーは無効になり、相関イベントは作成されません。
- ただし、30 秒の時点で、別の BitTorrent 転送が検出され、次のルールの条件が満たされます。
  - 30 秒マーカーでは、ホスト 1 からホスト D へ 2 MB（合計 9 MB）
- 最後に、相関イベントが生成されます。また、5 分間が無効にならなくても接続トラッカーインスタンスについてはトラッキング接続を停止します。この時点で BitTorrent TCP アプリケーションプロトコルを用いて新しい接続が検出されると、新しい接続トラッカーが生成されます。ホスト 1 が 2 MB すべてをホスト D に転送した後に相関イベントが生成される点にご注意ください。これは、セッションが終了するまで接続データを計算することはないためです。

スヌーズ期間および非アクティブ期間

相関ルールでスヌーズ期間を設定することができます。スヌーズ期間を設定すると、相関ルールがトリガーとして使用されたとき、指定した時間間隔内にルール違反が再び発生しても、システムはその期間中はルールのトリガーを停止します。スヌーズ期間が経過すると、ルールは再びトリガー可能になります（新しいスヌーズ期間が始まります）。

たとえば、通常はトラフィックを全く生成しないはずのホストがネットワーク上にあるとします。このホストが関与する接続がシステムで検出されるたびにトリガーとして使用される単純な相関ルールの場合、このホストで送受信されるネットワーク トラフィックによっては、短時間に多数の相関イベントが生成される可能性があります。ポリシー違反を示す相関イベントの数を制限するために、スヌーズ期間を追加できます。これにより、（指定した期間内に）システムで検出されたそのホストに関連する最初の接続に対してのみ、システムは相関イベントを生成します。

また、相関ルールで非アクティブ期間を設定することもできます。非アクティブ期間中は、相関ルールはトリガーとして使用されません。非アクティブ期間を毎日、毎週、または毎月繰り返すように設定できます。たとえば、ホストオペレーティングシステム変更を探すために内部ネットワークで夜間に Nmap スキャンを実行するとします。この場合、相関ルールが誤ってトリガーとして使用されないよう、毎日のスキャン時間帯に、該当する相関ルールで非アクティブ期間を設定することができます。

相関ルールの作成メカニズム

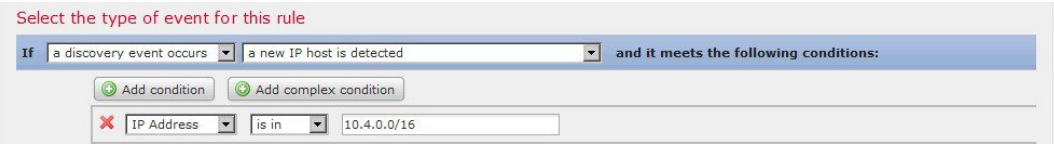
相関ルールは、ルールがトリガーされる条件を指定して作成します。条件で使用できるシンタックスは、作成しようとしている要素により異なりますが、メカニズムはすべて同じです。

ほとんどの条件は、カテゴリ、演算子、値の 3 つの部分からなります。

- 相関ルール トリガー、ホスト プロファイル認定、接続トラッカー、ユーザ認定のどれを作成しているのかに応じて、選択できるカテゴリが異なります。相関ルール トリガーでは、さらにルールの基本イベント タイプにより選択できるカテゴリが異なります。条件によっては、それぞれ独自の演算子と値を持つ複数のカテゴリが含まれることがあります。
- 条件に使用可能な演算子はカテゴリによって異なります。
- 条件の値を指定するために使用できるシンタックスは、カテゴリと演算子に応じて異なります。場合によっては、テキスト フィールドに値を入力する必要があります。それ以外の場合、ドロップダウンリストから値（1 つあるいは複数の値）を選択できます。

たとえば、新しいホストが検出されるたびに相関イベントを生成するには、条件を一切含まない単純なルールを作成できます。

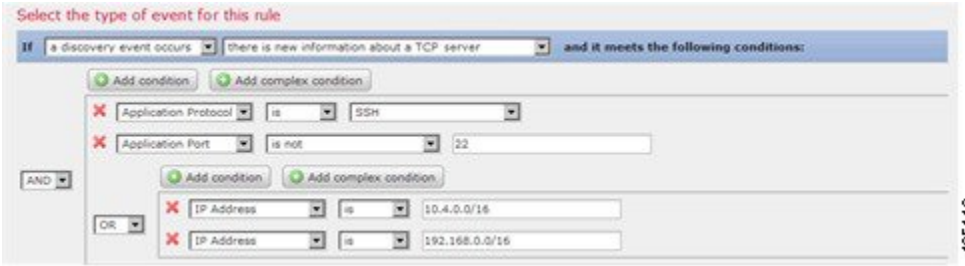
ルールをさらに制約して、新しいホストが 10.4.x.x ネットワークで検出された場合にのみイベントを生成するには、1 つの条件を追加できます。



構造に複数の条件を含める場合は、それらの条件を AND または OR 演算子でつなげる必要があります。同じレベルにある複数の条件は、次のように一緒に評価されます。

- AND 演算子は、制御対象のレベルにあるすべての条件が満たされなければならないことを示します。
- OR 演算子は、制御対象のレベルにある少なくとも 1 つの条件が満たされなければならないことを示します。

10.4.x.x ネットワークおよび 192.168.x.x ネットワーク上の非標準ポートで SSH アクティビティを検出する以下のルールには、4 つの条件が設定されており、下の 2 つは複合条件を形成しています。



論理的には、ルールは次のように評価されます。

```
(A and B and (C or D))
```

表 *213*：ルールの評価

値	条件で指定する内容
A	アプリケーション プロトコルが SSH である
B	アプリケーション ポートが 22 ではない
C	IP アドレスが 10.0.0.0/8 内にある
D	IP アドレスが 196.168.0.0/16 内にある

注意 頻繁に発生するイベントによってトリガーされる複雑な相関ルールを評価することにより、システム パフォーマンスが低下する可能性があります。たとえば、ロギングするすべての接続に対して、複数の条件からなるルールをシステムが評価しなければならない場合、リソースが過負荷になる可能性があります。

相関ルールへの条件の追加とリンク設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

手順

ステップ 1 相関ルールエディタで、単純条件または複合条件を追加します。

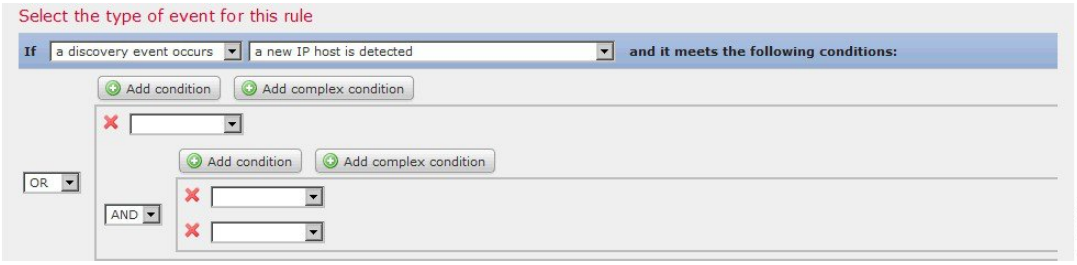
- 単純：[条件の追加（Add condition）] をクリックします。
- 複合：[複合条件の追加（Add complex condition）] をクリックします。

ステップ 2 条件の左にあるドロップダウン リストから [AND] または [OR] 演算子を選択して条件を結合します。

例:単純条件と複合条件の対比

次の図は、単純条件 2 つを [OR] 演算子で結合した相関ルールを示したものです。

次の図は、単純条件 1 つと、複合条件 1 つを [OR] 演算子で結合した相関ルールを示したものです。複合条件は 2 つの単純条件を [AND] 演算子で結合して構成します。



相関ルール条件での複数の値の使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

相関条件を作成するときに、条件の構文でドロップダウン リストから値を選択できる場合、通常はリストから複数の値を選択できます。

手順

ステップ 1 相関ルール エディタで、演算子として [存在する（is in）] または [存在しない（is not in）] を選択して 1 つの条件を作成します。

ステップ 2 テキスト フィールド内の任意の場所または [編集（Edit）] リンクをクリックします。

ステップ 3 [使用可能（Available）] の下にある複数の値を選択します。また、クリックしてドラッグすることで、隣接する複数の値を選択できます。

ステップ 4 右矢印（>）をクリックして、選択した項目を [Selected] に移動します。

ステップ 5 [OK] をクリックします。

相関ルールの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

マルチドメイン展開では、現在のドメインで作成された相関ルールとグループが表示されます。これらは編集可能です。また、先祖ドメインからの選択した相関ルールとグループも表示されますが、これらは編集できません。下位のドメインで作成された相関ルールとグループを表示および編集するには、そのドメインに切り替えます。

（注） 設定に無関係なドメイン（名前、管理対象デバイスなど）に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。

アクティブな相関ポリシーのルールへの変更は、即座に反映されます。

はじめる前に

- ルールを削除する場合は、そのルールをすべての相関ポリシーから削除します。詳細については、相関ポリシーの管理, （1637 ページ）を参照してください。

手順

ステップ 1 [ポリシー（Policies）]>[相関（Correlation）] を選択して、[ルール管理（Rule Management）] タブをクリックします。

ステップ 2 ルールを管理します。

- 作成：[ルールの作成（Create Rule）] をクリックします。相関ルールの設定，（1638 ページ）を参照してください。
- グループの作成：[グループの作成（Create Group）] をクリックし、グループの名前を入力して、[保存（Save）] をクリックします。グループにルールを追加するには、ルールを編集します。
- 編集：編集アイコン（  ）をクリックします。相関ルールの設定，（1638 ページ）を参照してください。代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ルールまたはルール グループの削除：削除アイコン（  ）をクリックします。ルール グループを削除すると、ルールのグループ化が解除されます。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

相関応答グループの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

アラートおよび修復の相関応答グループを作成し、グループをアクティブにして、アクティブな相関ポリシー内の相関ルールに割り当てることができます。システムは、ネットワーク トラフィックが相関ルールに一致すると、すべてグループ化された応答を開始します。

アクティブなグループまたはいずれかのグループ化された応答に対する変更は、アクティブな相関ポリシーで行う場合、ただちに有効になります。

手順

ステップ 1 [ポリシー（Policies）]>[相関（Correlation）] を選択し、[グループ（Group）] をクリックします。

ステップ 2 [グループの作成（Create Group）] をクリックします。

ステップ 3 名前を入力します。

ステップ 4 作成時にグループをアクティブにする場合は、[アクティブ（Active）] チェックボックスをオンにします。
非アクティブ化されたグループは応答を開始しません。

ステップ 5 グループに [使用可能な応答（Available Responses）] を選択し、右矢印（>）をクリックして、それらを [グループ内の応答（Responses in Group）] に移動します。応答を他の方法で移動するには、左矢印（<）を使用します。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- 作成時にグループをアクティブにしなかった場合、アクティブにするには、スライダをクリックします。

相関応答グループの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

応答グループは、相関ポリシーで使用されていない場合は削除できます。応答グループを削除することで、その応答のグループ化を解除します。また、応答グループを削除せずに、一時的に非アクティブにすることもできます。これにより、グループはシステムに残りますが、ポリシーに違反するときにはグループが開始されなくなります。

マルチドメイン展開では、現在のドメインで作成されたグループが表示されます。これは編集できます。先祖ドメインで作成されたグループも表示されますが、これは編集できません。下位のドメインで作成されたグループを表示および編集するには、そのドメインに切り替えます。

アクティブな使用中の応答グループへの変更は、即座に反映されます。

手順

ステップ 1 [ポリシー（Policies）] > [相関（Correlation）] を選択して、[グループ（Group）] をクリックします。

ステップ 2 応答グループを管理します。

- アクティブ化または非アクティブ化：スライダをクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 作成：[グループの作成（Create Group）] をクリックします。相関応答グループの設定，（1676ページ）を参照してください。
- 編集：編集アイコン（  ）をクリックします。相関応答グループの設定，（1676ページ）を参照してください。代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- 削除：削除アイコン（）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

第 71 章

トラフィック プロファイル

ここでは、トラフィック プロファイルの設定方法について説明します。

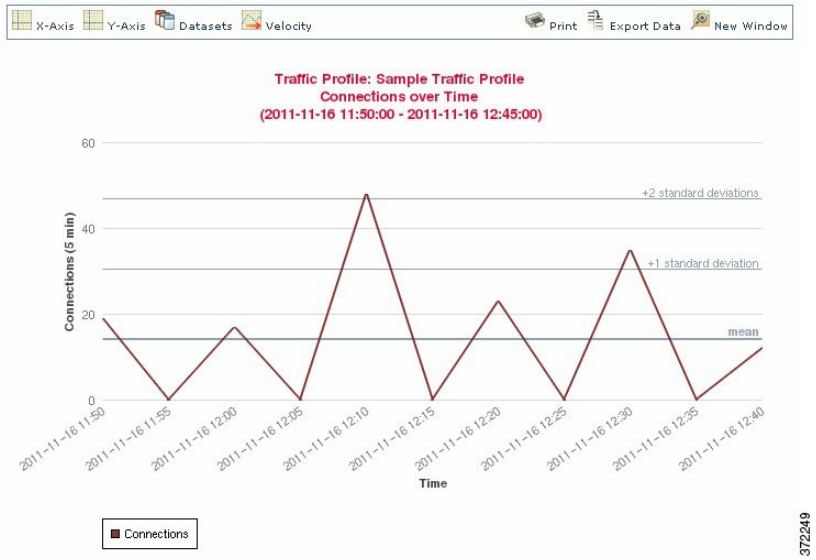
トラフィック プロファイルの概要

トラフィックプロファイルはプロファイル生成時間枠（PTW）内に収集した接続データを基に、ネットワーク トラフィックをグラフで表したものです。この測定結果が正常なネットワーク トラフィックを表しているものと推定します。学習期間が経過すると、新たなトラフィックをプロファイルに照らして評価することで異常なネットワーク トラフィックを検出します。

デフォルト PTW は 1 週間ですが、最短で 1 時間、最長で数週間に変更できます。デフォルトで、トラフィック プロファイルは 5 分間隔でシステム生成の接続イベントに関する統計情報を生成します。ただし、このサンプリング レートは最大 1 時間間隔まで拡大することができます。

ヒント シスコは少なくとも 100 のデータ ポイントを含む PTW の設定を推奨します。統計的に意味のある十分なデータがトラフィック プロファイルに含まれるように、PTW とサンプリング レートを設定する必要があります。

次の図は、PTW を 1 日、サンプリング レートを 5 分としたトラフィック プロファイルを示しています。



また、トラフィック プロファイルの非アクティブ期間を設定することもできます。トラフィック プロファイルは非アクティブ期間もデータ収集を行いますが、収集したデータをプロファイル統計の計算に使用しません。トラフィック プロファイルの時系列グラフでは、非アクティブ期間が網掛け領域として示されます。

たとえば、すべてのワークステーションが毎日深夜0:00にバックアップされるネットワーク インフラストラクチャがあるとします。バックアップには約 30 分かかり、その間はネットワーク トラフィックが急増します。予定されたバックアップ時間に合わせてトラフィック プロファイルの非アクティブ期間を繰り返すよう設定します。

（注） システムは接続の終了データを使って接続グラフとトラフィック プロファイルを作成します。トラフィック プロファイルを使用するには、必ず Firepower Management Center データベースに接続の終了イベントをロギングしてください。

トラフィック プロファイルの実装

トラフィック プロファイルを有効にすると、システムは設定した学習期間（PTW）の間接続データを収集し、評価します。システムは学習期間が経過すると、トラフィック プロファイルを対象にした相関ルールを評価します。

たとえば、ネットワークを通過するデータ量（パケット数、KB 数、または接続数で測定）が、平均トラフィック量に比べて標準偏差の 3 倍も急激に上昇した場合、攻撃または他のセキュリティ ポリシー違反を示す可能性があると判断してトリガーするルールを作成できます。その後、このルールを相関ポリシーに組み込んで、トラフィックの急増に関するアラートを出したり、応答として修復を実行したりできます。

トラフィック プロファイルの対象設定

トラフィックプロファイルは、プロファイル条件とホストプロファイル限定による制約を受けます。

プロファイル条件を使って、すべてのネットワーク トラフィックをプロファイリングすることもできます。また、トラフィック プロファイルの対象を絞って、特定のドメイン、特定のドメイン内や複数のドメイン内のサブネット、または個別のホストをモニタすることもできます。マルチドメイン展開では次のプロファイリングが可能です。

- リーフ ドメイン管理者は、リーフ ドメイン内のネットワーク トラフィックをプロファイリングできます。
- 高位レベル ドメインの管理者は、ドメイン内または複数ドメインでトラフィックのプロファイリングができます。

また、プロファイル条件では接続データに基づく基準を設けてトラフィック プロファイルを制約することもできます。たとえば、特定のポート、プロトコル、アプリケーションが使われているセッションのみトラフィック プロファイルでプロファイリングを行うようにプロファイル条件を設定できます。

また、トラッキング対象のホストに関する情報を使用してトラフィック プロファイルを制約することもできます。この制約は、ホスト プロファイル限定と呼ばれます。たとえば、重要度の高いホストに限定して接続データを収集できます。

（注） トラフィック プロファイルを高位レベルのドメインに制約すると、**各**子孫リーフ ドメインのトラフィックと**同じ**種類のトラフィックが集約され、プロファイリングされることになります。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、ドメイン間のトラフィックをプロファイルすると、予期しない結果になる可能性があります。

トラフィック プロファイル条件

単純なトラフィックプロファイル条件とホストプロファイル限定を作成できます。また、複数の条件の組み合わせとネストによってより複雑な構造を作成することもできます。

条件には、カテゴリ、演算子、および値という 3 つの部分があります。

- 使用できるカテゴリは、トラフィックプロファイル条件を作成しているか、それともホストプロファイル限定を作成しているかに応じて異なります。
- 使用できる演算子は、選択したカテゴリによって異なります。
- 条件の値を指定するために使用できる構文は、カテゴリと演算子に応じて異なります。場合によっては、テキストフィールドに値を入力する必要があります。それ以外の場合、ドロップダウンリストから 1 つ以上の値を選択できます。

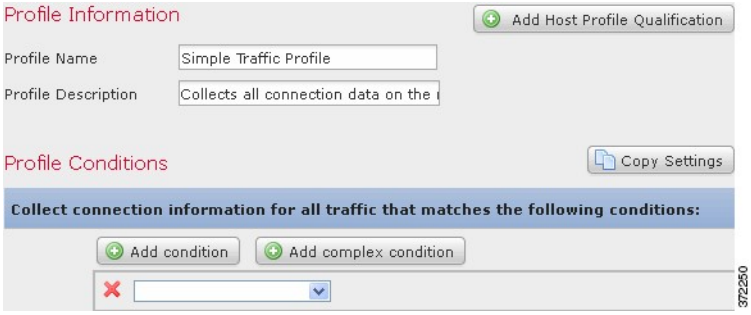
ホスト プロファイル限定の場合、開始側または応答側のホストに関する情報のデータを使用して、トラフィック プロファイルに制約を適用するかどうかを指定する必要もあります。

構造に複数の条件を含める場合は、それらの条件を[および（AND）]演算子または[または（OR）]演算子で結合する必要があります。同じレベルにある複数の条件は、次のように一緒に評価されます。

- AND 演算子は、制御対象のレベルにあるすべての条件が満たされなければならないことを示します。
- [または（OR）]演算子は、制御対象のレベルにある複数の条件の少なくとも 1 つが満たされている必要があることを示します。

制約が適用されていないトラフィック プロファイル

モニタ対象ネットワーク セグメント全体のデータを収集するトラフィック プロファイルを作成する場合、次の図に示すように、条件を含まない非常に単純なプロファイルを作成できます。



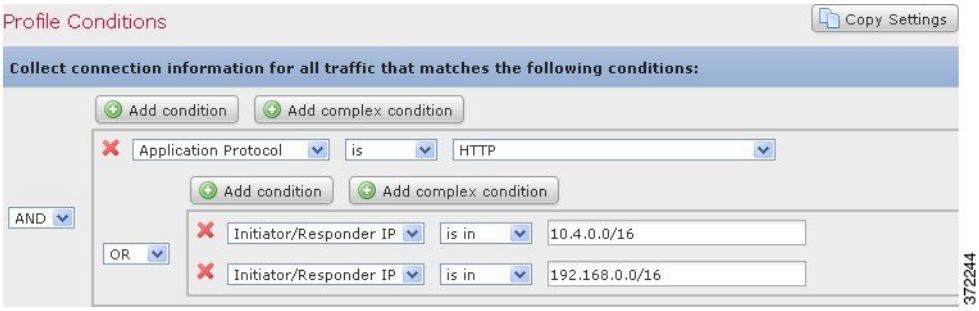
単純なトラフィック プロファイル

プロファイルに制約を適用して、1 つのサブネットのデータのみを収集するには、次の図に示すように 1 つの条件を追加できます。

複雑なトラフィック プロファイル

次のトラフィック プロファイルには、[および（AND）] で結合された 2 つの条件が含まれています。つまり、両方の条件とも満たされる場合に限り、このトラフィック プロファイルは接続データを収集します。この例では、特定のサブネット内の IP アドレスを持つすべてのホストに関する HTTP 接続を収集します。

一方、次のトラフィック プロファイルでは、2つのサブネットのいずれかのHTTPアクティビティに関する接続データを収集しますが、最後は複合条件を構成しています。



論理的には、上記のトラフィック プロファイルは次のように評価されます。

```
(A and (B or C))
```

条件	条件で指定する内容
A	アプリケーション プロトコル名が HTTP である
B	IP アドレスが 10.4.0.0/16 内にある
C	IP アドレスが 192.168.0.0/16 内にある

トラフィック プロファイルの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

アクティブで完全なトラフィック プロファイルに対して記述されたルールのみが、相関ポリシー違反をトリガーできます。各トラフィック プロファイルの横にあるスライダ アイコンは、プロファイルがアクティブでありデータを収集しているかどうかを示します。経過表示バーは、トラフィック プロファイルの学習期間のステータスを示します。

マルチドメイン展開では、現在のドメインで作成されたトラフィック プロファイルが表示されます。これは、編集が可能なプロファイルです。また、先祖ドメインからの選択したトラフィック プロファイルも表示されますが、これは編集できません。下位のドメインで作成されたトラフィック プロファイルを表示および編集するには、そのドメインに切り替えます。

（注） プロファイルの条件が無関係なドメインに関する情報（名前や管理対象デバイスなど）を公開する場合、システムは先祖ドメインからのトラフィック プロファイルを表示しません。

手順

ステップ 1 [ポリシー（Policies）] > [相関（Correlation）] を選択して、[トラフィック プロファイル（Traffic Profiles）] タブをクリックします。

ステップ 2 トラフィック プロファイルを管理します。

- アクティブ化/非アクティブ化：トラフィック プロファイルをアクティブ化または非アクティブ化するには、スライダをクリックします。トラフィック プロファイルを非アクティブ化すると、そのプロファイルに関連するデータが削除されます。プロファイルを再度アクティブ化する場合は、そのプロファイルに関して作成されたルールがトリガーするようになるまで、PTW の長さだけ待つ必要があります。
- 作成：新しいトラフィック プロファイルを作成するには、[新規プロファイル（New Profile）] をクリックして、トラフィック プロファイルの設定, （1685 ページ）で説明する手順を実行します。また、コピー アイコン（）をクリックして、既存のトラフィック プロファイルのコピーを編集することもできます。
- 削除：トラフィック プロファイルを削除するには、削除アイコン（）をクリックして、選択内容を確認します。
- 編集：既存のトラフィック プロファイルを変更するには、編集アイコン（）をクリックして、トラフィック プロファイルの設定, （1685 ページ）で説明する手順を実行します。トラフィック プロファイルがアクティブな場合は、そのプロファイルの名前と説明のみを変更できます。
- グラフ：グラフとしてトラフィック プロファイルを表示するには、グラフ アイコン（）をクリックします。マルチドメイン展開では、グラフが無関係なドメインに関する情報を公開する場合、先祖ドメインに属しているトラフィック プロファイルのグラフを表示できません。

トラフィック プロファイルの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

トラフィックプロファイルを高レベルのドメインに制約すると、**各**子孫リーフドメインの**同じ**タイプのトラフィックが集約およびプロファイルされます。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、ドメイン間のトラフィックをプロファイルすると、予期しない結果になる可能性があります。

手順

ステップ 1 [ポリシー（Policies）] > [相関（Correlation）] を選択し、[トラフィック プロファイル（Traffic Profiles）] タブをクリックします。

ステップ 2 [新規プロファイル（New Profile）] をクリックします。

ステップ 3 プロファイル名を入力し、オプションでプロファイルの説明を入力します。

ステップ 4 オプションで、トラフィック プロファイルを制約します。

- 設定のコピー：既存のトラフィックプロファイルから設定をコピーするには、[設定のコピー（Copy Settings）] をクリックし、使用するトラフィック プロファイルを選択して [ロード（Load）] をクリックします。
- プロファイル条件：トラッキング対象の接続の情報を使用してトラフィック プロファイルを制約するには、トラフィック プロファイル条件の追加, （1686ページ）の説明に従って続行します。
- ホスト プロファイル認定：トラッキング対象のホストの情報を使用してトラフィック プロファイルを制約するには、トラフィック プロファイルへのホスト プロファイル認定の追加, （1687 ページ）の説明に従って続行します。
- プロファイルの時間帯（PTW）：プロファイルの時間帯を変更するには、時間の単位を入力し、[時間（hour(s)）]、[日（day(s)）]、または [週（week(s)）] を選択します。
- サンプリング レート：サンプリング レートを分単位で選択します。
- 非アクティブ期間：[非アクティブ期間の追加（Add Inactive Period）] をクリックし、ドロップダウン リストを使用して、トラフィック プロファイルを非アクティブなままにする日時と頻度を指定します。非アクティブなトラフィック プロファイルは、相関ルールをトリガーしません。トラフィック プロファイルでは、プロファイルの統計情報に非アクティブな期間のデータを含めません。

ステップ 5 トラフィック プロファイルを保存します。

- プロファイルを保存し、ただちにデータを収集し始めるには、[保存してアクティブにする（Save & Activate）] をクリックします。
- アクティブ化せずにプロファイルを保存するには、[保存（Save）] をクリックします。

トラフィック プロファイル条件の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

手順

ステップ 1 トラフィック プロファイル エディタの [プロファイル条件（Profile Conditions）] で、追加する各条件について [条件の追加（Add condition）] または [複合条件の追加（Add complex condition）] をクリックします。同レベルの条件は一緒に評価されます。

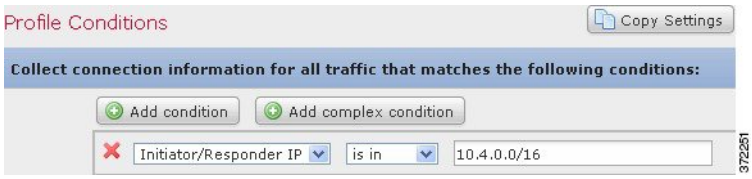
- 演算子で結ばれた同一のレベルのすべての条件が満たされるべきことを指定するには、[AND] を選択します。
- 演算子で結ばれた同一のレベルの 1 つの条件だけが満たされるべきことを指定するには、[OR] を選択します。

ステップ 2 トラフィック プロファイル条件の構文, （1688 ページ） と トラフィック プロファイル条件, （1681 ページ） の説明に従い、各条件のカテゴリ、演算子、値を指定します。
演算子として [含まれる（is in）] または [含まれない（is not in）] を選択した場合は、トラフィック プロファイル条件での複数の値の使用, （1692 ページ） に説明してあるように単一の条件で複数の値を選択できます。

カテゴリが IP アドレスを表している場合、演算子として [含まれる（is in）] または [含まれない（is not in）] を選択すると、IP アドレス範囲内にその IP アドレスが含まれるのか、含まれないのかを指定できます。

例

次のトラフィック プロファイルは、特定のサブネットの情報を集めます。条件のカテゴリは [イニシエータ/レスポンダ IP（Initiator/Responder IP）]、演算子は [含まれる（is in）]、値は `10.4.0.0/16` です。



トラフィック プロファイルへのホスト プロファイル認定の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

手順

ステップ 1 トラフィック プロファイル エディタで、[ホスト プロファイル認定の追加（Add Host Profile Qualification）] をクリックします。

ステップ 2 [ホスト プロファイル認定（Host Profile Qualification）] で、追加する各条件について [条件の追加（Add condition）] または [複合条件の追加（Add complex condition）] をクリックします。同レベルの条件は一緒に評価されます。

- 演算子で結ばれた同一のレベルのすべての条件が満たされるべきことを指定するには、[AND] を選択します。
- 演算子で結ばれた同一のレベルの 1 つの条件だけが満たされるべきことを指定するには、[OR] を選択します。

ステップ 3 トラフィック プロファイルのホスト プロファイル限定の構文, （1689 ページ） と トラフィック プロファイル条件, （1681 ページ） の説明に従い、各条件のホストタイプ、カテゴリ、演算子、値を指定します。
演算子として [含まれる（is in）] または [含まれない（is not in）] を選択した場合は、トラフィック プロファイル条件での複数の値の使用, （1692 ページ） に説明してあるように単一の条件で複数の値を選択できます。

例

次のホストプロファイル認定によりトラフィック プロファイルが制約され、検出された接続内の応答側ホストで任意のバージョンの Microsoft Windows が実行されている場合にのみ、接続データが収集されます。

トラフィック プロファイル条件の構文

次の表で、トラフィック プロファイル条件を作成する方法について説明します。トラフィック プロファイルの作成に使用可能な接続データは、トラフィックの特性と検出方法を含む複数の要因によって変わることに留意してください。

表 *214*：トラフィック プロファイル条件の構文

次を選択できます。	選択する演算子と内容
アプリケーション プロトコル	アプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコル カテゴリを 1 つ以上選択します。
クライアント	クライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアント カテゴリを 1 つ以上選択します。
接続タイプ	プロファイルが Firepower システムの管理対象デバイスによってモニタされるトラフィックからの接続データ、またはエクスポートされた NetFlow レコードからの接続データを使用するかどうかを選択します。 接続タイプを指定しない場合、トラフィック プロファイルには両方が含まれます。
接続先（国）または送信元（国）	国を 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。
イニシエータ IP、レスポンダ IP、またはイニシエータ/レスポンダ IP	IP アドレス、または IP アドレスの範囲を入力します。 システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

次を選択できます。	選択する演算子と内容
NetFlow デバイス	トラフィック プロファイルの作成に使用するデータの NetFlow エクスポータを選択します。
レスポンダ ポート/ICMP コード	ポート番号または ICMP コードを入力します。
セキュリティ インテリジェンス カテゴリ	セキュリティ インテリジェンスのカテゴリを 1 つ以上選択します。 トラフィック プロファイル条件にセキュリティ インテリジェンスのカテゴリを使用するには、アクセス コントロール ポリシーでそのカテゴリを [ブロック（Block）] ではなく [モニタ（Monitor）] に設定する必要があります。
SSL 暗号化セッション	[正常に復号（Successfully Decrypted）] を選択します。
トランスポート プロトコル	トランスポート プロトコルとして TCP または UDP と入力します。
Web アプリケーション	Web アプリケーションを 1 つ以上選択します。
[Web アプリケーションのカテゴリ（Web Application Category）]	Web アプリケーションのカテゴリを 1 つ以上選択します。

トラフィック プロファイルのホスト プロファイル限定の構文

ホストプロファイル限定の条件を作成するときには、まず、トラフィックプロファイルを制約するために使用するホストを選択する必要があります。[レスポンダホスト（Responder Host）] または [イニシエータ ホスト（Initiator Host）] のいずれかを選択できます。ホスト ロールを選択したら、ホスト プロファイル限定の条件の作成を続行します。

NetFlow レコードを使用してネットワーク マップにホストを追加できますが、これらのホストに関する利用可能な情報は限定されています。たとえば、これらのホストに利用可能なオペレーティングシステムデータは得られません（ただしホスト入力機能を使って指定する場合を除く）。さらに、エクスポートされた NetFlow レコードからの接続データをトラフィック プロファイルで使用する場合、NetFlow レコードには、どのホストが接続のイニシエータで、どのホストがレスポンダであるかを示す情報が含まれないことに注意してください。システムは、NetFlow レコードを処理するときに、それぞれのホストが使用しているポートとそれらのポートが既知かどうかに基づいて、この情報を判断するアルゴリズムを使用します。

暗黙的（または汎用の）クライアントを照合するには、クライアントに応答するサーバで使われるアプリケーションプロトコルに基づいてホストプロファイル限定を作成します。接続のイニシエータ（または送信元）として機能するホスト上のクライアント リストに含まれるアプリケーション プロトコル名の後にクライアントが続いている場合、そのクライアントは実際には暗黙的クライアントである可能性があります。つまり、検出されたクライアント トラフィックに基づい

てではなく、そのクライアントのアプリケーション プロトコルを使用するサーバ応答トラフィックに基づいて、システムがそのクライアントを報告します。

たとえば、ホスト上のクライアントとして HTTPS クライアントがシステムにより報告される場合、[アプリケーション プロトコル（Application Protocol）] を [HTTPS] に設定した [レスポンダ ホスト（Responder Host）] のホスト プロファイル限定を作成します。これは、レスポンダまたは宛先ホストから送られる HTTPS サーバ応答トラフィックに基づいて HTTPS クライアントが汎用クライアントとして報告されるためです。

表 *215*：ホスト プロファイル限定の構文

次を選択できます。	選択する演算子と内容
[アプリケーションプロトコル（Application Protocol）] >[アプリケーションプロトコル（Application Protocol）]	アプリケーション プロトコルを 1 つ以上選択します。
[アプリケーションプロトコル（Application Protocol）] >[アプリケーション ポート（Application Port）]	アプリケーション プロトコルのポート番号を入力します。
[アプリケーションプロトコル（Application Protocol）] > [プロトコル（Protocol）]	プロトコルを選択します。
[アプリケーションプロトコル カテゴリ（Application Protocol Category）]	アプリケーション プロトコル カテゴリを 1 つ以上選択します。
[クライアント（Client）] > [クライアント（Client）]	クライアントを 1 つ以上選択します。
[クライアント（Client）] > [クライアント バージョン（Client Version）]	クライアント バージョンを入力します。
[クライアント カテゴリ（Client Category）]	クライアント カテゴリを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。
[ハードウェア（Hardware）]	モバイルデバイスのハードウェア モデルを入力します。たとえば、すべての Apple iPhone に一致させるには `iPhone` と入力します。

次を選択できます。	選択する演算子と内容
[ホストの重要度（Host Criticality）]	ホストの重要度を選択します。
[ホスト タイプ（Host Type）]	ホスト タイプを 1 つ以上選択します。通常のホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
[IOC タグ（IOC Tag）]	IOC タグを 1 つ以上選択します。
[ジェイルブロークン（Jailbroken）]	イベントのホストがジェイルブレイクされたモバイル デバイスであることを示すには [はいい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
[MAC アドレス（MAC Address）] > [MAC アドレス（MAC Address）]	ホストの MAC アドレス全体またはその一部を入力します。
[MAC アドレス（MAC Address）] > [MAC タイプ（MAC Type）]	MAC タイプが [ARP/DHCP で検出（ARP/DHCP Detected）] されるかどうかを選択します。つまり、次のいずれかです。 • システムは MAC アドレスがホストに属していることをポジティブに識別した（[ARP/DHCP で検出（is ARP/DHCP Detected）]） • たとえば、デバイスとホスト間にはルータがあるため、システムはその MAC アドレスを持つ多くのホストを認識している（[ARP/DHCP で検出されない（is not ARP/DHCP Detected）]） • MAC タイプが無関係（[どれでもない（is any）]）
[MAC ベンダー（MAC Vendor）]	ホストが使用するハードウェアの MAC ベンダー全体またはその一部を入力します。
Mobile	イベントのホストがモバイル デバイスであることを示すには [はいい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
[NETBIOS 名（NETBIOS Name）]	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
[オペレーティング システム（Operating System）] > [OS ベンダー（OS Vendor）]	オペレーティング システムのベンダー名を 1 つ以上選択します。

次を選択できます。	選択する演算子と内容
[オペレーティング システム（Operating System）] > [OS 名（OS Name）]	オペレーティング システムの名前を 1 つ以上選択します。
[オペレーティング システム（Operating System）] > [OS バージョン（OS Version）]	オペレーティング システムのバージョンを 1 つ以上選択します。
[トランスポート プロトコル（Transport Protocol）]	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポート プロトコルの名前または番号を入力します。
VLAN ID（Admin. VLAN ID）	ホストの VLAN ID 番号を入力します。 システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の VLAN タグを使用してこの設定を抑制すると、予期しない結果になる可能性があります。
Web アプリケーション	Web アプリケーションを 1 つ以上選択します。
[Web アプリケーションのカテゴリ（Web Application Category）]	Web アプリケーションのカテゴリを 1 つ以上選択します。
使用可能な任意のホスト属性（デフォルト コンプライアンス ホワイトリスト ホスト属性を含む）	選択するホスト属性のタイプに応じて、適切な値を次のように指定します。 • ホスト属性タイプが Integer の場合、その属性で定義されている範囲内の整数値を入力します。 • ホスト属性タイプが Text の場合、テキスト値を入力します。 • ホスト属性タイプが List の場合、有効なリスト文字列を選択します。 • ホスト属性タイプが URL の場合、URL 値を入力します。

トラフィック プロファイル条件での複数の値の使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

条件を作成するときに、条件の構文でドロップダウン リストから値を選択できる場合、通常はリストから複数の値を選択できます。

たとえば、ホストで何らかの UNIX フレーバを実行している必要があることを示すホスト プロファイル限定をトラフィック プロファイルに追加するには、多数の条件を OR 演算子で結合する代わりに、以下の手順を使用できます。

手順

ステップ 1 トラフィック プロファイルまたはホスト プロファイルの資格条件を作成するときに、演算子として [存在する（is in）] または [存在しない（is not in）] を選択します。
ドロップダウン リストがテキスト フィールドに変わります。

ステップ 2 テキスト フィールド内の任意の場所または [編集（Edit）] リンクをクリックします。

ステップ 3 [使用可能（Available）] の下にある複数の値を選択します。

ステップ 4 右矢印をクリックして、選択した項目を [選択済み（Selected）] に移動します。

ステップ 5 [OK] をクリックします。

第 72 章

修復

以下のトピックでは、修復の設定について説明します。

修復の概要

修復は Firepower システムが相関ポリシー違反に応じて起動するプログラムです。

修復を実行すると、システムは修復ステータスイベントを生成します。修復ステータスイベントには、修復の名前、相関ポリシー、修復をトリガーしたルール、終了ステータス メッセージなどの詳細が含まれています。

システムは以下に挙げる複数の修復モジュールをサポートしています。

- Cisco IOS Null ルート：相関ポリシー違反に関連するホストやネットワークへ送信されるトラフィックをブロックします（Cisco IOS バージョン 12.0 以降が必要）。
- Nmap スキャン：ホストをスキャンして、実行中のオペレーティング システムおよびサーバを決定します。
- 属性値の設定：相関ポリシー違反に関連するホストのホスト属性を設定します。

ヒント 他のタスクを実行するカスタム モジュールをインストールすることもできます。*Firepower System Remediation API Guide*を参照してください。

修復の実装

修復を実装するには、まず選択したモジュールに対して少なくとも 1 つのインスタンスを作成します。モジュールごとに複数のインスタンスを作成することができ、各インスタンスは別々に設定できます。たとえば、Cisco IOS Null ルート修復モジュールを使用して複数のルータと通信するには、そのモジュールのインスタンスを複数設定します。

次に、ポリシー違反の際に実行するアクションを説明する複数の修復を各インスタンスに追加します。

最後に、相関ポリシーに応じてシステムが修復を開始するように相関ポリシーで修復とルールを関連付けます。

修復およびマルチテナンシー

マルチドメイン展開では、どのドメインのレベルでもカスタムの修復モジュールをインストールできます。システム提供のモジュールはグローバル ドメインに属します。

先祖ドメインで作成されたインスタンスに修復を追加することはできませんが、現在のドメインで同様に設定されるインスタンスを作成し、そのインスタンスに修復を追加することは可能です。また、先祖ドメインで作成した修復は、相関応答として使用することもできます。

Cisco IOS Null ルート修復

Cisco IOS Null ルート修復モジュールでは、シスコ「null route」コマンドを使って、個別の IP アドレスまたは IP アドレスの範囲をブロックすることができます。これにより、ホストまたはネットワークに送信されるすべてのトラフィックがルータの NULL インターフェイスにルーティングされ、ドロップされます。違反ホストまたはネットワークから送信されるトラフィックはブロックされません。

（注） ディスカバリまたはホスト入力イベントに基づく相関ルールへの応答として接続先ベースの修復を使用しないでください。これらのイベントは、送信元ホストに関連付けられます。

注意 Cisco IOS 修復がアクティブになる際、タイムアウト期間はありません。IP アドレスまたはネットワークのブロックを解除するには、ルータから手動でルーティング変更をクリアする必要があります。

Cisco IOS ルータ用修復の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	管理者ディスカバリ管理者

（注） 検出またはホスト入力イベントに基づく相関ルールへの応答として、宛先ベースの修復を使用しないでください。これらのイベントは、送信元ホストに関連付けられます。

注意 Cisco IOS 修復がアクティブになる際、タイムアウト期間はありません。IP アドレスまたはネットワークのブロックを解除するには、ルータから手動でルーティング変更をクリアする必要があります。

はじめる前に

- Cisco ルータが Cisco IOS 12.0 以降を実行していることを確認します。
- ルータへのレベル 15 の管理アクセス権を持っていることを確認します。

手順

ステップ 1 Cisco ルータまたは IOS ソフトウェアに付属のドキュメントの説明に従って、Cisco ルータで Telnet を有効にします。

ステップ 2 Firepower Management Center で、使用する予定の各 Cisco IOS ルータに対する Cisco IOS ヌル ルートインスタンスを追加します。Cisco IOS インスタンスの追加, （1698 ページ）を参照してください。

ステップ 3 相関ポリシーに違反した場合にルータで実現する応答のタイプに基づき、インスタンスごとに修復を作成します。

- Cisco IOS ブロック宛先の修復の追加, （1699 ページ）
- Cisco IOS ブロック宛先ネットワークの修復の追加, （1699 ページ）
- Cisco IOS ブロック送信元の修復の追加, （1701 ページ）
- Cisco IOS ブロック送信元ネットワークの修復の追加, （1701 ページ）

次の作業

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する, （1636 ページ） を参照）。

Cisco IOS インスタンスの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	管理者ディスカバリ管理者

修復を送信するルータが複数ある場合は、各ルータに対して別々のインスタンスを作成します。

はじめる前に

- ルータまたは IOS ソフトウェアのドキュメントの説明に従って、Cisco IOS ルータの Telnet アクセスを設定します。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]を選択します。

ステップ 2 [新しいインスタンスの追加（Add a New Instance）] リストから [Cisco IOS Null ルート（Cisco IOS Null Route）] を選択し、[追加（Add）] をクリックします。

ステップ 3 [インスタンス名（Instance Name）] と [説明（Description）] を入力します。

ステップ 4 [ルータ IP（Router IP）] フィールドに、修復のために使用する Cisco IOS ルータの IP アドレスを入力します。

ステップ 5 [ユーザ名（Username）] フィールドに、ルータの Telnet ユーザ名を入力します。このユーザは、ルータでレベル 15 管理アクセスを持っている必要があります。

ステップ 6 [接続パスワード（Connection Password）] フィールドに、Telnet ユーザのパスワードを入力します。

ステップ 7 [イネーブル パスワード（Enable Password）] フィールドに、Telnet ユーザのイネーブル パスワードを入力します。これは、ルータの特権モードに入るために使用するパスワードです。

ステップ 8 [ホワイトリスト（White List）] フィールドに、修復から除外する IP アドレスまたは範囲を 1 行につき 1 つ入力します。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 9 [作成（Create）] をクリックします。

次の作業

- Cisco IOS ブロック宛先の修復の追加, （1699 ページ）、Cisco IOS ブロック宛先ネットワークの修復の追加, （1699 ページ）、Cisco IOS ブロック送信元の修復の追加, （1701 ページ）、および Cisco IOS ブロック送信元ネットワークの修復の追加, （1701 ページ）の説明に従い、相関ポリシーで使用する特定の修復を追加します。

Cisco IOS ブロック宛先の修復の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	管理者ディスカバリ管理者

Cisco IOS ブロック宛先修復は、ルータから、相関ポリシー違反に関与している宛先ホストに送信されるトラフィックをブロックします。この修復を、検出またはホスト入力イベントに基づく相関ルールへの応答として使用しないでください。これらのイベントは、送信元ホストに関連付けられています。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

はじめる前に

- Cisco IOS インスタンスの追加, （1698 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（  ）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[宛先のブロック（Block Destination）] を選択し、[追加（Add）] をクリックします。
コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次の作業

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する, （1636 ページ） を参照）。

Cisco IOS ブロック宛先ネットワークの修復の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	管理者ディスカバリ管理者

Cisco IOS ブロック宛先ネットワーク修復は、ルータから、相関ポリシー違反に関与している宛先ホストのネットワークに送信されるトラフィックをブロックします。この修復を、検出またはホスト入力イベントに基づく相関ルールへの応答として使用しないでください。 これらのイベントは、送信元ホストに関連付けられています。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

はじめる前に

- Cisco IOS インスタンスの追加, （1698 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（  ）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[宛先ネットワークのブロック（Block Destination Network）] を選択し、[追加（Add）] をクリックします。
コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [ネットマスク（Netmask）] フィールドに、サブネットマスクを入力するか、または CIDR 表記を使用して、トラフィックをブロックするネットワークを記述します。
たとえば、1 つのホストがルールをトリガーとして使用したときにクラス C ネットワーク全体へのトラフィックをブロックするには、ネットマスクとして `255.255.255.0` または `24` を使用します。

別の例として、トリガーの IP アドレスを含む 30 個のアドレスへのトラフィックをブロックするには、ネットマスクとして `255.255.255.224` または `27` を指定します。この場合、IP アドレス `10.1.1.15` が修復をトリガーとして使用し、`10.1.1.1` と `10.1.1.30` の間のすべての IP アドレスがブロックされます。トリガーの IP アドレスのみをブロックするには、このフィールドは空のままにして、`32` を入力するか、または `255.255.255.255` を入力します。

ステップ 6 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次の作業

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する, （1636 ページ） を参照）。

Cisco IOS ブロック送信元の修復の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	管理者ディスカバリ管理者

Cisco IOS ブロック送信元修復は、ルータから、相関ポリシー違反に関与している送信元ホストに送信されるトラフィックをブロックします。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

はじめる前に

- Cisco IOS インスタンスの追加, （1698 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（  ）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[送信元のブロック（Block Source）] を選択し、[追加（Add）] をクリックします。
コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次の作業

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する, （1636 ページ） を参照）。

Cisco IOS ブロック送信元ネットワークの修復の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	管理者ディスカバリ管理者

Cisco IOS ブロック送信元ネットワーク修復は、ルータから、相関ポリシー違反に関与している送信元ホストのネットワークに送信されるトラフィックをブロックします。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

はじめる前に

- Cisco IOS インスタンスの追加, （1698 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（  ）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[送信元ネットワークのブロック（Block Source Network）] を選択し、[追加（Add）] をクリックします。
コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [ネットマスク（Netmask）] フィールドに、トラフィックをブロックするネットワークの説明となるサブネット マスクまたは CIDR 表記を入力します。
たとえば、1 つのホストがルールをトリガーとして使用したときにクラス C ネットワーク全体へのトラフィックをブロックするには、ネットマスクとして `255.255.255.0` または `24` を使用します。

別の例として、トリガーの IP アドレスを含む 30 個のアドレスへのトラフィックをブロックするには、ネットマスクとして `255.255.255.224` または `27` を指定します。この場合、IP アドレス `10.1.1.15` が修復をトリガーとして使用し、`10.1.1.1` と `10.1.1.30` の間のすべての IP アドレスがブロックされます。トリガーの IP アドレスのみをブロックするには、このフィールドは空のままにして、`32` を入力するか、または `255.255.255.255` を入力します。

ステップ 6 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次の作業

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する, （1636 ページ） を参照）。

Nmap スキャン修復

Firepower システムには、Nmap™ という、ネットワーク調査およびセキュリティ監査を目的としたオープン ソースのアクティブ スキャナが統合されています。Nmap 修復を使用して、相関ポリシー違反に対応できます。これは、Nmap スキャン修復をトリガーします。

Nmap スキャンの詳細については、Nmap スキャン, （1479 ページ）を参照してください。

セット属性値修復

トリガー イベントが発生したホストでホスト属性値を設定することにより、相関ポリシー違反に応答できます。テキストのホスト属性の場合、イベントの説明を属性値として使用できます。

セット属性修復の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	管理者 ディスカバリ 管理者

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]を選択します。

ステップ 2 セット属性値インスタンスの追加, （1703 ページ）の説明に従って、セット属性インスタンスを作成します。

ステップ 3 セット属性値修復の追加, （1704 ページ）の説明に従って、セット属性修復を追加します。

次の作業

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する, （1636 ページ） を参照）。

セット属性値インスタンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	管理者 ディスカバリ 管理者

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]を選択します。

ステップ 2 [新しいインスタンスの追加（Add a New Instance）] リストから [セット属性値（Set Attribute Value）] を選択し、[追加（Add）] をクリックします。

ステップ 3 [インスタンス名（Instance Name）] と [説明（Description）] を入力します。

ステップ 4 [作成（Create）] をクリックします。

次の作業

- セット属性値修復の追加, （1704 ページ） の説明に従って、セット属性修復を作成します。

セット属性値修復の追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	管理者ディスカバリ管理者

セット属性値修復は相関ポリシー違反に関与したホストにホスト属性を設定します。属性を設定する各属性の値について修復を作成します。テキスト属性の場合、トリガーイベントの説明を属性値として使用できます。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

はじめる前に

- セット属性値インスタンスの追加, （1703ページ） の説明に従って、セット属性インスタンスを作成します。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（🔍）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[セット属性値（Set Attribute Value）] を選択し、[追加（Add）] をクリックします。
コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 送信元データ、宛先データをもつイベントへの応答としてこの修復を使用するには、[イベントが決定するホストを更新（Update Which Host(s) From Event）] オプションを選択します。

ステップ 6 テキスト属性の場合、以下に従い [属性値にイベントからの説明を使用（Use Description From Event For Attribute Value）] を指定します。

- イベントの説明を属性値として使用するには、[オン（On）] をクリックし、設定する [属性値（Attribute Value）] を入力します。
- 修復の [属性値（Attribute Value）] 設定を属性値として使用するには、[オフ（Off）] をクリックします。

ステップ 7 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次の作業

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する，（1636 ページ） を参照）。

修復モジュールの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	管理者ディスカバリ管理者

マルチドメイン展開では、現在のドメインでインストールされた修復モジュールが表示されます。このモジュールは削除可能です。また、先祖ドメインでインストールされたモジュールも表示されますが、これは削除できません。下位ドメインの修復モジュールを管理するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [モジュール（Modules）]を選択します。

ステップ 2 修復モジュールを管理します。

- 設定：モジュールの [モジュール詳細（Module Detail）] ページを表示して、そのモジュールのインスタンスと修復を設定するには、表示アイコン（🔍）をクリックします。マルチドメイン展開では、[モジュール詳細（Module Detail）] ページを使用して、先祖ドメインでインストールされたモジュールに対応する現在のドメイン内のインスタンスを追加、削除、または編集することはできません。代わりに、[インスタンス（Instances）] ページ（[ポリシー

（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]）を使用します。修復インスタンスの管理, （1706 ページ）を参照してください。

- 削除：使用されていないカスタムモジュールを削除するには、削除アイコン（）をクリックします。システム付属のモジュールは削除できません。
- インストール：カスタム モジュールをインストールするには、[ファイルの選択（Choose File）] をクリックしてモジュールを参照し、[インストール（Install）] をクリックします。詳細については、*Firepower System Remediation API Guide*を参照してください。

修復インスタンスの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	管理者ディスカバリ管理者

[インスタンス（Instances）]ページには、すべての修復モジュールのすべての設定済みインスタンスがリスト表示されます。

マルチドメイン展開では、現在のドメインで作成された修復インスタンスが表示されます。このインスタンスは編集可能です。また、先祖ドメインで作成されたインスタンスも表示されますが、これは編集できません。下位ドメインの修復インスタンスを管理するには、そのドメインに切り替えます。

先祖ドメインで作成したインスタンスに修復を追加することはできませんが、同様の設定済みインスタンスを現在のドメインに作成して、そのインスタンスに修復を追加することはできます。また、先祖ドメインで作成した修復は、相関応答として使用することもできます。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]を選択します。

ステップ 2 修復インスタンスを管理します。

- 追加：インスタンスを追加するには、インスタンスを追加する修復モジュールを選択して、[追加（Add）] をクリックします。システム付属のモジュールについては、次を参照してください。
  - Cisco IOS インスタンスの追加, （1698 ページ）
  - Nmap スキャン インスタンスの追加, （1493 ページ）

- セット属性値インスタンスの追加, （1703 ページ）

カスタムモジュールを追加する際のヘルプは、そのモジュールのドキュメントを参照してください（使用可能な場合）。

- 設定：インスタンスの詳細を設定して、インスタンスに修復を追加するには、表示アイコン（  ）をクリックします。
- 削除：使用されていないインスタンスを削除するには、削除アイコン（  ）をクリックします。

1 つの修復モジュールのインスタンスの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	管理者ディスカバリ管理者

[モジュール詳細（Module Detail）] ページには、特定の修復モジュールに設定されたインスタンスと修復がすべて表示されます。

マルチドメイン展開では、現在のドメインと先祖ドメインにインストールされた修復モジュールの [モジュール詳細（Module Detail）] ページにアクセスできます。ただし、[モジュール詳細（Module Detail）] ページを使用して、先祖ドメインにインストールされているモジュールに対応する現在のドメイン内のインスタンスを追加、削除または編集することはできません。代わりに、[インスタンス（Instances）] ページ（[ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]）を使用します。修復インスタンスの管理, （1706 ページ）を参照してください。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [モジュール（Modules）] を選択します。

ステップ 2 管理するインスタンスを持つ修復モジュールの横にある表示アイコン（  ）をクリックします。

ステップ 3 修復インスタンスを管理します。

- 追加：インスタンスを追加するには、[追加（Add）] をクリックします。システム付属のモジュールについては、次を参照してください。
  - Cisco IOS インスタンスの追加, （1698 ページ）
  - Nmap スキャン インスタンスの追加, （1493 ページ）

◦ セット属性値インスタンスの追加, （1703 ページ）

カスタムモジュールのインスタンスを追加する際のヘルプは、そのモジュールのドキュメントを参照してください（提供されている場合）。

- 設定：インスタンスの詳細を設定して、インスタンスに修復を追加するには、表示アイコン（  ）をクリックします。
- 削除：使用されていないインスタンスを削除するには、削除アイコン（  ）をクリックします。

第 XVIII 部

レポートとアラート

第 73 章

レポートの操作

以下のトピックでは、Firepower システムでレポートを操作する方法について説明します。

レポートの概要

Firepower システムは柔軟なレポート作成システムを提供しており、Firepower Management Center で表示されるイベント ビューやダッシュボードを使用して、複数のセクションがあるレポートを短時間で簡単に生成できます。独自のカスタム レポートを最初から設計することもできます。

レポートは、通信しようとしている内容が含まれるドキュメント ファイルで、PDF、HTML、またはCSV形式になります。レポートテンプレートは、データの検索設定とレポートおよびそのセクションの形式を指定します。Firepowerシステムには強力なレポートデザイナが含まれていて、レポートテンプレートの設計を自動的に行います。Webインターフェイスに表示されるイベントビュー テーブルやダッシュボードのグラフィックの内容を複製できます。

レポート テンプレートは必要な数だけ作成できます。各レポート テンプレートは、レポートの個々のセクションを定義し、レポートの内容を作成するデータベース検索設定を指定し、表示形式（表、グラフ、詳細表示など）とタイム フレームも指定します。さらに、テンプレートでは、表紙や目次の情報、ドキュメント ページにヘッダーとフッターを付けるかどうかなどのドキュメント属性も指定します（PDF 形式のレポートでのみ指定可能）。レポート テンプレートを 1 つの設定パッケージ ファイルとしてエクスポートし、別の Firepower Management Center にインポートして再使用できます。

テンプレートに入力パラメータを組み込んで実用性を向上させることができます。入力パラメータを使用すると、同じレポートを用途に合わせて異なる様々なレポートに変えることができます。入力パラメータのあるレポートを生成するときには、生成プロセスで各入力パラメータの値を入力するよう求められます。ユーザが入力する値は、レポートの内容をその 1 回だけ決定するものです。たとえば、侵入イベントのレポートを作成する検索の宛先 IP フィールドに入力パラメータを使用できます。この場合、レポートの生成時に、宛先 IP アドレスの入力を求められたときに特定の部門のネットワーク セグメントを指定できます。その結果、この特定の部門に関する情報だけが含まれるレポートが生成されます。

レポート テンプレート

レポート テンプレートを使用して、レポートの各セクション内のデータの内容と形式や、レポート ファイルのドキュメント属性（表紙、目次、ページ ヘッダー、ページ フッター）を定義します。レポートの生成後、削除しない限りテンプレートは再利用可能な状態になります。

レポートには、1 つ以上の情報セクションが含まれます。個々のセクションごとに形式（テキスト、表、またはグラフ）を選択します。セクションの形式の選択内容によっては、組み込めるデータが制約される場合があります。たとえば、円グラフの形式を使用すると、特定の表に時間ベースの情報を表示できません。いつでもセクションのデータの基準や形式を変更して、表示を最適にすることができます。

定義済みイベント ビューのレポートの初期設計をベースにするか、定義済みのダッシュボード、ワークフロー、または要約から内容をインポートして設計を開始できます。空のテンプレート シェルから始めて、1 つずつセクションを追加したり属性を定義したりすることもできます。

（注） マルチドメイン導入では、先祖ドメインに属するレポート テンプレートを表示することはできますが、編集することはできません。これらのテンプレートからレポートを生成するには、テンプレートを現在のドメインにコピーする必要があります。

レポート テンプレート フィールド

表 *216*：レポート セクション タイトル バー エレメント

属性（Attribute）	定義（Definition）
セクション タイトル	レポート内に表示されるときには、セクション名を含みます。このシステムでは、レポート セクション ページに長いセクション タイトル名が表示されると、セクション タイトル名を切り捨てます。
セクション タイトル アイコン	（＋）セクションを複製します。（－）セクションを最小化します。（×）確認後セクションを削除します。

表 *217*：レポート セクション フィールド

フィールド名	定義（Definition）
テーブル	セクション データの抽出元のテーブルを選択できるドロップダウンメニューを表示します。
プリセット（Preset）	定義済み検索設定のドロップダウンメニューを表示します。新しい検索設定を定義する際に、該当する事前設定を選択して、検索条件を初期化できます。
フォーマット（Format）	セクション データ フォーマットを選択できるアイコンを表示します。次のオプションがあります。 棒グラフ：選択した変数の数量を比較します。 折れ線グラフ：選択した変数の時間の経過に伴う傾向/変化を示します。時間ベースのテーブルにのみ使用できます。 円グラフ：選択した各変数を全体の割合として示します。数量がゼロの変数はグラフからドロップされます。ごくわずかな数量は、ラベル [その他（Other）] カテゴリに集められます。 表形式の表示：レコードごとの属性の値を示します。要約や統計のデータには使用できません。 詳細表示：パケット（侵入イベントの場合）やホスト プロファイル（ホスト イベントの場合）など、特定のイベントに関連付けられた複合オブジェクトのデータを示します。フォーマットは、この種のオブジェクトが関係する特定のイベント タイプだけに使用できます。出力が多数要求されている場合には、パフォーマンスが低下することがあります。
検索またはフィルタ（Search or Filter）	検索フィルタまたはアプリケーション フィルタのドロップダウンメニューを表示します。 ほとんどのテーブルの場合、定義済みまたは保存済みの [検索（Search）] を使用してレポートを制約できます。編集アイコン（）をクリックして、新しい検索を作成することもできます。 アプリケーション統計表では、ユーザ定義のアプリケーションの [フィルタ（Filter）] を使用して、レポートを制約できます。
X 軸（X-Axis）	選択したグラフの X 軸の使用可能なデータ列のドロップダウンメニューを表示します。グラフチャートを選択する場合にのみ表示されます。折れ線グラフの場合、X 軸の値は常に [時刻（Time）] です。棒グラフと円グラフの場合、X 軸の値として [時刻（Time）] を選択できません。
Y 軸（Y-Axis）	選択したグラフの Y 軸の使用可能なデータ カラムのドロップダウンメニューを表示します。
セクションの説明（Section Description）	セクション内で検索データの前にある説明テキストを定義します。テキストと入力パラメータの組み合わせを入力します。新しいセクションのデフォルトは、`$<Time Window>` と `$<Constraints>` の 2 つの入力パラメータのセットです。

フィールド名	定義（Definition）
時間枠（Time Window）	セクションに表示されるデータの時間枠を定義します。セクションで時間ベースのテーブルを検索する場合、チェックボックスを選択して、レポートのグローバル時間枠を継承できます。または、セクションの特定の時間枠を設定することもできます。
結果（Results）	[トップ（Top）] または [ボトム（Bottom）] を選択して、セクションに含めるレコードの最大数を入力します。
カラー（Color）	セクション内でグラフ化されるデータの色を定義します。必要に応じて、1つ以上の色を選択します。

レポート テンプレートの作成

レポートテンプレートは、独自のデータベースクエリから個別に構築されたセクションのフレームワークです。

新しいレポート テンプレートを作成するには、新しいテンプレートを作成する、既存のテンプレートを使用する、イベント ビューをテンプレートのベースにする、ダッシュボードまたはワークフローをインポートするという方法があります。

既存のレポート テンプレートをコピーしない場合は、まったく新しいテンプレートを作成できます。テンプレート作成の最初の手順として、セクションを追加したり形式設定したりできるフレームワーク シェルを生成します。次に、ご希望の順序で、個々のテンプレート セクションを設計し、レポート ドキュメントの属性を設定します。

各テンプレート セクションは、検索設定やフィルタによって生成されたデータセットで構成され、表示モードを確定する形式の仕様（表や円グラフなど）があります。出力に含めるデータ レコードのフィールドを選択し、タイム フレームと表示するレコード数も選択して、さらにセクションの内容を確定します。

（注） セクション プレビュー ユーティリティを使用して、カラムの選択内容や、円グラフの色などの出力の特性を検査します。このインジケータは、設定済みの検索設定を必ずしも正確に反映するとは限りません。

テンプレートから生成したレポートには、表紙、ヘッダーとフッター、ページ番号など、すべてのセクションにまたがって機能を制御する複数のドキュメント属性があります。

CSV をドキュメントの形式として選択した場合は、ドキュメントの属性を設定できないことに注意してください。

既存のテンプレートの中に適切なモデルがあれば、そのテンプレートをコピーして属性を編集することで、新しいレポートテンプレートを作成できます。また、Ciscoから一連の定義済みレポート テンプレートも提供されています。これらのテンプレートは、[レポート（Reports）] タブのテンプレートの一覧で確認できます。

イベント ビューからレポート テンプレートを作成し、必要に応じて変更することができます。セクションを追加したり、自動的に組み込まれるセクションを変更したり、セクションを削除したりできます。

ダッシュボード、ワークフロー、統計の要約をインポートして、新しいレポートをすばやく作成できます。インポートすると、ダッシュボードのウィジェット グラフィックごと、およびワークフローのイベント ビューごとにセクションが作成されます。最も重要な情報に焦点が当たるように不要なセクションを削除できます。

カスタム レポート テンプレートの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 [概要（Overview）] > [レポート（Reporting）]を選択します。

ステップ 2 [レポート テンプレート（Report Templates）] タブをクリックします。

ステップ 3 [レポート テンプレートの作成（Create Report Template）] をクリックします。

ステップ 4 必要に応じて、[レポート タイトル（Report Title）] フィールドに新しいテンプレートの名前を入力し、[保存（Save）] をクリックします。

ステップ 5 レポート タイトルに入力パラメータを追加するには、タイトル内でパラメータ値を表示する位置にカーソルを置き、入力パラメータの挿入アイコン（  ）をクリックします。

ステップ 6 必要に応じて、[レポート セクション（Report Sections）] タイトル バーの下にある追加アイコンのセットを使用し、セクションを挿入します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 レポート テンプレートの設定, （1719 ページ）の説明に従ってセクション コンテンツを設定します。

ヒント セクションのウィンドウの下部にある [プレビュー（Preview）] をクリックして、選択したカラムのレイアウトやグラフィックの形式を表示できます。

ステップ 9 [詳細（Advanced）] をクリックし、レポート テンプレート内のドキュメント属性, （1731 ページ）の説明に従って PDF および HTML レポートの属性を設定します。

既存のテンプレートからのレポート テンプレートの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 [概要（Overview）] > [レポート（Reporting）]を選択します。

ステップ 2 [レポート テンプレート（Report Templates）] タブをクリックします。

ステップ 3 コピーするレポート テンプレートの横にあるコピー アイコン（  ）をクリックします。

ステップ 4 [レポート タイトル（Report Title）] フィールドに、名前を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 必要に応じてテンプレートを変更します。

イベント ビューからのレポート テンプレートの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 レポートに含めるイベントをイベント ビューに入力します。

- イベント検索設定を使用して、表示するイベントを定義します。
- イベント ビューに該当するイベントが表示されるまでワークフローをドリルダウンします。

ステップ 2 イベント ビューのページから、[レポート デザイナ（Report Designer）] をクリックします。[レポート セクション（Report Sections）]ページが表示され、キャプチャされるワークフロー内のビューごとにセクションが示されます。

ステップ 3 オプションで、[レポート タイトル（Report Title）] フィールドに新しい名前を入力し、[保存（Save）] をクリックします。

ステップ 4 次の操作を実行できます。

- 表紙、目次、開始ページ番号、またはヘッダーおよびフッター テキストを追加します：[詳細設定（Advanced Settings）] をクリックします。
- 改ページを追加します：改ページの追加アイコン（  ）をクリックし、新しい改ページオブジェクトを、テンプレートの下部から新しいページを開始するセクションの先頭にドラッグします。
- テキスト セクションを追加します：テキスト セクションの追加アイコン（  ）をクリックし、新しいテキスト セクションを、テンプレートの下部からレポート テンプレート内で表示する位置にドラッグします。
- セクションのタイトルを変更します：タイトル バーでセクション タイトルをクリックし、セクション タイトルを入力して、[OK] をクリックします。
- レポート セクションを設定します。各セクションのフィールド設定を調整します。

  ヒント セクションの現在のカラムのレイアウトやグラフの形式を表示する場合は、そのセクションの [プレビュー（Preview）] リンクをクリックします。
- レポートからテンプレート セクションを除外します：セクションのタイトル バーで削除アイコン（）をクリックし、削除を確認します。

  （注） 一部のワークフロー内の最後のレポートセクションには詳細ビューが含まれ、ワークフローに応じてパケット、ホスト プロファイル、または脆弱性が示されます。レポートの生成時に、これらの詳細ビューがあるイベントを多数取得すると、Firepower Management Center のパフォーマンスに影響を与えることがあります。

ステップ 5 [保存（Save）] をクリックします。

ダッシュボードまたはワークフローのインポートによるレポートテンプレートの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 レポート内で複製するダッシュボード、ワークフロー、または要約を識別します。

ステップ 2 [概要（Overview）] > [レポート（Reporting）]を選択します。

ステップ 3 [レポート テンプレート（Report Templates）] タブをクリックします。

ステップ 4 [レポート テンプレートの作成（Create Report Template）] をクリックします。

ステップ 5 [レポート タイトル（Report Title）] フィールドに新しいレポート テンプレートの名前を入力します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 インポート セクション アイコン（  ）をクリックします。[インポート レポート セクション（Import Report Sections）] のデータ ソース オプション, （1718 ページ）で説明されているデータ ソースのいずれかを選択できます。

ステップ 8 ドロップダウン メニューからダッシュボード、ワークフロー、または要約を選択します。

ステップ 9 追加するデータ ソースの、[インポート（Import）] をクリックします。
ダッシュボードの場合、ウィジェット グラフィックごとに独自のセクションがあります。ワークフローの場合、イベント ビューごとに独自のセクションがあります。

ステップ 10 必要に応じてセクションの内容を変更します。

（注） 一部のワークフロー内の最後のレポート セクションには詳細ビューが含まれ、ワークフローに応じてパケット、ホスト プロファイル、または脆弱性が示されます。レポートの生成時に、これらの詳細ビューがあるイベントを多数取得すると、Firepower Management Center のパフォーマンスに影響を与えることがあります。

ステップ 11 [保存（Save）] をクリックします。

[インポート レポート セクション（Import Report Sections）] のデータ ソース オプション

表 *218* : *[インポート レポート セクション（Import Report Sections）]* ウィンドウのデータ ソース オプション

選択オプション	インポート対象
ダッシュボードのインポート（Import Dashboard）	選択したダッシュボード上のカスタム分析ウィジェット。
ワークフローのインポート（Import Workflow）	定義済みのワークフローまたはカスタム ワークフロー。 選択項目の形式は次のようになっています。 `Table - Workflow name` たとえば、`Connection Events - Traffic by Port` は、Connection Events テーブルから生成された Traffic by Port ワークフロー内のビューをインポートします。

選択オプション	インポート対象
インポート要約セクション（Import Summary Sections）	次の一般的な要約： • 侵入の詳細サマリー（Intrusion Detailed Summary） • 侵入の概要サマリー（Intrusion Short Summary） • ディスカバリの詳細サマリー（Discovery Detailed Summary） • ディスカバリの概要サマリー（Discovery Short Summary）

レポート テンプレートの設定

レポート テンプレートを作成すれば、そのテンプレートを変更およびカスタマイズできます。さまざまなレポート セクションの属性を変更して、セクションとそのデータ表示の内容を調整できます。

レポートテンプレート内の各セクションでは、データベーステーブルを照会して、そのセクションの内容を生成します。セクションのデータ形式を変更する際にも同じデータ クエリーが使用されますが、形式のタイプごとの分析の目的に従って、セクションに表示されるフィールドが変わります。たとえば、侵入イベントの表形式の表示では、イベント レコードごとに多数のデータ フィールドがセクションに入力され、円グラフのセクションでは、選択した各属性が表すすべての一致レコードの割合が示され、個々のイベントに関する詳細情報は表示されません。棒グラフのセクションでは、特定の属性を持つ一致レコードの合計数が比較されます。折れ線グラフでは、1 つの属性に関係する一致レコード数の変化が時系列で要約されます。折れ線グラフは時間ベースのデータの場合のみ使用でき、ホスト、ユーザ、サードパーティの脆弱性などに関する情報の場合は使用できません。

レポートセクションの検索設定やフィルタは、セクションの内容のベースになるデータベース クエリーを指定します。ほとんどのテーブルの場合、定義済み検索設定か保存済み検索設定を使用してレポートを制約するか、新しい検索設定を即座に作成することができます。

- 定義済み検索設定は特定のイベント テーブルの検索サンプルの役割を果たし、レポートに含めようとしている、ネットワークに関する重要情報にクイック アクセスできます。
- 保存済みイベント検索設定には、自分や他のユーザが作成したすべてのパブリック イベント検索設定と、自分で保存したすべてのプライベート イベント検索設定が含まれます。
- 現在のレポート テンプレートの保存済み検索設定は、そのレポート テンプレート自体に限りアクセスできます。保存済みレポート テンプレートの検索設定の名前は、末尾が文字列「Custom Search」になります。ユーザは、レポートの設計時にこれらの検索設定を作成します。

[アプリケーションの統計（Application Statistics）] テーブルにユーザ定義のアプリケーション フィルタを使用して、レポートに制約を適用します。

セクション内にテーブルのデータを組み込む場合、データ レコード内のどのフィールドを表示するか選択できます。テーブル内のすべてのフィールドを包含対象または除外対象にできます。レポートの目的を達成するのに必要なフィールドを選択し、それに従って配列したりソートしたりします。

テンプレートにテキスト セクションを追加して、レポート全体や個々のセクションに概要などのカスタム テキストを用意することができます。

テンプレート内のどのセクションの前後にも改ページを追加できます。この機能は、複数のセクションから成るレポートで、各種セクションの概要を示すテキスト ページがある場合に特に便利です。

レポート テンプレートの時間枠によって、テンプレートのレポート作成期間が定義されます。

（注） セキュリティ アナリストは、自分が作成したレポート テンプレートだけを編集できます。マルチドメイン導入では、先祖ドメインのレポート テンプレートは編集できませんが、レポート テンプレートをコピーして子孫バージョンを作成することができます。

レポート テンプレート セクションのテーブルとデータ形式の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 [レポート テンプレート（Rreport Template）] セクションで、[テーブル（Table）] ドロップダウンメニューを使用して、問い合わせるテーブルを選択します。
選択したテーブルで使用できる出力形式ごとに、アイコンが [形式（Format）] フィールドに表示されます。

ステップ 2 セクションに該当する出力形式のアイコンを選択します。

ステップ 3 検索制約を変更するには、[検索（Search）] フィールドか [ファイルタ（Filter）] フィールドの横にある編集アイコン（）クリックします。

ステップ 4 グラフ出力形式（円グラフや棒グラフなど）の場合、ドロップダウンメニューを使用して、[X 軸（X-Axis）] と [Y 軸（Y-Axis）] のパラメータを調整します。
X 軸の値を選択すると、互換性のある値だけが Y 軸のドロップダウンメニューに表示されます。その逆も同様です。

ステップ 5 テーブル出力の場合、出力内のカラム、表示順序、ソート順序を選択します。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

レポート テンプレート フィールド, （1712 ページ）

レポート テンプレート セクションの検索またはフィルタの指定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 [レポート テンプレート（Rreport Template）] セクションで、[テーブル（Table）] ドロップダウン メニューからクエリを行うデータベース テーブルを選択します。

- ほとんどのテーブルでは、[検索（Search）] ドロップダウン リストが表示されます。
- [アプリケーション統計（Application Statistics）] テーブルでは、[フィルタ（Filter）] ドロップダウン リストが表示されます。

ステップ 2 レポートの制約に使用する検索かフィルタを選択します。

編集アイコン（  ）をクリックして、検索条件を表示したり、新しい検索を作成したりできます。

関連トピック

アプリケーション フィルタ, （393 ページ）

表形式のセクションに表示される検索フィールドの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 表形式のレポート セクションで、[フィールド（Fields）] パラメータの横にある編集アイコン（）をクリックします。

ステップ 2 セクションを変更する場合、フィールドを追加/削除し、望むカラムの順番にそれらのフィールドアイコンをドラッグします。

ステップ 3 どの列でもソート順序を変更する場合、各フィールドアイコンのドロップダウンリストを使用して、ソート順序および優先順位を設定する必要があります。

ステップ 4 [OK] をクリックします。

レポート テンプレートへのテキスト セクションの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

テキスト セクションには、複数のフォント サイズやフォント スタイル（太字や斜体など）を使用できるリッチ テキスト、入力パラメータ、インポート済みイメージを使用できます。

ヒント テキスト セクションは、レポートやそのセクションの概要説明に役立ちます。

手順

ステップ 1 レポートテンプレートエディタで、テキストセクション追加アイコン（  ）をクリックします。

ステップ 2 新しいテキスト セクションを、レポート テンプレート内のご希望の位置にドラッグします。

ステップ 3 テキストセクションをページの最初または最後に移動するには、テキストセクションの前または後に改ページを挿入します。

ステップ 4 テキスト セクションの総称名を変更するには、タイトルバーのセクション名をクリックし、新しい名前を入力します。

ステップ 5 テキスト セクションの本文に形式設定済みのテキストやイメージを追加します。
レポートの生成時に動的に更新する入力パラメータを組み込むことができます。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

入力パラメータ，（1727 ページ）

レポート テンプレートへの改ページの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 レポート テンプレート エディタで、改ページアイコン（  ）をクリックします。
改ページがテンプレートの下部に表示されます。

ステップ 2 改ページを、セクションの前後のご希望の場所にドラッグします。

ステップ 3 [保存（Save）] をクリックします。

グローバル時間枠とレポート テンプレート セクション

時間ベースのデータ（侵入イベントや検出イベントなど）があるレポート テンプレートにはグローバル時間枠があります。この時間枠は、テンプレート内の時間ベースのセクションでデフォルトで作成時に継承されます。グローバル時間枠を変更すると、グローバル時間枠を継承するように設定されているセクションのローカル時間枠が変更されます。[時間枠の継承（Inherit Time Window）] チェックボックスをクリアすると、個々のセクションの時間枠の継承を無効にできます。それから、ローカル時間枠を編集できます。

（注） グローバル時間枠の継承は、侵入イベントや検出イベントなど、時間ベースのテーブルからのデータがあるレポート セクションだけに適用されます。ネットワーク アセット（ホストやデバイス）と関連情報（脆弱性など）を報告するセクションの場合、各時間枠を個別に設定する必要があります。

レポート テンプレートとそのセクションのグローバル時間枠の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

ヒント　レポート内のセクションごとに別の時間枠を使用できます。たとえば、最初のセクションを月の要約にして、残りのセクションで週レベルの詳細情報へドリルダウンするようにできます。この場合、セクション レベルの時間枠を個別に設定します。

手順

ステップ 1　レポート テンプレート エディタで [生成（Generate）] をクリックします。

ステップ 2　グローバル時間枠を変更するには、時間枠のアイコン（）をクリックします。

ステップ 3　[イベント時間枠（Events Time Window）] タブで時間設定を変更します。

ステップ 4　[適用（Apply）] をクリックします。

ステップ 5　[生成（Generate）] をクリックしてレポートを生成し、[はい（Yes）] をクリックして確認します。

レポート テンプレート セクションのローカル時間枠の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1　テンプレートの [レポート セクション（Report Sections）] ページで、セクションの [時間枠の継承（Inherit Time Window）] チェック ボックスが存在する場合はクリアします。

ステップ 2　セクションのローカル時間枠を変更するには、時間枠のアイコン（）をクリックします。

（注）　統計テーブルからのデータがあるセクションでは、スライド式の時間枠のみ使用できます。

ステップ 3 [イベント時間枠（Events Time Window）] で [適用（Apply）] をクリックします。

ステップ 4 [保存（Save）] をクリックします。

レポート テンプレート セクションの名前変更

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 レポート テンプレート エディタで、セクション ヘッダーの現在のセクション名をクリックします。

ステップ 2 新しいセクション名を入力します。

ステップ 3 [OK] をクリックします。

レポート テンプレート セクションのプレビュー

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

プレビュー機能は、表形式の表示のフィールドのレイアウトとソート順序や、円グラフの色などのグラフの読みやすさに関する重要な特性を表示します。

手順

ステップ 1 レポート テンプレート セクションの編集中は、いつでも、そのセクションの [プレビュー（Preview）] をクリックできます。

ステップ 2 プレビューを閉じるには、[OK] をクリックします。

レポート テンプレート セクションでの検索

レポートが正常に作成されるかどうかは、レポートのセクションへの入力内容を決める検索設定の定義が重要な要素になります。Firepowerシステムには検索エディタが備わっており、レポートテンプレートで使用できる検索設定を表示したり、新しいカスタム検索設定を定義したりできます。

レポート テンプレートのセクションの検索

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 レポート テンプレート内の関連するセクションから、[検索（Search）] フィールドの横にある編集アイコン（）をクリックします。

ステップ 2 事前定義済みの検索に基づいてカスタム検索を作成する場合は、[保存済み検索（Saved Searches）] ドロップダウンリストから事前定義された検索を選択する必要があります。
このリストには、このテーブルに対して使用可能な事前定義済みの検索設定がすべて表示されます。システム規模の事前定義済み検索設定とレポート固有の事前定義済み検索設定も含まれています。

ステップ 3 該当するフィールドで検索条件を編集します。
特定のフィールドでは、制約にイベント検索設定と同じ演算子（< や <> など）を含めることができます。複数の条件を入力すると、すべての基準を満たすレコードだけが検索で返されます。

ステップ 4 制約値を入力する代わりに、ドロップダウン メニューから入力パラメータを挿入する場合は、入力パラメータ アイコン（  ）をクリックする必要があります。

（注） レポートの検索設定の制約を編集すると、システムにより *section* `custom search` という名前で編集済みの検索設定が保存されます。*section* は、セクションのタイトル バーに示される文字列 `custom search` の前の名前の部分です。保存するカスタム検索設定の名前をわかりやすくするには、セクション名を変更した後で編集済みの検索設定を保存するようにしてください。保存したレポートの検索設定の名前は変更できません。

ステップ 5 [OK] をクリックします。

入力パラメータ

レポートの生成時に動的に更新できる入力パラメータをレポート テンプレート内で使用できます。入力パラメータのアイコン（  ）は、入力パラメータを処理できるフィールドを示します。次の 2 種類の入力パラメータがあります。

- 定義済みの入力パラメータは、内部システム関数か設定情報によって解決されます。たとえば、レポートの生成時に、システムにより `$<Time>` パラメータは現在の日時に置き換えられます。
- ユーザ定義の入力パラメータは、セクション検索で制約を行えます。入力パラメータを使用して検索設定を制約すると、レポートの生成時に要求者から値を収集するようにシステムに指示できます。この方法で、テンプレートを変更せずに、レポートを生成時に動的に調整して特定のデータのサブセットを表示できます。たとえば、レポートセクションの検索設定の [接続先 IP（Destination IP）] フィールドに入力パラメータを指定できます。指定後、レポートの生成時に、特定の部門の IP ネットワークのセグメントを入力して、その部門のデータだけを取得できます。

  文字列タイプの入力パラメータを定義して、電子メール（件名または本文）、レポート ファイル名、テキスト セクションなどのレポートの特定のフィールドに動的テキストを追加することもできます。すべて同じテンプレートを利用し、カスタマイズしたレポート ファイル名、電子メール アドレス、電子メール メッセージを使用して、さまざまな部門用にレポートをパーソナライズできます。

定義済み入力パラメータ

表 *219*：定義済み入力パラメータ

このパラメータを入力すると、	テンプレートに次の情報が含まれます：
`$<Logo>`	選択した更新ロゴ
`$<Report Title>`	レポート タイトル
`$<Time>`	レポートを実行する日付、時刻、粒度 1 秒
`$<Month>`	現在の月
`$<Year>`	現在の西暦
`$<System Name>`	Firepower Management Center 名
`$<Model Number>`	Firepower Management Center のモデル番号
`$<Time Window>`	レポート セクションに現在適用されている時間窓

このパラメータを入力すると、	テンプレートに次の情報が含まれます：
`$<Constraints>`	レポート セクションに現在適用されている検索制約

表 *220*：定義済み入力パラメータの使用法

パラメータ	レポート テンプレート カバー ページ	レポート テンプレート レポート タイトル	レポート テンプレート セクションの説明	レポート テンプレート本文セクション	レポート ファイル名の作成	レポート電子メールの主題、本文の作成
`$<Logo>`	Yes	No	No	No	No	No
`$<Report Title>`	Yes	No	Yes	Yes	Yes	Yes
`$<Time>`	Yes	Yes	Yes	Yes	Yes	Yes
`$<Month>`	Yes	Yes	Yes	Yes	Yes	Yes
`$<Year>`	Yes	Yes	Yes	Yes	Yes	Yes
`$<System Name>`	Yes	Yes	Yes	Yes	Yes	Yes
`$<Model Number>`	Yes	Yes	Yes	Yes	Yes	Yes
`$<Time Window>`	No	No	Yes	No	No	No
`$<Constraints>`	No	No	Yes	No	No	No

ユーザ定義の入力パラメータ

入力パラメータを使用して、検索設定の実用性を向上させます。入力パラメータにより、レポートの生成時に要求者から値を収集するようにシステムに指示できます。この方法で、検索設定を変更せずに、レポートを生成時に動的に制約して特定のデータのサブセットを表示できます。たとえば、レポート セクションの [宛先 IP（Destination IP）] フィールドに入力パラメータを指定して、部門レベルでセキュリティ イベントをドリルダウンできます。レポートの生成時に、特定の部門の IP ネットワークのセグメントを入力して、その部門のデータだけを取得できます。

入力パラメータのタイプにより、そのパラメータを使用できる検索フィールドが決まります。特定のタイプは、該当するフィールドでのみ使用できます。たとえば、ユーザ パラメータを文字列タイプとして定義すると、テキスト フィールド内への挿入には使用できますが、IP アドレスを使用するフィールドでは使用できません。

定義する入力パラメータごとに名前とタイプがあります。

表 *221*：ユーザ定義の入力パラメータのタイプ

パラメータのタイプ	使用先のフィールド内のデータ
ネットワーク/IP（Network/IP）	CIDR 形式の IP アドレスまたはネットワーク セグメント
Application	アプリケーション プロトコル、クライアント アプリケーション、または Web アプリケーションの名前
イベント メッセージ（Event Message）	イベント ビュー メッセージ
Device	Management Center または管理対象デバイス
[ユーザ名（Username）]	イニシエータ ユーザやレスポンダ ユーザなどのユーザ ID
番号（VLAN ID、Snort ID、Vuln ID）（Number (VLAN ID, Snort ID, Vuln ID)）	VLAN ID、Snort ID、または脆弱性 ID
文字列	アプリケーションや OS のバージョン、注記、説明などのテキスト フィールド

ユーザ定義の入力パラメータの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 入力パラメータ追加アイコン（  ）をクリックします。

ステップ 3 パラメータの [名前（Name）] を入力します。

ステップ 4 [タイプ（Type）] ドロップダウン リストから値を選択します。

ステップ 5 [OK] をクリックしてパラメータを追加します。

ステップ 6 [OK] をクリックしてエディタに戻ります。

ユーザ定義の入力パラメータの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

レポート テンプレートの [入力パラメータ（Input Parameters）] セクションに、テンプレートに使用可能なユーザ定義パラメータがすべてリストされます。

手順

ステップ 1 レポート テンプレート エディタで、[詳細設定（Advanced）] をクリックします。

ステップ 2 変更するパラメータの横にある編集アイコン（  ）をクリックします。

ステップ 3 [名前（Name）] に新しい名前を入力します。

ステップ 4 [タイプ（Type）] ドロップダウン リストを使用して、パラメータ タイプを変更します。

ステップ 5 [OK] をクリックして変更を保存します。

ステップ 6 入力パラメータを削除するには、入力パラメータの横にある削除アイコン（  ）をクリックし、確認します。

ステップ 7 [OK] をクリックしてレポート テンプレート エディタに戻ります。

ユーザ定義の入力パラメータによる検索の制約

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

定義した入力パラメータは、そのパラメータのタイプと一致する検索フィールドでのみ使用できます。たとえば、ネットワーク/IP タイプのパラメータは、CIDR 形式の IP アドレスまたはネットワーク セグメントを受け入れるフィールドだけで使用できます。

手順

ステップ 1 レポート テンプレート エディタで、セクション内の [検索（Search）] フィールドの横にある編集アイコン（  ）をクリックします。

入力パラメータを使用できるフィールドは、入力パラメータのアイコン（  ）のマークが付けられます。

ステップ 2 フィールドの横にある入力パラメータのアイコン（）をクリックして、ドロップダウンメニューから入力パラメータを選択します。
ユーザ定義の入力パラメータは、アイコン（  ）のマークが付けられます。

ステップ 3 [OK] をクリックします。

レポート テンプレート内のドキュメント属性

レポートを生成する前に、レポートの外観に影響を与えるドキュメント属性を設定できます。これらの属性には、オプションの表紙と目次が含まれます。一部の属性のサポートは、レポートの形式に PDF、HTML、CSV のいずれを選択したかによって異なります。

表 *222*：ドキュメント属性のサポート

属性（Attribute）	PDF のサポート	HTML のサポート	CSV のサポート
表紙	可能、オプションでロゴと外観のカスタマイズ	可能、オプションでロゴと外観のカスタマイズ	No
目次	Yes	Yes	No
ページのヘッダーとフッター	可能、オプションでフィールド内にテキストかロゴ	No	No
カスタムの開始ページ番号	Yes	No	No
先頭ページに番号を付けないオプション	Yes	No	No

レポート テンプレート内のドキュメント属性の編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 次の選択肢があります。

- 表紙の追加：表紙を追加するには、[表紙を含める（Include Cover Page）] チェックボックスをオンにします。
- 表示のカスタマイズ：表紙のデザインを編集するには、表紙のカスタマイズ, （1732 ページ）を参照してください。
- 目次の追加：目次を追加するには、[目次を含める（Include Table of Contents）] チェックボックスをオンにします。
- ロゴの管理：テンプレートに関連付けられたロゴ イメージを管理するには、レポート テンプレートのロゴの管理, （1733 ページ）を参照してください。
- ヘッダーとフッターの設定：テンプレートのヘッダーとフッターの要素を指定するには、[ヘッダー（Header）] フィールドと [フッター（Footer）] フィールのドロップダウン リストを使用します。
- 最初のページ番号の設定：レポートの最初のページ番号を指定するには、[ページ番号の開始（Page Number Start）] の値を入力します。
- 最初のページ番号の表示：レポートの最初のページのページ番号を表示するには、[最初のページに番号を付けますか（Number First Page?）] チェックボックスをオンにします。このオプションを選択すると、表紙には番号が付けられません。

ステップ 3 [OK] をクリックして変更を保存します。

表紙のカスタマイズ

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

レポートテンプレートの表紙をカスタマイズできます。表紙には、複数のフォントサイズやフォントスタイル（太字や斜体など）を使用できるリッチテキスト、入力パラメータ、インポート済みイメージを使用できます。

手順

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 [表紙のデザイン（Cover Page Design）] の横にある編集アイコン（  ）をクリックします。

ステップ 3 リッチ テキスト エディタで表紙のデザインを編集します。

ステップ 4 [OK] をクリックします。

レポート テンプレートのロゴの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

Firepower Management Center で複数のロゴを保存し、さまざまなレポート テンプレートに関連付けることができます。ロゴの関連付けは、テンプレートを設計する際に設定します。テンプレートをエクスポートすると、エクスポート パッケージにロゴが含まれます。

Firepower Management Center にロゴをアップロードすると、そのロゴは次のものに使用できます。

- Firepower Management Center のすべてのレポート テンプレート、または
- マルチドメイン展開では、現在のドメイン内のすべてのレポート テンプレート

ロゴ画像は、PNG 形式、JPG 形式、または GIF 形式することができます。

レポート内のロゴは、Firepower Management Center にアップロードされているいずれかの JPG 画像に変更できます。たとえば、テンプレートを再使用する場合は、別の組織のロゴをレポートに関連付けることができます。

アップロードしたロゴは、削除できます。ロゴを削除すると、そのロゴが使用されているすべてのテンプレートから削除されます。削除を取り消すことはできません。事前定義済のシスコ ロゴは削除できない点に注意してください。

手順

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。
テンプレートに現在関連付けられているロゴは、[一般設定（General Settings）] の [ロゴ（Logo）] の下に表示されます。

ステップ 2 ロゴの横にある編集アイコン（  ）をクリックします。

ステップ 3 次の選択肢があります。

- 追加：新しいロゴを追加します。詳細については、新しいロゴの追加, （1734 ページ）を参照してください。
- 変更：レポート テンプレートのロゴを変更します。詳細については、レポート テンプレートのロゴの変更, （1734 ページ）を参照してください。
- 削除：ロゴを削除します。詳細については、ロゴの削除, （1735 ページ）を参照してください。

新しいロゴの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 [ロゴ（Logo）] フィールドの横にある編集アイコン（  ）をクリックします。

ステップ 3 [ロゴのアップロード（Upload Logo）] をクリックします。

ステップ 4 [参照（Browse）] ボタンをクリックし、ファイルの場所を参照し、[開く（Open）] をクリックします。

ステップ 5 [アップロード（Upload）] をクリックします。

ステップ 6 新しいロゴを現在のテンプレートに関連付けるには、それを選択し、[OK] をクリックします。

レポート テンプレートのロゴの変更

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 [ロゴ（Logo）] フィールドの横にある編集アイコン（  ）をクリックします。

ステップ 3 [ロゴの選択（Select Logo）] ダイアログで、レポート テンプレートに関連付けるロゴを選択します。

ステップ 4 [OK] をクリックします。

ロゴの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 [ロゴ（Logo）] フィールドの横にある編集アイコン（）をクリックします。

ステップ 3 [ロゴの選択（Select Logo）] ダイアログで、削除するロゴを選択します。

ステップ 4 [ロゴの削除（Delete Logo）] をクリックします。

ステップ 5 [OK] をクリックします。

レポート テンプレートの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

マルチドメイン展開では、現在のドメインで作成されたレポート テンプレートが表示されます。このテンプレートは編集可能です。先祖ドメインで作成されたレポート テンプレートも表示されますが、これは編集できません。下位のドメインのレポート テンプレートを表示および編集する

には、そのドメインに切り替えます。システムによって表示されるレポートは、現在のドメインで作成されたもののみです。

手順

ステップ 1 [概要（Overview）] > [レポート（Reporting）]を選択します。

ステップ 2 [レポート テンプレート（Report Templates）] タブをクリックします。

ステップ 3 次の選択肢があります。

- 削除：削除するテンプレートの横にある削除アイコン（）をクリックして確認します。システム付属のレポート テンプレートは削除できません。セキュリティ アナリストは、自分が作成したレポートテンプレートのみを削除できます。マルチドメイン展開では、現在のドメインに属しているレポート テンプレートのみを削除できます。
- 編集：レポートテンプレートを編集する場合は、レポートテンプレートの編集，（1736 ページ）を参照してください。
- エクスポート：レポート テンプレートをエクスポートする場合は、レポート テンプレートのエクスポート，（1738 ページ）を参照してください。

  ヒント また、標準設定のエクスポート プロセスを使用してレポート テンプレートをエクスポートすることもできます。設定のエクスポート，（189 ページ）を参照してください。
- インポート：レポートテンプレートをインポートする場合は、設定のインポート，（190 ページ）を参照してください。

レポート テンプレートの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成されたレポート テンプレートが表示されます。このテンプレートは編集可能です。先祖ドメインで作成されたレポート テンプレートも表示されますが、これは編集できません。下位のドメインのレポート テンプレートを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [概要（Overview）] > [レポート（Reporting）]を選択します。

ステップ 2 [レポート テンプレート（Report Templates）] タブをクリックします。

ステップ 3 編集するテンプレートの編集アイコン（  ）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 次の選択肢があります。

- 改ページを追加します。レポート テンプレートへの改ページの追加, （1723 ページ）を参照してください。
- テキスト セクションを追加します。レポート テンプレートへのテキスト セクションの追加, （1722 ページ）を参照してください。
- レポート テンプレートの設定, （1719 ページ）の説明に従ってセクション コンテンツを設定します。
- 入力パラメータを作成します。ユーザ定義の入力パラメータの作成, （1729 ページ）を参照してください。
- 入力パラメータを編集します。ユーザ定義の入力パラメータの編集, （1730 ページ）参照してください。
- ドキュメントの属性を編集します。レポート テンプレート内のドキュメント属性の編集, （1731 ページ）を参照してください。
- テンプレート セクションを検索します。レポート テンプレートのセクションの検索, （1726 ページ）を参照してください。
- [詳細設定（Advanced）] をクリックし、レポート テンプレート内のドキュメント属性, （1731 ページ）の説明に従ってドキュメント属性を設定します。
- グローバル時間枠を設定します。レポート テンプレートとそのセクションのグローバル時間枠の設定, （1724 ページ）を参照してください。
- ローカル時間枠を設定します。レポート テンプレート セクションのローカル時間枠の設定, （1724 ページ）を参照してください。
- 検索フィールドを設定します。表形式のセクションに表示される検索フィールドの設定, （1721 ページ）参照してください。
- 表とデータ形式を設定します。レポート テンプレート セクションのテーブルとデータ形式の設定, （1720 ページ）を参照してください。
- 検索とフィルタを指定します。レポート テンプレート セクションの検索またはフィルタの指定, （1721 ページ）を参照してください。

レポート テンプレートのエクスポート

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

手順

ステップ 1 [概要（Overview）] > [レポート（Reporting）]を選択します。

ステップ 2 [レポート テンプレート（Report Templates）] タブを選択します。

ステップ 3 エクスポートするテンプレートのエクスポート アイコン（  ）をクリックします。

ステップ 4 [ファイルの保存（Save file）] と [OK] をクリックして、ローカル コンピュータにファイルを保存します。

テンプレートを使用したレポートの生成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

レポート テンプレートを作成してカスタマイズすると、レポート生成の準備が完了します。生成プロセスでは、レポートの形式（HTML、PDF、またはCSV）を選択できます。レポートのグローバル時間枠を調整することもできます。この時間枠は、免除していないすべてのセクションに一貫した時間枠を適用します。

Unicode（UTF-8）文字を使用したファイル名はPDF レポートではサポートされません。PDF 形式のレポートを生成すると、特殊な Unicode ファイル名が含まれるレポート セクション（ファイル イベントやマルウェア イベントで表示されるセクションなど）では、そのファイル名は書き直された形式で表示されます。

レポート テンプレートの検索の指定にユーザ入力パラメータが含まれている場合、生成プロセスで値を入力するよう求められ、このレポートの実行内容がデータのサブセットに合わせて調整されます。

DNSサーバの設定およびIPアドレス解決が有効化されている場合、正常に解決されたホスト名がレポートに取り込まれます。

マルチドメイン展開では、先祖ドメインでレポートを生成すると、そのレポートにはすべての子孫ドメインからの結果を含めることができます。特定のリーフ ドメインのレポートを生成するには、そのドメインに切り替えます。

手順

ステップ 1 [概要（Overview）] > [レポート（Reporting）]を選択します。

ステップ 2 [レポート テンプレート（Report Templates）] タブをクリックします。

ステップ 3 レポートの生成に使用するテンプレートの横にあるレポートアイコン（  ）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ヒント 先祖のテンプレートからレポートを生成するには、そのテンプレートを現在のドメインにコピーします。

ステップ 4 必要に応じて、レポート名を設定します。

- 新しい[ファイル名（File Name）]を入力します。新しい名前を入力しないと、システムはレポート テンプレートで指定した名前を使用します。
- 入力パラメータのアイコン（  ）を使用して、1 つ以上の入力パラメータをファイル名に追加します。

ステップ 5 対応するアイコン（HTML、PDF、または CSV）をクリックして、レポートの出力形式を選択します。

ステップ 6 グローバル時間枠を変更する場合は、時間枠のアイコン（  ）をクリックします。

（注） グローバル時間枠の設定は、個々のレポート セクションのうちグローバル設定を継承するように設定されているものの内容だけに影響します。

ステップ 7 [入力パラメータ（Input Parameters）] セクションに表示されるフィールドの値を入力します。

ヒント フィールドにワイルドカード文字 * を入力すると、ユーザ パラメータを無視できます。こうすると、検索設定がユーザ パラメータで制約されなくなります。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、リテラルの IP アドレスまたは VLAN タグを使用してレポート結果を制約すると、予期しない結果になる可能性があります。

ステップ 8 電子メール リレー ホストを Firepower Management Center 構成で有効化した場合は、[電子メール（Email）] をクリックして、レポートの生成時にレポートが自動的に電子メール配信されるようにします。

ステップ 9 プロンプトが表示されたら、[OK] [生成（Generate）]をクリックして確認します。

ステップ 10 次の選択肢があります。

- レポート リンクをクリックして、新しいウィンドウにレポートを表示します。

- [OK] をクリックして、レポート テンプレート エディタに戻ります。

レポートの生成オプション

レポートの生成オプションは、以下のように設定できます。

- Firepower システム スケジューラを使用してレポートの生成を自動化します。毎日、毎週、毎月など、さまざまな範囲のタイムフレームに基づいたスケジュールでもカスタマイズできます。
- スケジューラを使用してメール レポートを配信します。タスクをスケジュールする**前に**、レポート テンプレートとメール リレー ホストを設定する必要があります。
- レポートを生成すると、そのレポートが受信者リストにメールの添付ファイルとして自動的に送信されます。レポートを電子メールで配信するように、メール リレー ホストを適切に設定する必要があります。
- 新しく生成されたレポート ファイルを、設定されたリモート ストレージの場所に保存します。リモート ストレージを使用するには、まずリモート ストレージの場所を設定します。

（注） リモートに保存してから、ローカル ストレージに切り替えた場合、リモート ストレージ内のレポートは [レポート（Reports）] タブのリストに表示されません。同様に、あるリモート ストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

レポートの生成時の電子メール配布

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 [概要（Overview）] > [レポート（Reporting）]を選択します。

ステップ 2 [レポート テンプレート（Report Templates）] タブをクリックします。

ステップ 3 レポートの生成に使用するテンプレートの横にあるレポート アイコン（  ）をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ヒント 先祖のテンプレートからレポートを生成するには、そのテンプレートを現在のドメインにコピーします。

ステップ 4 このウィンドウの [電子メール（Email）] セクションを展開します。

ステップ 5 [電子メール オプション（Email Options）] フィールドで、[電子メールの送信（Send Email）] を選択します。

ステップ 6 [受信者リスト（Recipient List）]、[CC] および [BCC] フィールドで、カンマ区切りリストの形式で受信者の電子メール アドレスを入力します。

ステップ 7 [件名（Subject）] フィールドに、電子メールの件名を入力します。

ヒント [件名（Subject）] フィールドやメッセージ本文に入力パラメータを使用して、電子メール内にタイムスタンプや Firepower Management Center の名前などの情報を動的に生成できます。

ステップ 8 必要に応じて、電子メールの本文にカバー レターを入力します。

ステップ 9 [OK] をクリックして確定します。

関連トピック

メール リレー ホストおよび通知アドレスの設定, （596 ページ）

生成されたレポートの操作について

以前に生成されたレポートには、[レポート（Reports）] タブのページからアクセスして操作します。

レポートの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

[レポート（Reports）] タブには、以前に生成されたすべてのレポートと、そのレポート名、生成日時、生成したユーザ、そのレポートがローカルに保存されたかリモートに保存されたかが一覧表示されます。ステータスのカラムには、レポートがすでに生成されているか、生成キュー内にある（スケジュール済みタスクの場合など）か、それとも生成できなかった（ディスク領域不足などの理由で）かが示されます。

管理者アクセス権を持つユーザはすべてのレポートを表示でき、その他のユーザは自分が生成したレポートだけを表示できることに注意してください。

マルチドメイン展開では、現在のドメインで作成されたレポートだけを表示できます。

[レポート（Reports）] タブのページには、ローカルに保存されたレポートがすべて示されます。現在リモート ストレージが設定されている場合、リモートに保存されたレポートも示されます。リモートで保存されたレポートの [場所（Location）] カラム データは、「`Remote`」になります。

（注） リモートに保存してから、ローカル ストレージに切り替えた場合、リモート ストレージ内のレポートは [レポート（Reports）] タブのリストに表示されません。同様に、あるリモート ストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

手順

ステップ 1 [概要（Overview）] > [レポート（Reporting）]を選択します。

ステップ 2 [レポート（Reports）] タブをクリックします。

ステップ 3 表示するレポートを選択します。

レポートのダウンロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

ローカルコンピュータにレポートファイルをダウンロードできます。そのコンピュータから、電子メールや他の使用可能な方法で電子的に配布できます。

マルチドメイン導入では、現在のドメインで生成されたレポートのみをダウンロードできます。

手順

ステップ 1 [概要（Overview）] > [レポート（Reporting）]を選択します。

ステップ 2 [レポート（Reports）] タブをクリックします。

ステップ 3 ダウンロードするレポートの横にあるチェック ボックスをオンにして、[ダウンロード（Download）] をクリックします。

ヒント ページ上のすべてのレポートをダウンロードするには、そのページの左上にあるチェック ボックスをオンにします。複数のレポートが複数のページにある場合は、2 つ目のチェック ボックスが表示されます。これをクリックすると、すべてのページ上のすべてのレポートをダウンロードできます。

ステップ 4 ブラウザのプロンプトに従って、レポートをダウンロードします。複数のレポートを選択すると、1 つの `.zip` ファイルでダウンロードされます。

リモートでのレポートの保存

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

[概要（Overview）] > [レポート（Reporting）] > [レポート（Reports）] ページの下部に、現在設定されているレポート ストレージの場所が表示され、ローカル、NFS、SMB ストレージの場合はディスク使用率も表示されます。SSH を使用してリモート ストレージにアクセスする場合、ディスク使用率のデータは利用できません。

（注） リモートに保存してから、ローカル ストレージに切り替えた場合、リモート ストレージ内のレポートは [レポート（Reports）] タブのリストに表示されません。同様に、あるリモート ストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

はじめる前に

- リモート ストレージの場所を設定します。詳細については、リモート ストレージ管理, （582 ページ）を参照してください。

手順

ステップ 1 [概要（Overview）] > [レポート（Reporting）]を選択します。

ステップ 2 [レポート（Reports）] タブを選択します。

ステップ 3 ページ下部の [レポートのリモート ストレージの有効化（Enable Remote Storage of Reports）] チェック ボックスをオンにします。

次の作業

- ローカル ストレージからリモート ストレージにレポートを移動します（リモート ストレージへのレポートの移動, （1744 ページ）を参照）。

関連トピック

リモート ストレージ管理, （582 ページ）
リモート ストレージへのレポートの移動, （1744 ページ）

リモート ストレージへのレポートの移動

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

バッチ モードまたは単独で、ローカル ストレージ内のレポートをリモート ストレージの場所に移動できます。

（注） リモートに保存してから、ローカル ストレージに切り替えた場合、リモート ストレージ内のレポートは [レポート（Reports）] タブのリストに表示されません。同様に、あるリモート ストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

はじめる前に

- リモート ストレージの場所を設定します。詳細については、リモート ストレージ管理, （582 ページ）を参照してください。

手順

ステップ 1 [概要（Overview）] > [レポート（Reporting）]を選択します。

ステップ 2 [レポート（Reports）] タブを選択します。

ステップ 3 移動するレポートの横にあるチェックボックスをオンにして、[移動（Move）] をクリックします。

ヒント ページ上のすべてのレポートを移動するには、そのページの左上にあるチェックボックスをオンにします。レポートのページが複数にわたる場合は、2 つ目のチェックボックスが表示されます。すべてのページのすべてのレポートを移動する場合は、このチェックボックスをオンにします。

ステップ 4 レポートの移動を確認します。

レポートの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

レポート ファイルはいつでも削除できます。この手順ではファイルが完全に削除され、リカバリは不可能になります。レポートの生成に使用したレポート テンプレートがまだ残っていますが、時間枠を拡大したりスライドしたりした場合は、特定のレポート ファイルを再生成するのは難しくなることがあります。テンプレートで入力パラメータを使用した場合も、再生成するのが難しくなることがあります。

マルチドメイン導入では、現在のドメインで生成されたレポートのみを削除できます。

手順

ステップ 1 [概要（Overview）] > [レポート（Reporting）]を選択します。

ステップ 2 [レポート（Reports）] タブをクリックします。

ステップ 3 次の選択肢があります。

- [選択項目の削除（Delete selected）]：削除するレポートの隣のチェック ボックスをオンにしてから、[削除（Delete）] をクリックします。
- [すべて削除（Delete all）]：ページ上のすべてのレポートを削除するには、そのページの左上にあるチェック ボックスをオンにします。複数のレポートが複数のページにある場合は、2 つ目のチェック ボックスが表示され、すべてのページ上のすべてのレポートを削除するよう選択できます。

ステップ 4 削除を確認します。

第 74 章

アラート応答による外部アラート

次のトピックでは、アラート応答を使用して Firepower Management Center から外部イベント アラートを送信する方法を示します。

Firepower Management Center アラート応答

SNMP、syslog、または電子メールでの外部イベント通知はクリティカルなシステムのモニタリングに役立ちます。Firepower Management Center はアラート応答を構成して外部サーバと対話します。これらのアラート応答はさまざまなログインやアラートの設定で使用し、イベントのロギングに加えて、あるいはその代わりに外部アラートを Firepower システム データベースに送信します。

（注） アラート応答を使用するアラートは、Firepower Management Center によって送信されます。アラート応答を使用しない侵入の電子メール アラートも、Firepower Management Center によって送信されます。対照的に、個別の侵入ルールのトリガーに基づく SNMP および syslog アラートは管理対象デバイスから直接送信されます。詳細については、侵入イベントに関する外部アラート，（1757 ページ）を参照してください。

ほとんどの場合、外部アラートに含まれる情報はデータベースにロギングされたいずれかの関連イベントに含まれる情報と同じです。ただし、相関ルールに接続トラッカーが含まれる相関イベ

ントアラートについては、受信する情報はベースのイベントの種類に関係なく、トラフィック プロファイル変更のアラート情報と同じです。

アラート応答の作成や管理は [アラート（Alerts）] ページ（[ポリシー（Policies）] > [アクション（Actions）] > [アラート（Alerts）]）で行います。新しいアラート応答は自動的に有効になります。アラート応答を削除するのではなく無効にすることで、アラートの生成を一時的に止めることができます。

アラート応答を使って SNMP トラップまたは syslog サーバに接続ログを送信している場合（外部電子メール アラートは接続イベントではサポートされていません）、これらのアラート応答を編集したあとに設定の変更を展開する必要があります。そうしないと、アラート応答への変更はただちに反映されます。

マルチドメイン展開では、アラート応答を作成すると、作成された応答は現在のドメインに属します。このアラート応答は子孫ドメインでも使用できます。

アラート応答のサポート設定

アラート応答を作成した後、それを使用して、次のような外部アラートを Firepower Management Center から送信できます。

アラート/イベントのタイプ	詳細情報
侵入イベント（インパクト フラグ別）	影響フラグ アラートの設定, （1754 ページ）
検出イベント（タイプ別）	検出イベント アラートの設定, （1755 ページ）
ネットワークベースのマルウェアとレトロスペクティブ マルウェアのイベント	AMP for Firepower アラートの設定, （1755 ページ）
相関イベント（相関ポリシー違反ごと）	ルールとホワイトリストに応答を追加する, （1636 ページ）
相関イベント（ログ ルールまたはデフォルト アクション別）（電子メールアラートのサポートなし）	設定可能な接続ロギング, （1908 ページ）
ヘルス イベント（ヘルス モジュールおよび重大度レベル別）	ヘルス モニタ アラートの作成, （268 ページ）

SNMP アラート応答の作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

SNMPv1、SNMPv2、または SNMPv3 を使用して SNMP アラート応答を作成できます。

（注） SNMP プロトコルの SNMP バージョンを選択する場合、SNMPv2 では読み取り専用コミュニティのみがサポートされ、SNMPv3 では読取り専用ユーザのみがサポートされることに注意してください。SNMPv3 は、AES128 での暗号化をサポートします。

SNMP で 64 ビット値をモニタする場合は、SNMPv2 または SNMPv3 を使用する必要があります。SNMPv1 は 64 ビットのモニタリングをサポートしていません。

はじめる前に

- ネットワーク管理システムで Firepower Management Center の管理情報ベース（MIB）ファイルが必要な場合は、`/etc/sf/DCEALERT.MIB` で取得できます。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [アラート（Alerts）]を選択します。

ステップ 2 [アラートの作成（Create Alert）] ドロップダウン メニューから、[SNMP アラートの作成（Create SNMP Alert）] を選択します。

ステップ 3 SNMP 応答を識別する [名前（Name）] を入力します。

ステップ 4 [トラップサーバ（Trap Server）] フィールドに、SNMP トラップ サーバのホスト名または IP アドレスを入力します。

（注） このフィールドに無効な IPv4 アドレス（192.169.1.456 など）を入力した場合でも、システムは警告を表示しません。無効なアドレスはホスト名として扱われます。

ステップ 5 [バージョン（Version）] ドロップダウンリストから、使用する SNMP バージョンを選択します。SNMP v3 がデフォルトです。

ステップ 6 使用する SNMP のバージョンに応じて、次のいずれかを実行します。

- SNMP v1 または SNMP v2 の場合は、[コミュニティ ストリング（Community String）] フィールドに SNMP コミュニティ名を入力して、手順 12 に進みます。

- SNMP v3 の場合、[ユーザ名（User Name）] フィールドに SNMP サーバで認証するユーザの名前を入力し、次の手順に進みます。

ステップ 7 [認証プロトコル（Authentication Protocol）] ドロップダウンリストから、認証に使用するプロトコルを選択します。

ステップ 8 [認証パスワード（Authentication Password）] フィールドに、SNMP サーバの認証に必要なパスワードを入力します。

ステップ 9 [プライバシー プロトコル（Privacy Protocol）] リストから、[なし（None）] を選択してプライバシー プロトコルを使用しないか、または [DES] を選択してプライバシー プロトコルにデータ暗号規格を使用します。

ステップ 10 [プライバシー パスワード（Privacy Password）] フィールドに、SNMP サーバに必要なプライバシー パスワードを入力します。

ステップ 11 [エンジン ID（Engine ID）] フィールドに、SNMP エンジンの識別子を偶数桁の 16 進表記で入力します。
SNMPv3 を使用する場合、メッセージの符号化には エンジン ID 値が使用されます。SNMP サーバでは、メッセージをデコードするためにこの値が必要です。

Firepower Management Center の IP アドレスの 16 進数バージョンを使用することを推奨します。たとえば、Firepower Management Center の IP アドレスが `10.1.1.77` である場合、`0a01014D0` を使用します。

ステップ 12 [保存（Save）] をクリックします。

Syslog アラート応答の作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

syslog アラート応答を設定する際、syslog サーバで確実に正しく処理されるようにするために、syslog メッセージに関連付けられる重大度とファシリティを指定できます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。ファシリティと重大度は syslog に示される実際のメッセージには表示されませんが、syslog メッセージを受信するシステムに対して、メッセージの分類方法を指示するために使用されます。

ヒント syslog の機能とその設定方法の詳細については、ご使用のシステムのマニュアルを参照してください。UNIX システムでは、`syslog` および `syslog.conf` の `man` ページで概念情報および設定手順が説明されています。

syslogアラート応答の作成時に任意のタイプのファシリティを選択できますが、syslogサーバに基づいて意味のあるものを選択する必要があります。すべてのsyslogサーバがすべてのファシリティをサポートしているわけではありません。UNIX syslog サーバの場合、`syslog.conf` ファイルで、どのファシリティがサーバ上のどのログ ファイルに保存されるかを示す必要があります。

はじめる前に

- syslog サーバがリモート メッセージを受け入れられることを確認します。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [アラート（Alerts）]を選択します。

ステップ 2 [アラートの作成（Create Alert）] ドロップダウン メニューから、[Syslog アラートの作成（Create Syslog Alert）] を選択します。

ステップ 3 [名前（Name）] にアラートの名前を入力します。

ステップ 4 [ホスト（Host）] フィールドに、syslog サーバのホスト名または IP アドレスを入力します。

（注） このフィールドに無効な IPv4 アドレス（192.168.1.456 など）を入力した場合でも、システムは警告を表示しません。無効なアドレスはホスト名として扱われます。

ステップ 5 [ポート（Port）]フィールドに、サーバがsyslogメッセージに使用するポートを入力します。この値はデフォルトで 514 です。

ステップ 6 Syslogアラートファシリティ，（1751ページ）で説明されているとおりに、[ファシリティ（Facility）] リストからファシリティを選択します。

ステップ 7 syslog重大度レベル，（1752ページ）で説明されているとおりに、[重大度（Severity）]リストから重大度を選択します。

ステップ 8 [タグ（Tag）] フィールドに、syslog メッセージとともに表示するタグ名を入力します。
たとえば、syslog に送信されるすべてのメッセージの前に `FromMC` を付ける場合、このフィールドに `FromMC` と入力します。

ステップ 9 [保存（Save）] をクリックします。

Syslog アラート ファシリティ

次の表に、選択可能な syslog ファシリティを示します。

表 *223*：使用可能な *syslog* ファシリティ

ファシリティ	説明
ALERT	アラート メッセージ。
AUDIT	監査サブシステムによって生成されるメッセージ。

ファシリティ	説明
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CLOCK	クロック デーモンによって生成されるメッセージ。 Windows オペレーティング システムを実行している syslog サーバは CLOCK ファシリティを使用することに注意してください。
CRON	クロック デーモンによって生成されるメッセージ。 Linux オペレーティング システムを実行している syslog サーバは CRON ファシリティを使用することに注意してください。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージは表示されるときにコンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。
NTP	NTP デーモンによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザレベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

syslog 重大度レベル

次の表に、選択可能な標準の syslog 重大度レベルを示します。

表 *224* : *syslog* 重大度レベル

水準器	説明
ALERT	ただちに修正する必要がある状態。
CRIT	クリティカルな状態。
DEBUG	デバッグ情報を含むメッセージ。
EMERG	すべてのユーザに配信されるパニック状態。
ERR	エラー状態。
INFO	情報メッセージ。
NOTICE	エラー状態ではないが、注意が必要な状態。
WARNING	警告メッセージ。

電子メール アラート応答の作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

はじめる前に

- Firepower Management Center で、自身の IP アドレスを逆解決できることを確認します。
- メール リレー ホストおよび通知アドレスの設定, （596 ページ）の説明に従って、メール リレー ホストを設定します。

（注） 電子メール アラートを使用して、接続をログに記録することは**できません**。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [アラート（Alerts）]を選択します。

ステップ 2 [アラートの作成（Create Alert）] ドロップダウン メニューから、[電子メール アラートの作成（Create Email Alert）] を選択します。

ステップ 3 [名前（Name）] にアラート応答の名前を入力します。

ステップ 4 [宛先（To）] フィールドに、アラートを送信する電子メール アドレスをカンマで区切って入力します。

ステップ 5 [送信元（From）] フィールドに、アラートの送信者として表示する電子メール アドレスを入力します。

ステップ 6 [リレーホスト（Relay Host）] の横に表示されるメール サーバが、アラートの送信に使用するサーバであることを確認します。

ヒント 電子メール サーバを変更するには、編集アイコン（）をクリックします。

ステップ 7 [保存（Save）] をクリックします。

影響フラグ アラートの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin

特定のインパクト フラグを持つ侵入イベントが発生するたびにアラートが生成されるようにシステムを設定できます。インパクト フラグは、侵入データ、ネットワーク検出データ、および脆弱性情報を関連付けることにより、侵入がネットワークに与える影響を評価するのに役立ちます。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [アラート（Alerts）]を選択します。

ステップ 2 [インパクト フラグ アラート（Impact Flag Alerts）] タブをクリックします。

ステップ 3 [アラート（Alerts）] セクションで、各アラート タイプで使用するアラート応答を選択します。

ヒント 新しいアラート応答を作成するには、任意のドロップダウン リストから [新規（New）] を選択します。

ステップ 4 [インパクト設定（Impact Configuration）] セクションで、該当するチェックボックスをオンにして、各インパクト フラグに対して受信するアラートを指定します。

ステップ 5 [保存（Save）] をクリックします。

検出イベント アラートの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

特定のタイプの検出イベントが発生するたびにアラートが生成されるようにシステムを設定できます。

はじめる前に

- ネットワーク検出イベント ロギングの設定, （1574 ページ）の説明に従って、アラートを設定する検出イベント タイプを記録するようにネットワーク検出ポリシーを設定します。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [アラート（Alerts）]を選択します。

ステップ 2 [検出イベント アラート（Discovery Event Alerts）] タブをクリックします。

ステップ 3 [アラート（Alerts）] セクションで、各アラート タイプで使用するアラート応答を選択します。

ヒント 新しいアラート応答を作成するには、任意のドロップダウン リストから [新規（New）] を選択します。

ステップ 4 [イベント設定（Events Configuration）] セクションで、各検出イベント タイプに対して、受信するアラートに対応するチェックボックスを選択します。

ステップ 5 [保存（Save）] をクリックします。

AMP for Firepower アラートの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
マルウェア	マルウェア	任意（Any）	任意（Any）	Admin

ネットワークベースのマルウェアイベント（レトロスペクティブイベントを含む）が発生するたびにアラートが生成されるようにシステムを設定できます。ただし、エンドポイント ベースの（AMP for Endpoints）マルウェア イベントではアラートを生成できません。

はじめる前に

- マルウェア クラウド ルックアップを実行するファイル ポリシーを設定し、侵入ポリシーとファイル ポリシーを使用したアクセス制御, （815 ページ）の説明に従って、そのポリシーをアクセス コントロール ルールに関連付けます。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [アラート（Alerts）]を選択します。

ステップ 2 [高度なマルウェア保護アラート（Advanced Malware Protections Alerts）] タブをクリックします。

ステップ 3 [アラート（Alerts）] セクションで、各アラート タイプで使用するアラート応答を選択します。

ヒント 新しいアラート応答を作成するには、任意のドロップダウン リストから [新規（New）] を選択します。

ステップ 4 [イベント設定（Event Configuration）] セクションで、各マルウェア イベント タイプに対して、受信するアラートに対応するチェックボックスを選択します。
[すべてのネットワークベースのマルウェア イベント（All network-based malware events）] には [レトロスペクティブ イベント（Retrospective Events）] が含まれることに注意してください。

ステップ 5 [保存（Save）] をクリックします。

第 75 章

侵入イベントに関する外部アラート

次のトピックでは、侵入イベントに関する外部アラートを設定する方法について説明します。

侵入イベントの外部アラートについて

外部侵入イベント通知は、クリティカルなシステム モニタリングに役立ちます。

- SNMP：侵入ポリシーごとに設定し、管理対象デバイスが送信します。SMNP アラートは侵入ルールごとに有効にすることができます。
- syslog：侵入ポリシーごとに設定し、管理対象デバイスが送信します。1 つの侵入ポリシーの syslog アラートを有効にすると、ポリシーに含まれるすべてのルールに適用されます。
- 電子メール：すべての侵入ポリシーに設定され、Firepower Management Center が送信します。電子メールアラートは侵入ルールごとに有効にすることができ、長さと頻度を制限することもできます。

侵入イベントの抑制やしきい値を設定すると、システムは、ルールがトリガーされるたびに侵入イベントを生成しなくなる（したがってアラートを送信しなくなる）場合があるのでご注意ください。

マルチドメイン導入環境では、どのドメインでも外部アラートを設定できます。先祖ドメインでは、システムは子孫ドメインの侵入イベントの通知を生成します。

（注） Firepower Management Center も SNMP、syslog、および電子メール アラート応答を使って種々の外部アラートを送信します。Firepower Management Center アラート応答，（1747 ページ）を参照してください。システムは、個々の侵入イベントに対するアラートを送信するためにアラート応答を使用**しません**。

関連トピック

侵入ポリシーの侵入イベント通知のフィルタ，（1064 ページ）

侵入イベントの SNMP アラートの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

侵入ポリシーで外部 SNMP アラートを有効にした後、トリガー時に SNMP アラートを送信する個々のルールを設定できます。これらのアラートは管理対象デバイスから送信されます。

手順

ステップ 1 侵入ポリシーエディタのナビゲーション ウィンドウで、[詳細設定（Advanced Settings）] をクリックします。

ステップ 2 [SNMP アラート（SNMP Alerting）] が有効になっていることを確認し、[編集（Edit）] をクリックします。
ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。

ステップ 3 SNMP バージョンを選択し、侵入 SNMP アラートのオプション，（1759 ページ）の説明に従って構成オプションを指定します。

ステップ 4 ナビゲーション ウィンドウで [ルール（Rules）] をクリックします。

ステップ 5 [ルール（rules）] ペインで、SNMP アラートを設定するルールを選択し、[アラート（Alerting）] > [SNMP アラートの追加（Add SNMP Alert）] を選択します。

ステップ 6 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] を選択して、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

侵入 SNMP アラートのオプション

ネットワーク管理システムで Management Information Base（MIB）ファイルが必要な場合は、Firepower Management Center の `/etc/sf/DCEALERT.MIB` から取得できます。

SNMP v2 オプション

オプション	説明
トラップ タイプ	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[バイナリとして（as Binary）] を選択します。それ以外の場合は、[文字列として（as String）] を選択します。たとえば、HP OpenView では [文字列として（as String）] が必要になります。
トラップ サーバ（Trap Server）	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。
コミュニティ ストリング（Community String）	コミュニティ名。

SNMP v3 オプション

管理対象デバイスは、エンジン ID の値を使用して SNMPv3 アラートをエンコードします。アラートをデコードするには、SNMP サーバにこの値が必要です。この値は、送信デバイスの管理インターフェイスの IP アドレスの 16 進数のバージョンで、「01」が付加されています。

たとえば、SNMP アラートを送信するデバイスの管理インターフェイスの IP アドレスが 172.16.1.50 である場合、エンジン ID の値は 0xAC10013201 です。

オプション	説明
トラップ タイプ	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[バイナリとして（as Binary）] を選択します。それ以外の場合は、[文字列として（as String）] を選択します。たとえば、HP OpenView では [文字列として（as String）] が必要になります。
トラップ サーバ（Trap Server）	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。

オプション	説明
認証パスワード（Authentication Password）	認証に必要なパスワード。SNMP v3 は、設定に応じて Message Digest 5（MD5）ハッシュ関数またはセキュア ハッシュ アルゴリズム（SHA）ハッシュ関数のいずれかを使用し、このパスワードを暗号化します。 認証パスワードを指定すると、認証が有効になります。
プライベート パスワード（Private Password）	プライバシー用の SNMP キー。SNMP v3 は Data Encryption Standard（DES）ブロック暗号を使用して、このパスワードを暗号化します。SNMP v3 パスワードを入力すると、パスワードは初期設定時にはプレーン テキストで表示されますが、暗号化形式で保存されます。 プライベート パスワードを指定すると、プライバシーが有効になり、認証パスワードも指定する必要があります。
ユーザ名（User Name）	SNMP ユーザ名。

侵入イベントの Syslog アラートの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

侵入ポリシーで syslog アラートを有効にすると、管理対象デバイス自体または外部ホスト上の syslog にすべての侵入イベントが送信されます。外部ホストを指定した場合、syslog アラートは管理対象デバイスから送信されます。

手順

ステップ 1 侵入ポリシー エディタのナビゲーション ウィンドウで、[詳細設定（Advanced Settings）] をクリックします。

ステップ 2 [Syslog アラート（Syslog Alerting）] が有効になっていることを確認し、[編集（Edit）] をクリックします。
ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。

ステップ 3 syslog アラートを送信するロギング ホストの IP アドレスを入力します。
このフィールドを空のままにすると、管理対象デバイスは、独自の syslog 機能を使用して侵入イベントをログに記録します。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があり

ます。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ステップ 4 侵入 syslog アラートのファシリティとプライオリティ, （1761 ページ）の説明に従って、ファシリティと優先度レベルを選択します。

ステップ 5 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] を選択して、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

侵入 syslog アラートのファシリティとプライオリティ

管理対象デバイスは、特定のファシリティとプライオリティを使用して、侵入イベントを syslog アラートとして送信できるため、ロギング ホストがアラートを分類できます。ファシリティには、それを生成したサブシステムを指定します。プライオリティには、その重大度を指定します。これらのファシリティとプライオリティの値は、実際の syslog メッセージには表示されません。

ご使用の環境に基づいて意味のある値を選択します。ローカル設定ファイル（UNIX ベースのロギング ホストの syslog.conf など）では、どのログ ファイルにどのファシリティを保存するかを示すことができます。

Syslog アラート ファシリティ

ファシリティ	説明
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CRON	クロック デーモンによって生成されるメッセージ。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージは表示されるときにコンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。

ファシリティ	説明
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザレベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

Syslog アラートのプライオリティ

水準器	説明
EMERG	すべてのユーザにブロードキャストするパニック状態
ALERT	すぐに修正する必要がある状態
CRIT	重大な状態
ERR	エラー状態
WARNING	警告メッセージ
NOTICE	エラー状態ではないが、注意が必要な状態
INFO	通知メッセージ
DEBUG	デバッグ情報を含むメッセージ

侵入イベントに対する電子メール アラートの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

侵入の電子メール アラートを有効にした場合、どの管理対象デバイスまたは侵入ポリシーが侵入を検出したかに関係なく、システムは侵入イベントの生成時に電子メールを送信できます。これらのアラートは Firepower Management Center から送信されます。

はじめる前に

- 電子メール アラートを受信するようにメール ホストを設定します。メール リレー ホストおよび通知アドレスの設定, （596 ページ）を参照してください。
- Firepower Management Center が独自の IP アドレスを逆解決できることを確認します。

手順

ステップ 1 [ポリシー（Policies）] > [アクション（Actions）] > [アラート（Alerts）]を選択します。

ステップ 2 [侵入電子メール（Intrusion Email）] タブをクリックします。

ステップ 3 侵入電子メール アラートのオプション, （1763 ページ）の説明に従って、アラートを生成する侵入ルールや侵入グループを含むアラート オプションを選択します。

ステップ 4 [保存（Save）] をクリックします。

侵入電子メール アラートのオプション

On/Off

侵入電子メール アラートを有効または無効にします。

アドレス送信元/宛先（From/To Addresses）

電子メールの送信者と受信者。受信者のカンマ区切りリストを指定できます。

最大アラート数と頻度（Max Alerts and Frequency）

Firepower Management Center が時間間隔（[頻度（Frequency）]）ごとに送信する電子メール アラートの最大数（[最大アラート数（Max Alerts）]）。

合同アラート（Coalesce Alerts）

同じ送信元 IP とルール ID を持つアラートをグループ化することによって送信されるアラートの数を減らします。

サマリー出力（Summary Output）

テキスト制限されたデバイスに適した短いアラートを有効にします。短いアラートには、以下の情報が含まれています。

- Timestamp

- プロトコル
- 送信元と宛先の IP とポート
- メッセージ
- 同じ送信元 IP に対して生成された侵入イベントの数

例：`2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0 snort_decoder: Unknown Datagram decoding problem! (116:108)`

[サマリー出力（Summary Output）] を有効にする場合は、[合同アラート（Coalesce Alerts）] も有効にすることを検討してください。テキストメッセージの制限を超えないように、[最大アラート数（Max Alerts）] を下げることもできます。

タイム ゾーン

アラート タイムスタンプのタイム ゾーン。

特定のルール設定に基づく電子メール警告（Email Alerting on Specific Rules Configuration）

電子メール アラートを設定するルールを選択できます。

第 XIX 部

イベントとアセットの分析ツール

第 76 章

コンテキスト エクスプローラの使用

以下のトピックでは、Firepower システムでコンテキスト エクスプローラを使用する方法について説明します。

コンテキスト エクスプローラについて

Firepower システムの Context Explorer には、モニタ対象ネットワークのステータスに関するコンテキストでの詳細でインタラクティブなグラフィカル情報が表示されます。これには、アプリケーション、アプリケーション統計、接続、位置情報、侵害の兆候、侵入イベント、ホスト、サーバ、セキュリティ インテリジェンス、ユーザ、ファイル（マルウェア ファイルを含む）、関連 URL に関するデータが含まれます。各セクションには、このデータが鮮やかな色の折れ線グラフ、棒グラフ、円グラフ、ドーナツ グラフの形式で表示され、グラフとともに詳しいリストが示されます。1 番目のセクションに表示される時間の経過に伴うトラフィックとイベント数の変化を示した折れ線グラフは、ネットワークのアクティビティにおける最近の傾向の概要を示します。

分析を細かく調整するためのカスタム フィルタを容易に作成および適用できます。またグラフエリアをクリックするか、カーソルをグラフエリアに置くことでデータ セクションを詳しく調べることができます。過去 1 時間から過去 1 年までの期間を反映するように Explorer の時間範囲を設定することもできます。Context Explorer にアクセスできるユーザは、管理者、セキュリティ アナリスト、またはセキュリティ アナリスト（読み取り専用）のユーザ ロールが割り当てられているユーザだけです。

Firepower システムのダッシュボードは細かくカスタマイズすることができます。このダッシュボードは区分化されており、リアルタイムで更新されます。一方、Context Explorer は手動で更新

され、より幅広いデータのコンテキストを提供することを目的としており、アクティブなユーザ操作のために単一で一貫性のあるレイアウトを備えています。

特定のニーズに基づいてネットワークとアプライアンスのリアルタイムのアクティビティをモニタするには、ダッシュボードを使用します。逆に、詳細かつ明確なコンテキストで事前に定義されている最新のデータ セットを調査するには、Context Explorer を使用します。たとえば、ネットワークのホストのうち Linux を使用しているホストは 15% であるが、ほぼすべての YouTube トラフィックはこれらのホストによるものであることが判明した場合、Linux ホストのデータのみを表示するフィルタ、YouTube 関連のアプリケーション データのみを表示するフィルタ、あるいはこの両方のフィルタを簡単に適用できます。コンパクトで対象が絞り込まれているダッシュボード ウィジェットとは異なり、Context Explorer の各セクションは、Firepower システムの専門知識を持つユーザと一般的なユーザの両方に役立つ形式で、システム アクティビティを鮮明なビジュアル表現で提供します。

表示されるデータは、管理対象デバイスのライセンスおよび導入状況や、そのデータを提供する機能を設定しているかどうかによって異なります。また、Context Explorer のすべてのセクションで、フィルタを適用して表示するデータを制限することもできます。

マルチドメイン導入では、先祖ドメインで Context Explorer を表示すると、すべてのサブドメインからの集約データが表示されます。リーフ ドメインでは、そのドメインに固有のデータだけを表示できます。

ダッシュボードと Context Explorer の違い

次の表に、ダッシュボードと Context Explorer の主な相違点の要約を示します。

表 *225*：比較：ダッシュボードと *Context Explorer*

機能	ダッシュボード	コンテキスト エクスプローラ（Context Explorer）
表示可能なデータ	Firepower システムによってモニタされる任意の対象	アプリケーション、アプリケーション統計、位置情報、の侵害の兆候、侵入イベント、ファイル（マルウェア ファイルを含む）、ホスト、セキュリティ インテリジェンス イベント、サーバ、ユーザ、および URL
カスタマイズ可能かどうか	• ダッシュボードで選択されているウィジェットはカスタマイズ可能です • 個々のウィジェットはさまざまなレベルでカスタマイズ可能です	• 基本レイアウトは変更できません • 適用されたフィルタは Explorer URL に示され、後で使用するためにブックマークできます
データの更新頻度	自動（デフォルト）、ユーザ設定	手動（Manual）
データのフィルタリング	一部のウィジェットで可能です（ウィジェット設定を編集する必要があります）	Explorer のすべての部分で可能であり、複数フィルタに対応しています

機能	ダッシュボード	コンテキスト エクスプローラ（Context Explorer）
グラフィカル コンテキスト	一部のウィジェット（特にカスタム分析（Custom Analysis））では、データをグラフ形式で表示できます	すべてのデータの豊富なグラフィカル コンテキスト（独自の詳細なドーナツ グラフを含む）
関連 Web インターフェイス ページへのリンク	一部のウィジェット	すべてのセクション
表示データの時間範囲	ユーザ設定	ユーザ設定

[時系列のトラフィックおよび侵入イベント数（TrafficandIntrusionEventCountsTime）] グラフ

Context Explorer の上部には、時間の経過に伴うトラフィックおよび侵入イベント数の変化を示す折れ線グラフが表示されます。X 軸は時間間隔を示します（選択されている時間枠に応じて、5 分～ 1 か月の範囲）。Y 軸は、KB 単位のトラフィック（青色の線）と侵入イベント数（赤色の線）を示します。

X 軸の最小間隔が 5 分であることに注意してください。これに対応するため、選択された時間範囲の開始点と終了点が、システムにより、最も近い 5 分間間隔に調整されます。

このセクションには、デフォルトでは選択された時間範囲のすべてのネットワーク トラフィックと、生成されたすべての侵入イベントが示されます。フィルタを適用すると、フィルタに指定されている条件に関連するトラフィックと侵入イベントだけがグラフに表示されます。たとえば、[OS 名（OS Name）] に `Windows` を指定してフィルタリングすると、時間グラフには Windows オペレーティング システムを使用するホストに関連するトラフィックとイベントだけが表示されます。

侵入イベント データ（[優先順位（Priority）] が `High` に設定されたものなど）に基づいて Context Explorer をフィルタ処理すると、青色のトラフィックを示す線が非表示になり、侵入イベントだけにより焦点を当てることができます。

トラフィックとイベント数に関する正確な情報を表示するには、グラフの線上の任意のポイントにポインタを置きます。また、色付きの線の 1 つにポインタを置くと、その線がグラフの前面に移動し、コンテキストがより明確になります。

このセクションのデータは、主に [侵入イベント（Intrusion Events）] テーブルと [接続イベント（Connection Events）] テーブルから取得されます。

[侵害の兆候（Indications of Compromise）] セクション

コンテキスト エクスプローラの [侵害の兆候（IOC）（Indications of Compromise (IOC)）] セクションには、モニタ対象ネットワーク上でセキュリティが侵害されている可能性があるホストの概要

を示す2つのインタライクティブ セクション（トリガーとして使用された主なIOC種類の割合のビューと、トリガーとして使用された兆候の数をホストごとに表したビュー）が表示されます。

[兆候別ホスト（Hosts by Indication）] グラフ

[兆候別ホスト（Hosts by Indication）] グラフはドーナツ形式であり、モニタ対象ネットワーク上のホストでトリガーとして使用された侵害の兆候（IOC）を割合で表示します。内側のリングはIOCカテゴリ（[CnC接続（CnC Connected）] や [マルウェア検出（Malware Detected）] など）ごとに分割されており、外側のリングではそれがさらに具体的なイベントの種類（[影響2侵入イベント - 管理者として試行（Impact 2 Intrusion Event — attempted-admin）] や [ファイル転送中に脅威を検出（Threat Detected in File Transfer）] など）ごとに分割されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [ホスト（Hosts）] テーブルと [侵害の兆候（Indications of Compromise）] テーブルから取得されます。

[ホスト別兆候（Indications by Host）] グラフ

[ホスト別兆候（Indications by Host）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最もIOCが顕著な15のホストでトリガーとして使用された固有の侵害の兆候（IOC）の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [ホスト（Hosts）] テーブルと [侵害の兆候（Indications of Compromise）] テーブルから取得されます。

[ネットワーク情報（Network Information）] セクション

Context Explorer の [ネットワーク情報（Network Information）] セクションには、モニタ対象ネットワーク上の接続トラフィックの全体の概要（トラフィックに関連付けられている送信元、宛先、ユーザ、およびセキュリティ ゾーン、ネットワーク上のホストで使用されているオペレーティング システムの内訳、Firepowerシステムがネットワーク トラフィックに対して実行したアクセス制御アクションの割合のビュー）を示す6つのインタラクティブ グラフが含まれています。

[オペレーティング システム（Operating Systems）] グラフ

[オペレーティング システム（Operating Systems）] グラフはドーナツ グラフ形式で、モニタ対象ネットワークのホストで検出されたオペレーティング システムを割合で表示します。内側のリングはOS名（`Windows` や `Linux` など）ごとに分割され、外側のリングではそのデータがさらにオペレーティング システムのバージョン（`Windows Server 2008` や `Linux 11.x` など）ごとに分割されています。密接に関連するいくつかのオペレーティング システム（Windows 2000、Windows XP、Windows Server 2003 など）は1つにまとめられます。ごくまれにしか使用されないオペレーティング システムや認識されないオペレーティング システムは [その他（Other）] にまとめられます。

このグラフは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Context Explorer の時間範囲を変更しても、グラフは変化しません。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [ホスト（Hosts）] テーブルから取得されます。

[送信元 IP 別トラフィック（Traffic by Source IP）] グラフ

[送信元 IP 別トラフィック（Traffic by Source IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の送信元 IP アドレスのネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた送信元 IP アドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[送信元IP別トラフィック（Traffic by Source IP）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[送信元ユーザ別トラフィック（Traffic by Source User）] グラフ

[送信元ユーザ別トラフィック（Traffic by Source User）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の送信元ユーザのネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた送信元 IP アドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[送信元ユーザ別トラフィック（Traffic by Source User）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。このグラフには、権限のあるユーザのデータが表示されます。

[アクセス コントロール アクション別の接続（Connections by Access Control Action）] グラフ

[アクセス コントロール アクション別の接続（Connections by Access Control Action）] グラフは円グラフ形式であり、Firepower システム導入でモニタ対象トラフィックに対して実行されたアクセス制御アクション（[ブロック（Block）] や [許可（Allow）] など）の割合のビューを表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[送信元ユーザ別トラフィック（Traffic by Source User）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[宛先 IP 別トラフィック（Traffic by Destination IP）] グラフ

[宛先 IP 別トラフィック（Traffic by Destination IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の宛先 IP アドレスのネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた宛先 IP アドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[宛先IP別トラフィック（Traffic by Destination IP）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[入力/出力のセキュリティ ゾーン別トラフィック（Traffic by Ingress/Egress Security Zone）] グラフ

[入力/出力のセキュリティ ゾーン別トラフィック（Traffic by Ingress/Egress Security Zone）] グラフは棒グラフ形式で、モニタ対象ネットワークで設定されているセキュリティ ゾーンごとに、その着信/発信ネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。このグラフは、必要に応じて、入力（デフォルト）セキュリティ ゾーン情報または出力セキュリティ ゾーン情報のいずれかを表示するように設定できます。

リストされたセキュリティ ゾーンごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント グラフに制約を適用して、出力セキュリティ ゾーンのトラフィックだけが表示されるようにするには、グラフにポインタを置き、表示されたトグル ボタンの [出力（Egress）] をクリックします。デフォルトのビューに戻すには、[入力（Ingress）] をクリックします。このグラフは、Context Explorer から外部へ移動しても、デフォルトの [入力（Ingress）] ビューに戻ります。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[入力/出力のセキュリティ ゾーン別トラフィック（Traffic by Ingress/Egress Security Zone）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[アプリケーション情報（Information）] セクション

Context Explorer の [アプリケーション情報（Information）] セクションには、3 つのインタラクティブ グラフと 1 つの表形式リストが表示されます。これらのグラフとリストは、モニタ対象ネットワーク上でのアプリケーション アクティビティの概要（アプリケーションに関連するトラフィック、侵入イベント、およびホストを、各アプリケーションに割り当てられている推定リスクまたは推定ビジネス関連度ごとに編成したもの）を示します。[アプリケーション詳細リスト（Application Details List）] は、各アプリケーションとそのリスク、ビジネス関連度、カテゴリ、ホスト数を示すインタラクティブなリストです。

このセクションのすべての「アプリケーション」インスタンスについて、[アプリケーション情報（Application Information）] のグラフのセットは、デフォルトでは特にアプリケーション プロトコル（DNS、SSH など）を検査します。クライアント アプリケーション（PuTTY や Firefox など）や Web アプリケーション（Facebook や Pandora など）を特に検査するように [アプリケーション情報（Application Information）] セクションを設定することもできます。

[アプリケーション情報（Application Information）] セクションへのフォーカスの移動

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]を選択します。

ステップ 2 [アプリケーション プロトコル情報（Application Protocol Information）] セクションにポインタを重ねます。

（注） 以前に同じ Context Explorer セッションでこの設定を変更している場合は、セクション タイトルが [クライアント アプリケーション情報（Client Application Information）] または [Web アプリケーション情報（Web Application Information）] と表示されることがある点に注意してください。

ステップ 3 [アプリケーション プロトコル（Application Protocol）]、[クライアント アプリケーション（Client Application）]、または [Web アプリケーション（Web Application）] をクリックします。

[リスク/ビジネスとの関連性とアプリケーション別トラフィック（Traffic by Risk/Business Relevance and Application）] グラフ

[リスク/ビジネスとの関連性とアプリケーション別トラフィック（Traffic by Risk/Business Relevance and Application）] グラフはドーナツ形式で、モニタ対象ネットワークで検出されたアプリケーション トラフィックを、アプリケーションの推定リスク（デフォルト）または推定のビジネスとの関連性（ビジネス関連度）ごとの割合で表示します。内側のリングは推定のリスクまたはビジネスとの関連性レベル（`Medium` や `High` など）ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション（`SSH` や `NetBIOS` など）ごとに分割されます。まれにしか検出されないアプリケーションは [その他（Other）] にまとめられます。

このグラフは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Context Explorer の時間範囲を変更しても、グラフは変化しません。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント グラフに制約を適用して、ビジネスとの関連性とアプリケーションごとにトラフィックが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Business Relevance] をクリックします。デフォルト ビューに戻すには [リスク（Risk）] をクリックします。このグラフは、Context Explorer から外部へ移動しても、デフォルトの [リスク（Risk）] ビューに戻ります。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[リスク/ビジネスとの関連性とアプリケーション別トラフィック（Traffic by Risk/Business Relevance and Application）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルと [アプリケーション統計（Application Statistics）] テーブルから取得されます。

[リスク/ビジネスとの関連度別侵入イベントおよびアプリケーション（Intrusion Events by Risk/Business Relevance and Application）] グラフ

[リスク/ビジネスとの関連度別侵入イベントおよびアプリケーション（Intrusion Events by Risk/Business Relevance and Application）] グラフはドーナツ形式であり、モニタ対象ネットワークで検出された侵入イベントと、これらのイベントに関連するアプリケーションを、アプリケーションの推定リスク（デフォルト）または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定のリスクまたはビジネスとの関連性レベル（`Medium` や `High` など）ごとに分割され、外側のリングで

はそのデータがさらに具体的なアプリケーション（SSHやNetBIOSなど）ごとに分割されます。稀に検出されるアプリケーションは [その他（Other）] にまとめられます。

ドーナツ グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされるか、または（該当する場合には）アプリケーション情報が表示されます。

ヒント　グラフに制約を適用して、ビジネスとの関連性とアプリケーションごとに侵入イベントが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [ビジネスとの関連性（Business Relevance）] をクリックします。デフォルト ビューに戻すには [リスク（Risk）] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [リスク（Risk）] ビューに戻ることに注意してください。

このグラフのデータは主に [侵入イベント（Intrusion Events）] テーブルと [アプリケーションの統計（Application Statistics）] テーブルから取得されます。

[リスク/ビジネスとの関連度別ホストおよびアプリケーション（Hosts by Risk/Business Relevance and Application）] グラフ

[リスク/ビジネスとの関連度別ホストおよびアプリケーション（Hosts by Risk/Business Relevance and Application）] グラフはドーナツ形式であり、モニタ対象ネットワークで検出されたホストと、これらのホストに関連するアプリケーションを、アプリケーションの推定リスク（デフォルト）または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル（[中（Medium）] または [高（High）] など）ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション（[SSH] または [NetBIOS] など）ごとに分割されます。非常に少数のアプリケーションは [その他（Other）] にまとめられます。

ドーナツ グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、ビジネスとの関連性とアプリケーションに基づいてホストが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [ビジネスとの関連性（Business Relevance）] をクリックします。デフォルト ビューに戻すには [リスク（Risk）] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [リスク（Risk）] ビューに戻ることに注意してください。

このグラフのデータは主に [アプリケーション（Applications）] テーブルから取得されます。

アプリケーション詳細リスト

[アプリケーション情報（Application Information）] セクション下部に表示される [アプリケーション詳細リスト（Application Details List）] は、モニタ対象ネットワークで検出される各アプリケーションの推定リスク、推定ビジネス関連度、カテゴリ、ホスト数の情報を示す表です。アプリケーションは、関連ホスト数の降順でリストされます。

[アプリケーション詳細リスト（Application Details List）] テーブルをソートすることはできませんが、テーブル内の項目をクリックして、その情報でフィルタリングまたはドリルダウンしたり、（該当する場合に）アプリケーション情報を表示したりすることができます。このテーブルのデータは主に [アプリケーション（Applications）] テーブルから取得されます。

このリストは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Explorer の時間範囲を変更しても、リストは変化しません。

[セキュリティ インテリジェンス（Security Intelligence）] セクション

Context Explorer の [セキュリティ インテリジェンス（Security Intelligence）] セクションには、3 つのインタラクティブな棒グラフが表示されます。これらのグラフには、モニタ対象ネットワーク上の、ブラックリストに登録されているトラフィック、または Security Intelligence によってモニタされているトラフィックの全体の概要が示されます。これらのグラフでは、カテゴリ、送信元 IP アドレス、および宛先 IP アドレスに基づいてそれらのトラフィックがソートされ、トラフィックの量（KB/秒）と該当する接続の数の両方が表示されます。

[カテゴリ別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Category）] グラフ

[カテゴリ別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Category）] グラフは棒グラフ形式で、モニタ対象ネットワーク上のトラフィックのセキュリティ インテリジェンスの上位のカテゴリに関する、ネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[カテゴリ別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Category）] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント（Security Intelligence Events）] テーブルから取得されます。

[送信元 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Source IP）] グラフ

[送信元 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Source IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上でセキュリティ インテリジェンスによってモニタされたトラフィックの上位の送信元 IP アドレスに関する、ネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[送信元 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Source IP）] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント（Security Intelligence Events）] テーブルから取得されます。

[宛先 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Destination IP）] グラフ

[宛先 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Destination IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上でセキュリティ インテリジェンスによってモニタされたトラフィックの上位の宛先 IP アドレスに関する、ネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[宛先 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Destination IP）] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント（Security Intelligence Events）] テーブルから取得されます。

[侵入情報（Intrusion Information）] セクション

Context Explorer の [侵入情報（Intrusion Information）] セクションには 6 つのインタラクティブ グラフと 1 つの表形式リストが表示されます。これらのグラフとリストは、モニタ対象ネットワークの侵入イベントの概要（侵入イベントに関連付けられている影響レベル、攻撃元、攻撃対象先、ユーザ、優先レベル、およびセキュリティ ゾーンと、侵入イベントの分類、優先度、カウントを示す詳細なリスト）を示します。

[影響別侵入イベント（Intrusion Events by Impact）] グラフ

[影響別侵入イベント（Intrusion Events by Impact）] グラフは円グラフ形式であり、モニタ対象ネットワークの侵入イベントを推定影響レベル（0 ～ 4）のグループごとの割合で表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [侵入イベント（Intrusion Events）] テーブルと [IDS 統計情報（IDS Statistics）] テーブルから取得されます。

[上位の攻撃者（Top Attackers）] グラフ

[上位の攻撃者（Top Attackers）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の（侵入イベントを発生させた）上位の各攻撃元ホスト IP アドレスの侵入イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[上位のユーザ（Top Users）] グラフ

[上位のユーザ（Top Users）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最大侵入イベント数に関連付けられたユーザと、イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [IDS のユーザ統計（IDS User Statistics）] テーブルと [侵入イベント（Intrusion Events）] テーブルから取得されます。このグラフには、権限のあるユーザのデータが表示されます。

[優先度別侵入イベント（Intrusion Events by Priority）] グラフ

[優先度別侵入イベント（Intrusion Events by Priority）] グラフは円グラフ形式であり、モニタ対象ネットワークの侵入イベントを、推定優先度レベル（[高（High）]、[中（Medium）]、[低（Low）] など）のグループごとの割合で表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[上位のターゲット（Top Targets）] グラフ

[上位のターゲット（Top Targets）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の（侵入イベントを発生させた接続で攻撃対象となった）上位のターゲット ホスト（攻撃対象ホスト）の IP アドレスの侵入イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[入力/出力の上位セキュリティ ゾーン（Top Ingress/Egress Security Zones）] グラフ

[入力/出力の上位セキュリティ ゾーン（Top Ingress/Egress Security Zones）] グラフは棒グラフ形式で、モニタ対象ネットワーク上で設定されている各セキュリティ ゾーン（グラフ設定に応じて入力または出力）に関連付けられている侵入イベントの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、出力セキュリティ ゾーンのトラフィックだけが表示されるようにするには、グラフにポインタを置き、表示されたトグルボタンの [出力（Egress）] をクリックします。デフォルトのビューに戻すには、[入力（Ingress）] をクリックします。このグラフは、Context Explorer から外部へ移動しても、デフォルトの [入力（Ingress）] ビューに戻ります。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

このグラフは、必要に応じて、入力（デフォルト）セキュリティ ゾーン情報または出力セキュリティ ゾーン情報のいずれかを表示するように設定できます。

侵入イベント詳細リスト

[侵入情報（Intrusion Information）] セクション下部に表示される [イベント詳細リスト（Event Details List）] は、モニタ対象ネットワークで検出された各侵入イベントの分類、推定優先度、イベント数の情報を示すテーブルです。イベントは、イベント数の降順でリストされます。

[イベント詳細リスト（Event Details List）] テーブルはソートできませんが、テーブルの項目をクリックして、その情報でフィルタリングまたはドリルダウンすることができます。このテーブルのデータは主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[ファイル情報（Files Information）] セクション

Context Explorer の [ファイル情報（Files Information）] セクションには、6 つのインタラクティブ グラフが表示されます。これらのグラフは、モニタ対象ネットワーク上のファイルとマルウェア イベントの概要を示します。

このうち 5 つのグラフには、AMP for Firepower データ（ネットワーク トラフィックで検出されたファイルのファイル タイプ、ファイル名、マルウェアの性質、これらのファイルを送信（アップロード）および受信（ダウンロード）したホスト）が表示されます。最後のグラフには、AMP for Firepower または AMP for Endpoints のどちらで検出されたかにかかわらず、組織内で検出されたすべてのマルウェア脅威が表示されます。

（注）　侵入情報でフィルタリングすると、[ファイル情報（File Information）] セクション全体が非表示になります。

[上位のファイル タイプ（Top File Types）] グラフ

[上位のファイル タイプ（Top File Types）] グラフはドーナツ グラフ形式で、ネットワーク トラフィックで検出されたファイルタイプの割合のビュー（外側のリング）と、ファイルカテゴリのグループごとの割合のビュー（内側のリング）を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイル イベント（File Events）] テーブルから取得されます。

[上位のファイル名（Top File Names）] グラフ

[上位のファイル名（Top File Names）] グラフは棒グラフ形式で、ネットワーク トラフィックで検出された上位の一意のファイル名の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイル イベント（File Events）] テーブルから取得されます。

[性質別ファイル（Files by Disposition）] グラフ

[性質別ファイル（Files by Disposition）] グラフは円グラフ形式であり、AMP for Firepower で検出されたファイルのマルウェアの性質の割合のビューを表示します。Firepower Management Center がマルウェア クラウド検索を行ったファイルにのみ性質が設定されることに注意してください。クラウド検索をトリガーしなかったファイルには、`N/A` という性質が設定されます。`Unavailable` という性質は、Firepower Management Center がマルウェア クラウド検索を実行できなかったことを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイル イベント（File Events）] テーブルから取得されます。

[送信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフ

[送信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフは棒グラフ形式で、ネットワーク トラフィックで検出された、送信ファイル数上位のホストのIPアドレスに関するファイルの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、マルウェアを送信したホストだけが表示されるようにするには、グラフにポインタを置き、表示されたトグル ボタンの [マルウェア（Malware）] をクリックします。デフォルトのファイルのビューに戻すには、[ファイル（Files）] をクリックします。このグラフは、Context Explorer から外部へ移動してもデフォルトのファイルのビューに戻ります。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイル イベント（File Events）] テーブルから取得されます。

[受信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフ

[受信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフは棒グラフ形式で、ネットワーク トラフィックで検出された、受信ファイル数上位のホストの IP アドレスに関するファイルの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、マルウェアを受信したホストだけが表示されるようにするには、グラフにポインタを置き、表示されたトグル ボタンの [マルウェア（Malware）] をクリックします。デフォルトのファイルのビューに戻すには、[ファイル（Files）] をクリックします。このグラフは、Context Explorer から外部へ移動してもデフォルトのファイルのビューに戻ります。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイル イベント（File Events）] テーブルから取得されます。

[上位のマルウェア検出（Top Malware Detections）] グラフ

[上位のマルウェア検出（Top Malware Detections）] グラフは棒グラフ形式で、AMP for Firepower と AMP for Endpoints のいずれによるものかに関係なく、組織で検出された上位のマルウェア脅威の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイル イベント（File Events）] テーブルと [マルウェア イベント（Malware Events）] テーブルから取得されます。

[地理位置情報（Geolocation Information）] セクション

Context Explorer の [地理位置情報（Geolocation Information）] セクションには、3 つのインタラクティブなドーナツ グラフが表示されます。これらのグラフは、モニタ対象ネットワークのホストがデータを交換している国の概要（イニシエータ国またはレスポンダ国ごとの固有接続数、送信元または宛先の国ごとの侵入イベント数、および送信側または受信側の国ごとのファイル イベント数）を示します。

[イニシエータ/レスポンダの国別接続（Connections by Initiator/Responder Country）] グラフの表示

[イニシエータ/レスポンダの国別接続（Connections by Initiator/Responder Country）] グラフはドーナツ グラフ形式であり、ネットワーク上での接続にイニシエータ（デフォルト）またはレスポンダとして関わる国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、接続でレスポンダとなっている国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [レスポンダ（Responder）] をクリックします。デフォルト ビューに戻すには [イニシエータ（Initiator）] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [イニシエータ（Initiator）] ビューに戻ることに注意してください。

このグラフのデータは主に [接続サマリー データ（Connection Summary Data）] テーブルから取得されます。

[送信元/宛先国別侵入イベント（Intrusion Events by Source/Destination Country）] グラフ

[送信元/宛先国別侵入イベント（Intrusion Events by Source/Destination Country）] グラフはドーナツ グラフ形式であり、ネットワーク上の侵入イベントにイベントの送信元（デフォルト）または宛先として関わる国の割合を表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、侵入イベントの宛先となっている国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [宛先（Destination）] をクリックします。デフォルト ビューに戻すには [送信元（Source）] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [送信元（Source）] ビューに戻ることに注意してください。

このグラフのデータは主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[送信側/受信側の国別ファイル イベント（File Events by Sending/Receiving Country）] グラフ

[送信側/受信側の国別ファイル イベント（File Events by Sending/Receiving Country）] グラフはドーナツ グラフ形式であり、ネットワーク上のファイルイベントでファイルの送信側（デフォルト）または受信側として検出された国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、ファイルを受信する国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [受信者（Receiver）] をクリックします。デフォルト ビューに戻すには [送信者（Sender）] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [送信者（Sender）] ビューに戻ることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] テーブルから取得されます。

[URL 情報（URL Information）] セクション

Context Explorer の [URL 情報（URL Information）] セクションには、3 つのインタラクティブな棒グラフが表示されます。これらのグラフには、モニタ対象ネットワーク上のホストがデータを交換するために使用する URL の全体の概要（URL に関連付けられているトラフィックと固有接続数を個々の URL、URL カテゴリ、および URL レピュテーションでソートしたもの）が示されます。URL 情報でフィルタ処理を実行することはできません。

（注）　侵入イベントの情報でフィルタ処理を実行すると、[URL 情報（URL Information）] セクション全体が非表示になります。

このグラフで URL カテゴリとレピュテーション データを含めるには、URL フィルタリング ライセンスを所有している必要があることに注意してください。

[URL 別トラフィック（Traffic by URL）] グラフ

[URL 別トラフィック（Traffic by URL）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最も要求される上位 15 の URL のネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた URL ごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[URL 別トラフィック（Traffic by URL）] グラフは非表示になります。

このグラフで URL カテゴリとレピュテーション データを含めるには、URL フィルタリング ライセンスを所有している必要があることに注意してください。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[URL カテゴリ別トラフィック（Traffic by URL Category）] グラフ

[URL カテゴリ別トラフィック（Traffic by URL Category）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最も要求される URL カテゴリ（`Search Engines` や `Streaming Media` など）のネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた URL カテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[URL カテゴリ別トラフィック（Traffic by URL Category）] グラフは非表示になります。

このグラフで URL カテゴリとレピュテーション データを含めるには、URL フィルタリング ライセンスを所有している必要があることに注意してください。

このグラフのデータは、主に [URL 統計（URL Statistics）] テーブルと [接続イベント（Connection Events）] テーブルから取得されます。

[URL レピュテーション別トラフィック（Traffic by URL Reputation）] グラフ

[URL レピュテーション別トラフィック（Traffic by URL Reputation）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最も要求される URL レピュテーション グループ（`Well known` や `Benign sites with security risks` など）のネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた URL レピュテーションごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[URL レピュテーション別トラフィック（Traffic by URL Reputation）] グラフは非表示になります。

このグラフで URL カテゴリとレピュテーション データを含めるには、URL フィルタリング ライセンスを所有している必要があることに注意してください。

このグラフのデータは、主に [URL 統計（URL Statistics）] テーブルと [接続イベント（Connection Events）] テーブルから取得されます。

Context Explorer の更新

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

Context Explorer は、表示している情報を自動的に更新しません。新しいデータを組み込むには、Explorer を手動で更新する必要があります。

Context Explorer 自体をリロードすると（ブラウザ プログラムの更新または Context Explorer から外部へ移動した後に戻る操作などによるリロード）、すべての表示情報が更新されますが、セクション設定（入力（Ingress）/出力（Egress）グラフや [アプリケーション情報（Application Information）] セクションなど）に対して行った変更は保持されず、また、読み込みに時間がかかることがある点に注意してください。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]を選択します。

ステップ 2 右上にある [リロード（Reload）] をクリックします。
[リロード（Reload）] ボタンは、更新が終了するまでグレー表示になります。

Context Explorer の時間範囲の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

過去 1 時間（デフォルト）から過去 1 年までの期間を反映するように、Context Explorer の時間範囲を設定できます。時間範囲を変更しても、Context Explorer は変更を反映するために自動的に更

新されないことに注意してください。新しい時間範囲を適用するには、Explorer を手動で更新する必要があります。

時間範囲の変更は、Context Explorer から外部に移動したり、ログイン セッションを終了しても維持されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]を選択します。

ステップ 2 [リストを表示（Show the last）] ドロップダウンリストから、時間範囲を選択します。

ステップ 3 オプションで、新しい時間範囲のデータを表示するには、[リロード（Reload）] をクリックします。

ヒント [フィルタの適用（Apply Filters）] をクリックすると、時間範囲の更新が適用されます。

Context Explorer のセクションの最小化および最大化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

Context Explorer では 1 つ以上のセクションを最小化して非表示にできます。これは、特定のセクションだけを強調する場合や、ビューをシンプルにしたい場合に便利です。[トラフィックおよび侵入イベント数/時間（Traffic and Intrusion Event Counts Time）] グラフは最小化できません。

Context Explorer のセクションでは、ページを更新したり、アプライアンスからログアウトしたりしても、設定した最小化または最大化の状態が維持されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]を選択します。

ステップ 2 セクションを最小化するには、セクションのタイトルバーにある最小化アイコン（ー）をクリックします。

ステップ 3 セクションを最大化するには、最小化されたセクションのタイトル バーにある最大化アイコン（□）をクリックします。

Context Explorer データのドリルダウン

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

Context Explorer で許容されている詳細レベルよりもさらに詳細にグラフを調べたりデータをリストしたりするには、当該データのテーブル ビューにドリルダウンします。（[一定期間のトラフィックおよび侵入イベント（Traffic and Intrusion Events over Time）] グラフではドリル ダウンできないことに注意してください。）たとえば、[送信元 IP 別のトラフィック（Traffic by Source IP）] グラフの IP アドレスでドリルダウンすると、[接続イベント（Connection Events）] 表の [アプリケーション詳細付きの接続（Connections with Application Details）] ビューが表示されます。このビューには、選択した送信元 IP アドレスに関連するデータのみが表示されます。

調べるデータのタイプに応じて、コンテキスト メニューに追加のオプションが表示されることがあります。特定の IP アドレスに関連付けられているデータ ポイントの場合、選択した IP アドレスのホストまたはwhois情報を表示するためのオプションが表示されます。特定のアプリケーションに関連付けられているデータ ポイントの場合、選択したアプリケーションに関するアプリケーション情報を表示するためのオプションが表示されます。特定のユーザに関連付けられているデータ ポイントの場合、ユーザのユーザ プロファイル ページを表示するためのオプションが表示されます。侵入イベントのメッセージに関連付けられているデータ ポイントの場合、そのイベントに関連する侵入ルールに関するルール ドキュメントを表示するオプションが表示されます。特定のIPアドレスに関連付けられているデータ ポイントの場合、そのアドレスをブラックリストまたはホワイトリストに追加するためのオプションが表示されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]を選択します。

ステップ 2 [一定期間のトラフィックおよび侵入イベント（Traffic and Intrusion Events over Time）] 以外の任意のセクションで、調査するデータ ポイントをクリックします。

ステップ 3 選択するデータ ポイントに応じて、表示されるオプションが異なります。

- テーブル ビューでこのデータの詳細を表示するには、[詳細な分析を表示（Drill into Analysis）] を選択します。
- 特定の IP アドレスに関連付けられているデータ ポイントを選択している場合に、関連するホストに関する詳細情報を参照するには、[ホスト情報の表示（View Host Information）] を選択します。
- 特定の IP アドレスのデータ ポイントを選択している場合に、そのアドレスで whois 検索を行うには、[Whois] を選択します。
- 特定のアプリケーションに関連付けられているデータ ポイントを選択している場合に、そのアプリケーションに関する詳細情報を参照するには、[アプリケーション情報の表示（View Application Information）] を選択します。
- 特定のユーザに関連付けられているデータ ポイントを選択している場合に、そのユーザに関する詳細情報を参照するには、[ユーザ情報の表示（View User Information）] を選択します。
- 特定の侵入イベント メッセージに関連付けらているデータ ポイントを選択している場合に、関連する侵入ルールに関する詳細情報を参照するには、[ルール ドキュメントの表示（View Rule Documentation）] を選択します。
- 特定の IP アドレスに関連付けられているデータ ポイントを選択している場合に、Security Intelligence グローバル ブラックリストまたはホワイトリストにその IP アドレスを追加するには、[今すぐブラックリストに追加（Blacklist Now）] または [今すぐホワイトリストに追加（Whitelist Now）] のいずれか該当するオプションを選択します。

コンテキスト エクスプローラのフィルタ

コンテキスト エクスプローラに最初に表示される基本的で広範なデータをフィルタリングして、ネットワーク上のアクティビティのより詳細な状況を把握することができます。フィルタは URL 情報以外のすべての種類の Firepower システム データに対応し、除外と包含がサポートされており、Context Explorer のグラフ データ ポイントをクリックするだけですぐに適用でき、Explorer 全体に反映されます。一度に最大 20 のフィルタを適用できます。

コンテキスト エクスプローラ データにフィルタを追加する方法はいくつかあります。

- [フィルタの追加（Add Filter）] ダイアログを使用する。

- コンテキスト メニューを使用する（エクスプローラのデータ ポイントを選択する場合）。
- 特定の詳細表示ページ（[アプリケーションの詳細（Application Detail）]、[ホスト プロファイル（Host Profile）]、[ルールの詳細（Rule Detail）]、[ユーザ プロファイル（User Profile）]）に表示されるテキストリンクを使用する。これらのリンクをクリックすると、コンテキストエクスプローラが自動的に開き、詳細表示ページの当該データに基づいてコンテキストエクスプローラがフィルタリングされます。たとえば、ユーザ `jenkins` のユーザ詳細ページで[コンテキスト エクスプローラ（Context Explorer）] リンクをクリックすると、エクスプローラにはそのユーザに関連するデータだけが表示されます。

ファイル タイプの中には、相互に互換性がないタイプがあります。たとえば、侵入イベント関連のフィルタ（Device や Inline Result など）を、接続イベント関連フィルタ（Access Control Action など）と同時に適用することはできません。これは、システムでは接続イベント データを侵入イベント データによってソートできないためです。互換性のないフィルタの同時適用はシステムによって自動的に防止されます。互換性の問題が存在する場合、より後に適用された方のフィルタタイプと互換性のないタイプのフィルタは非表示になります。

複数のフィルタがアクティブな場合、同じデータ タイプの値は OR 検索条件として扱われます。つまり、いずれか 1 つの値と一致するデータがすべて表示されます。異なるデータ タイプの値は AND 検索条件として扱われます。つまり、データは各フィルタ データ タイプの 1 つ以上の値と一致する必要があります。たとえば、`Application: 2channel`、`Application: Reddit`、および `User: edickinson` というフィルタ セットで表示されるデータは、ユーザ `edickinson` に関連付けられており、**かつ**アプリケーション `2channel` **または**アプリケーション `Reddit` に関連付けられている必要があります。

マルチドメイン展開では、先祖ドメインでコンテキスト エクスプローラを表示している場合に複数の子孫ドメインでフィルタリングできます。この場合、IP Address フィルタも追加する場合は注意してください。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

表示されるデータは、管理対象デバイスのライセンスおよび展開方法やデータを提供する機能を設定するかどうかなどの要因によって異なります。

（注） フィルタは、必要とする正確な Firepower データ コンテキストをいつでも取得できるシンプルかつ俊敏性に優れたツールとして機能します。永続的に設定するものではなく、コンテキストエクスプローラから外部に移動するか、セッションを終了すると消去されます。後で使用するためにフィルタ設定を保存するには、フィルタ処理されたコンテキストエクスプローラ ビューの保存, （1794 ページ）を参照してください。

データ タイプ フィールド オプション

次の表に、フィルタとして使用できるデータ タイプと、各データ タイプの例と説明を示します。

表 *226*：フィルタ データ タイプ

タイプ（Type）	値の例	定義（Definition）
アクセス コントロール アクション（Access Control Action）	`Allow、Block`	トラフィックを許可またはブロックするためにアクセス コントロール ポリシーにより実行されるアクション。
アプリケーション カテゴリ（Application Category）	`web browser、email`	アプリケーションの主要機能の一般的な分類。
アプリケーション	`Facebook、HTTP`	アプリケーションの名前。
アプリケーションのリスク（Application Risk）	`Very High、Medium`	アプリケーションの推定セキュリティ リスク。
アプリケーション タグ（Application Tag）	`encrypts communications、sends mail`	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを使用できます（タグを使用しないことも可能です）。
アプリケーション タイプ（Application Type）	`Client、Web Application`	アプリケーション タイプ（アプリケーション プロトコル、クライアント、または Web アプリケーション）。
ビジネスとの関連性（Business Relevance）	`Very Low、High`	（娯楽ではない）ビジネス アクティビティに対するアプリケーションの推定関連度。
大陸（Continent）	`North America、Asia`	モニタ対象ネットワークで検出されたルーティング可能な IP アドレスに関連付けられている大陸。
国（Country）	`Canada、Japan`	モニタ対象ネットワークで検出されたルーティング可能な IP アドレスに関連付けられている国。
Device	`device1.example.com、192.168.1.3`	モニタ対象ネットワーク上のデバイスの名前または IP アドレス。
ドメイン（Domain）	`Asia Division、Europe Division`	グラフ表示するネットワーク アクティビティを行うデバイスのドメイン。このデータ タイプはマルチドメイン展開の場合にのみ存在します。
イベントの分類（Event Classification）	`Potential Corporate Policy Violation、Attempted Denial of Service`	侵入イベントの簡単な説明。侵入イベントをトリガーしたルール、デコーダ、またはプリプロセッサにより決定されます。

タイプ（Type）	値の例	定義（Definition）
イベント メッセージ（Event Message）	`dns response、P2P`	イベントによって生成されるメッセージ。イベントをトリガーしたルール、デコーダ、またはプリプロセッサにより決定されます。
ファイル傾向（File Disposition）	`Malware、Clean`	Firepower Management Center によるマルウェア クラウド検索の実行対象ファイルの性質。
ファイル名	`Packages.bz2`	ネットワーク トラフィックで検出されたファイルの名前。
ファイル SHA256（File SHA256）	任意の 32 ビット文字列	Firepower Management Center によるマルウェア クラウド検索の実行対象ファイルの SHA-256 ハッシュ値。
ファイル タイプ（File Type）	`GZ、SWF、MOV`	ネットワーク トラフィックで検出されたファイルのタイプ。
ファイル タイプ カテゴリ（File Type Category）	`Archive、Multimedia、Executables`	ネットワーク トラフィックで検出されたファイルのタイプの一般カテゴリ。
[IPアドレス（IP Address）]	`192.168.1.3、2001:0db8:85a3::0000/24`	IPv4 または IPv6 のアドレス、アドレス範囲、またはアドレス ブロック。 IP アドレスを検索すると、そのアドレスが送信元または宛先のいずれかになっているイベントが返されることに注意してください。
影響レベル（Impact Level）	`Impact Level 1、Impact Level 2`	モニタ対象ネットワークでのイベントの推定影響レベル。
インライン結果（Inline Result）	`dropped、would have dropped`	トラフィックがドロップされたか、ドロップされた可能性があるか、またはシステムによりトラフィックが処理されていないかのいずれかです。
IOC カテゴリ（IOC Category）	`High Impact Attack、Malware Detected`	トリガーとして使用された侵害の兆候（IOC）イベントのカテゴリ。
IOC イベント タイプ（IOC Event Type）	`exploit-kit、malware-backdoor`	特定の侵害の兆候（IOC）に関連付けられている ID。その兆候をトリガーしたイベントを示します。
マルウェア脅威名（Malware Threat Name）	`W32.Trojan.a6b1`	マルウェア脅威の名前。
OS 名（OS Name）	`Windows、Linux`	オペレーティング システムの名前。
OS Version	`XP、2.6`	オペレーティング システムの特定のバージョン。

タイプ（Type）	値の例	定義（Definition）
[プライオリティ（Priority）]	`high`、`low`	イベントの推定緊急度。
セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）	`Malware`、`Spam`	セキュリティ インテリジェンスにより判別される危険なトラフィックのカテゴリ。
セキュリティ ゾーン	`My Security Zone`、`Security Zone X`	トラフィックが分析されたインターフェイスのセット。インライン展開の場合は、トラフィックが通過するインターフェイスのセット。
SSL	`yes`、`no`	SSL暗号化トラフィックまたはTLS暗号化トラフィック。
ユーザ（User）	`wsmith`、`mtwain`	モニタ対象ネットワーク上のホストにログインしたユーザの ID。

[フィルタの追加（Add Filter）] ウィンドウからのフィルタの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

この手順を使用して、[フィルタの追加（Add Filter）] ウィンドウでフィルタを最初から作成します。（コンテキスト メニューを使用して、クイック フィルタを作成することもできます。）

Context Explorer の左上にある [フィルタ（Filters）] の下のプラス アイコン（+）をクリックすると表示される [フィルタの追加（Add Filter）] ウィンドウには、次の 2 つのフィールドだけが表示されます。

- [データ タイプ（Data Type）] ドロップダウンリストには、Context Explorer に制約を適用するために使用できる多数の Firepower システム データ タイプが含まれています。データ タイプの選択後に、そのタイプの固有の値を [フィルタ（Filter）] フィールドに入力します（たとえば、[大陸（Continent）] タイプの場合は値 [アジア（Asia）] など）。ユーザ支援のため、[フィルタ（Filter）] フィールドでは、選択したデータ タイプのさまざまな値の例がグレー表示で示されます。（フィールドにデータを入力すると、これらは消去されます。）
- [フィルタ（Filter）] フィールドには、イベント検索と同様に、* や ! などの特殊検索パラメータを入力できます。フィルタ パラメータの前に ! 記号を付けることで排他的なフィルタを作成できます。

（注） 追加したフィルタは自動的には適用されません。Context Explorer でフィルタを表示するには、[フィルタの適用（Apply Filters）] をクリックする必要があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]を選択します。

ステップ 2 左上にある [フィルタ（Filter）] の下で、プラス アイコン（+）をクリックします。

ステップ 3 [データ タイプ（Data Type）] ドロップダウンリストから、フィルタリングの条件として使用するデータ タイプを選択します。

ステップ 4 [フィルタ（Filter）] フィールドに、フィルタリングの条件として使用するデータ タイプ値を入力します。

ステップ 5 [OK] をクリックします。

ステップ 6 オプションで、前述の手順を繰り返し、必要なフィルタ セットが設定されるまで、フィルタを追加します。

ステップ 7 [フィルタの適用（Apply Filters）] をクリックします。

コンテキスト メニューからのクイック フィルタの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

Context Explorer のグラフとリストデータを詳しく調べるときに、データ ポイントをクリックし、コンテキスト メニューを使用してそのデータに基づいてフィルタ（包含または除外）を簡単に作成できます。コンテキスト メニューを使用して、[アプリケーション（Application）]、[ユーザ（User）]、[侵入イベント メッセージ（Intrusion Event Message）] データ タイプの情報、あるいは任意の個別ホストでフィルタリングする場合、フィルタ ウィジェットには、そのデータ タイプの該当する詳細ページ（アプリケーション データの場合は [アプリケーションの詳細（Application Detail）] など）にリンクするウィジェット情報アイコンが表示されます。URL データではフィルタリングできないことに注意してください。

特定のグラフまたはリストのデータを詳しく調査する場合にもコンテキスト メニューを使用できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]を選択します。

ステップ 2 [一定期間のトラフィックおよび侵入イベント（Traffic and Intrusion Events over Time）] セクションと URL データを含むセクション以外の Explorer セクションで、フィルタリングするデータ ポイントをクリックします。

ステップ 3 次の 2 つの対処法があります。

- このデータにフィルタを追加するには、[フィルタの追加（Add Filter）] をクリックします。
- このデータに除外フィルタを追加するには、[除外フィルタの追加（Add Exclude Filter）] をクリックします。このフィルタが適用されると、除外された値に関連付けられて**いない**すべてのデータが表示されます。除外フィルタでは、フィルタ値の前に感嘆符（!）が表示されます。

フィルタ処理されたコンテキスト エクスプローラ ビューの保存

コンテキスト エクスプローラから外部に移動した後、またはセッションを終了した後に、コンテキスト エクスプローラのフィルタ設定を保持するには、適切なフィルタを適用したコンテキスト エクスプローラのブラウザ ブックマークを作成します。適用されるフィルタはコンテキスト エクスプローラ ページ URL に組み込まれているので、そのページのブックマークを読み込むと、対応するフィルタも読み込まれます。

手順

適切なフィルタが適用されたコンテキスト エクスプ ローラーのブラウザ ブックマークを作成します。

フィルタ データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]を選択します。

ステップ 2 該当するフィルタ ウィジェットの情報アイコン（  ）をクリックします。

フィルタの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 [分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]を選択します。

ステップ 2 左上の [フィルタ（Filters）] の下で、任意のフィルタ ウィジェットのクリア アイコン（  ）をクリックします。

ヒント すべてのフィルタを一括削除するには、[クリア（Clear）] ボタンをクリックします。

第 77 章

ネットワーク マップの使用

ここでは、ネットワーク マップの使用方法について説明します。

ネットワーク マップ

Firepower システムは、ネットワークを通じて送信されるトラフィックをモニタし、トラフィック データを復号化してから、設定されているオペレーティング システムおよびフィンガープリントとそのデータを比較します。このシステムでは、次にそのデータを使用して、ネットワーク マップというネットワークの詳細な表示を生成します。マルチドメイン展開では、システムはリーフドメインごとの個々のネットワーク マップを生成します。

システムは、ネットワーク検出ポリシーのモニタリングで特定された管理対象デバイスからデータを収集します。管理対象デバイスでは、モニタされたトラフィックから直接ネットワーク アセットを検出したり、処理された NetFlow レコードから間接的にネットワーク アセットを検出したりします。複数のデバイスで同じネットワーク アセットを検出した場合、システムではそれらの情報をまとめてそのアセットの複合表示を生成します。

受動的に検出されるデータを補完するには、次のようにします。

- オープンソースの Nmap™ スキャナを使用してホストをアクティブにスキャンして、そのスキャン結果をネットワーク マップに追加します。
- ホスト入力機能を使用して、サードパーティ製のアプリケーションからホストデータを手動で追加できます。

ネットワークマップには、検出されたホストとネットワークデバイスの観点から見たネットワーク トポロジが表示されます。

ネットワーク マップを使用すれば、次のことを行えます。

- ネットワークの全体的なビューを即座に入手できます。

- 実行する分析に適したさまざまなビューを選択できます。ネットワーク マップの各ビューの形式は、展開可能なカテゴリおよびサブカテゴリを持つ階層ツリーからなる、同一の形式です。カテゴリをクリックすると、展開して、その下のサブカテゴリが表示されます。
- カスタム トポロジ機能を使用してサブネットを整理して識別できます。たとえば、組織の各部署が異なるサブネットを使用している場合、カスタム トポロジ機能を使用して、それらのサブネットに分かりやすいラベルを割り当てることができます。
- 任意のモニタ対象ホストのホスト プロファイルにドリルダウンすれば、詳細情報を表示できます。
- アセットの調査が不要になった場合は、そのアセットを削除できます。

（注） システムは、ネットワーク マップから削除されたホストに関連付けられているアクティビティを検出した場合、そのホストをネットワーク マップに再度追加します。同様に、削除されたアプリケーションは、システムでアプリケーションの変更（たとえば、Apache Web サーバが新しいバージョンにアップグレードされた場合）を検出すると、ネットワーク マップに再度追加されます。システムが特定のホストを脆弱にする変更を検出した場合、それらのホストの脆弱性が再びアクティブにされます。

ヒント ネットワーク マップからホストまたはサブネットを永続的に除外するには、ネットワーク検出ポリシーを変更します。ロード バランサおよび NAT デバイスで過剰なイベントまたは無関係なイベントを生成していることが判明した場合は、それらのデバイスをモニタリングから除外することができます。

関連トピック

ネットワーク検出ポリシーの設定, （1551 ページ）

ホストのネットワーク マップ

[ホスト（Hosts）] タブのネットワーク マップには、ホスト数と、ホストの IP アドレスと MAC アドレスのリストが表示されます。各アドレスまたはアドレスの一部は、次のレベルへのリンクです。このネットワーク マップ ビューは、ホストに 1 つの IP アドレスまたは複数の IP アドレスがあるかを問わず、システムによって検出されたすべての一意のホスト数を表示します。

ホストのネットワーク マップを使用して、サブネットによって階層ツリーに整理されたネットワークのホストを参照でき、特定のホストのホスト プロファイルにドリルダウンできます。

システムは、ホストをエクスポートされた NetFlow レコードからネットワーク マップに追加できますが、これらのホストに使用できる情報は限られます（NetFlowデータと管理対象デバイスデータの違い, （1442 ページ） を参照）。

ネットワークのカスタム トポロジを作成して、サブネットに意味のあるラベル（部門名など）を割り当てることができます。これはホストのネットワーク マップで表示されます。また、カスタム トポロジで指定した組織に基づいてホストのネットワーク マップを表示することもできます。

ホストのネットワーク マップからネットワーク全体、サブネット、または個々のホストを削除できます。ホストがネットワークに接続されていないことがわかっている場合など、分析を効率化するために削除できます。システムは削除されたホストに関連付けられたアクティビティを後で検出すると、ネットワーク マップにホストを再追加します。ネットワーク マップからホストまたはサブネットを永続的に除外するには、ネットワーク検出ポリシーを変更します。

注意 ネットワーク デバイスをネットワーク マップから削除しないでください。システムがネットワーク トポロジを判断するために必要です。

ネットワーク デバイスのネットワーク マップ

[ネットワーク デバイス（Network Devices）] タブのネットワーク マップには、ネットワークの 1 つのセグメントを別のセグメントに接続するネットワーク デバイス（ブリッジ、ルータ、NAT デバイス、およびロード バランサ）が表示されます。このマップには、IP アドレスで特定されたデバイスと、MAC アドレスで特定されたデバイスがリストされる 2 つのセクションがあります。

また、このマップには、デバイスに保持されている IP アドレスが 1 つか複数かに関係なく、システムによって検出されたすべての一意のネットワーク デバイスの数も表示されます。

ネットワークのカスタム トポロジを作成した場合、サブネットに割り当てられているラベルがネットワーク デバイスのネットワーク マップに表示されます。

ネットワーク デバイスを識別するためにシステムで使用される方法には、次のものがあります。

- Cisco Discovery Protocol（CDP）メッセージの分析。ネットワーク デバイスとそれらのタイプを識別できます（シスコ デバイスのみ）。
- スパニング ツリー プロトコル（STP）の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。

ネットワーク デバイスが CDP を使用して通信している場合、1 つ以上の IP アドレスを保持している可能性があります。ネットワーク デバイスが STP を使用して通信している場合は、1 つの MAC アドレスのみを保持している可能性があります。

ネットワーク デバイスをネットワーク マップから削除することはできません。これは、システムでそれらの場所を使用してネットワーク トポロジを判断するためです。

ネットワーク デバイスのホスト プロファイルには、[オペレーティング システム（Operating Systems）] セクションではなく [システム（Systems）] セクションがあります。このセクションに

は、ネットワーク デバイスの背後で検出されたモバイル デバイスすべてのハードウェア プラットフォームが反映された[ハードウェア（Hardware）]列が含まれています。[システム（Systems）]の下にハードウェアプラットフォームの値が表示され場合、システムは、ネットワークデバイスの背後で 1 つ以上のモバイル デバイスが検出されたことを示しています。モバイル デバイスはハードウェア プラットフォームの情報を持っていることも、持っていないこともありますが、モバイルデバイスではないシステムではハードウェアプラットフォーム情報は検出されないことに注意してください。

モバイル デバイスのネットワーク マップ

[モバイル デバイス（Mobile Devices）] タブのネットワーク マップには、ネットワークに接続されているモバイルデバイスが表示されます。また、このネットワークマップには、デバイスに設定されている IP アドレスが 1 つか複数かに関係なく、システムによって検出されたすべての一意のモバイル デバイスの数も表示されます。

各アドレスまたはアドレスの一部分は、次のレベルへのリンクです。また、サブネットまたは IP アドレスを削除することもできます。そして、システムでそのデバイスを再検出すると、そのデバイスをネットワーク マップに再度追加します。

さらに、ドリルダウンしてモバイルデバイスのホストプロファイルを表示することもできます。

モバイル デバイスを特定するために、システムでは次のことを行います。

- モバイル デバイスのモバイル ブラウザからの HTTP トラフィック内のユーザ エージェントの文字列を分析します。
- 特定のモバイル アプリケーションの HTTP トラフィックをモニタします。

ネットワークのカスタム トポロジを作成した場合、サブネットに割り当てられているラベルがモバイル デバイスのネットワーク マップに表示されます。

侵害の兆候のネットワーク マップ

[侵害の兆候（Indications of Compromise）] タブのネットワーク マップには、ネットワーク上で侵害されたホストが IOS カテゴリ別に編成されて表示されます。影響を受けているホストは各カテゴリの下に表示されます。各アドレスまたはアドレスの一部は、次のレベルへのリンクです。

システムは、ホストのセキュリティ侵害のステータスを判断するために、侵入イベント、セキュリティ インテリジェンス、Cisco Advanced Malware Protection（AMP）を含む複数のソースからのデータを使用します。

[侵害の兆候（Indications of Compromise）] タブのネットワーク マップから、何らかのセキュリティ侵害を受けたと判断される各ホストのホスト プロファイルを表示できます。さらに、IOC カテゴリまたは特定のホストを削除でき（解決済みにする）、これによって当該ホストから IOC タグが削除されます。たとえば、問題が対応済みで、繰り返し発生する可能性が低いと判断した場合に、IOC カテゴリをネットワーク マップから削除できます。

ネットワーク マップのホストやIOCカテゴリを解決済みにしても、ネットワークからは削除されません。システムがその IOC をトリガーする情報を新たに検出すると、解決済みのホストまたは IOC カテゴリはネットワーク マップに再表示されます。

アプリケーション プロトコルのネットワーク マップ

[アプリケーション プロトコル（Application Protocols）] タブのネットワーク マップには、ネットワークで稼働しているアプリケーションが、アプリケーション名、ベンダー、バージョン、各アプリケーションを実行しているホストを基準とした階層ツリー形式で表示されます。

システムが検出するアプリケーションは、システム ソフトウェアや VDB が更新された場合や、アドオンディテクタをインポートした場合に変わることがあります。各システムまたはVDBアップデートのリリース ノートまたはアドバイザリ テキストには、新規および更新されたディテクタの情報が含まれています。ディテクタを網羅した最新のリストについては、Cisco のサポート サイト（http://www.cisco.com/cisco/web/support/index.html）を参照してください。

このネットワーク マップから、特定のアプリケーションを実行している各ホストのホスト プロファイルを確認できます。

また、アプリケーションのカテゴリ、すべてのホストで実行されているアプリケーション、あるいは特定のホストで実行されているアプリケーションを削除することもできます。たとえば、あるアプリケーションがホスト上で無効化されているとわかっており、システムによる影響レベルの認定で使用されないようにする場合は、そのアプリケーションをネットワーク マップから削除します。

ネットワーク マップからアプリケーションを削除しても、ネットワークからは削除されません。削除したアプリケーションは、システムがアプリケーションの変更（たとえばApache Webサーバが新しいバージョンにアップグレードされた）を検出するか、ユーザがシステムの検出機能を再起動すると、ネットワーク マップに再表示されます。

何を削除するかによって、動作は次のように異なります。

- アプリケーション カテゴリ：アプリケーション カテゴリを削除すると、そのアプリケーション カテゴリがネットワーク マップから除去されます。削除したカテゴリの下にあるすべてのアプリケーションは、そのアプリケーションを含むすべてのホストプロファイルから削除されます。

  たとえば、[http] を削除した場合、[http] として示されるすべてのアプリケーションがすべてのホストプロファイルから削除され、[http]はネットワーク マップのアプリケーション ビューに表示されなくなります。

- 特定のアプリケーション、ベンダー、バージョン：これらの要素を削除すると、関連するアプリケーションがネットワーク マップから除去され、そのアプリケーションを含むホストプロファイルからもアプリケーションが除去されます。

  たとえば、[http] カテゴリを展開し、[Apache] を削除すると、[Apache] としてリストされているすべてのアプリケーションは、[Apache] の下にリストされているバージョンを問わず、それらを含むホストプロファイルから削除されます。同様に、[Apache] を削除する代わりに、特定のバージョン（[1.3.17] など）を削除すると、影響を受けるホスト プロファイルから、選択されたバージョンだけが削除されます。

- 特定の IP アドレス：IP アドレスを削除すると、その IP アドレスがアプリケーション リストから除去され、選択した IP アドレスのホスト プロファイルからアプリケーション自体が除去されます。

  たとえば、[http]、[Apache]、[1.3.17 (Win32)] の順に展開し、[172.16.1.50:80/tcp] を削除すると、Apache 1.3.17（Win32）アプリケーションは IP アドレス 172.16.1.50 のホスト プロファイルから削除されます。

[脆弱性（Vulnerabilities）] のネットワーク マップ

[脆弱性（Vulnerabilities）] タブのネットワーク マップには、システムによってネットワークで検出された脆弱性がレガシーの脆弱性 ID（SVID）、Bugtraq ID、CVE ID、または Snort ID ごとに編成されて表示されます。脆弱性は、デフォルトでは SVID ごとに表示されます。脆弱性は ID 番号順に並べられ、影響を受けるホストが各脆弱性の下にリストされます。

このネットワーク マップから、特定の脆弱性の詳細、および特定の脆弱性の影響を受けるホストのホスト プロファイルを表示できます。この情報は、影響を受ける特定のホストに対するその脆弱性によって生じる脅威を評価するために役立ちます。

特定の脆弱性がネットワーク上のホストに該当しないと判断した場合（たとえば、パッチの適用が完了した場合）、その脆弱性を非アクティブ化できます。非アクティブ化された脆弱性はネットワーク マップに表示され続けますが、これまで影響を受けていたそれらのホストの IP アドレスはグレーのイタリック体で表示されます。それらのホストのホスト プロファイルには、非アクティブ化された脆弱性は無効と表示されますが、個々のホストについて手動で有効とマークすることができます。

ホスト上のアプリケーションまたはオペレーティング システムにアイデンティティの競合がある場合、システムは可能性のあるアイデンティティの両方について脆弱性をリスト表示します。アイデンティティの競合が解決された場合、その脆弱性は現在のアイデンティティに関連付けられたままになります。

ネットワーク マップには、デフォルトではパケットにアプリケーションのベンダーとバージョンが含まれている場合にのみ、検出されたアプリケーションの脆弱性が表示されます。ただし、Firepower Management Center の構成でアプリケーションの脆弱性マッピングの設定を有効化することで、ベンダーとバージョンのデータがないアプリケーションの脆弱性をリストするようにシステムを設定できます。

脆弱性 ID（または脆弱性 ID の範囲）の隣の数字は、次の 2 つのカウントを表しています。

影響を受けるホスト数

最初の数字は、1 つまたは複数の脆弱性の影響を受ける 1 台とは限らないホストのカウントです。1 台のホストが複数の脆弱性の影響を受ける場合、このカウントは複数回数えられます。このため、このカウントがネットワーク上のホスト数を上回ることがありえます。脆弱性を非アクティブ化すると、このカウントはその脆弱性の影響を受ける可能性のあるホスト数の分減少します。1 つまたは複数の脆弱性の影響を受ける可能性のあるホストについて、脆弱性を 1 つも非アクティブ化していない場合、このカウントは表示されません。

影響を受ける可能性のあるホスト数

2 番目の数字は、1 つまたは複数の脆弱性の影響を受ける可能性があるとシステムが判断した 1 台とは限らないホストの総数のカウントです。

脆弱性を非アクティブ化すると、指定したホストについてのみ脆弱性が非アクティブになります。脆弱と判断されたすべてのホストか、指定した個々の脆弱なホストの脆弱性を非アクティブ化することができます。脆弱性が非アクティブ化されると、該当するホストの IP アドレスはネットワーク マップにグレーのイタリック体で表示されます。また、それらのホストのホストプロファイルでは、非アクティブ化された脆弱性が無効と表示されます。

その後でシステムが脆弱性が非アクティブ化されていないホストに（たとえば、ネットワーク マップ内の新しいホストに）その脆弱性を検出すると、システムはそのホストの脆弱性をアクティブ化します。新たに検出された脆弱性は明示的に非アクティブ化する必要があります。また、システムでは、ホストのオペレーティング システムまたはアプリケーションの変更を検出すると、関連付けられている非アクティブ化された脆弱性を再度アクティブ化することがあります。

ホスト属性のネットワーク マップ

[ホスト属性（Host Attributes）] タブのネットワーク マップには、ネットワーク上のホストがユーザ定義ホスト属性またはコンプライアンスホワイトリストホスト属性のいずれかを基準に編成されて表示されます。この表示では、定義済みホスト属性を使用してホストを編成することはできません。

ホストを編成するために使用するホスト属性を選択すると、Firepower Management Center はネットワーク マップで使用可能なその属性の値をリストし、割り当てられた値に基づいてホストをグループ化します。たとえば、ホワイトリスト ホスト属性でホストを編成することにすると、システムは [準拠（Compliant）]、[非準拠（Non-Compliant）]、[評価されていない（Not Evaluated）] カテゴリでホストを表示します。

また、特定のホスト属性値が割り当てられた任意のホストのホスト プロファイルを表示することもできます。

関連トピック

ホスト プロファイル内のホスト属性, （2077 ページ）

ネットワーク マップの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Any Security Analyst

手順

ステップ 1 [分析（Analysis）] > [ホスト（Hosts）] > [ネットワーク マップ（Network Map）]を選択します。

ステップ 2 表示するネットワーク マップのタブをクリックします。

ステップ 3 必要に応じて、以下の操作を続行します。

- ドメインの選択：マルチドメイン展開では、[ドメイン（Domain）] ドロップダウン リストからリーフ ドメインを選択します。
- ホストのフィルタリング：IP または MAC アドレスでフィルタリングするには、検索フィールドにアドレスを入力します。検索をクリアするには、クリアアイコン（✖）をクリックします。
- ドリル ダウン：カテゴリまたはホスト プロファイルを調べる場合、マップのカテゴリまたはサブネットからドリルダウンします。カスタム トポロジを定義した場合、[ホスト（host）] タブから [(トポロジ)（(topology)）] をクリックしてそのトポロジを表示し、デフォルトのビューに戻したい場合は、[(ホスト)（(hosts)）] をクリックします。
- 削除：該当する要素の横にある削除アイコン（）をクリックし、以下のことを行います。
  - [ホスト（Hosts）]、[ネットワーク デバイス（Network Devices）]、[モバイル デバイス（Mobile Devices）]、[アプリケーション プロトコル（Application Protocols）] タブのマップから要素を削除する。
  - [侵害の兆候（Indications of Compromise）] タブで IOC カテゴリ、侵害されたホスト、侵害されたホストのグループを解決済みとしてマークを付ける。
  - [脆弱性（Vulnerabilities）] タブですべてのホストまたは単一ホストの脆弱性を非アクティブ化する。
- 脆弱性クラスの指定：[脆弱性（Vulnerabilities）] タブで、[タイプ（Type）] ドロップダウン リストから、表示する脆弱性のクラスを選択します。
- 組織属性の指定：[ホスト属性（Host Attributes）] タブで、[属性（Attribute）] ドロップダウン リストから属性を選択します。

関連トピック

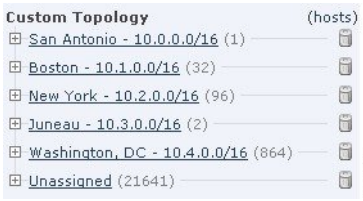
カスタム ネットワーク トポロジ, （1805 ページ）
ホスト プロファイル, （2055 ページ）

カスタム ネットワーク トポロジ

ホストおよびネットワークデバイスのネットワークマップでサブネットを整理および識別するために、カスタム トポロジ機能を使用します。

たとえば、部門内の各部署が異なるサブネットを使用している場合、カスタム トポロジ機能を使用して、これらのサブネットにラベルを付けられます。

また、カスタム トポロジで指定した部門に基づいてホストのネットワークマップを表示することもできます。



次のいずれかまたはすべての方法でカスタム トポロジのネットワークを指定できます。

- ネットワーク検出ポリシーからネットワークをインポートして、システムでモニタするように設定したネットワークをトポロジに追加します。
- 手動でネットワークをトポロジに追加します。

[カスタム トポロジ（Custom Topology）]ページにカスタム トポロジと各トポロジのステータスが一覧表示されます。ポリシー名の隣の電球アイコンが点灯している場合、そのトポロジはアクティブで、ネットワーク マップに影響します。消灯している場合、トポロジは非アクティブです。

関連トピック

ホストのネットワーク マップ，（1798 ページ）
ネットワーク デバイスのネットワーク マップ，（1799 ページ）

カスタム トポロジの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 ツールバーで [カスタム トポロジ（Custom Topology）] をクリックします。

ステップ 3 [トポロジの作成（Create Topology）] をクリックします。

ステップ 4 名前を入力します。

ステップ 5 必要に応じて、[説明（Description）] を入力します。

ステップ 6 トポロジにネットワークを追加します。次の方法のいずれかまたはすべてを使用できます。

- ネットワーク検出ポリシーからのネットワークのインポート, （1806 ページ）の説明に従って、ネットワーク検出ポリシーからネットワークをインポートします。
- 手動によるカスタム トポロジへのネットワークの追加, （1807 ページ）の説明に従って、手動でネットワークを追加します。

ステップ 7 [保存（Save）] をクリックします。

次の作業

- トポロジをアクティブ化します。詳細については、カスタム トポロジのアクティブおよび非アクティブの設定, （1808 ページ）を参照してください。

ネットワーク検出ポリシーからのネットワークのインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

手順

ステップ 1 ネットワークをインポートするカスタム トポロジにアクセスします。

- カスタム トポロジを作成します。カスタム トポロジの作成, （1805 ページ）を参照してください。

- 既存のカスタム トポロジを編集します。カスタム トポロジの編集, （1809 ページ）を参照してください。

ステップ 2 [ポリシー ネットワークのインポート（Import Policy Networks）] をクリックします。

ステップ 3 [ロード（Load）] をクリックします。システムにより、ネットワーク検出ポリシーのトポロジ情報が表示されます。

ステップ 4 トポロジを修正するには、次の手順を実行します。

- トポロジ内のネットワーク名を変更するには、ネットワークの横にある編集アイコン（）をクリックし、名前を入力してから [名前の変更（Rename）] をクリックします。
- トポロジからネットワークを削除するには、削除アイコン（）をクリックしてから [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

次の作業

- トポロジをアクティブ化します。詳細については、カスタムトポロジのアクティブおよび非アクティブの設定, （1808 ページ）を参照してください。

手動によるカスタム トポロジへのネットワークの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

手順

ステップ 1 ネットワークを追加するカスタム トポロジにアクセスします。

- カスタム トポロジを作成します。カスタム トポロジの作成, （1805 ページ）を参照してください。

- 既存のカスタム トポロジを編集します。カスタム トポロジの編集, （1809 ページ）を参照してください。

ステップ 2 [ネットワークの追加（Add Network）] をクリックします。

ステップ 3 ホストとネットワーク デバイスのネットワーク マップでネットワークのカスタム ラベルを追加するには、[名前（Name）] を入力します。

ステップ 4 追加するネットワークを表す [IP アドレス（IP Address）] と [ネットマスク（Netmask）]（IPv4）を入力します。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- トポロジをアクティブ化します。詳細については、カスタム トポロジのアクティブおよび非アクティブの設定, （1808 ページ）を参照してください。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）

カスタム トポロジのアクティブおよび非アクティブの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

（注） 常に 1 つのカスタム トポロジのみアクティブにできます。複数のトポロジを作成した場合、1 つをアクティブ化すると、自動的に現在アクティブなトポロジが非アクティブになります。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム トポロジ（Custom Topology）] を選択します。

ステップ 3 アクティブまたは非アクティブにするトポロジの横にあるスライダをクリックします。

カスタム トポロジの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

アクティブ トポロジに加える変更はただちに有効になります。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム トポロジ（Custom Topology）] をクリックします。

ステップ 3 編集するトポロジの横にある編集アイコン（  ）をクリックします。

ステップ 4 カスタム トポロジの作成, （1805 ページ）の説明に従って、トポロジを編集します。

ステップ 5 [保存（Save）] をクリックします。

第 78 章

インシデント

次のトピックでは、インシデント処理を設定する方法について説明します。

インシデント対応について

インシデント対応とは、セキュリティ ポリシーの違反が疑われる場合に組織が取る対応を指します。Firepowerシステムには、インシデントの調査に関連する情報の収集および処理をサポートする機能が含まれます。これらの機能を使用して、インシデントに関連する可能性のある侵入イベントおよびパケット データを収集することができます。攻撃の影響を軽減するためにFirepowerシステムの外部で実行するアクティビティに関する記録のためのリポジトリとしてインシデントを使用できます。たとえば、セキュリティ ポリシーによって、ネットワークの安全性に問題のあるホストの検疫が要求される場合は、インシデントにそのことを記録できます。

Firepowerシステムはインシデントのライフ サイクルもサポートします。これにより、攻撃への対応を進めるごとに、インシデントのステータスを変更できます。インシデントを閉じるときに、学んだ教訓の結果としてセキュリティ ポリシーに加えた変更を記録できます。

インシデントの定義

一般的に、インシデントとは、セキュリティ ポリシー違反の可能性があることが疑われる、1つ以上の侵入イベントと定義されます。Firepowerシステムでは、この用語は、インシデントへの応答を追跡するために使用できる機能について記述しています。

一部の侵入イベントは、ネットワーク資産の可用性、機密性、および整合性の点で他のイベントよりも重要になります。たとえば、ポート スキャン検出では、ネットワークでのポート スキャン

アクティビティについて通知することができます。しかし、セキュリティ ポリシーでは、ポートスキャンが明確に禁止されていなかったり、優先度の高い脅威とは見なされていなかったりすることがあります。それで、直接的なアクションの実行はしないで、代わりにすべてのポート スキャンのログを後の調査のために保持しておくことができます。

一方、ネットワーク内のホストが侵害されていることを示す、分散型サービス拒否（DDoS）攻撃に関係したイベントをシステムが生成する場合、そのアクティビティはセキュリティ ポリシーの明確な違反であると考えられます。それで、これらのイベントを調査して追跡できるように、Firepower システムでインシデントを作成する必要があります。

共通のインシデント対応プロセス

準備（Preparation）

インシデントの準備には次の 2 通りの方法があります。

- 明確で包括的なセキュリティ ポリシーと、それらを施行するためのハードウェアおよびソフトウェア リソースを配置する
- インシデントに対応するための明確に定義された計画と、その計画を実行できる適切なトレーニングを受けたチームを配置する

インシデント対応において重要なのは、ネットワークのどの部分が最も大きなリスクとなるかを理解することです。これらのネットワーク セグメントに Firepower システムを展開することで、インシデントがいつどのように発生するかについて理解を深めることができます。また、時間をかけて各管理対象デバイスに対する侵入ポリシーを慎重に調整することによって、生成されるイベントの品質を最大限に高めることができます。

検出と通知

インシデントを検出できなければ、インシデントに対応できません。インシデント対応プロセスでは、検出できるセキュリティ関連イベントのタイプと、それらを検出するために使用するメカニズム（ソフトウェアとハードウェアの両方）を識別する必要があります。また、セキュリティ ポリシーの違反を検出できるケースにも注意する必要があります。積極的あるいは受動的にモニタされないセグメントがネットワークに含まれている場合は、それらのセグメントにも注意する必要があります。

ユーザがネットワークに展開する管理対象デバイスは、それらがインストールされているセグメントのトラフィックの分析、侵入の検知、およびそれらを説明するイベントの生成を行う必要があります。各管理対象デバイスに展開するアクセス コントロール ポリシーが、検出するアクティビティの種類と優先度に影響を与えることに注意してください。インシデント チームが数百のイベントを取捨選択しなくてもよいように、特定のタイプの侵入イベントに対して通知オプションを設定することもできます。特定の優先順位の高い、重大度の高いイベントが検出されたときに自動的に通知するように指定できます。

調査と認定

インシデント対応プロセスでは、セキュリティ インシデントの検出後に、どのように調査を実施するかを指定する必要があります。一部の組織では、経験の浅いチーム メンバーがすべてのインシデントのトリアージを行い、重大度と優先度が比較的に低いケースは自分たちで処理し、熟練のチームメンバーが重大度と優先度が高いインシデントを処理しています。各チームメンバーがインシデントの重要度を繰り上げる基準について理解するように、エスカレーション プロセスの概要を慎重にまとめる必要があります。

エスカレーション プロセスでは、検出されたイベントがネットワーク資産のセキュリティにどのような影響を与えるかについての理解が不可欠です。たとえば、Microsoft SQL Server を実行するホストに対する攻撃は、それとは異なるデータベース サーバを使用する組織にとって優先度は高くありません。同様に、ネットワークで SQL Server を使用しているものの、すべてのサーバにパッチを適用済みで、その攻撃に対する脆弱性がないことを確信している場合には、その攻撃の重要度は低くなります。しかし、最近誰かが脆弱性のあるバージョンのソフトウェア コピーを（テスト目的などで）インストールしていたりすれば、簡易調査で指摘されるよりも大きな問題が発生するおそれがあります。

Firepowerシステムは、調査および認定のプロセスをサポートするのに特に適しています。独自のイベント分類を作成し、ネットワークの脆弱性を最も適切に示す方法で、それらを適用することができます。ネットワークのトラフィックによってイベントがトリガーされると、自動的に、そのイベントの優先度判別と認定が行われ、脆弱性があることが判明しているホストに対してどのような攻撃が行われるかを示す特別なインジケータが付けられます。

Firepowerシステムのインシデント トラッキング機能には、エスカレーションされたインシデントを示すためにユーザが変更できるステータス インジケータも含まれています。

コミュニケーション（Communication）

すべてのインシデント対応プロセスでは、インシデント対応チームと内部および外部の対象者の間でのインシデントについての連絡の方法が指定されている必要があります。たとえば、どの種類のインシデントが管理介入を必要とし、どのレベルでの介入が必要かを考慮する必要があります。また、プロセスでは、組織の外部との連絡の方法とタイミングが説明されている必要があります。次の点に注意してください。

- あるインシデントについて、法執行機関に通知する必要がありますか。
- ホストがリモート サイトに対する分散型サービス妨害（DDoS）に関与している場合、そのことを通知しますか。
- CERT 調整センター（CERT/CC）や FIRST などの組織と情報を共有する必要があるでしょうか。

Firepower システムには、HTML、PDF、CSV（カンマ区切り値）などの標準形式で侵入データを収集するために使用できる機能があり、侵入データを他のユーザと簡単に共有できます。

たとえば、CERT/CCはWebサイトのセキュリティ インシデントに関する標準情報を収集します。CERT/CC は、Firepower システムから簡単に抽出できる次のような情報を探します。

- 影響を受けるマシンに関する次のような情報

- ホスト名および IP
- タイム ゾーン
- ホストの目的や機能

- 攻撃元に関する次のような情報
  - ホスト名および IP
  - タイム ゾーン
  - 攻撃者と接触したことがあるかどうか
  - インシデント処理の概算コスト

- 次のようなインシデントの説明
  - 日付
  - 侵入方法
  - 使用された侵入者ツール
  - ソフトウェア バージョンとパッチ レベル
  - 侵入者ツールの出力
  - 悪用された脆弱性の詳細
  - 攻撃元
  - その他の関連情報

また、インシデントのコメント セクションを使用して、問題を伝えた日時と相手を記録することができます。

封じ込めとリカバリ

インシデント対応プロセスでは、ホストまたはその他のネットワーク コンポーネントが侵害された場合に、どのような手順を実行するかを明確に示す必要があります。封じ込めとリカバリの方法には、脆弱性のあるホストへのパッチの適用から、ターゲットのシャットダウンとネットワークからの除去まで、さまざまな選択肢があります。攻撃の性質と重大度によっては、刑事責任を追求する場合に備えて証拠を保存しておくことの重要性を考慮する必要もあります。

Firepower システムのインシデント機能を使用して、インシデントの封じ込めとリカバリのフェーズ中に実行するアクションを記録しておくことができます。

学んだ教訓

それぞれのセキュリティ インシデントは、攻撃が成功したかどうかに関わりなく、セキュリティ ポリシーを見直す機会となります。ファイアウォール ルールを更新する必要はありますか。パッチ管理に対するより構造化されたアプローチが必要ですか。不正なワイヤレスアクセスポイント

は新しいセキュリティ問題となりますか。それぞれの学んだ教訓は、セキュリティ ポリシーにフィードバックし、次のインシデントへのより良い対処のために役立てる必要があります。

Firepower システムのインシデント タイプ

作成する各インシデントにインシデント タイプを割り当てることができます。Firepower システムでは、以下のタイプがデフォルトでサポートされます。

- 侵入（Intrusion）
- サービス妨害（DoS）
- 不正な管理者アクセス
- Web サイトの改変
- システム整合性の侵害
- デマ ウイルス
- 盗難
- ダメージ
- 不明

独自のインシデント タイプを作成することもできます。

カスタム インシデント タイプの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

手順

ステップ 1 [分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）]を選択します。

ステップ 2 [インシデントの作成（Create Incident）] をクリックします。

ステップ 3 [タイプ（Type）] エリアで、[タイプ（Types）] をクリックします。
デフォルトのインシデント タイプがページの下部に表示されます。

ステップ 4 [インシデント タイプ名（Incident Type Name）] フィールドに、新しいインシデント タイプの名前を入力します。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 [完了（Done）] をクリックします。
次にインシデントを作成または編集するときに、新しいインシデント タイプを使用できます。

インシデントの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

マルチドメイン導入では、現在のドメインで作成されたインシデントのみを表示および変更できます。先祖ドメインでは、任意の子孫ドメインからのインシデントにイベントを追加できます。

手順

ステップ 1 [分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）]を選択します。

ステップ 2 [インシデントの作成（Create Incident）] をクリックします。

ステップ 3 [タイプ（Type）] ドロップダウン メニューから、インシデントを最も適切に説明するオプションを選択します。

ステップ 4 [滞留時間（Time Spent）] フィールドに、インシデントで費やした時間の合計を #d #h #m #s の形式で入力します。ここで、# は日数、時間数、分数、秒数を表します。

ステップ 5 [概要（Summary）] テキスト ボックスに、インシデントの簡単な説明（最大 255 文字の英数字、スペース、記号）を入力します。

ステップ 6 [コメントを追加（Add Comment）] テキスト ボックスに、インシデントのより詳細な説明（最大 8191 文字の英数字、スペース、記号）を入力します。

ステップ 7 インシデントにイベントを追加します。

- 選択したイベントを追加するには、クリップボードのイベントを選択して、[インシデントに追加（Add to Incident）] をクリックします。
- クリップボードからすべてのイベントを追加するには、[すべてをインシデントに追加（Add All to Incident）] をクリックします。

（注） クリップボードの複数のページにある個々のイベントを追加する場合は、1 つのページのイベントを追加してから、他のページのイベントを追加します（ページごとに追加します）。

ステップ 8 [保存（Save）] をクリックします。

インシデントの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

マルチドメイン導入では、現在のドメインで作成されたインシデントのみを表示および変更できます。先祖ドメインでは、すべての子孫ドメインからインシデントにイベントを追加できます。

手順

ステップ 1 [分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）]を選択します。

ステップ 2 編集するインシデントの横にある編集アイコン（  ）をクリックします。

ステップ 3 インシデントの以下の側面を編集できます。

- ステータスの変更
- タイプの変更
- クリップボードからのイベントの追加
- イベントの削除

ステップ 4 [滞留時間（Time Spent）] フィールドに、インシデントに費やした追加の時間の合計を入力します。

ステップ 5 [コメントを追加（Add Comment）] テキスト ボックスで、インシデントに対する変更点（最大 8191 文字の英数字、スペース、および記号）を示します。

ステップ 6 オプションで、インシデントにイベントを追加したり、削除したりすることができます。

- クリップボードからイベントを追加するには、クリップボードのイベントを選択して、[インシデントに追加（Add to Incident）] をクリックします。
- クリップボードからすべてのイベントを追加するには、[インシデントにすべてを追加（Add All to Incident）] をクリックします。
- インシデントから特定のイベントを削除するには、イベントを選択し、[削除（Delete）] をクリックします。
- インシデントからすべてのイベントを削除するには、[すべて削除（Delete All）] をクリックします。

- イベントを追加または削除せずにインシデントを更新するには、[保存（Save）] をクリックします。

インシデント レポートの生成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

Firepowerシステムを使用して、インシデント レポートを生成できます。このレポートには、インシデントの概要、インシデントのステータス、およびコメントに加えて、インシデントに追加するイベントの情報を含めることができます。また、レポートにイベントの概要情報を含めるかどうかも指定できます。

手順

ステップ 1 [分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）]を選択します。

ステップ 2 レポートに含めるインシデントの横にある編集アイコン（  ）をクリックします。

ステップ 3 次の 2 つの対処法があります。

- レポートにインシデントのすべてのイベントを含める場合は、[すべてのレポートの生成（Generate Report All）] をクリックします。
- レポートにインシデントの特定のイベントを含める場合は、目的のイベントの横にあるチェックボックスをオンにしてから、[レポートの生成（Generate Report）] をクリックします。

ステップ 4 レポートの名前を入力します。

ステップ 5 [インシデント レポートのセクション（Incident Report Sections）] で、レポートに含めるインシデントの部分（[ステータス（status）]、[概要（summary）]、および[コメント（comments）]のチェックボックスをオンにします。

ステップ 6 レポートにイベント情報を含める場合は、使用するワークフローを選択し、[レポートのセクション（Report Sections）] で、イベントの概要情報を含めるかどうかを指定します。

ステップ 7 レポートに含めるワークフロー ページの横にあるチェックボックスをオンにします。

ステップ 8 レポートに使用する出力形式（[PDF]、[HTML]、および [CSV]）の横にあるチェックボックスをオンにします。

（注） CSV ベースのインシデント レポートには、イベント情報のみが含まれます。インシデントのステータス、概要、コメントは含まれ**ません**。

ステップ 9 [レポートの生成（Generate Report）] をクリックして、レポート プロファイルの更新を確認します。

第 XX 部

ワークフロー（Workflows）

第 79 章

ワークフロー

以下のトピックでは、ワークフローの使用方法について説明します。

概要：ワークフロー

ワークフローは Firepower Management Center Web インターフェイス上でユーザに合わせて作成された一連のデータ ページで、アナリストはワークフローを使用して、システムで生成されたイベントを評価することができます。

Firepower Management Center では、以下のタイプのワークフローを使用できます。

定義済みワークフロー

システムに付属のプリセット ワークフローです。定義済みのワークフローの編集や削除を行うことはできません。ただし、定義済みワークフローをコピーして、そのコピーをカスタム ワークフローの基礎として使用することができます。

保存済みのカスタム ワークフロー

Firepower Management Center に付属の保存済みカスタム テーブルに基づくカスタム ワークフロー。これらのワークフローは編集、削除、コピーすることができます。

カスタム ワークフロー

特定のニーズに対応するために作成してカスタマイズするワークフロー、またはカスタム テーブルを作成するとシステムによって自動的に生成されるワークフローです。これらのワークフローは編集、削除、コピーすることができます。

通常、ワークフローに表示されるデータは、管理対象デバイスのライセンスおよび展開状況や、データを提供する機能を設定しているかどうかによって異なります。

定義済みワークフロー

以下の項で説明する定義済みワークフローは、システムに付属しているものです。定義済みワークフローを編集または削除することはできません。ただし、定義済みワークフローをコピーして、そのコピーをカスタム ワークフローのベースとして使用することができます。

定義済み侵入イベントのワークフロー

次の表では、Firepower System に備わっている定義済み侵入イベントのワークフローについて説明します。

表 *227*：定義済み侵入イベントのワークフロー

ワークフロー名	説明
[接続先ポート（Destination Port）]	接続先ポートは、通常、アプリケーションに紐付けされているため、このワークフローにより、異常な大容量アラートを経験しているアプリケーションを検出できます。接続先ポート カラムにより、ネットワーク上に存在してはならないアプリケーションを特定できます。
イベント特定	このワークフローでは、2つの有用な特徴を提供します。イベントが頻繁に発生する場合には、次のことを示します： • 誤検出 • ワーム • 不正確な誤設定ネットワーク 発生頻度の低いイベントは、対象となる攻撃を最も確実に示す証拠であり、特別な注意を必要とします。
優先度および分類によるイベント	このワークフローでは、イベントとタイプのリストをそれぞれのイベントが発生した回数と共にイベントの優先度の順に示します。
接続先に対するイベント	このワークフローでは、攻撃されているホスト IP アドレスや攻撃の本質のハイレベル ビューを提示します。利用可能な場合、攻撃に関与する国に関する情報を確認することもできます。
IP 特定	このワークフローでは、最も多くのアラートを発生するホストIPアドレスを示します。イベント数が最も多いホストは、対外に向けて、受信しているワーム タイプのトラフィック（調整を必要とする適切な場所を示す）であるか、またはアラートの原因を決定するために更に調査を必要とします。イベント数が最も少ないホストは、対象となる攻撃を受ける可能性があるため、調査の根拠となります。イベント数が少ない場合は、ホストがネットワークに属していないことを示す場合もあります。

ワークフロー名	説明
影響度と優先度	このワークフローにより、すぐに再度発生している影響度の高いイベントを検索します。レポートによる影響レベルは、イベントが発生した時間数で示します。この情報を使用して、最も頻繁に再発する影響度の高いイベントを特定できます。これがネットワーク上での広範な攻撃の指標となります。
影響度と送信元	このワークフローにより、進行中の攻撃の送信元を特定できます。レポートされた影響レベルは、イベントに対する関連の送信元IPアドレスにより示します。たとえば、影響レベルが1のイベントは、同じ送信元IPアドレスから繰返し発生している場合、これらは特定された脆弱なシステムであり、送信元IPアドレスを対象としている攻撃者を示すこともあります。
接続先への影響	このワークフローを使用して、脆弱なコンピュータ上で繰返し発生しているイベントを特定できます。このため、これらのシステムでの脆弱性を指定し、進行中の攻撃を停止できます。
送信元ポート	このワークフローは、最もアラートを発生しているサーバを示します。この情報を使用して、調整が必要なエリアを特定し、注意を要するサーバを決定できます。
送信元と接続先	このワークフローでは、高いレベルのアラートを共有するホストIPアドレスを特定します。リストのトップのペアは誤検出の可能性もあり、調整が必要なエリアを特定することもあります。評価する必要のないリソースを評価するユーザまたはネットワークに属していないホストについては、対象となる攻撃リストの下部にあるペアを確認できます。

定義済みマルウェアのワークフロー

次の表では、Firepower Management Center に備えられた定義済みマルウェアのワークフローについて説明します。定義済みマルウェアのワークフローでは、必ずマルウェア イベントのテーブルビューを使用します。

表 *228*：定義済みマルウェアのワークフロー

ワークフロー名	説明
マルウェア サマリ	このワークフローでは、ネットワーク トラフィック内で検出されたか、または AMP for Endpoints Connector によって検出されたマルウェアのリストを提供します。これらのリストは、それぞれの脅威ごとにグループ化されます。
マルウェア イベント サマリ	このワークフローでは、異なるマルウェア イベントのタイプやサブタイプの明細が迅速に表示されます。
ホスト受信マルウェア	このワークフローでは、マルウェアを受信したホスト IP アドレスのリストが表示されます。このリストは、マルウェア ファイル関連の処理ごとにグループ化されます。
ホスト送信マルウェア	このワークフローでは、マルウェアを送信したホスト IP アドレスのリストが表示されます。このリストは、マルウェア ファイル関連の処理ごとにグループ化されます。

ワークフロー名	説明
アプリケーション導入マルウェア	このワークフローでは、ファイルを受信したホストIPアドレスのリストが表示されます。このリストは、受信したファイルの関連したマルウェアの処理によってグループ化されます。

定義済みファイルのワークフロー

次の表では、Firepower Management Centerに備えられる定義済みファイルイベントのワークフローについて説明しています。定義済みファイルイベントのワークフローでは、必ずファイルイベントのテーブル ビューを使用します。

表 *229*：定義済みファイルのワークフロー

ワークフロー名	説明
ファイル サマリ（File Summary）	このワークフローでは、関連するマルウェアの処理と共に、異なるファイル イベント カテゴリやタイプの明細を迅速に表示します。
ホスト受信ファイル（Hosts Receiving Files）	このワークフローでは、ファイルを受信したホストIPアドレスのリストが表示されます。このリストは、受信したファイルの関連したマルウェアの処理によってグループ化されます。
ホスト送信ファイル（Hosts Sending Files）	このワークフローでは、ファイルを送信したホスト IP アドレスのリストを表示します。このリストは、これらのファイルの関連したマルウェアの処理によってグループ化されます。

定義済みキャプチャ ファイルのワークフロー

次の表では、Firepower Management Center での定義済みキャプチャ ファイルのワークフローについて説明しています。定義済みキャプチャファイルのワークフローは、必ずキャプチャファイルのテーブル ビューを使用します。

表 *230*：定義済みキャプチャ ファイルのワークフロー

ワークフロー名	説明
キャプチャ ファイル サマリ	このワークフローでは、タイプ、カテゴリ、脅威スコアに基づいてキャプチャ ファイルの詳細を提示します。
ダイナミック分析ステータス（Dynamic Analysis Status）	このワークフローでは、ダイナミック分析用に提示されたか否かに基づいて、キャプチャファイルの数を表示します。

定義済み接続データのワークフロー

次の表では、Firepower Management Center に備えられる定義済み接続データのワークフローについて説明しています。定義済み接続データ ワークフローでは、必ず接続データのテーブル ビューを使用します。

表 *231*：定義済み接続データのワークフロー

ワークフロー名	説明
接続イベント	このワークフローでは、ベーシックな接続に関する情報や検出されたアプリケーション情報のサマリー ビューを提示し、このサマリー ビューを使用して、イベントのテーブル ビューをドリルダウンできます。
アプリケーションごとの接続（Connections by Application）	このワークフローには、検出された接続情報の数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなアプリケーションのグラフを含みます。
イニシエータごとの接続（Connections by Initiator）	このワークフローには、ホストが接続トランザクションを開始した接続の数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなホスト IP アドレスのグラフが含まれています。
ポートごとの接続（Connections by Port）	このワークフローには、検出された接続の数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなポートのグラフが含まれています。
レスポンダごとの接続（Connections by Responder）	このワークフローには、ホスト IP が接続トランザクションでレスポンダである接続の数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなホスト IP アドレスのグラフが含まれています。
時間の経過ごとの接続（Connections over Time）	このワークフローには、監視対象のネットワーク セグメントでの時間の経過ごとの合計接続数のグラフが含まれています。
アプリケーションごとのトラフィック（Traffic by Application）	このワークフローには、送信されたキロバイト数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなアプリケーションのグラフが含まれています。
イニシエータごとのトラフィック（Traffic by Initiator）	このワークフローには、各アドレスから送信された合計キロバイト数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなホスト IP アドレスのグラフが含まれています。
ポートごとのトラフィック（Traffic by Port）	このワークフローには、送信されたキロバイト数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなポートのグラフが含まれています。

ワークフロー名	説明
レスポンダごとのトラフィック（Traffic by Responder）	このワークフローには、各アドレスが受信した合計キロバイト数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブなホスト IP アドレスのグラフが含まれています。
時間の経過ごとのトラフィック	このワークフローには、監視対象のネットワーク セグメントで送信される時間の経過ごとの合計キロバイト数のグラフが含まれています。
レスポンダごとの一意イニシエータ	このワークフローには、各アドレスでコンタクトした一意イニシエータの数に基づく監視対象のネットワーク セグメントでの 10 個の最もアクティブな応答ホスト IP アドレスのグラフが含まれています。
イニシエータごとの一意レスポンダ（Unique Responders by Initiator）	このワークフローには、アドレスにコンタクトする一意レスポンダの数に基づく、監視対象のネットワーク セグメントでの 10 個の最もアクティブな開始ホスト IP アドレスのグラフが含まれています。

定義済みセキュリティ インテリジェンスのワークフロー

次の表では、Firepower Management Center に備えられている定義済みセキュリティ インテリジェンスのワークフローについて説明しています。定義済みセキュリティ インテリジェンスのワークフローでは、必ずセキュリティ インテリジェンス イベントのテーブル ビューを使用します。

表 *232*：定義済みセキュリティ インテリジェンスのワークフロー

ワークフロー名	説明
セキュリティ インテリジェンス イベント	このワークフローでは、基礎的なセキュリティインテリジェンスや検出されたアプリケーション情報のサマリ ビューを表示し、イベントのテーブル ビューをドリルダウンする際に使用できます。
セキュリティ インテリジェンス サマリ	このワークフローは、セキュリティ インテリジェンス イベントのワークフローと同じものですが、セキュリティ インテリジェンス サマリ ページから始まり、カテゴリや数ごとにセキュリティ インテリジェンス イベントのみのリストを表示します。
セキュリティ インテリジェンスと DNS 詳細	このワークフローは、セキュリティ インテリジェンス イベントのワークフローと同じものですが、DNS 詳細のあるセキュリティ インテリジェンス ページから始まり、カテゴリや DNS 関連特性ごとにセキュリティ インテリジェンス イベントのリストを表示します。

定義済みホストのワークフロー

次の表では、ホスト データと共に使用できる定義済みワークフローについて説明します。

表 *233*：定義済みホストのワークフロー

ワークフロー名	説明
Hosts	このワークフローには、ホストのテーブル ビューと、その後にホスト ビューが含まれます。ホスト テーブルに基づくワークフロー ビューでは、ホストに関連付けられているすべての IP アドレスのデータを容易に表示できます。
オペレーティング システム サマリ（Operating System Summary）	このワークフローを用いて、ネットワーク上で使用中のオペレーティング システムを分析できます。

定義済み侵害の兆候のワークフロー

次の表では、IOC（侵害の兆候）と共に使用できる定義済みワークフローについて説明します。

表 *234*：定義済み侵害の兆候のワークフロー

ワークフロー名	説明
の侵害の兆候	このワークフローは、数とカテゴリごとにグループ化した IOC データのサマリー ビューから始まり、さらにサマリ データをイベント タイプごとに分割した詳細ビューを表示します。 [分析（Analysis）]>[ホスト（Hosts）] メニューからこのワークフローにアクセスします。
ホストごとの侵害の兆候	このワークフローを使用して、最も侵害する可能性の高いネットワーク上のホストを判断できます（IOC データに基づく）。 [分析（Analysis）]>[ホスト（Hosts）] メニューからこのワークフローにアクセスします。

定義済みアプリケーション ワークフロー

次の表では、アプリケーション データと共に使用できる定義済みワークフローについて説明しています。

表 *235*：定義済みアプリケーション ワークフロー

ワークフロー名	説明
アプリケーションのビジネスとの関連性	このワークフローを使用して、ネットワーク上で実行中のそれぞれ予想されるビジネスとの関連性レベルのアプリケーションを分析できます。そのため、ネットワーク リソースが適切に使用されているかを監視できます。

ワークフロー名	説明
アプリケーション カテゴリ	このワークフローを使用して、ネットワーク上で各カテゴリの実行中のアプリケーションを分析できます（電子メール、検索エンジン、ソーシャルネット ワーキングなど）。そのため、ネットワーク リソースが適切に使用されているかを監視できます。
アプリケーションのリスク	このワークフローを使用して、ネットワーク上でそれぞれ予想されるセキュリティ リスク レベルの実行中のアプリケーションを分析できます。このため、ユーザのアクティビティの考えられるリスクを予想し、適切なアクションを取ることできます。
アプリケーション サマリ	このワークフローを使用して、ネットワークのアプリケーションや関連するホストに関する詳細情報を取得できます。このため、ホストのアプリケーションのアクティビティを正確に調べることができます。
アプリケーション	このワークフローを使用して、ネットワーク上の実行中のアプリケーションを分析できます。このため、ネットワークの使用状況の概要を取得できます。

定義済みアプリケーション詳細ワークフロー

次の表では、アプリケーションの詳細とクライアント データと共に使用できる定義済みワークフローについて説明しています。

表 *236*：定義済みアプリケーション詳細ワークフロー

ワークフロー名	説明
アプリケーション詳細（Application Details）	このワークフローを用いて、ネットワーク上のクライアント アプリケーションをさらに詳しく分析することができます。また、このワークフローでは、クライアントアプリケーションのテーブル ビューを表示し、その後ホスト ビューを表示します。
Clients	このワークフローには、クライアント アプリケーションのテーブル ビューと、その後にホスト ビューが含まれます。

定義済みサーバのワークフロー

次の表では、サーバ データと共に使用できる定義済みワークフローについて説明します。

表 *237*：定義済みサーバのワークフロー

ワークフロー名	説明
数別ネットワーク アプリケーション	このワークフローを使用して、ネットワーク上で最も多く使用されるアプリケーションを分析できます。

ワークフロー名	説明
ヒット別ネットワーク アプリケーション	このワークフローを使用して、ネットワーク上で最もアクティブなアプリケーションを分析できます。
サーバの詳細	このワークフローを使用して、ベンダや検出されたサーバ アプリケーション プロトコルのバージョンを詳細に分析できます。
サーバ	このワークフローには、アプリケーションのテーブル ビューと、その後にホスト ビューが含まれます。

定義済みホスト属性のワークフロー

次の表では、ホスト属性データと共に使用できる定義済みワークフローについて説明します。

表 *238*：定義済みホスト属性のワークフロー

ワークフロー名	説明
属性（Attributes）	このワークフローを使用して、ネットワーク上のホスト IP アドレスやホスト ステータスを監視できます。

定義済み検出イベントのワークフロー

次の表では、検出データとアイデンティティ データの表示に使用できる定義済みワークフローについて説明しています。

表 *239*：定義済み検出イベント ワークフロー

ワークフロー名	説明
検出イベント（Discovery Events）	このワークフルーでは、テーブル ビュー形式の検出イベント詳細リストが提示され、その次にホスト ビューが提示されます。

定義済みユーザ ワークフロー

次の表では、ユーザ検出データとユーザ アイデンティティ データの表示に使用できる定義済みワークフローを説明します。

表 *240*：定義済みユーザ ワークフロー

ワークフロー名	説明
Users	このワークフローでは、ユーザ ID ソースによって収集されるユーザ情報リストが表示されます。

定義済み脆弱性のワークフロー

次の表では、Firepower Management Center に備えられている定義済み脆弱性のワークフローについて説明します。

表 *241*：定義済み脆弱性のワークフロー

ワークフロー名	説明
脆弱性（Vulnerabilities）	このワークフローを使用して、ネットワーク上で検出されたホストに適用するこれらのアクティブな脆弱性のみのテーブル ビューなど、データベース内の脆弱性を検討できます。このワークフローにより脆弱性詳細ビューが提供され、これには制約に適合するそれぞれの脆弱性に関する詳細な説明が含まれています。

定義済みのサードパーティ脆弱性のワークフロー

次の表では、Firepower Management Center に備えられた定義済みのサードパーティ脆弱性のワークフローについて説明します。

表 *242*：定義済みのサードパーティ脆弱性のワークフロー

ワークフロー名	説明
IP アドレスごとの脆弱性	このワークフローを使用して、監視対象のネットワーク上のホスト IP アドレスごとに検出されたサードパーティの脆弱性の数をすぐに確認できます。
送信元ごとの脆弱性	このワークフローを使用して、QualysGuard Scanner などサードパーティの脆弱性の送信元ごとに検出されたサードパーティの脆弱性の数をすぐに確認できます。

定義済み相関ワークフロー、ホワイト リスト ワークフロー

相関データ、ホワイト リスト イベント、ホワイト リスト違反、修復ステータス イベントのそれぞれのタイプには、定義済みワークフローがあります。

表 *243*：定義済み相関ワークフロー

ワークフロー名	説明
相関イベント（Correlation Events）	このワークフローには、相関イベントのテーブル ビューが含まれています。
ホワイト リスト イベント（White List Events）	このワークフローには、ホワイト リスト イベントのテーブル ビューが含まれています。
ホスト違反数（Host Violation Count）	このワークフローには、少なくとも 1 つのホワイト リストに違反しているすべてのホスト IP アドレスのリストを示す一連のページが表示されます。
ホワイト リスト違反（White List Violations）	このワークフローには、すべての違反を列挙し、リストのトップに直前に検出された違反を示す、ホワイト リスト違反のテーブル ビューが含まれています。テーブル内の各列には、検出された違反が 1 つずつ表示されます。
ステータス（Status）	このワークフローには、修復ステータスのテーブル ビューを含み、違反したポリシー名、適用された修復名や修復状況が表示されています。

定義済みのシステムのワークフロー

Firepower System には、監査イベントやヘルスイベントなどのシステム イベントなど、いくつかの追加のワークフロー、ルール更新インポート、アクティブ スキャンの結果をリストにしたワークフローが提供されています。

表 *244*：追加の定義済みワークフロー

ワークフロー名	説明
監査ログ（Audit Log）	このワークフローでは、監査イベントをリストした監査ログのテーブル ビューを含みます。
ヘルス イベント（Health Events）	このワークフローでは、ヘルス監視ポリシーによりトリガーされるイベントを表示します。
ルール更新インポート ログ（Rule Update Import Log）	このワークフローは、成功したルールの更新インポートと失敗したルールの更新インポートに関する情報をリストしたテーブル ビューを含みます。
スキャン結果（Scan Results）	このワークフローには、それぞれ完了したスキャンをリストしたテーブル ビューを含みます。

カスタム テーブル ワークフロー

カスタムテーブルの機能を使用して、複数のイベントタイプのデータを使用するテーブルを作成することができます。これにより、たとえば、ユーザが侵入イベントのデータとディスカバリデータを関連付けるテーブルおよびワークフローを作成して、重要なシステムに影響を及ぼすイベントを簡単に検索できるようになるため、役立ちます。

カスタム テーブルを作成すると、システムは自動的にワークフローを作成します。このテーブルを使って関連するイベントを表示することができます。ワークフローの機能は、使用するテーブルのタイプによって異なります。たとえば、侵入イベントテーブルに基づいたカスタムテーブルのワークフローは、必ずパケット ビューで終了します。ただし、検出イベントに基づいたカスタム テーブルのワークフローは、必ずホスト ビューで終了します。

事前定義のイベントテーブルに基づいたワークフローとは異なり、カスタムテーブルに基づいたワークフローには、他のタイプのワークフローへのリンクがありません。

ワークフローの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	（ワークフローに応じて） Admin/Maint/Any Security Analyst

手順

ステップ 1 ワークフローの選択, （1837ページ）に記載されているように、適切なメニューパスとオプションを選択します。

ステップ 2 現在のワークフロー内で移動します。

- 選択したイベントデータタイプで利用可能な列をすべて表示するには、テーブル ビューページを使用します。テーブル ビュー ページの使用, （1845 ページ）を参照してください。
- 選択したイベントデータタイプで利用可能な列のサブセットを表示するには、ドリルダウンページを使用します。ドリルダウン ページの使用, （1844 ページ）を参照してください。
- ワークフローの次のページの対応する行を表示するには、青い下矢印アイコン（  ）をクリックします。
- マルチページ ワークフローのページ間を移動するには、各ページの下部にあるツールを使用します。ワークフロー ページのトラバーサル ツール, （1840ページ）を参照してください。

- 別のタイプのイベントに対してワークフロー内で適用された同じ制約を表示するには、[移動先（Jump to）] をクリックし、ドロップダウンリストからイベント ビューを選択します。

ステップ 3 現在のワークフローの表示を変更します。

- ページ上で 1 つ以上の行のチェックボックスにマークを付けて、処理を反映させる行を表示し、ページの下部にあるいずれかのボタン（[表示（View）] ボタンなど）をクリックして、選択したすべての行に対してそのアクションを実行します。
- 行の上部にあるチェックボックスにマークを付けて、ページ上のすべての行を選択し、ページの下部にあるいずれかのボタン（[表示（View）] ボタンなど）をクリックして、ページ上のすべての行に対してそのアクションを実行します。
- 非表示にする列ヘッダーの閉じるアイコン（ ）をクリックして、表示する列を制約します。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）]をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効にした列をビューに戻すには、展開の矢印をクリックして検索の制約を展開し、[無効な列（Disabled Columns）] の下の列名をクリックします。
- 選択したフィールドに対して選択した値でデータ ビューを制約します。詳細については、イベント ビューの制約, （1863 ページ）および複合イベント ビューの制約, （1865 ページ）を参照してください。
- イベント ビューの時間の制約を変更します。ページの右上隅に表示される日付の範囲は、ワークフローに含めるイベントの時間範囲を設定します。詳細については、イベント時間の制約, （1855 ページ）を参照してください。

  （注） イベント ビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあります。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。
- データを列でソートするには、列の名前をクリックします。ソート順序を反転させるには、もう一度列の名前をクリックします。矢印のアイコンは、データのソート基準になっている列、およびソートが昇順である（ ）か、または降順である（ ）かを表します。
- ワークフローページのリンクをクリックして、アクティブな制約を使用しているページを表示します。ワークフローページのリンクは、事前定義されたワークフローテーブル ビュー、およびドリルダウン ページの左上隅の、イベントの上で、ワークフロー名の下に示されます。

ステップ 4 現在のワークフロー内の追加データを表示します。

- ファイルのトラジェクトリ マップを新しいウィンドウで表示するには、ファイル名と SHA-256 ハッシュ値の列のネットワーク ファイル トラジェクトリ アイコンをクリックします。アイコンは、ファイル ステータスによって異なります。ファイル トラジェクトリ アイコン, （1841 ページ）を参照してください。

- IP アドレスに関連付けられたホスト プロファイルのポップアップ ウィンドウを表示するには、IP アドレスの列のホスト プロファイル アイコンをクリックします。アイコンは、ファイル ステータスによって異なります。ホスト プロファイルのアイコン，（1842 ページ）を参照してください。
- ファイルに関連付けられた最も高い脅威スコアの動的分析サマリー レポートを表示するには、いずれかの脅威スコア列の脅威スコア アイコンをクリックします。アイコンは、ファイルの最も高い脅威スコアによって異なります。脅威スコア アイコン，（1842 ページ）を参照してください。
- ユーザ プロファイル情報を表示するには、いずれかのユーザ ID 列でユーザ アイコン（  、または侵害の兆候に関連付けられたユーザの場合は  ）をクリックします。ユーザ アイコンは、そのユーザがデータベースにない場合（つまり、AMP for Endpoints Connector ユーザの場合）は淡色表示されます。
- サードパーティの脆弱性の脆弱性詳細を表示するには、いずれかのサードパーティの脆弱性の ID 列の脆弱性アイコン（  ）をクリックします。
- 集約データ ポイントを表示する場合は、ポインタをフラグ アイコンの上に合わせて国名を表示します。
- 個々のデータ ポイントを表示する場合は、フラグ アイコンをクリックして、位置情報（GeoLocation），（1845 ページ）に記載されている地理位置情報詳細を表示します。

ステップ 5 別のワークフローに移動します。
別のワークフローを使用して同じイベント タイプを表示するには、ワークフローのタイトルの横にある（ワークフローの切り替え）をクリックして、使用するワークフローを選択します。スキャン結果には別のワークフローを使用**できない**ことに注意してください。

ユーザ ロールによるワークフローへのアクセス

ワークフローへのアクセスはユーザのロールにより異なります。詳細については、次の表を参照してください。

ユーザ ロール	アクセス可能なワークフロー
管理者（Administrator）	すべてのワークフローにアクセスできます。また、Administrator は監査ログ、スキャン結果、およびルール更新のインポート ログにアクセスできる唯一のユーザです。
メンテナンスユーザ	ヘルス イベントにアクセスできます。

ユーザ ロール	アクセス可能なワークフロー
セキュリティ アナリストとセキュリティ アナリスト（読み取り専用）	侵入、マルウェア、ファイル、接続、検出、脆弱性、相関、ヘルスワークフローにアクセスできます。

ワークフローの選択

Firepowerシステムには、次の表に記載されているデータのタイプに対して、事前定義のワークフローが用意されています。

表 *245*：ワークフローを使用する機能

機能	メニュー パス	オプション
侵入イベント	[分析（Analysis）] > [侵入（Intrusions）]	イベント 確認済みイベント クリップボード [インシデント（Incidents）]
マルウェア イベント	[分析（Analysis）] > [ファイル（Files）]	マルウェア イベント
ファイル イベント	[分析（Analysis）] > [ファイル（Files）]	ファイル イベント
キャプチャ ファイル	[分析（Analysis）] > [ファイル（Files）]	キャプチャ ファイル（Captured Files）
接続イベント	[分析（Analysis）] > [接続（Connections）]	イベント
セキュリティ インテリジェンス イベント	[分析（Analysis）] > [接続（Connections）]	セキュリティ インテリジェンス イベント
ホスト イベント	[分析（Analysis）] > [ホスト（Hosts）]	ネットワーク マップ Hosts Indications of Compromise アプリケーション アプリケーション詳細（Application Details） サーバ ホスト属性（Host Attributes） 検出イベント（Discovery Events）

機能	メニュー パス	オプション
ユーザ イベント	[分析（Analysis）] > [ユーザ（Users）]	ユーザ アクティビティ Users
脆弱性イベント	[分析（Analysis）] > [脆弱性（Vulnerabilities）]	脆弱性 サードパーティの脆弱性
相関イベント	[分析（Analysis）] > [相関（Correlation）]	相関イベント（Correlation Events） ホワイトリスト イベント（White List Events） ホワイトリスト違反（White List Violations） ステータス（Status）
監査イベント	[システム（System）] > [モニタリング（Monitoring）]	監査（Audit）
ヘルス イベント	[ヘルス（Health）] > [イベント（Events）]	適用対象外
ルール更新インポート ログ	[システム（System）] > [更新（Updates）]	適用対象外
スキャン結果	[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]	適用対象外

上記の表に記載されているいずれかの種類のデータを表示する場合、そのデータのデフォルトのワークフローの最初のページにイベントが表示されます。イベント ビューの設定項目を設定することによって、別のデフォルト ワークフローを指定することができます。ワークフローへのアクセス権限は、ユーザの役割によって異なります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

関連トピック

イベント ビュー設定の設定, （38 ページ）

ワークフローのページ

ワークフローのタイプによってデータは異なりますが、すべてのワークフローで共通の機能セットを共有しています。ワークフローには、数種類のページを含めることができます。ユーザがワークフローのページ上で実行できるアクションは、ページのタイプによって異なります。

ワークフローのドリルダウンのページとテーブル ビューのページを使用すれば、データのビューをすばやく絞り込むことができるため、分析にとって重要なイベントに集中できます。テーブル

ビューのページとドリルダウンのページの両方で、ユーザが表示するイベント セットに制約を適用したり、ワークフローをナビゲートしたりするために使用できる機能が多数サポートされています。ドリルダウンページ、またはワークフロー内のテーブル ビューでデータを表示する場合、ソートに使用できる任意のカラムに基づいてデータを昇順または降順でソートできます。1 つのワークフローのページに表示できるイベント数よりも多くのイベントがデータベースに含まれている場合は、ページの下部にあるリンクをクリックして、さらにイベントを表示できます。これらのリンクの 1 つをクリックすると時間枠が自動的に一時停止されるため、同じイベントが 2 回表示されません。準備ができたら時間枠の一時停止を解除できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

テーブル ビュー

ページがデフォルトで有効になっている場合、テーブル ビューには、ワークフローのベースとなるデータベースの各フィールドに対するカラムが含まれています。

テーブル ビューでカラムを無効にし、それによって同じ行が複数生成される場合、Firepower システムによってイベント ビューに [カウント（Count）] カラムが追加されます。テーブル ビュー ページで 1 つの値をクリックすると、その値によって制約することができます。カスタム ワークフローを作成する場合は、[テーブル ビューの追加（Add Table View）] をクリックしてテーブル ビューを追加します。

ドリルダウン ページ

ドリルダウン ページは、通常テーブル ビューのページに移動する前に調査対象を絞り込むために使用する中間ページです。ドリルダウン ページには、データベースで使用できるカラムのサブセットが含まれています。

たとえば、検出イベントのドリルダウン ページには、[IP アドレス（IP Address）]、[MAC アドレス（MAC Address）]、および [時刻（Time）] カラムだけが含まれています。また、侵入イベントのドリルダウン ページには、[優先順位（Priority）]、[影響フラグ（Impact Flag）]、[インラインの結果（Inline Result）]、および [メッセージ（Message）] カラムが含まれています。

ドリルダウン ページを使用すれば、表示するイベントの範囲を絞り込んだり、ワークフローで先へ進んだりできます。ドリルダウン ページで 1 つの値をクリックすると（たとえば、その値で制約を加えて、ワークフローの次のページに進んだ場合）、選択した値に一致するイベントをさらに詳しく調べることができます。ドリルダウン ページで値をクリックした場合、次のページがテーブル ビューであっても、値が存在するカラムは無効になりません。事前定義のワークフローのドリルダウン ページには、必ず [カウント（Count）] カラムがあることに注意してください。カスタム ワークフローを作成する場合は、[ページの追加（Add Page）] をクリックしてドリルダウン ページを追加します。

グラフ

接続データに基づくワークフローには、グラフ ページ（接続グラフとも呼ばれる）を含めることができます。

たとえば接続グラフには、一定期間にシステムで検出された接続の数を示す線グラフを表示することができます。一般的に接続グラフは、ドリルダウン ページと同様に、ユーザが調査対象を絞り込むために使用する中間ページです。

最終ページ

ワークフローの最終ページは、ワークフローがベースとするイベントのタイプによって異なります。

- ホスト ビューとは、アプリケーション、アプリケーションの詳細、検出イベント、ホスト、侵害の兆候（IOC）、サーバ、ホワイトリスト違反、ホスト属性、またはサードパーティ製の脆弱性に基づいたワークフローの最終ページです。このページからホストプロファイルを表示することにより、ユーザは、複数のアドレスを持つホストに関連付けられているすべての IP アドレス上のデータを簡単に表示することができます。
- ユーザの詳細ビューとは、ユーザとユーザ アクティビティに基づいたワークフローの最終ページです。
- 脆弱性の詳細ビューとは、Cisco の脆弱性に基づいたワークフローの最終ページです。
- パケット ビューは、侵入イベントに基づいたワークフローの最終ページです。

他の種類のイベント（監査ログイベントやマルウェアイベントなど）に基づいたワークフローには、最終ページがありません。

ワークフローの最終ページで詳細セクションを展開して、ワークフローの進行中に絞り込んだセットの各オブジェクトについて、具体的な情報を表示することができます。Web インターフェイスでは、ワークフローの最終ページに制約が表示されませんが、以前に設定した制約は保持されており、データのセットに適用されます。

ワークフロー ページのナビゲーション ツール

ワークフローのページには、ページ間の移動と、イベントの分析中に表示する情報の選択を容易にする視覚的なキューが用意されています。

ワークフロー ページのトラバーサル ツール

ワークフローに複数のデータ ページが含まれている場合は、各ページの下部にワークフロー内のページ数と、ページ間を移動するために使用できるツールが表示されます。これらのツールを次の表に示します。

表 *246*：ワークフロー ページのトラバーサル ツール

ページのトラバーサル ツール	操作
ページ番号 （別のページを表示するには、表示する番号を入力して Enter キーを押します。）	別のページを表示する
>	次のページを表示する
<	前のページを表示する
>|	最後のページに移動する
|<	最初のページに移動する

ファイル トラジェクトリ アイコン

ワークフローページで、新しいウィンドウにファイルのトラジェクトリ マップを表示する機会があるときは、ネットワーク トラジェクトリ アイコンが表示されます。このアイコンは、ファイルのステータスによって変わります。

表 *247*：ファイル トラジェクトリ アイコン

ファイル トラジェクトリ アイコン	ファイル ステータス
	正常
	マルウェア
	カスタム検出
	不明

ファイル トラジェクトリ アイコン	ファイル ステータス
	応対不可（Unavailable）

ホスト プロファイルのアイコン

ワークフローページでは、IPアドレスに関連付けられたホストプロファイルをポップアップ ウィンドウで表示することができ、ホスト プロファイル アイコンが表示されます。ホスト プロファイルのアイコンがグレー表示になっている場合は、ネットワーク マップ内にそのホストが存在することができないため、ホスト プロファイルを表示できません（0.0.0.0 など）。このアイコンは、ホストのステータスによって異なって表示されます。

表 *248*：ホスト プロファイルのアイコン

ホスト プロファイルのアイコン	ホスト ステータス
	ホストは潜在的に危険にさらされているとタグ付けされていません。
	ホストは、トリガーされた侵害の兆候（IOC）ルールによって潜在的に危険にさらされているとタグ付けされています。
	ブラックリスト化されています（セキュリティ インテリジェンス データに基づいて、トラフィック フィルタリングを実行している場合にのみ表示されます）。
	ブラックリスト化され、モニタに設定されています（セキュリティ インテリジェンス データに基づいて、トラフィック フィルタリングを実行している場合にのみ表示されます）。

脅威スコア アイコン

ワークフロー ページで、ファイルに関連付けられているスコアが最も高い脅威に関する動的分析サマリ レポートを表示すると、脅威スコア アイコンが表示されます。このアイコンは、ファイルの最も高い脅威スコアに応じて異なります。

表 *249*：脅威スコア アイコン

脅威スコア アイコン	脅威スコア レベル
	低（Low）
	中規模（Medium）
	高（High）
	非常に高い（Very high）

ワークフロー ツールバー

ワークフローの各ページには、関連する機能へすばやくアクセスするためのツールバーがあります。次の表で、ツールバー上の各リンクについて説明します。

表 *250*：ワークフロー ツールバーのリンク

機能	説明
このページをブックマーク	後でそのページに戻れるように、現在のページをブックマークします。ブックマークすると、表示中のページに適用されている制約が取得され、データがまだ存在している場合は後で同じデータに戻ることができます。
レポート作成者	現在制約されているワークフローを選択基準として使用して、レポート デザイナを開きます。
ダッシュボード	現行のワークフローに関連するダッシュボードを開きます。たとえば、[接続イベント（Connection Events）] ワークフローは [接続サマリ（Connection Summary）] ダッシュボードと関連付けられています。
ブックマークの表示	ユーザが選択できる、保存したブックマークのリストを表示します。
検索（Search）	ワークフローのデータについて高度な検索を実行できる [検索（Search）] ページが表示されます。下向きの矢印アイコンをクリックし、保存済みの検索を選択して使用することもできます。

関連トピック

ブックマーク，（1867 ページ）
イベント ビューからのレポート テンプレートの作成，（1716 ページ）
ダッシュボードについて，（223 ページ）
イベントの検索，（1871 ページ）

ドリルダウン ページの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

手順

ステップ 1 「表 245：ワークフローを使用する機能」の説明に従って、適切なメニュー パスとオプションを選択してワークフローにアクセスします。

ステップ 2 すべてのワークフローで、次のオプションを選択できます。

- 特定の値に制限して、次のワークフロー ページにドリルダウンするには、行内の値をクリックします。この処理はドリルダウン ページでのみ可能でることに注意してください。テーブルの行内の値をクリックしても、テーブル ビューが制約されるだけで、次のページにはドリル ダウンしません。
- いくつかのイベントによって制約したまま次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示させるイベントの横のチェック ボックスを選択し、[表示（View）] をクリックします。
- 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[すべて表示（View All）] をクリックします。

ヒント テーブル ビューでは、必ずページ名に「Table View」が含まれます。

テーブル ビュー ページの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

テーブル ビュー ページには、ドリルダウン、ホスト ビュー、パケット ビュー、脆弱性の詳細ページでは利用できない機能が用意されています。これらの機能は次のように使用します。

手順

ステップ 1 ワークフローの選択，（1837 ページ）の説明に従って、適切なメニュー パスとオプションを選択してワークフローにアクセスします。

ステップ 2 ワークフローの名前の下に表示されるワークフロー パスからテーブル ビューを選択します。

ステップ 3 必要に応じて、次に示す機能を使用してテーブル ビュー内に配置したり、移動したりします。

- 無効なカラムのリストを表示するには、[検索制約（Search Constraints）] の展開矢印（▶）をクリックします。
- 無効なカラムのリストを非表示するには、[検索制約（Search Constraints）] の折りたたみ矢印（▶）をクリックします。
- 無効になったカラムをイベント ビューに戻すには、[検索制約（Search Constraints）] の展開アイコン（▶）をクリックして検索制約を展開し、[無効カラム（Disabled Columns）] の下にあるカラム名をクリックします。
- カラムを表示または非表示（無効）にするには、各カラム名の横にあるクリアアイコン（✖）をクリックします。表示されるポップアップ ウィンドウで、該当するチェックボックスをオンまたはオフにして、どのカラムを表示するかを指定し、[適用（Apply）] をクリックします。

位置情報（GeoLocation）

地理位置情報機能によって、ルート可能な IP アドレスの地理的な送信元についてのデータ（国や大陸など）が提供されます。この情報は、イベント、資産のプロファイル、コンテキスト エクスプローラ、ダッシュボードやその他の分析ツールで使用できます。

（注） 国間を移動するモバイル デバイスやその他のホストが検出された場合、システムは特定の国ではなく大陸名を報告する可能性があります。

地理位置情報データを使用してネットワーク トラフィックをフィルタできます。たとえば、接続の発信元または終端が、組織と関連性のない国であるかどうかを判別できます。インライン展開では、これらの接続をブロックするか、またはを行うことができます。

地理位置情報データはシステムの地理位置情報データベース（GeoDB）内に保存されます。シスコでは、GeoDB の定期的な更新を提供しています。[概要（About）] ページ（[ヘルプ（Help）] > [概要（About）]）に GeoDB の現在の更新バージョンが表示されています。

GeoDB の更新を許可する場合、Firepower Management Center Web インターフェイスで小さな国旗のアイコンと ISO 国番号をクリックして特定の IP アドレスに関する地理位置情報の詳細を取得することができます。地理情報の詳細情報, （1846ページ）を参照してください。また、サードパーティのマップ ツールを使用して、検出された場所を特定することもできます。GeoDB を更新しない場合、これらの詳細情報は取得できません。

[接続のサマリ（Connection Summary）] ダッシュボードなど、集約的な地理位置情報から詳細の地理位置情報を表示することはできません。

関連トピック

ネットワーク条件, （345 ページ）
地理位置情報オブジェクト, （396 ページ）
相関ポリシーとルールの概要, （1633 ページ）
トラフィック プロファイル条件, （1681 ページ）
地理位置情報データベースの更新, （169 ページ）

地理情報の詳細情報

可用性に応じて、[地理情報の詳細（Geolocation Details）] ページに多数のフィールドが表示される場合があります。次の表で、これらのフィールドの情報について示します。（情報がないフィールドは表示されません。）

表 *251*：地理情報の詳細フィールド

フィールド	目次
国（Country）	ホスト IP アドレスに関連付けられている国が国旗とともに示されます。大陸はカッコ内に表示されます。例：`United States (North America)`、`Equatorial Guinea (Africa)`
地域	ホストが存在する国の州、県、またはその他の小区域。例：`VA`、`35`
市区町村郡（City）	ホストが存在する市。例：`Seattle`、`Fukuoka`

フィールド	目次
[郵便番号（Postal Code）]	ホストが存在する地域の郵便番号。例：361000、90210
緯度/経度（Latitude/Longitude）	ホストの場所の正確な座標。例：40.0375, -76.1053、53.4050, -0.5484
マップ	外部のマッピング サイト（Google Maps、Yahoo Maps、Bing Maps、OpenStreetMap など）へのリンク。ホストのおよその位置のコンテキストマップを表示するには、リンクをクリックします。
タイムゾーン（Timezone）	ホストの場所のタイム ゾーン（該当する場合には夏時間が示されます）。例：GMT+8:00、GMT-4:00 (In DST)
ASN	ホストIPアドレスに関連付けられている自律システム番号（ASN）、およびそのASNに関する追加情報。例：14618 (Amazon.com Inc.)、4837 (Cncgroup China169 Backbone)
ISP	ホストのIPアドレスに関連付けられているインターネット サービス プロバイダー（ISP）。例：Atlantic Broadband、China Unicom Ip Network
自宅/会社（Home/Business）	ホストの接続が自宅または会社のどちらの目的であるかを示します。
Organization	ホストの IP アドレスに関連付けられている組織。例：Amazon.com、Bank of America
ドメイン名（Domain Name）	ホストの IP アドレスに関連付けられているドメイン名。例：amazonaws.com、xmcnc.net
接続タイプ（Connection Type）	ホストの IP アドレスに関連付けられている接続タイプ。例：Broadband、DSL
プロキシ タイプ（Proxy Type）	使用するプロキシのタイプ。例：Anonymous、Corporate

接続イベント グラフ

システムは、テーブル形式のドリル ダウン ページを使ったワークフローや最終的なイベントのテーブル表示に加えて、5分間隔で集計されたデータを使用して、特定の接続データをグラフィック表示することができます。グラフ表示できるのは、データを集約するのに使用する情報（送信元と宛先のIPアドレス（およびこれらのホストに関連するユーザ）、宛先ポート、トランスポート プロトコルとアプリケーション プロトコル）のみです。

ヒント　セキュリティ インテリジェンス イベントを関連する接続イベントとは別にグラフ表示することはできません。セキュリティ インテリジェンスのフィルタリング アクティビティの概要をグラフィック表示するには、ダッシュボードとコンテキスト エクスプローラを使用します。

接続グラフは 3 種類あります。

- 円グラフは、1 つのデータセットのデータをカテゴリ分けして表示します。
- 棒グラフは、1 つあるいは複数のデータセットのデータをカテゴリ分けして表示します。
- 折れ線グラフは、時間の経過に伴って 1 つあるいは複数のデータセットのデータをプロットします。標準ビューあるいは速度（変化のペース）ビューを使用します。

（注）　システムは、トラフィック プロファイルを線グラフで表示します。他の接続グラフと同様に操作可能ですが、いくつか規制があります。トラフィック プロファイルを表示するには、管理者アクセス権が必須です。

ワークフロー テーブルと同様に、ワークフロー グラフもドリル ダウンし、制約を加えることで分析の的を絞ることができます。

棒グラフおよび折れ線グラフはどちらも複数のデータセットを表示できます。つまり、各 X 軸データ ポイントに対し、Y 軸に複数の値を表示できます。たとえば、一意のイニシエータとレスポンダの総数を表示することができます。円グラフでは、1つのデータセットのみ表示できます。

X 軸または Y 軸、もしくは両方を変更することによって、接続グラフにさまざまなデータやデータセットを表示できます。円グラフでは、X 軸を変更すると独立変数が変わり、Y 軸を変更すると従属変数を変わります。

関連トピック

接続の概要（グラフ用集約データ），（1922 ページ）
接続の概要（グラフ用集約データ），（1922 ページ）

接続イベント グラフの使用方法

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	（ワークフローに応じて） Admin/Maint/Any Security Analyst

Firepower Management Center では、検索する情報に応じて、接続イベント グラフを表示したり操作したりできます。

接続グラフにアクセスしたときに表示されるページは、使用するワークフローによって異なります。接続イベントのテーブル ビューで終了する、事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [接続（Connections）] > [イベント（Events）]を選択します。

（注） 接続イベント テーブルがグラフの代わりに表示される場合、または別のグラフを表示する場合は、ワークフロー タイトルの横にある（ワークフローの切り替え）をクリックし、グラフが含まれる事前定義されたワークフローまたはカスタム ワークフローを選択します。接続グラフを含むすべての事前定義された接続イベント ワークフローは、接続のテーブル ビューで終了します。

ステップ 2 次の選択肢があります。

- [時間範囲（Time Range）]：時間範囲を調整する場合は（グラフがブランクの場合に役立ちます）、時間枠の変更, （1859 ページ）を参照してください。
- [フィールド名（Field Name）]：ユーザが図示可能なデータの詳細については、接続およびセキュリティ インテリジェンス イベント フィールド, （1923 ページ）を参照してください。
- [ホスト プロファイル（Host Profiles）]：IP アドレスのホスト プロファイルを表示するには、発信側または応答側による接続データが表示されているグラフで、棒グラフの棒または円グラフの扇形をクリックし、[ホスト プロファイルの表示（View Host Profile）]を選択します。
- [ユーザ プロファイル（User Profile）]：ユーザ プロファイル情報を表示するには、発信側ユーザによる接続データが表示されているグラフで、棒グラフの棒または円グラフの扇形をクリックし、[ユーザ プロファイルの表示（View User Profile）] を選択します。
- [その他の情報（Other Information）]：図示されたデータに関する詳細については、折れ線グラフの点、棒グラフの棒、または円グラフの扇形の上にカーソルを置きます。
- [固定（Constrain）]：ワークフローを次のページに進めずに接続グラフを X 軸（独立した変数）基準で固定するには、折れ線グラフの点、棒グラフの棒、または円グラフの扇形をクリックし、[表示方法（View by）] オプションを選択します。
- [データ選択（Data Selection）]：グラフに表示されるデータを変更するには、[X 軸（X-Axis）] または [Y 軸（Y-Axis）] をクリックし、図示する新しいデータを選択します。X 軸を [時間（Time）] に変更、または [時間（Time）] から変更すると、グラフ タイプも変更されます。Y 軸を変更すると、表示されるデータセットに影響します。
- [データセット（Datasets）]：グラフのデータセットを変更するには、[データセット（Datasets）] をクリックし、新しいデータセットを選択します。
- [切り離し（Detach）]：デフォルトの時間範囲に影響を与えることなくさらに分析を実行できるように接続グラフを分離するには、[切り離し（Detach）] をクリックします。

ヒント　コピーを作成するには、分離したグラフで [新規ウィンドウ] をクリックします。分離した各グラフ上で、別々の分析ができるようになります。トラフィック プロファイルは、分離したグラフです。

- [詳細（Drill-Down）]：ワークフローで次のページにドリルダウンするには、折れ線グラフの点、棒グラフの線、または円グラフの扇形をクリックし、[詳細（Drill-Down）] を選択します。折れ線グラフで点をクリックすると、次のページの時間枠は、クリックした点を中心とする 10 分間に変更されます。棒グラフの棒または円グラフの扇形をクリックすると、その棒または扇形が表す基準に基づいて次のページが制約されます。
- [エクスポート（Export）]：グラフの接続データを CSV（カンマ区切り値）ファイルとしてエクスポートするには、[データのエクスポート（Export Data）] を選択します。次に、[CSV ファイルのダウンロード（Download CSV File）] をクリックし、ファイルを保存します。
- [グラフ タイプ（Graph Type）]：[折れ線（Line）]- 標準と速度（変化のペース）の折れ線グラフを切り替えるには、[速度（Velocity）] をクリックし、[標準（Standard）] または [速度（Velocity）] を選択します。
- [グラフ タイプ（Graph Type）]：[棒と円（Bar and Pie）] - 棒グラフと円グラフを切り替えるには、[棒グラフに切り替え（Switch to Bar）] または [円グラフに切り替え（Switch to Pie）] をクリックします。円グラフには複数のデータセットを表示できないため、複数のデータセットを持つ棒グラフから円グラフに切り替えた場合、円グラフは自動的に選択された 1 つのデータセットだけを表示します。表示するデータセットを選択する際、Firepower Management Center は、発信側と応答側の統計情報よりも全体の統計情報を優先し、応答側の統計情報よりも発信側の統計情報を優先します。
- [ページ間の移動（Navigate Between Pages）]：現在のワークフローで現在の制約を保持したままページ間を移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- [イベント ビュー間の移動（Navigate Between Event Views）]：他のイベント ビューに移動して関連するイベントを表示するには、[移動先（Jump to）] をクリックし、ドロップダウンリストからイベント ビューを選択します。
- [再センタリング（Recenter）]：時間範囲の長さを変更せずにある時点を中心に折れ線グラフを再センタリングするには、その点をクリックし、[再センタリング（Recenter）] を選択します。
- [ズーム（Zoom）]：ズームインまたはズームアウトしながらある時点を中心に折れ線グラフを再センタリングするには、その点をクリックし、[ズーム（Zoom）] を選択してから新しい時間枠を選択します。

（注）　分離したグラフを使用している場合を除いて、制約、再センタリング、およびズームすると Firepower Management Center のデフォルトの時間範囲が変わります。

例：接続グラフの制約

ある期間の接続のグラフについて考えてみましょう。グラフ上の点をポートによって制約すると、検出された接続イベント数に基づいて、最もアクティブだった10のポートを示す棒グラフが表示されますが、クリックした点を中心とする 10 分間の時間枠によって制約されます。

棒の 1 つをクリックし、[発信側 IP による表示（View by Initiator IP）] を選択してグラフをさらに制約すると、それまでと同じ10分間の時間枠だけでなく、クリックした棒が表すポートでも制約された新しい棒グラフが表示されます。

例：円グラフの X 軸と Y 軸の変更

ポートごとのキロバイト数を表示する円グラフについて考えてみましょう。この場合、X 軸は レスポンダ ポート、Y 軸は キロバイト です。この円グラフは、ある間隔に監視対象ネットワークで送信されたデータの合計キロバイト数を表します。円の中の扇形は、各ポートで検出されたデータの比率を表します。

- グラフの X 軸を アプリケーション プロトコル に変更すると、引き続き円グラフは送信データの合計キロバイト数を表しますが、円の中の扇形は検出された各アプリケーション プロトコルの送信データの比率を表します。
- グラフの Y 軸を パケット に変更すると、円グラフはある間隔に監視対象ネットワークで送信された合計パケット数を表し、円の中の扇形は各ポートで検出された合計パケット数の割合を表します。

関連トピック

ワークフローの使用, （1834 ページ）
イベント ビュー設定の設定, （38 ページ）
ワークフローの使用, （1834 ページ）
イベント ビュー設定の設定, （38 ページ）

接続グラフ データ オプション

X 軸または Y 軸、もしくは両方を変更することによって、接続グラフにさまざまなデータを表示できます。円グラフでは、X 軸を変更すると独立変数が変わり、Y 軸を変更すると従属変数を変わります。

表 *252*：*X* 軸オプション

X 軸オプション	グラフの種類	次の基準でこのデータをグラフ化する
アプリケーション プロトコル（Application Protocol）	棒グラフまたは円グラフ	最もアクティブな 10 個のアプリケーション プロトコルに基づいて

X 軸オプション	グラフの種類	次の基準でこのデータをグラフ化する
Device	棒グラフまたは円グラフ	最もアクティブな 10 台の管理対象デバイスに基づいて
イニシエータ IP（Initiator IP）	棒グラフまたは円グラフ	最もアクティブな 10 個のイニシエータ ホスト IP アドレスに基づいて
イニシエータ ユーザ（Initiator User）	棒グラフまたは円グラフ	最もアクティブな 10 名のイニシエータ ユーザに基づいて
レスポンダ IP（Responder IP）	棒グラフまたは円グラフ	最もアクティブな 10 個のレスポンダ ホスト IP アドレスに基づいて
レスポンダ ポート（Responder Port）	棒グラフまたは円グラフ	最もアクティブな 10 個のレスポンダ ポートに基づいて
送信元デバイス（Source Device）	棒グラフまたは円グラフ	最もアクティブな 10 個の NetFlow データ エクスポータと、Firepower システムの管理対象デバイスによって検出されたすべての接続の `Firepower` という名前の送信元デバイスに基づいて。
時刻（Time）	ライン	時系列 Y 軸と [時刻（Time）] を切り替えることでグラフの種類も変わり、データセットを変更できます。

表 *253*：*Y* 軸オプション

Y 軸オプション	X 軸の基準を使用してこのデータをグラフ化する
バイト（Bytes）	送信バイト数
接続（Connections）	接続数
KB（KBytes）	送信キロバイト数
KB/秒（KBytes Per Second）	KB/秒
パケット（Packets）	送信パケット数

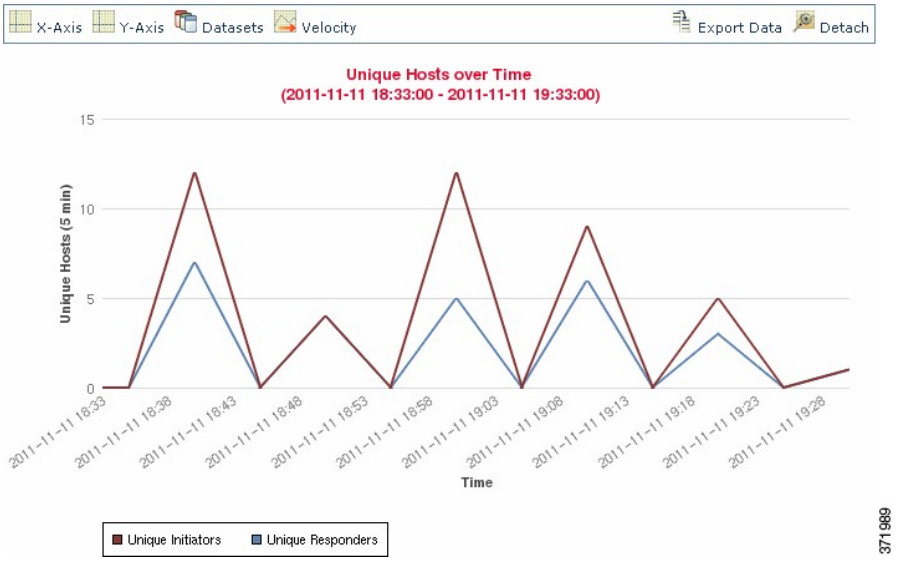
Y 軸オプション	X 軸の基準を使用してこのデータをグラフ化する
固有のホスト（Unique Hosts）	検出された固有のホスト数
固有のアプリケーション プロトコル（Unique Application Protocols）	固有のアプリケーション プロトコル数
固有ユーザ（Unique Users）	固有ユーザ数

複数のデータセットの接続グラフ

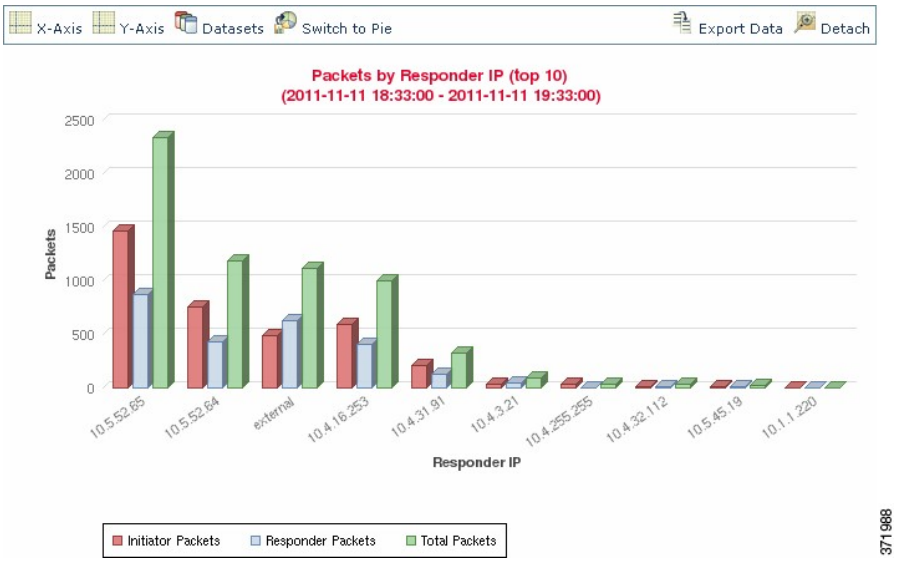
棒グラフおよび折れ線グラフはどちらも複数のデータセットを表示できます。つまり、各 X 軸データ ポイントに対し、Y 軸に複数の値を表示できます。たとえば、一意のイニシエータとレスポンダの総数を表示することができます。

（注） 円グラフには複数のデータセットを表示**できません**。複数のデータセットを持つ棒グラフから円グラフに切り替えた場合、円グラフは自動的に選択された1つのデータセットだけを表示します。表示するデータセットを選択する際、Firepower Management Center は、イニシエータとレスポンダの統計情報よりも全体の統計情報を優先し、イニシエータの統計情報よりもレスポンダの統計情報を優先します。

折れ線グラフでは、複数のデータセットは複数の線として、それぞれ異なる色で表示されます。たとえば次のグラフは、監視対象ネットワークにおいて1時間の間に検出された一意のイニシエータの合計数と一意のレスポンダの合計数を表示しています。



棒グラフでは、複数のデータセットが X 軸データ ポイントごとに色分けされた棒として表示されます。たとえば次の棒グラフは、監視対象ネットワーク上で送信されたパケットの合計数と、イニシエータによって送信されたパケット数、レスポンダによって送信されたパケット数を表示しています。



接続グラフ データセット オプション

次の表では、接続グラフの x 軸に表示できるデータセットについて説明します。

表 *254*：データセット オプション

y 軸が表示されている場合は、	データベースとして選択できます。
接続（Connections）	デフォルトのみです。監視対象のネットワークで検出された接続数（[接続（Connections）]）です。これは、トラフィック プロファイル グラフ用の唯一のオプションです。
KB（KBytes）	以下を組み合わせています。 • 監視対象のネットワークで送信される合計キロバイト（[合計キロバイト（Total KBytes）]） • 監視対象のネットワークでホスト IP アドレスから送信されるキロバイト数（[イニシエータのキロバイト（Initiator KBytes）]） • 監視対象のネットワークでホスト IP アドレスによって受信されるキロバイト数（[レスポンダのキロバイト（Responder KBytes）]）
KB/秒（KBytes Per Second）	デフォルトのみです。監視対象ネットワーク上で送信される合計キロバイト/秒（[合計キロバイト/秒（Total KBytes Per Second）]）です。

y 軸が表示されている場合は、	データベースとして選択できます。
パケット	以下を組み合わせています。 • 監視対象ネットワークで送信される合計パケット（[合計パケット（Total Packets）]） • 監視対象ネットワークのホスト IP アドレスから送信されたパケット数（[イニシエータ パケット（Initiator Packets）]） • 監視対象ネットワークのホスト IP アドレスによって受信されたパケット数（[レスポンダ パケット（Responder Packets）]）です。
固有のホスト（Unique Hosts）	以下を組み合わせています。 • 監視対象ネットワークの固有セッション イニシエータ数（[固有イニシエータ（Unique Initiators）]）です。 • 監視対象ネットワークの固有セッション レスポンダ数（[固有レスポンダ（Unique Responders）]）
固有のアプリケーション プロトコル（Unique Application Protocols）	デフォルトのみです。監視対象ネットワークの固有のアプリケーション プロトコル数（[固有アプリケーション プロトコル（Unique Application Protocols）]）です。
固有ユーザ（Unique Users）	デフォルトのみです。監視対象のネットワークでのセッション イニシエータにログインした固有ユーザ数（[固有イニシエータ ユーザ（Unique Initiator Users）]）です。

イベント時間の制約

各イベントには、そのイベントがいつ発生したかを示すタイム スタンプがあります。時間枠（時間範囲とも呼ばれる）を設定することによって、いくつかのワークフローに表示される情報を制約することができます。

時間によって制約できるイベントに基づいたワークフローには、ページの上部に時間範囲を表す行が含まれています。デフォルトでは、シスコ アプライアンス上のワークフローは、1 時間前が開始時間として設定された時間枠を使用します。たとえば、午前 11:30 にログインした場合、午前 10:30～11:30 の間に発生したイベントが表示されます。時間が経過するにしたがって、時間枠が拡張されます。午後 12:30 には、午前 10:30～午後 12:30 の間に発生したイベントが表示されます。

イベント ビューの設定で独自のデフォルト時間枠を設定することによって、この動作を変更することができます。これにより、次の 3 つのプロパティが影響を受けます。

- 時間枠のタイプ（静的、拡張、またはスライディング）

- 時間枠の長さ
- 時間枠の数（複数の時間枠、または単一のグローバル時間枠）

ページの上部にある時間範囲をクリックして[日時（Date/Time）]ポップアップ ウィンドウを表示し、デフォルトの時間枠の設定に関係なく、イベントの分析中に時間枠を手動で変更することができます。設定した時間枠の数、および使用しているアプライアンスのタイプに応じて[日時（Date/Time）]ウィンドウを使用して、表示しているイベントのタイプに対するデフォルトの時間枠を変更することもできます。

最後に、時間枠は一時停止することができるため、時間枠の変更と削除、または必要のないイベントを追加することなく、ワークフローで提供されたデータを調べることができます。ページの下部にあるリンクをクリックしてイベントの他のページを表示する場合は、異なるワークフローページで同じイベントを表示しないように、時間枠が自動的に一時停止することに注意してください。準備ができたら時間枠の一時停止を解除できます。

関連トピック

イベント ビュー設定の設定, （38 ページ）
接続およびセキュリティ インテリジェンス イベント テーブルの使用, （1951 ページ）

イベントの時間枠のカスタマイズ

デフォルトの時間枠に関係なく、イベントの分析中に時間枠を手動で変更することができます。

（注） 手動による時間枠の設定は、現在のセッションについてのみ有効です。いったんログアウトしてからもう一度ログインすると、時間枠はデフォルトにリセットされます。

ユーザが設定した時間枠の数によっては、1 つのワークフローの時間枠の変更が、アプライアンス上の他のワークフローに影響を与えることがあります。たとえば、単一のグローバル時間枠がある場合、1 つのワークフローの時間枠を変更すると、アプライアンス上の他のすべてのワークフローの時間枠が変更されます。一方、複数の時間枠を使用している場合は、監査ログまたはヘルス イベントのワークフローの時間枠を変更しても、他の時間枠には影響を与えませんが、他の種類のイベントの時間枠を変更すると、時間で制約できるすべてのイベント（監査イベントとヘルス イベントは除く）が影響を受けます。

すべてのワークフローを時間によって制約できるわけではないため、時間枠の設定は、ホスト、ホスト属性、アプリケーション、アプリケーションの詳細、脆弱性、ユーザ、またはホワイトリスト違反に基づいたワークフローには影響を与えないことに注意してください。

[日付/時刻（Date/Time）]ウィンドウの[時間枠（Time Window）]タブを使用して、時間枠を手動で設定します。デフォルトの時間枠設定で設定した時間枠の数によって、タブのタイトルは以下のいずれかになります。

- [イベントの時間枠（Events Time Window）]：複数の時間枠を設定し、監査ログまたはヘルス イベントのワークフロー以外のワークフローに対して時間枠を設定している場合

- [ヘルス モニタリングの時間枠（Health Monitoring Time Window）]：複数の時間枠を設定し、ヘルス イベントのワークフローに対して時間枠を設定している場合
- [監査ログの時間枠（Audit Log Time Window）]：複数の時間枠を設定し、監査ログに対して時間枠を設定している場合
- [グローバル時間枠（Global Time Window）]：単一の時間枠を設定している場合

時間枠を設定する場合には、最初に、使用する時間枠のタイプを決定する必要があります。

- 静的（*static*）の時間枠では、特定の開始時刻から特定の終了時刻までの間に生成されたすべてのイベントが表示されます。
- 拡張（*expanding*）の時間枠では、特定の開始時刻から現在までの間に生成されたすべてのイベントが表示されます。そして、時間の経過とともに時間枠が拡張され、新しいイベントがイベント ビューに追加されます。
- スライディング（*sliding*）の時間枠では、特定の開始時刻（たとえば、1 週間前）から現在までの間に生成されたすべてのイベントが表示されます。そして、時間の経過とともに時間枠が「スライド」するため、設定した範囲（この例では、過去 1 週間）のイベントのみが表示されます。

選択したタイプによって、[日付/時刻（Date/Time）] ウィンドウが変化し、さまざまな設定オプションが提供されます。

（注） Firepower システムでは、タイム ゾーンの設定に指定された時間に基づいて、24 時間の時計を使用します。

時間枠の設定

次の表で、[時間枠（Time Window）] タブで設定できるさまざまな項目について説明します。

表 *255*：時間枠の設定

設定	時間枠のタイプ	説明
[時間枠タイプ（time window type）] ドロップダウン リスト	適用対象外	使用する時間枠のタイプとして、[静的（static）]、[拡張（expanding）]、または [スライディング（sliding）] のいずれかを選択します。 イベント ビューを時間で制約している場合は、（グローバルであるかイベントに特有であるかに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

設定	時間枠のタイプ	説明
[開始時刻（Start Time）] カレンダー	[静的（static）] および [拡張（expanding）]	時間枠の開始日と時刻を指定します。すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時（UTC）～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。 カレンダーを使用する代わりに、下記で説明するプリセット オプションを使用することもできます。
[終了時刻（End Time）] カレンダー	静的	時間枠の終了日と時刻を指定します。すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時（UTC）～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。 拡張時間枠を使用している場合は、[終了時刻（End Time）] カレンダーがグレー表示になり、終了時刻が「現在の時刻（Now）」と示されることに注意してください。 カレンダーを使用する代わりに、下記で説明するプリセット オプションを使用することもできます。
[最後を表示（Show the Last）] フィールドおよびドロップダウン リスト	[スライディング（sliding）]	スライディング時間枠の長さを設定します。
[プリセット（Presets）]：[最後（Last）]	すべて	リスト内のいずれかの時間範囲をクリックし、アプライアンスのローカル時刻に基づいて時間枠を変更します。たとえば、[1 週間（1 week）] をクリックすると、最後の 1 週間を反映するように時間枠が変わります。プリセットをクリックすると、選択したプリセットを反映するようにカレンダーが変わります。
[プリセット（Presets）]：[現在（Current）]	[静的（static）] および [拡張（expanding）]	リスト内のいずれかの時間範囲をクリックし、アプライアンスのローカル時刻と日付に基づいて時間枠を変更します。プリセットをクリックすると、選択したプリセットを反映するようにカレンダーが変わります。 次の点に注意してください。 • 現在の日付は午前 0 時から始まる • 現在の週は日曜日の午前 0 時から始まる • 現在の月は、月の最初の日の午前 0 時から始まる

設定	時間枠のタイプ	説明
[プリセット（Presets）]：[同期先（Synchronize with）]	すべて（グローバルな時間枠を使用している場合は使用不可）	以下のいずれかをクリックします。 • [イベントの時間枠（Events Time Window）]：現在の時間枠とイベントの時間枠を同期する場合 • [ヘルス モニタリングの時間枠（Health Monitoring Time Window）]：現在の時間枠とヘルス モニタリングの時間枠を同期する場合 • [監査ログの時間枠（Audit Log Time Window）]：現在の時間枠と監査ログの時間枠を同期する場合

時間枠の変更

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じる）

手順

ステップ 1 時間により制約されたワークフローで、時間範囲のアイコン（）をクリックし、[日付と時間（Date/Time）] ウィンドウを開きます。

ステップ 2 [イベントの時間枠（Events Time Window）] タブで、時間枠の設定, （1857 ページ）に記載されているように時間枠を設定します。

ヒント 時間枠をデフォルトの設定に戻すには、[リセット（Reset）] をクリックします。

ステップ 3 [適用（Apply）] をクリックします。

イベントのデフォルト時間枠

イベントの分析中に、[日付/時間（Date/Time）] ウィンドウの [設定（Preferences）] タブを使用し、表示しているイベントのタイプに対するデフォルトの時間枠を（イベント ビューの設定を使用せずに）変更することができます。

この方法でデフォルトの時間枠を変更すると、表示しているイベントのタイプのデフォルト時間枠のみが変わります。たとえば、複数の時間枠を設定している場合に [設定（Preferences）] タブ

でデフォルトの時間枠を変更すると、イベント、ヘルスモニタリング、または監査ログウィンドウのいずれかの設定が変更されます。つまり、最初のタブで示されている時間枠が変更されます。1 つの時間枠を設定している場合に [設定（Preferences）] タブでデフォルトの時間枠を変更すると、イベントのすべてのタイプのデフォルト時間枠が変わります。

関連トピック

デフォルト時間枠, （41 ページ）

イベント タイプのデフォルトの時間枠オプション

次の表で、[設定（Preferences）] タブで設定できるさまざまな設定について説明します。

表 *256*：時間枠の設定

設定	説明
更新間隔（Refresh Interval）	イベント ビューの更新間隔を分単位で設定します。ゼロを入力すると、更新オプションは無効になります。
時間枠の数（Number of Time Windows）	使用する時間枠の数を指定します。 • 監査ログ、ヘルスイベント、および時間によって制約可能なイベントに基づいたワークフローに対してそれぞれ別のデフォルト時間枠を設定する場合は、[複数（Multiple）] を選択します。 • すべてのイベントに適用されるグローバルな時間枠を使用する場合は、[単一（Single）] を選択します。
デフォルト時間枠：[最後を表示 - スライディング（Show the Last - Sliding）]	この設定を選択すると、指定する長さのスライディングのデフォルト時間枠を設定できます。 アプライアンスは、特定の開始時刻（たとえば1時間前）から現在までに生成されたすべてのイベントを表示します。イベント ビューの変更と共に、時間枠は「スライド」して、常に最後の 1 時間内のイベントが表示されます。
デフォルト時間枠：[最後を表示 - 静的/拡張（Show the Last - Static/Expanding）]	この設定を選択すると、指定する長さの、静的または拡張のデフォルト時間枠を設定できます。 **静的な**時間枠の場合（[終了時間を使用（Use End Time）] チェックボックスをオンにした場合）、アプライアンスは特定の開始時間（1 時間前などの）から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[終了時間を使用（Use End Time）] チェックボックスをオフにしたの場合）、アプライアンスは特定の開始時間（1 時間前などの）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。

設定	説明
デフォルト時間枠：[本日 - 静的/拡張（Current Day - Static/Expanding）]	この設定を選択すると、現在の日付に対して静的または拡張のデフォルト時間枠を設定できます。現在の日付は、現行セッションのタイム ゾーン設定に基づいて午前 0 時に始まります。 **静的な**時間枠の場合（[終了時間を使用（Use End Time）] チェックボックスをオンにした場合）、アプライアンスは午前0時から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[終了時間を使用（Use End Time）] チェックボックスをオフにした場合）、アプライアンスは午前0時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 24 時間を超えて分析を続けた場合、この時間枠は 24 時間よりも長くなる可能性があることに注意してください。
デフォルト時間枠：[今週 - 静的/拡張（Current Week - Static/Expanding）]	この設定を選択すると、現在の週に対して静的または拡張のデフォルト時間枠を設定できます。現在の週は、現行セッションのタイム ゾーン設定に基づいて直前の日曜日の午前 0 時に始まります。 **静的な**時間枠の場合（[終了時間を使用（Use End Time）] チェックボックスをオンにした場合）、アプライアンスは午前0時から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[終了時間を使用（Use End Time）] チェックボックスをオフにした場合）、アプライアンスは日曜日の午前0時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 1 週間を超えて分析を続けた場合、この時間枠は 1 週間よりも長くなる可能性があることに注意してください。

イベント タイプのデフォルトの時間枠の変更

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst

手順

ステップ 1 時間により制約されたワークフローで、時間範囲のアイコン（）をクリックし、[日付と時間（Date/Time）] ウィンドウを開きます。

ステップ 2 [優先（Preferences）] タブをクリックし、イベント タイプのデフォルトの時間枠オプション，（1860 ページ）に記載されているようにプリファレンスを変更します。

ステップ 3 [設定の保存（Save Preferences）] をクリックします。

ステップ 4 次の 2 つの対処法があります。

- 使用しているイベント ビューに新しいデフォルト時間枠の設定を適用するには、[適用（Apply）] をクリックして [日付と時間（Date/Time）] ウィンドウを閉じてイベント ビューをリフレッシュします。
- デフォルトの時間枠設定を適用せずに分析を続けるには、[適用（Apply）] をクリックせずに [日付と時間（Date/Time）] ウィンドウを閉じます。

時間枠の進行

時間枠は一時停止することができます。これにより、ワークフローから提供されたデータのスナップショットを調べることができます。一時停止が解除されたワークフローが更新されると、それによって、調査したいイベントが削除されたり、調査対象外のイベントが追加されたりすることがあるため、この機能は役立ちます。

静的（static）の時間枠は一時停止できないことに注意してください。また、イベントの時間枠の一時停止はダッシュボードに影響を与えず、ダッシュボードの一時停止もイベントの時間枠の一時停止に影響を与えません。

分析が完了したら、時間枠の一時停止を解除できます。時間枠の一時停止を解除すると、設定に従って時間枠が更新されます。また、一時停止を解除した時間枠を反映するようにイベントビューも更新されます。

1 つのワークフローのページに表示できるイベント数よりも多くのイベントがデータベースに含まれている場合は、ページの下部にあるリンクをクリックして、さらにイベントを表示できます。リンクをクリックすると、同じイベントが 2 回表示されないように時間枠が自動的に一時停止します。

時間枠の一時停止/一時停止解除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst（ワークフローによる）

手順

時間で制約されているワークフローでは、目的の時間範囲コントロールを選択できます。

- 時間枠を一時停止するには、時間範囲コントロールの一時停止アイコン（）をクリックします。
- 時間枠の一時停止を解除するには、時間範囲コントロールの再生アイコン（）をクリックします。

イベント ビューの制約

ワークフロー ページに表示される情報は、ユーザが設定した制約によって異なります。たとえばイベント ワークフローを最初に開いた場合、情報は、最後の 1 時間に生成されたイベントに制約されています。

ワークフローの次のページに進んで、表示されるデータを特定の値で制約する場合は、ページでこれらの値を持つ行を選択し、[表示（View）] をクリックします。現在の制約を保持し、すべてのイベントを含めた状態でワークフローの次のページに進むには、[すべて表示（View All）] を選択します。

（注） 複数の不可算値を持つ行を選択し、[表示（View）] を選択すると、複合的な制約が作成されます。

ワークフローのデータを制約するための 3 番目の方法があります自身が選択した値を持つ行のみが表示されるようページを制約し、ページの上部に示される制約リストに選択した値を追加するには、ページの行で値をクリックします。たとえば、記録された接続のリストを表示する場合に、アクセス制御を使用して、自身が許可したものだけがリストに示されるよう制約する場合は、[アクション（Action）] カラムで [許可（Allow）] をクリックします。他の例では、侵入イベントを表示する場合に、宛先ポートが 80 のイベントのみがリストに示されるよう制約する場合は、[宛先ポート/ICMP コード（Destination Port/ICMP Code）] カラムで [80（http）/tcp（80 (http)/tcp）] をクリックします。

ヒント モニタ ルールの条件に基づいて接続イベントを制約するための手順は少し異なり、いくつかの追加手順が必要になる場合があります。また、関連付けられているファイルや侵入情報によって接続イベントを制約することはできません。

検索を使用して、ワークフローの情報を制約することもできます。1 つのカラム内の複数の値について制約する場合は、この機能を使用します。たとえば、2 つの IP アドレスに関連しているイベントを表示する場合は、[検索の編集（Edit Search）] をクリックし、[検索（Search）] ページで

対象の [IP アドレス（IP address）] フィールドを変更して両方のアドレスが含まれるようにして、[検索（Search）] をクリックします。

検索ページで入力した検索条件はページの上部に制約として表示され、これに従って制約されたイベントが合わせて表示されます。Firepower Management Center では、複合的な制約でない限り、他のワークフローにナビゲートしたときにも現在の制約が適用されます。

検索する場合は、検索対象のテーブルに検索の制約を適用するかどうかに注意する必要があります。たとえば、クライアント データは接続サマリーでは使用できません。接続で検出されたクライアントに基づいて接続イベントを検索し、結果を接続サマリーイベント ビューで表示すると、Firepower Management Center では、制約が設定されていない場合と同じように接続データが表示されます。無効な制約は、非適用（N/A）とラベルが付けられ、取り消し線が付けられます。

イベントの制約

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

手順

ステップ 1 ワークフローの選択，（1837 ページ）の説明に従って適切なメニューパスとオプションを選択し、ワークフローにアクセスします。

ステップ 2 すべてのワークフローで、次のオプションを選択できます。

- ビューを単一の値と一致するイベントに制約するには、ページの行内の目的の値をクリックします。
- ビューを複数の値と一致するイベントに制約するには、その値を持つイベントのチェックボックスをオンにし、[表示（View）] をクリックします。

  （注） 行に複数の不可算値が含まれている場合は、複合的な制約が追加されます。

- 制約を解除するには、[制約の検索（Search Constraints）] の展開矢印（▶）をクリックし、展開された [制約の検索（Search Constraints）] リストで制約の名前をクリックします。
- 検索ページを使用して制約を編集するには、[検索の編集（Edit Search）] をクリックします。
- 保存済み検索として制約を保存するには、[検索の保存（Save Search）] をクリックし、クエリに名前を付けます。

（注） 複合的な制約が含まれているクエリは保存できません。

- 別のイベント ビューで同じ制約を使用するには、[移動先（Jump to）] をクリックし、イベント ビューを選択します。

  （注） 別のワークフローに切り替えると、複合的な制約は保持されません。

- 制約の表示を切り替えるには、[制約の検索（Search Constraints）] の展開矢印（▶）または [制約の検索（Search Constraints）] の折りたたみ開矢印（▶）をクリックします。制約のリストが長く、画面の大半を占有する場合に、この機能は役立ちます。

複合イベント ビューの制約

複合的な制約は、特定のイベントに対するすべての不可算値に基づいています。複数の不可算値を持つ行を選択する場合は、ページ上の対象行におけるすべての不可算値と一致するイベントのみを取得する複合的な制約を設定します。たとえば、送信元 IP アドレスが `10.10.31.17` で、宛先 IP アドレスが `10.10.31.15` である行と、送信元 IP アドレスが `172.10.10.17` で宛先 IP アドレスが `172.10.10.15` である行を選択すると、次のすべての結果が取得されます。

- 送信元 IP アドレスが 10.10.31.17 で、かつ宛先 IP アドレスが 10.10.31.15 のイベント

  または

- 送信元 IP アドレスが 172.10.31.17 で、かつ宛先 IP アドレスが 172.10.31.15 のイベント

複合的な制約と単純な制約を組み合わせると、複合的な制約の各セットに単純な制約が追加されます。たとえば、上記に記載されている複合的な制約に対して、プロトコル値 `tcp` の単純な制約を追加すると、次のすべての結果が取得されます。

- 送信元 IP アドレスが 10.10.31.17 で、かつ宛先 IP アドレスが 10.10.31.15 で、かつプロトコルが tcp であるイベント

  または

- 送信元 IP アドレスが 172.10.31.17 で、かつ宛先 IP アドレスが 172.10.31.15 で、かつプロトコルが tcp であるイベント

複合的な制約について、検索および検索の保存を実行することはできません。また、別のワークフローに切り替えるのに、イベント ビューのリンクを使用した場合、または [ワークフロー切り替え（switch workflow）] をクリックした場合は、複合的な制約は保持できません。複合的な制約が適用されているイベント ビューをブックマークしても、制約はブックマークに保存されません。

複合イベント ビュー制約の使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

手順

ステップ 1 ワークフローの選択, （1837ページ）の説明に従って、適切なメニューパスとオプションを選択してワークフローにアクセスします。

ステップ 2 複合制約を管理する場合、次の選択肢があります。

- 複合制約を作成するには、カウント以外の値を持つ 1 つ以上の行を選択し、[表示（View）] をクリックします。
- 複合制約をクリアするには、[検索制約（Search Constraints）] の展開矢印（▶）をクリックし、[複合制約（Compound Constraints）] をクリックします。

ワークフロー間のナビゲーション

ワークフロー ページの [移動（Jump to...）] ドロップダウン リストのリンクを使用して、他のワークフローへ移動できます。ドロップダウン リストを選択し、追加のワークフローを表示および選択します。

新しいワークフローを選択すると、（適切な場合は）、選択する行で共有されているプロパティおよび設定する制約が、新しいワークフローで使用されます。設定した制約またはイベントのプロパティが、新しいワークフローのフィールドにマップされない場合は、これらはドロップされます。また、ワークフローを切り替えた場合には、複合的な制約は保持されません。キャプチャ ファイルのワークフローの制約は、ファイルおよびマルウェアのイベント ワークフローのみに転送されます。

（注） 所定の時間範囲のイベント数を表示する場合、詳細なデータを利用できるイベントの数が、イベントの総数に反映されないことがあります。これは、ディスク領域の使用率を管理するために、古いイベントの詳細がシステムによってプルーニングされることがあるために発生します。イベント詳細のプルーニングを最小限にするために、対象の展開にとって最も重要なイベントだけを記録するようにイベント ロギングを調整できます。

時間枠を一時停止していない場合、または静的な時間枠を設定していない場合、ワークフローを変更したときに時間枠も変更されることに注意してください。

この機能により、疑わしいアクティビティの調査が強化されます。たとえば、接続データを表示していて、内部ホストが異常に大量のデータを外部サイトに転送していることに気付いた場合は、応答側の IP アドレスとポートを制約として選択し、[アプリケーション（Applications）] ワークフローへ移動することができます。[アプリケーション（Applications）] ワークフローは応答側の IP アドレスとポートを IP アドレスとポートの制約として使用し、アプリケーションの種類などの追加情報を表示することができます。ページの上部にある [ホスト（Hosts）] をクリックして、リモート ホストのホスト プロファイルを表示することもできます。

アプリケーションに関する詳細を検索した後で、[相関イベント（Correlation Events）] を選択して接続データ ワークフローに戻る、制約から応答側の IP アドレスを削除する、制約にイニシエータの IP アドレスを追加する、[アプリケーションの詳細（Application Details）] を選択して、データをリモート ホストに転送するときに開始側のホストでユーザがどのクライアントを使用しているかを確認する、といったことができます。ポートの制約は、[アプリケーション詳細（Application Details）]ページには転送されないことに注意してください。ローカル ホストを制約として保持したまま、追加情報を検索するために他のナビゲート ボタンを使用することもできます。

- ローカル ホストがいずれかのポリシーに違反しているかどうかを検出するには、IP アドレスを制約として保持したままで [移動（Jump to）] ドロップダウン リストから [相関イベント（Correlation Events）] を選択します。
- ホストに対して侵入ルールがトリガーされた（侵害を表している）かどうかを確認するには、[移動（Jump to）] ドロップダウン リストから [侵入イベント（Intrusion Events）] を選択します。
- ローカル ホストのホスト プロファイルを表示し、ホストが、悪用された可能性のある脆弱性の影響を受けやすくなっているかどうかを判断するには、[移動（Jump to）] ドロップダウン リストから [ホスト（Hosts）] を選択します。

ブックマーク

イベントの分析の特定の場所と時間にすばやく戻りたい場合には、ブックマークを作成します。ブックマークは、次の情報が含まれます。

- 使用中のワークフロー
- ワークフローの表示中の部分
- ワークフローのページ番号

- 検索の制約
- 無効になっているカラム
- 使用している時間範囲

あるユーザが作成したブックマークは、ブックマークアクセスを持っているすべてのユーザアカウントで利用できます。これは、より詳細な分析を必要とするイベントセットを発見した場合、簡単にブックマークを作成し、適切な権限を持った他のユーザに調査を引き継ぐことが可能であることを意味します。

（注） ブックマークに表示されているイベントが（ユーザによって直接、またはデータベースの自動クリーンアップによって）削除されると、そのブックマークにあった元のイベントは表示されなくなります。

ブックマークの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

マルチドメイン導入では、現在のドメインで作成されたブックマークのみを表示できます。

手順

ステップ 1 イベントの分析中に、表示されている対象のイベントで [このページをブックマーク（Bookmark This Page）] をクリックします。

ステップ 2 [名前（Name）] フィールドに、名前を入力します。

ステップ 3 [ブックマークの保存（Save Bookmark）] をクリックします。

ブックマークの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

マルチドメイン導入では、現在のドメインで作成されたブックマークのみを表示できます。

手順

すべてのイベント ビューで、以下の 2 つの方法を選択できます。

- [ブックマークの表示（View Bookmarks）]の上にポインタを合わせ、ドロップダウン メニューから目的のブックマークをクリックします。
- [ブックマークの表示（View Bookmarks）] をクリックし、[ブックマークの表示（View Bookmarks）]ページで目的のブックマーク名をクリックするか、その横にある表示アイコン（  ）をクリックします。

（注） 最初にブックマークに表示されていたイベントが（ユーザによって直接、またはデータベースの自動クリーンアップによって）削除されると、そのブックマークにはイベントの元のセットは表示されません。

第 80 章

イベントの検索

以下のトピックでは、ワークフロー内のイベントの検索方法について説明します。

イベントの検索

Firepower システムでは、データベース テーブルにイベントとして保存される情報が生成されます。イベントには、アプライアンスがイベントを生成する原因となったアクティビティを示すいくつかのフィールドが含まれます。ご使用の環境用にカスタマイズされた、さまざまなイベント タイプの検索を作成および保存し、後で再使用するために保存できます。

検索設定を保存するときには、その検索設定の名前を付け、それを自分だけで使用するか、それともアプライアンスの全ユーザが使用できるようにするかを指定します。カスタム ユーザ ロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。以前に検索設定を保存した場合、それをロードし、必要に応じて修正して、検索を開始することができます。カスタム分析のダッシュボード ウィジェット、レポート テンプレート、カスタム ユーザ ロールも、保存した検索を使用できます。保存済みの検索設定がある場合、[検索（Search）] ページからそれらを削除できます。

いくつかのイベント タイプに関しては、Firepower システムに備わっている定義済みの検索設定をサンプルとして使用すると、ネットワークについての重要な情報にすばやくアクセスできます。ネットワーク環境に合わせて定義済み検索設定のフィールドを変更し、検索設定を保存して、後で再利用することができます。

検索の種類に応じて、使用できる検索条件は異なりますが、メカニズムは同じです。検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。

（注） カスタム テーブルの検索には、若干異なる手順が必要です。

関連トピック

カスタム テーブルの検索, （1902 ページ）

検索の制約

データベース テーブルごとに、検索を制約する値を入力できる独自の検索ページがあります。入力した値は、そのテーブルに定義されているフィールドに適用されます。フィールドのタイプによっては、特殊なシンタックスを使用して、ワイルドカード文字や数値の範囲などの基準を指定できます。

検索結果はワークフロー ページに表示され、カラム式レイアウトでテーブルの各フィールドが示されます。一部のデータベース テーブルは、ワークフロー ページにカラムとして表示されないフィールドを使用した検索も行えます。ワークフロー ページで結果を確認する際に、該当する制約が検索結果に適用されているかどうかを判別するには、展開アイコン（  ）をクリックして、検索に現在有効になっている制約を表示します。

一般的な検索の制約

イベントを検索するときは、次の一般的な注意事項を順守してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を1つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「A」または「B」または「C, D, E」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- フィールドでその情報を利用できないイベントを示すには、そのフィールドで `n/a` を指定します。フィールドに情報が入力されているイベントを示すには `!n/a` を使用します。
- 多くの数値フィールドの前には、より大きい（`>`）、以上（`>=`）、より小さい（`<`）、以下（`<=`）、等しい（`=`）または等しくない（`<>`）の演算子を付けることができます。

ヒント　長い複雑な値を（SHA-256ハッシュ値など）を含むフィールドを検索する場合は、ソース資料から検索基準値をコピーし、検索ページの適切なフィールドに貼り付けることができます。

検索で使用するワイルドカードと記号

検索ページの多くのテキスト フィールドでは、文字列内の文字に一致させるために、アスタリスク（*）を使用することができます。たとえば `net*` と指定すると、`network`、`netware`、`netscape` などに一致します。

英数字以外の文字（アスタリスク文字を含む）を検索するには、検索文字列を引用符で囲みます。たとえば、次の文字列を検索するとします。

```
Find an asterisk (*)
```

この場合は、次のように入力します。

```
"Find an asterisk (*)"
```

ワイルドカードを使用できるテキスト フィールドで、文字列の部分一致を検索するには、ワイルドカードを使用する**必要**があります。たとえば、ページ ビューを含む（つまりメッセージが「Page View」である）すべての監査レコードを監査ログ内で検索する場合、「`Page`」を検索しても結果は返されません。代わりに、「`Page*`」と指定してください。

一部のフィールドでは、アスタリスクを使用せずにフィールドの内容をすべてまたは一部検索することができます。完全一致の場合は、検索文字列を引用符で囲む必要があります。引用符で囲まなかった場合は、部分一致が実行されます。たとえば、フィールド検索で、引用符を使用せずに `Scan Completed with Detection` という文字列を検索すると、該当フィールドに次の文字列が含まれているレコードと、該当フィールドが検索文字列と完全に一致するレコードが返されます。

```
Scan Completed, No Detections
Scan completed With Detections
```

検索でのオブジェクトとアプリケーションのフィルタ

Firepowerシステムでは、ネットワーク構成の一部として使用可能な名前付きオブジェクト、オブジェクト グループ、およびアプリケーション フィルタを作成できます。検索を実行または保存するときには、検索条件としてこれらのオブジェクト、グループ、およびフィルタを使用できます。

検索を実行するときに、オブジェクト、オブジェクト グループ、およびアプリケーション フィルタは `${object_name}` という形式で表示されます。たとえば、オブジェクト名 `ten_ten_network` であるネットワーク オブジェクトは、検索では `${ten_ten_network}` と表されます。

検索基準としてオブジェクトを使用できる検索フィールドの横にはオブジェクト追加アイコン（＋）が表示され、これをクリックすることができます。

関連トピック

オブジェクト マネージャ，（379 ページ）

検索で指定する時間制約

時間値を指定できる検索条件フィールドで使用可能な形式を、次の表に示します。

表 *257*：検索フィールドにおける時間指定

時間の形式	例
`today [at HH:MMam|pm]`	`today` `today at 12:45pm`
`YYYY-DDMM- HH:MM:SS`	`2006-03-22 14:22:59`

時間値の前に、以下のいずれか 1 つの演算子を指定できます。

表 *258*：時間指定の演算子

演算子	例	説明
<	`< 2006-03-22 14:22:59`	2006 年 3 月 22 日午後 2 時 23 分より前のタイムスタンプを持つイベントを返します。
>	`> today at 2:45pm`	今日の午後 2 時 45 分より後のタイムスタンプを持つイベントを返します。

検索での IP アドレス

検索で IP アドレスを指定するときには、個別の IP アドレス、複数アドレスのカンマ区切りリスト、アドレス ブロック、またはハイフン（-）で区切った IP アドレス範囲を入力することができます。また、否定を使用することもできます。

IPv6 をサポートする検索（侵入イベント、接続データ、相関イベントの検索など）では、IPv4 アドレス、IPv6 アドレス、および CIDR/プレフィックス長アドレス ブロックを任意に組み合わせて入力できます。IP アドレスを使用してホストを検索した場合、結果には、少なくとも 1 つの IP アドレスが検索条件と一致するホストがすべて含まれます（つまり、IPv6 のアドレスの検索では、プライマリ アドレスが IPv4 であるホストが返されることがあります）。

CIDR またはプレフィックス長の表記を使用して IP アドレスのブロックを指定する場合、Firepower システムは、マスクまたはプレフィックス長で指定されたネットワーク IP アドレスの部分**のみ**を使用します。たとえば `10.1.2.3/8` と入力すると、Firepower システムは `10.0.0.0/8` を使用します。

IP アドレスをネットワーク オブジェクトによって表すことができるため、IP アドレス検索フィールドの横にあるネットワーク オブジェクト追加アイコン（＋）をクリックして、ネットワーク オブジェクトを IP アドレス検索基準として使用することもできます。

表 *259*：使用可能な *IP* アドレス構文

指定する項目	タイプ	例
単一の IP アドレス	その IP アドレス。	`192.168.1.1` `2001:db8::abcd`
リストを使用した複数の IP アドレス	IP アドレスからなるカンマ区切りリスト。カンマの前後にスペースを追加**しない**でください。	`192.168.1.1,192.168.1.2` `2001:db8::b3ff,2001:db8::0202`
CIDR ブロックまたはプレフィックス長で指定できる IP アドレスの範囲	IPv4 CIDR または IPv6 プレフィクス長表記の IP アドレス ブロック。	`192.168.1.0/24` これは、サブネット マスク 255.255.255.0 である 192.168.1.0 ネットワーク内の任意の IP を指定します（つまり 192.168.1.0 から 192.168.1.255 まで）。
CIDR ブロックやプレフィクスで指定できない IP アドレスの範囲	ハイフンを使用した IP アドレス範囲。ハイフンの前後にスペースを入力**しない**でください。	`192.168.1.1-192.168.1.5` `2001:db8::0202-2001:db8::8329`

他の方法で否定を使用して IP アドレスまたは IP アドレス範囲を指定	IP アドレス、ブロック、または範囲の先頭に感嘆符を付ける。	`192.168.0.0/32,!192.168.1.10`
		`!2001:db8::/32`
		`!192.168.1.10,!2001:db8::/32`

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）

検索での管理対象デバイス

管理対象デバイスを制約として使用して検索を作成する場合、[デバイス（Device）] 検索条件フィールドに次のいずれかを指定できます。

- 管理対象デバイス名、IP アドレス、またはホスト名
- デバイス グループ名
- デバイス スタック名
- 7000 または 8000 シリーズ デバイス高可用性ペアの名前

システムでグループ、デバイス高可用性ペア、またはスタックの一致が検出されると、検索を実行するために、そのグループ名、デバイス高可用性ペア名、またはスタック名が適切なメンバー デバイス名に置き換えられます。デバイス フィールドのデバイス グループ、デバイス高可用性ペ

ア、またはスタックを使用する検索を保存すると、デバイス フィールドで指定した名前がシステムによって保存され、検索が実行されるたびにデバイス名の置換が再度実行されます。

検索でのポート

Firepower System では、検索においてポート番号の特定の構文に対応しています。次の入力が可能です。

- 1 つのポート番号
- コンマで区切られたポート番号リスト
- ポート番号範囲を示すのにダッシュで区切られた 2 つのポート番号
- ポート番号の後ろにスラッシュで区切ってプロトコルの略語（侵入イベントを検索する場合のみ）
- 特定のポートの否定を示すエクスクラメーションマークの後ろにポート番号またはポート番号範囲

（注） ポート番号またはポート範囲を指定する場合はスペースは使用しないでください。

表 *260*：ポート構文例

例	説明
`21`	ポート 21 でのすべてのイベント（TCP イベントや UDP イベントなど）を戻します。
`!23`	ポート 23 のイベントを除き、すべてのイベントを戻します。
`25/tcp`	ポート 25 の TCP 関連侵入イベントをすべて戻します。
`21/tcp,25/tcp`	ポート 21、25 の TCP 関連侵入イベントをすべて戻します。
`21-25`	ポート 21 から 25 のイベントをすべて戻します。

検索のイベント フィールド

イベントを検索するときは、検索条件として次のフィールドを使用できます。

- 監査ログのワークフロー フィールド，（2175 ページ）
- アプリケーション データ フィールド，（2130 ページ）
- アプリケーションの詳細データ フィールド，（2133 ページ）

- キャプチャされたファイルのフィールド, （2043 ページ）
- ホワイト リスト イベントのフィールド, （2164 ページ）
- 接続およびセキュリティ インテリジェンス イベント フィールド, （1923 ページ）
- 相関イベントのフィールド, （2159 ページ）
- ディスカバリ イベントのフィールド, （2108 ページ）
- [ヘルス イベント（Health Events）] テーブル, （283 ページ）
- ホスト属性データ フィールド, （2118 ページ）
- ホスト データ フィールド, （2110 ページ）
- ファイルおよびマルウェア イベント フィールド, （2019 ページ）
- 侵入イベント フィールド, （1961 ページ）
- ルール アップデートのインポート ログの詳細ビュー, （166 ページ）
- 修復ステータスのテーブル フィールド, （2169 ページ）
- Nmap スキャン結果のフィールド, （1505 ページ）
- サーバ データ フィールド, （2126 ページ）
- サードパーティの脆弱性データのフィールド, （2142 ページ）
- ユーザ関連フィールド, （2144 ページ）
- 脆弱性データのフィールド, （2135 ページ）
- ホワイト リスト違反のフィールド, （2166 ページ）

検索の実行

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 [分析（Analysis）] > [検索（Search）]を選択します。

ヒント また、ワークフローの任意のページから [検索（Search）] をクリックすることもできます。

ステップ 2 テーブルのドロップダウンリストから、検索するイベントまたはデータのタイプを選択します。

ステップ 3 該当するフィールドに検索条件を入力します。検索の制約, （1872 ページ）を参照してください。

ステップ 4 将来検索を再度使用する場合は、その検索を保存します。詳細については、検索設定の保存, （1878 ページ）を参照してください。

ステップ 5 [検索（Search）] をクリックして、検索を開始します。検索結果は、検索されるテーブルのデフォルト ワークフローで表示され、該当する場合には時間で制約されます。

次の作業

- ワークフローを使用して検索結果を分析する場合は、ワークフローの使用, （1834 ページ）を参照してください。

関連トピック

イベント ビュー設定の設定, （38 ページ）

検索設定の保存

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成された保存済みの検索が表示されます。これは編集できます。先祖ドメインで作成された保存済みの検索も表示されますが、これは編集できません。下位のドメインで作成された検索を表示および編集するには、そのドメインに切り替えます。

はじめる前に

- 検索の実行, （1877 ページ）で説明するように検索条件を設定するか、保存済み検索設定のロード, （1879 ページ）で説明するように保存した検索をロードします。

手順

ステップ 1 [検索（Search）] ページから、自分だけがアクセスできるように検索設定をプライベートとして保存する場合は、[プライベート（Private）] チェックボックスをオンにします。

ヒント カスタム ユーザ ロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。

ステップ 2 次の 2 つの対処法があります。

- ロードした検索設定の新しいバージョンを保存する場合は、[新規に保存（Save As New）] をクリックします。
- 新しい検索結果を保存する場合や、同じ名前を使用してカスタム検索を上書きする場合は、[保存（Save）] をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

保存済み検索設定のロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成された保存済みの検索が表示されます。これは編集できます。先祖ドメインで作成された保存済みの検索も表示されますが、これは編集できません。下位のドメインで作成された検索を表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [分析（Analysis）] > [検索（Search）]を選択します。

ヒント また、ワークフローの任意のページから [検索（Search）] をクリックすることもできます。

ステップ 2 テーブルのドロップダウンリストから、検索するイベントまたはデータのタイプを選択します。

ステップ 3 [カスタム検索（Custom Searches）] リストまたは [定義済の検索（Predefined Searches）] リストから、ロードする検索を選択します。

ステップ 4 別の検索条件を使用するには、検索の制約を変更します。

ステップ 5 変更した検索を将来再度使用する場合は、検索を保存しておきます。詳細については、検索設定の保存, （1878 ページ）を参照してください。

ステップ 6 [検索（Search）] をクリックします。

シェルによるクエリのオーバーライド

システム管理者は、シェル ベースのクエリ管理ツールを使用して、実行時間の長いクエリを検出および停止することができます。

クエリ管理ツールでは指定した分数よりも実行時間が長いクエリを検索し、それらのクエリを停止することができます。ユーザがクエリを停止すると、このツールにより監査ログと syslog にイベントが記録されます。

Firepower Management Center でのシェル アクセスを持つローカル作成されたユーザだけが、admin ユーザであることに注意してください。シェル アクセスを与える外部認証オブジェクトを使用する場合、シェル アクセス フィルタに一致するユーザもまたシェルにログインできます。

（注） Webインターフェイス内の検索ページを終了しても、クエリは停止しません。長い時間をかけて結果を返すクエリは、クエリ実行中にシステム全体のパフォーマンスに影響を与えます。

シェルベースのクエリ管理の構文

実行時間が長いクエリを管理するには、次の構文を使用します。

```
query_manager [-v] [-l [minutes]] [-k query_id [...]] [--kill-all minutes]
```

表 *261*：*query_manager* オプション

オプション	説明
`-h, --help`	短いヘルプ メッセージを出力します。
`-l, --list [minutes]`	指定された時間（分単位）を超えるすべてのクエリをリストします。デフォルトで、1 分より長くかかっているすべてのクエリを表示します。
`-k, --kill query_id [...]`	指定されたIDを持つクエリを強制終了します。オプションは複数の ID を取得する場合があります。
`--kill-all minutes`	指定された時間（分単位）を超えるすべてのクエリを強制終了します。
`-v, --verbose`	完全な SQL クエリを含む詳細な出力。

注意 シェル アクセスを、システム管理者のみに制限する必要があります。

実行時間が長いクエリの停止

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	`admin` またはシェルアクセスが付与されたユーザ

手順

ステップ 1 `ssh` を使用して Firepower Management Center に接続します。

ステップ 2 シェルベースのクエリ管理の構文, （1880 ページ）で説明された構文を使用して、`sudo` で `query_manager` を実行します。

第 81 章

カスタム ワークフロー

次のトピックでは、カスタム ワークフローの使用方法について説明します。

カスタム ワークフローの概要

シスコが提供する事前定義のカスタム ワークフローがニーズに合わない場合は、カスタム ワークフローを作成して管理することができます。

カスタム ワークフローは、組織に特有のニーズに合わせて作成するワークフローです。カスタム ワークフローを作成する場合は、ワークフローのベースとなるイベント（またはデータベース テーブル）の種類を選択します。Firepower Management Center では、カスタム ワークフローをカスタムテーブルのベースにすることができます。また、カスタム ワークフローに含まれるページを選択することもできます。カスタム ワークフローには、ドリルダウン、テーブル ビュー、ホストまたはパケット ビューのページを含めることができます。

イベント評価プロセスが変わった場合には、新しいニーズを満たすようにカスタム ワークフローを編集することができます。事前定義のワークフローは編集できないことに注意してください。

ヒント　任意のイベント タイプについて、デフォルト ワークフローとしてカスタム ワークフローを設定することができます。

保存済みカスタム ワークフロー

Firepower Management Center は、変更可能な定義済みのワークフローの他に保存済みのカスタム ワークフローを含みます。それぞれのワークフローは、カスタム テーブルに基づき、いずれも変更可能です。

マルチドメイン展開では、これらの保存されたワークフローは、グローバル ドメインに属し、下位ドメインでは変更できません。

表 *262*：保存済みカスタム ワークフロー

ワークフロー名	説明
影響度、優先度、ホストの重要度によるイベント	このワークフローを使用して、ネットワークにとって重要であり、現在脆弱であり、現在攻撃を受けている可能性のあるホストを迅速に選択して、そのホストに焦点を合わせることができます。 このワークフローは、宛先重要度のカスタム テーブルのある侵入イベントに基づいています。
優先度および分類によるイベント	このワークフローでは、イベントとタイプのリストをそれぞれのイベントが発生した回数と共にイベントの優先度の順に示します。 このワークフローは、侵入イベントのカスタム テーブルに基づきます。
宛先、影響度、ホストの重要度を有するイベント	このワークフローを使用して、ネットワークにとって重要であり、現在脆弱であるホストの最新の攻撃を検出できます。 このワークフローは、宛先重要度のカスタム テーブルのある侵入イベントに基づいています。
サーバのデフォルト ワークフローのあるホスト	このワークフローを使用すると、サーバのカスタム テーブルと共にホストの基本的な情報をすぐに表示できます。 このワークフローは、サーバのカスタム テーブルのあるホストに基づきます。
宛先重要度のデフォルト ワークフローのある侵入イベント	このワークフローを使用すると、宛先重要度のカスタム テーブルと共に侵入イベントの基本的な情報をすぐに表示できます。 このワークフローは、宛先重要度のカスタム テーブルのある侵入イベントに基づいています。
送信元重要度のデフォルト ワークフローのある侵入イベント	このワークフローを使用すると、送信元重要度のカスタム テーブルと共に侵入イベントの基本的な情報をすぐに表示できます。 このワークフローは、送信元重要度のカスタム テーブルのある侵入イベントに基づいています。

ワークフロー名	説明
サーバとホストの詳細	このワークフローを使用して、ネットワークで最も高頻度で使用されているサーバやそのサーバを稼働しているホストを決定できます。 このワークフローは、サーバのカスタム テーブルのあるホストに基づきます。

カスタム ワークフローの作成

シスコが提供する事前定義のカスタム ワークフローがニーズに合わない場合は、カスタム ワークフローを作成することができます。

ヒント 新しいカスタム ワークフローを作成する代わりに、別のアプライアンスからカスタム ワークフローをエクスポートし、それを自身のアプライアンスへインポートすることができます。その後でニーズに合わせて、インポートしたワークフローを編集することができます。

カスタム ワークフローを作成する場合は、次の操作を行います。

- ワークフローのソースとなるテーブルを選択する
- ワークフローの名前を指定する
- ワークフローにドリル ダウン ページおよびテーブル ビュー ページを追加する

ワークフローの各ドリル ダウン ページでは、次のことができます。

- Web インターフェイスのページの上部に表示される名前を指定する
- 1 ページにつき最大 5 個のカラムを含める
- デフォルトのソート順（昇順または降順）を指定する

ワークフロー ページの順序において、任意の場所にテーブル ビュー ページを追加することができます。これらのページには編集可能なプロパティ（ページ名、ソート順、ユーザ定義可能なカラム位置など）がありません。

（注） カスタム ワークフローには、イベントのドリル ダウン ページまたはテーブル ビューを少なくとも 1 つ追加する必要があります。

（注） テーブル タイプに [脆弱性（Vulnerabilities）] を選択し、テーブル カラムに [IP アドレス（IP Address）] を追加しても、検索機能を使用して特定の IP アドレスまたはアドレスのブロックを表示するようワークフローを制約しない限り、カスタム ワークフローを使用して脆弱性を表示する場合に [IP アドレス（IP Address）] カラムは表示されません。

カスタム ワークフローの最終ページは、次の表に記載されているように、ワークフローのベースにしているテーブルによって異なります。これらの最終ページは、ワークフローを作成したときにデフォルトで追加されます。

表 *263*：カスタム ワークフローの最終ページ

イベント/アセット タイプ	最終ページ
ディスカバリ イベント	ホスト
脆弱性	脆弱性の詳細
サードパーティの脆弱性	ホスト
Users	Users
侵害の兆候	ホスト
侵入イベント	パケット

システムは、他の種類のイベント（監査ログやマルウェアイベントなど）に基づくカスタム ワークフローには最終ページを追加しません。

接続データに基づくカスタム ワークフローもその他のカスタム ワークフローと同様です。ただし、接続データに基づくカスタム ワークフローには接続の要約データを含むドリル ダウン ページや個々の接続とテーブル ビュー ページを含むドリル ダウン ページを入れることができます。

非接続データに基づくカスタム ワークフローの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 [分析（Analysis）] > [カスタム（Custom）] > [カスタム ワークフロー（Custom Workflows）]を選択します。

ステップ 2 [カスタム ワークフローの作成（Create Custom Workflow）] をクリックします。

ステップ 3 [名前（Name）] フィールドにワークフローの名前を入力します。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 [テーブル（Table）] ドロップダウン リストから、対象とするテーブルを選択します。

ステップ 6 ワークフローに 1 つ以上のドリルダウン ページを追加する場合は、[ページの追加（Add Page）] をクリックします。

ステップ 7 [ページ名（Page Name）] フィールドにページの名前を入力します。

ステップ 8 [カラム 1（Column 1）] で、ソートの優先順位およびテーブルのカラムを選択します。このカラムは、ページの最も左のカラムとして表示されます。

例：
たとえば、対象とする宛先ポートを示すページを作成し、カウントでページをソートするには、[ソートの優先順位（Sort Priority）] ドロップダウン リストから [2] を選択し、[フィールド（Field）] ドロップダウン リストから [宛先ポート/ICMP コード（Destination Port/ICMP Code）] を選択します。

ステップ 9 ページに表示するすべてのフィールドが指定されるまで、含めるフィールドの選択とソートの優先順位の設定を続けます。

ステップ 10 ワークフローにテーブル ビュー ページを追加するには、[テーブル ビューの追加（Add Table View）] をクリックします。

ステップ 11 [保存（Save）] をクリックします。

カスタム接続データ ワークフローの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

接続データに基づいたカスタム ワークフローは他のカスタム ワークフローと似ていますが、ドリルダウン ページとテーブル ビュー ページだけでなく、接続データ グラフのページも含めることができます。必要に応じて、ワークフローにそれぞれのタイプのページを任意の数だけ、任意の順序で含めることができます。それぞれの接続データ グラフのページには 1 つのグラフ（線グラフ、棒グラフ、または円グラフ）が含まれます。線グラフと棒グラフには、複数のデータセットを含めることができます。

手順

ステップ 1 [分析（Analysis）] > [カスタム（Custom）] > [カスタム ワークフロー（Custom Workflows）]を選択します。

ステップ 2 [カスタム ワークフローの作成（Create Custom Workflow）] をクリックします。

ステップ 3 [名前（Name）] フィールドにワークフローの名前を入力します。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 [テーブル（Table）] ドロップダウン リストから、[接続イベント（Connection Events）] を選択します。

ステップ 6 ワークフローに 1 つ以上のドリルダウン ページを追加する場合は、次の 2 つのオプションがあります。

- 個々の接続に関するデータが含まれているドリルダウン ページを追加するには、[ページの追加（Add Page）] をクリックします。
- 接続の概要データが含まれているドリルダウン ページを追加するには、[サマリー ページの追加（Add Summary Page）] をクリックします。

ステップ 7 [ページ名（Page Name）] フィールドにページの名前を入力します。

ステップ 8 [カラム 1（Column 1）] で、ソートの優先順位およびテーブルのカラムを選択します。このカラムは、ページの最も左のカラムとして表示されます。

ステップ 9 ページに表示するすべてのフィールドが指定されるまで、含めるフィールドの選択とソートの優先順位の設定を続けます。

例：
たとえば、監視対象ネットワーク経由で転送されるトラフィックの量を表示するページを作成し、トラフィックの転送量が最も多い応答側によってページをソートするには、[ソートの優先順位（Sort Priority）] ドロップダウン リストで [1] を選択し、[フィールド（Field）] ドロップダウン リストで [応答側のバイト数（Responder Bytes）] を選択します。

ステップ 10 ワークフローに 1 つ以上のグラフ ページを追加する場合は、[グラフの追加（Add Graph）] をクリックします。

ステップ 11 [グラフ名（Graph Name）] フィールドにページの名前を入力します。

ステップ 12 ページに含めるグラフのタイプを選択します。

- 線グラフ（  ）
- 棒グラフ（  ）
- 円グラフ（  ）

ステップ 13 グラフの X 軸と Y 軸を選択し、グラフ化するデータの種類を指定します。
円グラフでは、X 軸は独立変数を表し、Y 軸は従属変数を表します。

ステップ 14 グラフに含めるデータセットを選択します。

円グラフには 1 つのデータセットしか含めることができないことに注意してください。

ステップ 15 接続データのテーブル ビューを追加するには、[テーブル ビューの追加（Add Table View）] をクリックします。
テーブル ビューは設定できません。

ステップ 16 [保存（Save）] をクリックします。

カスタム ワークフローの使用と管理

ワークフローが、事前定義のイベントテーブルまたはカスタムテーブルのいずれに基づいているかによって、ワークフローの表示に使用する方法が異なります。

カスタムワークフローが事前定義のイベントテーブルに基づいている場合は、アプライアンスに付属しているワークフローにアクセスするのと同じ方法でアクセスします。たとえば、ホストテーブルに基づいているカスタム ワークフローにアクセスするには、[分析（Analysis）] > [ホスト（Hosts）] > [ホスト（Hosts）] を選びます。また、カスタム ワークフローがカスタム テーブルに基づいている場合は、[カスタム テーブル（Custom Tables）] ページからアクセスする必要があります。

イベント評価プロセスが変わった場合には、新しいニーズを満たすようにカスタム ワークフローを編集することができます。事前定義のワークフローは編集できないことに注意してください。

ヒント 任意のイベント タイプについて、デフォルト ワークフローとしてカスタム ワークフローを設定することができます。

事前定義されたテーブルに基づいたカスタム ワークフローの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

手順

ステップ 1 ワークフローの選択, （1837ページ）の説明に従って、カスタム ワークフローのベースとなるテーブルについて、適切なメニュー パスとオプションを選択します。

ステップ 2 カスタムワークフローも含め、別のワークフローを使用するには、現在のワークフロータイトルの横にある [(ワークフローの切り替え)（(switch workflow)）] をクリックします。

ステップ 3 イベントが表示されず、ワークフローを時間によって制約できる場合は、時間範囲の調整が必要なことがあります（イベント時間の制約, （1855 ページ）を参照）。

カスタム テーブルに基づいたカスタム ワークフローの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成されたカスタム ワークフローが表示されます。これは編集できます。先祖ドメインで作成されたカスタム ワークフローも表示されますが、これは編集できません。下位のドメインのカスタム ワークフローを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [分析（Analysis）]>[カスタム（Custom）]>[カスタム テーブル（Custom Tables）]を選択します。

ステップ 2 表示するカスタム テーブルの隣にある表示アイコン（  ）をクリックするか、またはカスタム テーブルの名前をクリックします。

ステップ 3 カスタムワークフローも含め、別のワークフローを使用するには、現在のワークフロータイトルの横にある [(ワークフローの切り替え)（(switch workflow)）] をクリックします。

ステップ 4 イベントが表示されず、ワークフローを時間によって制約できる場合は、時間範囲の調整が必要なことがあります（イベント時間の制約, （1855 ページ）を参照）。

カスタム ワークフローの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成されたカスタム ワークフローが表示されます。これは編集できます。先祖ドメインで作成されたカスタム ワークフローも表示されますが、これは編集できません。下位のドメインのカスタム ワークフローを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [分析（Analysis）] > [カスタム（Custom）] > [カスタム ワークフロー（Custom Workflows）]を選択します。

ステップ 2 編集するワークフロー名の横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ワークフローに必要な変更を加えます。

ステップ 4 [保存（Save）] をクリックします。

第 82 章

カスタム テーブル

次のトピックでは、カスタム テーブルの使用方法について説明します。

カスタム テーブルの概要

Firepower システムがネットワークに関する情報を収集し、Firepower Management Center がその情報を一連のデータベース テーブルに保存します。結果として生成される情報を表示するためにワークフローを使用する場合、Firepower Management Center はそれらのテーブルのいずれかからデータを取り出します。たとえば、[カウントに基づいたネットワーク アプリケーション（Network Applications by Count）] ワークフローの各ページのカラムは、[アプリケーション（Applications）] テーブルのフィールドから取得されます。

さまざまなテーブルのフィールドを結合することにより、ネットワークのアクティビティの分析が向上する場合、カスタム テーブルを作成できます。たとえば、定義済みの [ホスト属性（Host Attributes）] テーブルのホスト重大度情報と、定義済みの [接続データ（Connection Data）] テーブルのフィールドを結合してから、新しいコンテキストで接続データを検証できます。

定義済みのテーブルまたはカスタムテーブルのどちらについても、カスタム ワークフローを作成できます。

定義済みのカスタム テーブル

カスタム テーブルには、2 つまたは 3 つの定義済みテーブルのフィールドを含みます。Firepower System は、いくつかのシステム定義のカスタム テーブルと共に配布されますが、特定のニーズに適合する情報のみを含む追加のカスタム テーブルを作成できます。

たとえば、Firepower System は、侵入イベントとホスト データを相関するシステム定義のカスタムテーブルと共に配布されます。そのため、クリティカルシステムに影響を及ぼすイベントを検索でき、1 つのワークフローにその検索結果を表示できます。

マルチドメイン展開では、定義済みのカスタムテーブルは、グローバル ドメインに属し、下位ドメインで変更することはできません。

次の表では、システムと共に提供されるカスタム テーブルについて説明します。

表 *264*：システム定義カスタム テーブル

テーブル	説明
ホストとサーバ（Hosts with Servers）	ホストテーブルおよびサーバテーブルのフィールドを含み、ネットワーク上で実行されている検出されたアプリケーションに関する情報やこれらのアプリケーションを実行するホストに関する基本的なオペレーティング システム情報を提供します。
侵入イベントと宛先重要度（Intrusion Events with Destination Criticality）	侵入イベントテーブルとホストテーブルのフィールドを含み、侵入イベントに関する情報と各侵入イベントに含まれる宛先ホストのホスト重要度を提供します。 このテーブルを使用して、ホスト重要度の高い宛先ホストに関与する侵入イベントを検索できます。
侵入イベントと送信元重要度（Intrusion Events with Source Criticality）	侵入イベントテーブルとホストテーブルのフィールドを含み、侵入イベントに関する情報と各侵入イベントに含まれる送信元ホストのホスト重要度を提供します。 このテーブルを使用して、ホスト重要度の高い送信元ホストに関与する侵入イベントを検索できます。

可能なテーブルの組み合わせ

カスタム テーブルを作成する場合、関連データのある定義済みのテーブルのフィールドを組み合わせことができます。次の表では、新しいカスタム テーブルを作成するために組み合わせることのできる定義済みのテーブルを列挙します。2 つ以上の定義済みのカスタム テーブルのフィールドを組み合わせるカスタム テーブルを作成できます。

表 *265*：カスタム テーブルの組み合わせ

組み合わせ可能なカスタム テーブル	フィールド
アプリケーション	• 相関イベント（Correlation Events） • 侵入イベント（Intrusion Events） • 接続サマリ データ（Connection Summary Data） • ホスト属性（Host Attributes） • アプリケーションの詳細（Application Details） • 検出イベント（Discovery Events） • 接続イベント（Connection Events） • ホスト（Hosts） • サーバ • ホワイト リスト イベント（White List Events）
相関イベント（Correlation Events）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts）
侵入イベント（Intrusion Events）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts） • サーバ
接続サマリ データ（Connection Summary Data）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts） • サーバ

組み合わせ可能なカスタム テーブル	フィールド
の侵害の兆候（Host Indications of Compromise）	• アプリケーション • アプリケーションの詳細（Application Details） • キャプチャ ファイル（Captured Files） • 接続イベント（Connection Events） • 接続サマリ データ（Connection Summary Data） • 相関イベント（Correlation Events） • 検出イベント（Discovery Events） • ホスト属性（Host Attributes） • ホスト（Hosts） • 侵入イベント（Intrusion Events） • セキュリティインテリジェンスイベント（Security Intelligence Events） • サーバ • ホワイト リスト イベント（White List Events）
ホスト属性（Host Attributes）	• アプリケーション • 相関イベント（Correlation Events） • 侵入イベント（Intrusion Events） • 接続サマリ データ（Connection Summary Data） • アプリケーションの詳細（Application Details） • 検出イベント（Discovery Events） • 接続イベント（Connection Events） • ホスト（Hosts） • サーバ • ホワイト リスト イベント（White List Events）
アプリケーションの詳細（Application Details）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts）

組み合わせ可能なカスタム テーブル	フィールド
検出イベント（Discovery Events）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts）
接続イベント（Connection Events）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts） • サーバ
セキュリティ インテリジェンス イベント（Security Intelligence Events）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts） • サーバ
ホスト（Hosts）	• アプリケーション • 相関イベント（Correlation Events） • 侵入イベント（Intrusion Events） • 接続サマリ データ（Connection Summary Data） • ホスト属性（Host Attributes） • アプリケーションの詳細（Application Details） • 検出イベント（Discovery Events） • 接続イベント（Connection Events） • サーバ • ホワイト リスト イベント（White List Events）

組み合わせ可能なカスタム テーブル	フィールド
サーバ	• アプリケーション • 侵入イベント（Intrusion Events） • 接続サマリ データ（Connection Summary Data） • ホスト属性（Host Attributes） • 接続イベント（Connection Events） • ホスト（Hosts）
ホワイト リスト イベント（White List Events）	• アプリケーション • ホスト属性（Host Attributes） • ホスト（Hosts）

1 つのテーブルのフィールドを別のテーブルの 1 つ以上のフィールドにマッピングすることもあります。たとえば、定義済みの [宛先の重要度による侵入イベント（Intrusion Events with Destination Criticality）] のカスタム テーブルを侵入イベント テーブルとホスト テーブルのフィールドと組み合わせます。侵入イベント テーブルの各イベントは、そのイベントに関連付けられた 2 つの IP アドレス、送信元 IP アドレスと宛先 IP アドレスがあります。しかしホスト テーブル内の「イベント」は、それぞれ 1 つのホスト IP アドレスを示します（ホストには複数の IP アドレスがあることもあります）。このため、侵入イベント テーブルとホスト テーブルに基づいてカスタム テーブルを作成すると、ホスト テーブルで表示されたデータを侵入イベント テーブルのホスト送信元 IP アドレスまたはホスト宛先 IP アドレスに適用できるかを選択する必要があります。

新しいカスタム テーブルを作成すると、テーブル内のすべての列を表示するデフォルトのワークフローが自動的に作成されます。また、定義済みのテーブルのように、ネットワークの分析に使用するデータについてカスタム テーブルを検索できます。定義済みのテーブルを使用して可能であるように、カスタム テーブルに基づいてレポートを作成できます。

ユーザ定義のカスタム テーブル

ヒント 新しいカスタム テーブルを作成する代わりに、別の Firepower Management Center からカスタム テーブルをエクスポートし、Firepower Management Center にインポートすることができます。

カスタム テーブルを作成するには、Firepower システムに付属しているどの定義済みテーブルに、カスタム テーブルに組み込むフィールドが含まれているかを判断します。その後、組み込むフィー

ルドを選択できます。さらに、必要に応じて、共通フィールドのフィールド マッピングを設定することもできます。

ヒント [ホスト（Hosts）] テーブルを含むデータでは、1 つの IP アドレスではなく、1 つのホストのすべての IP アドレスに関連したデータを表示できます。

例として、[相関イベント（Correlation Events）] テーブルと [ホスト（Hosts）] テーブルのフィールドを結合するカスタムテーブルについて考慮します。このカスタムテーブルを使用して、相関ポリシーの違反に関係するホストの詳細情報を取得できます。注意すべき点として、[相関イベント（Correlation Events）] テーブルの送信元 IP アドレスと宛先 IP アドレスのどちらと一致する [ホスト（Hosts）] テーブル データを表示するかを決定する必要があります。

このカスタム テーブルのイベントのテーブル ビューを表示する場合、相関イベントが 1 行に 1 つずつ表示されます。次の情報を含むようにカスタム テーブルを設定できます。

- イベントが生成された日時
- 違反された相関ポリシーの名前
- 違反をトリガーとして使用した規則の名前
- 相関イベントに関係する送信元ホスト（開始ホスト）に関連付けられた IP アドレス
- 送信元ホストの NetBIOS 名
- 送信元ホストが実行しているオペレーティング システムおよびバージョン
- 送信元ホストの重大度

ヒント 宛先ホスト（応答ホスト）の同じ情報を表示する同様のカスタム テーブルを作成することもできます。

カスタム テーブルの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Any/Admin

手順

ステップ 1 [分析（Analysis）]>[カスタム（Custom）]>[カスタム テーブル（Custom Tables）]を選択します。

ステップ 2 [カスタム テーブルの作成（Create Custom Table）] をクリックします。

ステップ 3 [名前（Name）] フィールドに、カスタム テーブルの名前を入力します。

例：
たとえば、`Correlation Events with Host Information (Src IP)` と入力します。

ステップ 4 [テーブル（Tables）] ドロップダウン リストから、[相関イベント（Correlation Events）] を選択します。

ステップ 5 [フィールド（Fields）] で [時間（Time）] を選択し、[追加（Add）] をクリックして、相関イベントが生成された日時を追加します。

ステップ 6 手順 5 を繰り返して、[ポリシー（Policy）] および [ルール（Rule）] フィールドを追加します。

ヒント Ctrl または Shift を押しながらクリックすることにより、複数のフィールドを選択できます。また、クリックしてドラッグすることで、隣接する複数の値を選択できます。ただし、テーブルに関連したイベントのテーブル ビューでフィールドが表示される順序を指定する場合は、フィールドを一度に 1 つずつ追加します。

ステップ 7 [テーブル（Tables）] ドロップダウンリストから [ホスト（Hosts）] を選択します。

ステップ 8 [IP アドレス（IP Address）]、[NetBIOS 名（NetBIOS Name）]、[OS 名（OS Name）]、[OS バージョン（OS Version）]、[ホストの重大度（Host Criticality）] フィールドをカスタム テーブルに追加します。

ステップ 9 [相関イベント（Correlation Events）] の隣にある [共通フィールド（Common Fields）] で、[送信元 IP（Source IP）] を選択します。
相関イベントに関係する送信元ホスト（開始ホスト）用に手順 8 で選択したホスト情報を表示するように、カスタム テーブルが設定されます。

ヒント 相関イベントに関係する宛先ホスト（応答ホスト）に関する詳細なホスト情報を表示するカスタム テーブルを作成する場合も、この手順に従いますが、[送信元 IP（Source IP）] ではなく、[送信先 IP（Destination IP）] を選択します。

ステップ 10 [保存（Save）] をクリックします。

カスタム テーブルの変更

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Any/Admin

マルチドメイン展開では、現在のドメインで作成されたカスタム テーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタム テーブルも表示されますが、これは編集できません。下位のドメインのカスタム テーブルを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [分析（Analysis）]>[カスタム（Custom）]>[カスタム テーブル（Custom Tables）]を選択します。

ステップ 2 編集するテーブルの横にある編集アイコン（）をクリックします。
代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 除外するフィールドの横にある削除アイコン（）をクリックして、テーブルからフィールドを除外することもできます。
（注） レポートで現在使用中のフィールドを削除すると、それらのフィールドを使用しているセクションをそれらのレポートから除外するか確認するプロンプトが表示されます。

ステップ 4 必要に応じて、その他の変更を実行します。

ステップ 5 [保存（Save）] をクリックします。

カスタム テーブルの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Any/Admin

マルチドメイン導入では、現在のドメインで作成されたカスタム テーブルが表示されます。これは削除できます。先祖ドメインで作成されたカスタム テーブルも表示されますが、これは削除できません。下位のドメインのカスタム テーブルを削除するには、そのドメインに切り替えます。

手順

ステップ 1 [分析（Analysis）]>[カスタム（Custom）]>[カスタム テーブル（Custom Tables）]を選択します。

ステップ 2 削除するカスタム テーブルの隣にある削除アイコン（）をクリックします。
コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

カスタム テーブルに基づいたワークフローの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Any/Admin

カスタム テーブルを作成すると、そのデフォルトのワークフローがシステムによって自動的に作成されます。このワークフローの最初のページには、イベントのテーブル ビューが表示されます。カスタム テーブルに侵入イベントを含める場合、ワークフローの 2 番目のページはパケット ビューになります。それ以外の場合、ワークフローの 2 番目のページはホスト ページになります。カスタム テーブルに基づいて、独自のカスタム ワークフローを作成することもできます。

ヒント　カスタム テーブルに基づいてカスタム ワークフローを作成する場合、それをそのテーブルのデフォルトのワークフローとして指定できます。

同じ手法を使用して、定義済みのテーブルに基づいたイベント ビューに使用するカスタム テーブルでイベントを表示できます。

マルチドメイン展開では、現在のドメインで作成されたカスタム テーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタム テーブルも表示されますが、これは編集できません。下位のドメインのカスタム テーブルを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1　[分析（Analysis）]>[カスタム（Custom）]>[カスタム テーブル（Custom Tables）]を選択します。

ステップ 2　表示するワークフローに関連するカスタム テーブルの隣にある表示アイコン（）をクリックします。

カスタム テーブルの検索

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Any/Admin

マルチドメイン展開では、現在のドメインで作成されたカスタム テーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタム テーブルも表示されますが、これは編集で

きません。下位のドメインのカスタム テーブルを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [分析（Analysis）]>[カスタム（Custom）]>[カスタム テーブル（Custom Tables）]を選択します。

ステップ 2 検索するカスタム テーブルの隣にある表示アイコン（  ）をクリックします。

ヒント カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [（ワークフローの切り替え）（(switch workflow)）] をクリックします。

ステップ 3 [検索（Search）] をクリックします。

ヒント 別の種類のイベントやデータについてデータベースを検索する場合は、その種類をテーブル ドロップダウンリストから選択します。

ステップ 4 該当するフィールドに、検索条件を入力します。
複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。

ヒント 検索基準としてオブジェクトを使用する場合は、検索フィールドの横にあるオブジェクト アイコン（）をクリックします。

ステップ 5 必要に応じて、検索を保存する場合は、[プライベート（Private）] チェックボックスをオンにして、プライベートとして検索を保存すると、その検索に本人のみがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント カスタム ユーザ ロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。

ステップ 6 必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [保存（Save）] をクリックして、検索条件を保存します。[プライベート（Private）] チェックボックスをオンにすると、その検索は本人のアカウントでのみ表示できるようになります。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[新規に保存（Save As New）] をクリックします。[プライベート（Private）] チェックボックスをオンにすると、その検索は本人のアカウントでのみ保存および表示できるようになります。

ステップ 7 [検索（Search）] をクリックして、検索を開始します。
検索結果は、現在の時間範囲によって制限されている、カスタム テーブルのデフォルトのワークフローに表示されます（該当する場合）。

第 XXI 部

イベントとアセット

第 83 章

接続ロギング

次のトピックでは、モニタ対象ネットワークでホストから実行される接続を記録するようFirepowerシステムを設定する方法について説明します。

接続ロギングについて

システムは管理対象デバイスで検出された接続のログを生成できます。このログは接続イベントと呼ばれます。ルールやポリシーの設定を行うことで、ログに記録する接続の種類、接続をログに記録するタイミング、およびデータを保存する場所をきめ細かく制御できます。セキュリティインテリジェンス イベントと呼ばれる特別な接続イベントは、レピュテーションベースのセキュリティ インテリジェンス機能によってブラックリストに登録（ブロック）された接続を表します。

接続イベントには、検出されたセッションに関するデータも含まれています。個々の接続イベントで入手可能な情報はいくつかの要因に応じて異なりますが、一般的には次のものがあります。

- タイムスタンプ、送信元と宛先の IP アドレス、入出力ゾーン、接続を処理したデバイスなど、基本的な接続特性
- アプリケーション、要求されるURL、または接続に関連付けられているユーザなど、システムによって検出または推測される追加の接続特性

- どの設定がトラフィックを処理したか、接続が許可またはブロックされていたかどうか、暗号化された接続および復号された接続に関する詳細など、接続がログに記録された理由に関するメタデータ

（注） エクスポートしたNetFlowレコードから生成された接続データを使い、管理対象デバイスで収集された接続ログを補うことができます。これは、Firepowerシステムの管理対象デバイスでモニタできないネットワーク上にNetFlow対応ルータやその他のデバイスを配置した場合に特に有効です。

接続ロギング ストラテジー

部門のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。目標が生成するイベントの数を抑えパフォーマンスを向上させることである場合は、分析のために重要な接続のロギングのみを有効にします。しかし、プロファイリングの目的でネットワークトラフィックの広範な表示が必要な場合は、追加の接続のロギングを有効にできます。

ヒント 接続データの詳細な分析を実行するため、シスコはクリティカルな接続の終了をFirepower Management Centerデータベースに記録することを推奨します。

システムは1つの接続をさまざまな理由でロギングすることがあるため、1ヵ所でロギングを無効にしても、一致する接続がロギングされないとは限りません。また、接続イベント ストレージを無効にしない限り、システムが自動でロギングする接続もあります。検出したファイル、マルウェア、侵入、インテリジェント アプリケーション バイパス（IAB）に関連する接続がその例です。

8000シリーズのファースト パス ルールでファースト パスされた接続をロギングすることはできません。

設定可能な接続ロギング

重要な接続のみがロギングされるように、ルールごとの接続ロギングを有効にします。あるルールに対し接続ロギングを有効にすると、システムはそのルールによって処理されたすべての接続をロギングします。

また、ポリシーのデフォルト アクションにより処理された接続をロギングすることもできます。ルールやデフォルト アクションにより（アクセス制御の場合は、ルールのインスペクション設定により）、ロギングのオプションは異なります。

SSLポリシー：ルールとデフォルト アクション

SSLルールまたはSSLポリシーのデフォルト アクションに一致する接続をロギングすることができます。

ブロックされた接続の場合、システムは即座にセッションを終了し、イベントを生成します。監視対象の接続やアクセス コントロール ルールに渡す接続の場合、システムはセッションが終了するとイベントを生成します。

アクセス コントロール ポリシー：セキュリティ インテリジェンスによる判断

接続がレピュテーションベースのセキュリティ インテリジェンス機能によってブラックリスト登録（ブロック）される場合は、その接続をログに記録できます。

オプションで、セキュリティインテリジェンスフィルタリングにはモニタ専用設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブラックリスト登録されるはずの接続をシステムがさらに分析できるだけでなく、ブラックリストと一致する接続をログに記録することもできます。セキュリティ インテリジェンス モニタリングによって、セキュリティ インテリジェンス情報を使用してトラフィック プロファイルを作成することもできます。

セキュリティ インテリジェンスのフィルタリングの結果、システムが接続イベントをロギングすると、一致するセキュリティインテリジェンスイベントもロギングされます。そのイベントは特殊なタイプの接続イベントで、個別に表示および分析することができ、また個別に保存、プルーニングされます。接続でブラックリスト登録されたIPアドレスを特定できるように、IPアドレスの横にあるホスト アイコンは、ブラックリスト登録された IP アドレスとモニタされた IP アドレスではイベント ビューアで少々異なる表示になっています。

アクセス コントロール ポリシー：ルールとデフォルト アクション

アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに一致する接続をロギングすることができます。

自動接続ロギング

接続イベントのストレージを無効にしない限り、システムは他のロギング設定に関係なく、Firepower Management Center データベースに次の接続終了イベントを保存します。

侵入に関連付けられた接続

システムは、接続がアクセス コントロール ポリシーのデフォルト アクションで処理されなければ、侵入イベントに関連付けられた接続を自動的にログに記録します。

アクセスコントロールのデフォルトアクションに関連付けられた侵入ポリシーによって侵入イベントが生成された場合、システムは、そのイベントに関連する接続の終了を自動的にログに記録**しません**。代わりに、デフォルトのアクション接続のロギングを明示的に有効にする必要があります。これは、接続データをログに記録する必要がない、侵入防御専用の展開環境で役立ちます。

ただし例外として、デフォルト アクションの接続開始ロギングを有効にした場合はその限りではありません。この場合、関連付けられた侵入ポリシーがトリガーされると、システムは接続の開始だけでなく、接続の終了もログに記録**します**。

ファイル イベントとマルウェア イベントに関連付けられた接続

システムは、ファイルイベントとマルウェアイベントに関連付けられた接続を自動的にログに記録します。

（注） NetBIOS-ssn（SMB）トラフィックのインスペクションによって生成されるファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。システムはクライアントまたはサーバがセッションを終了した後に接続イベントを生成します。

インテリジェント アプリケーション バイパスに関連付けられた接続

システムは、IAB に関連付けられたバイパスされた、およびバイパスされるはずだった接続をログに記録します。

接続開始のロギングと終了のロギングの比較

接続は、次の例外となるブロックされたトラフィックを除き、接続開始時あるいは終了時にログを記録することができます。

- ブロックされたトラフィック：ブロックされたトラフィックは、さらに検査されることなくすぐさま拒否されるため、通常、ブロックされたトラフィックやブラックリストに登録されたトラフィックについては、接続開始イベントのみ記録可能です。ログに記録される個々の接続終了はありません。
- ブロックされた暗号化トラフィック：SSL ポリシーで接続のロギングを有効にすると、システムは接続開始イベントではなく接続終了イベントをログに記録します。これは、システムは接続がセッション内で最初のパケットを使用して暗号化されているかどうかを判定できず、暗号化されたセッションを即座にブロックできないためです。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。何らかの理由で接続をモニタリングすると、接続終了ロギングが強制されます。単一のブロックされていない接続の場合、接続終了イベントには、接続開始イベントに含まれるすべての情報に加えて、セッション期間中に収集された情報も含まれます。

次の表では、接続開始イベントと接続終了イベントの違い（それぞれをロギングする利点を含む）を詳細に説明します。

表 *266*：接続開始イベントと接続終了イベントの比較

	接続開始イベント	接続終了イベント
次の場合に生成可能です	システムが接続の開始を検出した場合（または、イベントの生成がアプリケーションまたは URL の識別に依存する場合は最初の数パケットの後）	システムが以下の状態の場合 • 接続のクローズを検出した場合 • 一定期間後に接続の終了を検出しない場合 • メモリ制約によりセッションを追跡できなくなった場合
次のものについてロギングが可能です	SSL ポリシーによってブロックされた接続を除くすべての接続	すべての接続。ただし、すべての場所で接続終了ロギングを設定できない場合があります。
次を含みます	最初のパケット（または、イベントの生成がアプリケーションまたは URL の識別に依存する場合は最初の数パケット）で判定できる情報のみ	接続開始イベント内のすべての情報と、セッション期間を通してトラフィックを検査して判別された情報（たとえば伝送されたデータ総量、接続の最後のパケットのタイムスタンプなど）
次の場合に有用です	次のものをロギングする場合 • ブロックされた接続。 • 接続終了情報はユーザにとって重要ではないので、接続の開始のみ	目的 • SSL ポリシーによって処理される暗号化接続をロギングする場合 • セッションの期間にわたって収集された情報であらゆる種類の詳細な分析を実行する場合、またはその情報を使用して相関ルールをトリガーする場合 • カスタム ワークフローで接続の概要（集約接続データ）を表示する場合、グラフ形式で接続データを表示する場合、またはトラフィック プロファイルを作成して使用する場合

Firepower Management Center と外部ロギング

接続イベントとセキュリティ インテリジェンス イベントは Firepower Management Center データベースにロギングできます（Web インターフェイスの [イベント ビューア（Event Viewer）]）。Firepower Management Center に保存できるイベントの数はモデルによって異なります。アラート

応答と呼ばれる接続を設定し、それを使って外部 syslog や SNMP トラップ サーバにイベントをロギングすることもできます。

Firepower Management Center データベースにロギングすると、Firepower システムのレポート、分析、およびデータ相関関係の多くの機能を活用できます。次に例を示します。

- ダッシュボードおよびコンテキストエクスプローラでは、システムによってロギングされた接続をグラフ形式によって一目で確認できます。
- イベント ビューには、システムによってロギングされた接続の詳細情報が提示され、グラフ形式や表形式で表示したり、レポートに要約することもできます。
- トラフィック プロファイリングは、接続データを使用して正常なネットワーク トラフィックのプロファイルを作成します。ユーザはそのプロファイルを基準として使用して、異常な動作を検出および追跡できます。
- 相関ポリシーを使用して、イベントを生成し、特定のタイプの接続またはトラフィック プロファイルの変更に対する応答（アラートや外部修復など）をトリガーできます。

（注） これらの機能を使用するには、接続（ほとんどの場合、接続の開始ではなく接続の終了）を Firepower Management Center データベースにロギングする必要があります。システムがクリティカルな接続（ログに記録された侵入、禁止されたファイルおよびマルウェアに関連付けられているもの）を自動的にロギングするのはこのためです。

アクションと接続ロギング

接続ロギングを設定する場合、ルール アクションおよびポリシーのデフォルト アクションにより、一致するトラフィックをシステムがどのように検査、処理するのかだけでなく、一致するトラフィックの詳細をいつ、どのようにロギングするかが決まります。接続イベントには、接続がロギングされた理由を記述したメタデータが含まれています。メタデータにはトラフィックがどの設定によって処理されたかなどの情報が含まれます。

モニタされた監視接続のロギング

システムは常に、以下の設定と一致するトラフィックの接続終了をロギングします。このことは、トラフィックに一致する他のルールがなく、デフォルト アクションのロギングを有効にしていない場合でも該当します。

- セキュリティ インテリジェンス：モニタするように設定されたブラックリスト（セキュリティ インテリジェンス イベントも生成されます）
- SSL ルール：[モニタ（Monitor）] アクション
- アクセス コントロール ルール：[モニタ（Monitor）] アクション

システムは、1 つの接続が 1 つのモニタ ルールに一致するたびに 1 つの別個のイベントを生成するわけではありません。1 つの接続が複数のモニタ ルールに一致する可能性があるため、各接続

イベントには、接続が一致する最初の 8 つのモニタ アクセス コントロール ルールに関する情報だけでなく、最初の一致する SSL モニタ ルールに関する情報を含めて表示することができます。

同様に、外部 syslog または SNMP トラップ サーバに接続イベントを送る場合、システムは 1 つの接続が 1 つのモニタ ルールに一致するたびに 1 つの別個のアラートを送信するわけではありません。代わりに、接続の終了時にシステムから送られるアラートに、接続が一致したモニタ ルールの情報が含まれます。

信頼されている接続のロギング

信頼されている接続の開始と終了をロギングできます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- アクセス コントロール ルール：[信頼する（Trust）] アクション
- アクセス コントロールのデフォルト アクション：[すべてのトラフィックを信頼する（Trust All Traffic）]

信頼されている接続には、ディープ インスペクションまたはディスカバリは適用されません。したがって、信頼されている接続の接続イベントに含まれる情報は限られます。

システムは、接続を検出したデバイスに応じて異なる方法で、信頼アクセス コントロール ルールによって処理された TCP 接続をロギングします。

- 7000 および 8000 シリーズ デバイスでは、信頼ルールによって最初のパケットで検出された TCP 接続は、すでに有効になっているモニタ ルールの有無に応じて異なるイベントを生成します。モニタ ルールがアクティブな場合、システムはパケットを評価し、接続開始および接続終了イベントを生成します。アクティブなモニタ ルールがない場合、システムは接続終了イベントだけを生成します。
- 他のすべてのモデルでは、信頼ルールによって最初のパケットで検出された TCP 接続は、接続終了イベントだけを生成します。システムは、最後のセッション パケットの 1 時間後にイベントを生成します。

ブロックされた接続のロギング

ブロックされた接続をロギングできます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- セキュリティ インテリジェンス：ブロックするブラックリストが設定されます（セキュリティ インテリジェンス イベントも生成されます）
- SSL ルール：[ブロック（Block）] および [リセットしてブロック（Block with reset）]
- SSL のデフォルト アクション：[ブロック（Block）] および [リセットしてブロック（Block with reset）]
- アクセス コントロール ルール：[ブロック（Block）]、[リセットしてブロック（Block with reset）]、[インタラクティブ ブロック（Interactive Block）]

- アクセス コントロールのデフォルト アクション：[すべてのトラフィックをブロック（Block All Traffic）]

トラフィックをブロックできるデバイスは、インライン（つまり、ルーテッド インターフェイス、スイッチドインターフェイス、トランスペアレントインターフェイス、インラインインターフェイスのペア）で展開されているもののみです。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

注意 サービス妨害（DoS）攻撃の間にブロックされた TCP 接続をロギングすると、システム パフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロック ルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニタするかどうかを検討します。

ブロックされた接続の接続開始ロギングと接続終了ロギングとの比較

ブロックされた接続をロギングするときは、システムがその接続をどのようにロギングするかは接続がブロックされた理由によって異なります。これは、接続ログに基づいて相関ルールを設定する際に留意しておくことが重要です。

- 暗号化されたトラフィックをブロックする SSL ルールおよび SSL ポリシーのデフォルト アクションの場合、システムは接続**終了**イベントをロギングします。これは、システムが接続がセッション内で最初のパケットを使用して暗号化されているかどうかを決定できないためです。
- 他のブロッキング アクションについては、システムは接続**開始**イベントをロギングします。一致するトラフィックは、追加のインスペクションなしで拒否されます。

バイパスされるインタラクティブ ブロックのロギング

インタラクティブ ブロッキング アクセス コントロール ルール（このルールではユーザが禁止されている Web サイトを参照するとシステムによって警告ページが表示されます）を使用すると、接続終了ロギングを設定できます。その理由は、警告ページをユーザがクリック スルーすると、その接続は新規の、許可された接続と見なされ、システムによってモニタとロギングができるためです。

したがって、[インタラクティブ ブロック（Interactive Block）] ルールまたは [リセットしてインタラクティブ ブロック（Interactive Block with reset）] ルールにパケットが一致する場合、システムは以下の接続イベントを生成できます。

- ユーザの要求が最初にブロックされ警告ページが表示されたときの接続開始イベント。このイベントにはアクション [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] が関連付けられます。

- 複数の接続開始または終了イベント（ユーザが警告ページをクリック スルーし、要求した最初のページをロードした場合）。これらのイベントには [許可（Allow）] アクションおよび理由 [ユーザ バイパス（User Bypass）] が関連付けられます。

許可された接続のロギング

許可された接続をロギングができます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- SSL ルール：[複合（Decrypt）] アクション
- SSL ルール：[複合しない（Do not decrypt）] アクション
- SSL のデフォルト アクション：[複合しない（Do not decrypt）] アクション
- アクセス コントロール ルール：[許可（Allow）] アクション
- アクセス コントロールのデフォルト アクション：[ネットワーク検出のみ（Network Discovery Only）] および任意の侵入防御オプション

これらの設定に対するロギングを有効にすると、接続が確実にロギングされると同時に、インスペクションおよびトラフィック処理の次のフェーズが許可（または指定）されます。SSL ロギングは常に接続終了ロギングですが、アクセス コントロール設定で接続開始ロギングも可能にすることができます。

アクセス コントロール ルールまたはデフォルト アクションでトラフィックを許可する場合、関連する侵入ポリシーを使用してトラフィックをさらに検査し、侵入をブロックすることができます。アクセス コントロール ルールでは、ファイル ポリシーを使用して、マルウェアを含む禁止されたファイルを検出し、ブロックすることもできます。接続イベント ストレージを無効にしない限り、システムは、侵入イベント、ファイルイベント、マルウェアイベントに関連する許可された接続のほとんどを自動的にロギングします。詳細については、自動接続ロギング，（1909 ページ）を参照してください。ペイロードが暗号化される接続には、ディープ インスペクションは適用されません。したがって、暗号化接続の接続イベントに含まれる情報は限られることに注意してください。

許可された接続のファイルおよびマルウェア イベントのロギング

ファイル ポリシーによってファイルが検出またはブロックされると、以下のいずれかのイベントが Firepower Management Center データベースにロギングされます。

- ファイル イベント：検出またはブロックされたファイル（マルウェア ファイルを含む）を表します
- マルウェア イベント：検出されたまたはブロックされたマルウェア ファイルのみを表します
- レトロスペクティブ マルウェア イベント：以前に検出されたファイルでのマルウェア処理が変化した場合に生成されます

このロギングは、アクセス コントロール ルールごとに無効にすることができます。または、ファイル イベントおよびマルウェア イベント ストレージを完全に無効にすることもできます。

（注） Cisco では、ファイル イベントおよびマルウェア イベントのロギングを有効のままにすることを推奨しています。

SSL ルールによる復号可能接続のロギング

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 SSL ポリシー エディタで、ロギングを設定するルールの横にある編集アイコン（）をクリックします。
代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 [ロギング（Logging）] タブをクリックします。

ステップ 3 [接続の終了時にロギングする（Log at End of Connection）] をオンにします。
モニタ対象トラフィックに対して、接続の終了時のロギングが必要になります。

ステップ 4 接続イベントの送信先を指定します。
接続イベントについて Firepower Management Center ベースの分析を実行する場合は、イベントをイベント ビューアに送信します。モニタ対象トラフィックに対して、これが必要になります。

ステップ 5 [保存（Save）] をクリックしてルールを保存します。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

セキュリティ インテリジェンスによる接続のロギング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス（Security Intelligence）] タブをクリックします。

ステップ 2 ロギング アイコン（ ）をクリックして、次の条件を使用するセキュリティ インテリジェンス ロギングを有効にします。

- IP アドレス別：[ネットワーク（Networks）] の横にあるロギング アイコンをクリックします。
- URL 別：[URL（URLs）] の横にあるロギング アイコンをクリックします。
- ドメイン名別：[DNS ポリシー（DNS Policy）] ドロップダウンリストの横にあるロギング アイコンをクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 3 [接続のロギング（Log Connections）] チェックボックスをオンにします。

ステップ 4 接続イベントとセキュリティ インテリジェンス イベントの送信先を指定します。Firepower Management Center ベースの分析を実行する場合や、ブラックリストに登録されたオブジェクトをモニタ専用に設定する場合は、イベントをイベント ビューアに送信します。

ステップ 5 [OK] をクリックしてロギング オプションを設定します。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

アクセス制御ルールによる接続のロギング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

ルールアクションと詳細検査のオプションの選択によって、ロギング オプションは異なります。アクションと接続ロギング，（1912 ページ）を参照してください。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、ロギングを設定するルールの横にある編集アイコン（）をクリックします。
代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 [ロギング（Logging）] タブをクリックします。

ステップ 3 [接続の開始時にロギングする（Log at Beginning of Connection）] または [接続の終了時にロギングする（Log at End of Connection）] を指定します。
パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。

ステップ 4 （オプション）[ファイルのロギング（Log Files）] チェックボックスをオンにして、接続に関連付けられているファイル イベントとマルウェア イベントをロギングします。
シスコは、このオプションを有効のままにすることを推奨します。

ステップ 5 接続イベントの送信先を指定します。
接続イベントに対し、Management Center ベースの分析を実行する場合や、ルール アクションが [モニタ（Monitor）] の場合は、イベントを Firepower Management Center に送信します。

ステップ 6 [保存（Save）] をクリックしてルールを保存します。

次の作業

- 設定変更を展開します。設定変更の導入，（320 ページ）を参照してください。

ポリシーのデフォルト アクションによる接続のロギング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

ポリシーのデフォルト アクションにより、システムがポリシー内のルールのいずれにも一致しないトラフィックを処理する方法が決定されます（ただし、トラフィックの照合およびロギングを実行し、トラフィックの処理や調査は実行しないモニタ ルールを除きます）。

また、システムが複合化できないセッションをロギングする方法は、SSL ポリシーのデフォルト アクションのロギング設定でも制御されます。

手順

ステップ 1 ポリシー エディタで、[デフォルト アクション（Default Action）] ドロップダウンリストの横にあるロギング アイコン（ ）をクリックします。

ステップ 2 一致する接続をロギングするタイミングを指定します。

- 接続の開始時にロギングする：SSL のデフォルト アクションではサポートされていません。
- 接続の終了時にロギングする：アクセス制御の [すべてのトラフィックをブロック（Block All Traffic）] デフォルト アクションを選択するとサポートされなくなります。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。アクセス コントロール ポリシーでは、設定が先祖ポリシーから継承されることもあります。

ステップ 3 接続イベントの送信先を指定します。
接続イベントについて Firepower Management Center ベースの分析を実行する場合は、イベントをイベント ビューアに送信します。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

長い URL のロギングの制限

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

HTTP トラフィックの接続の終了イベントは、監視対象ホストによって要求された URL を記録します。URL の保管を無効にすることや保管する URL 文字数を制限することで、システムパフォーマンスが向上する可能性があります。URL のロギングを無効化しても（保管する文字数を 0 にしても）、URL フィルタリングには影響しません。システムは、要求された URL に基づいてトラフィックをフィルタリングします。それらの URL を記録しない場合も同じです。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックして、[一般設定（General Settings）] の横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、先祖ドメインに属しており、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 2 [接続イベントで保存する URL の最大文字数（Maximum URL characters to store in connection events）] を入力します。

ステップ 3 [OK] をクリックします。

ステップ 4 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入, （320 ページ）を参照してください。

第 84 章

接続イベントとセキュリティ インテリジェンス イベント

次のトピックでは、接続およびセキュリティ イベント テーブルを使用する方法について説明します。

接続イベントについて

システムは、管理対象デバイスが検出した接続のログを生成することができます。このログは接続イベントと呼ばれます。ルールやポリシーの設定を行うことで、ログに記録する接続の種類、接続をログに記録するタイミング、およびデータを保存する場所をきめ細かく制御できます。セキュリティ インテリジェンス イベントは特殊な接続イベントで、レピュテーションベースのセキュリティ インテリジェンス機能によってブラックリストに登録されている（ブロックされた）接続を表します。詳細については、接続ロギング，（1907 ページ）を参照してください。

関連トピック

セキュリティ インテリジェンスについて，（831 ページ）

接続イベントとセキュリティ インテリジェンス イベントの比較

セキュリティ インテリジェンス イベントは、レピュテーションベースのセキュリティ インテリジェンス機能によりセッションがブラックリストに登録された（ブロックされた）ときに生成される接続イベントです。

ただし、各セキュリティ インテリジェンス イベントには同一の接続イベントがあり、セキュリティ インテリジェンス イベントを個別に表示、分析できます。また、システムはセキュリティ インテリジェンス イベントを個別に保存およびプルーニングします。

システムは、より多くのリソースを消費する評価を行う前に、セキュリティ インテリジェンスを実施することに注意してください。接続がセキュリティ インテリジェンスによってブロックされた場合、結果として生成されるイベントには、その後の評価によってシステムで収集されることになっていた情報（ユーザ ID など）が含まれません。

（注） 本書では違うと明記されていない限り、接続イベントに関する情報は、セキュリティ インテリジェンス イベントに関する情報でもあります。

NetFlow 接続

管理対象デバイスで収集された接続データを補うために、NetFlow エクスポータによってブロードキャストされたレコードを使用して接続イベントを生成できます。この方法が特に役立つのは、NetFlow エクスポータが、管理対象デバイスでモニタしているネットワークとは別のネットワークをモニタしている場合です。

システムは NetFlow レコードを単方向の接続終了イベントとして Firepower Management Center データベースに記録します。これらの接続に関して使用可能な情報は、アクセス コントロール ポリシーで検出された接続の情報とは若干異なります。NetFlow データと管理対象デバイス データの違い，（1442 ページ）を参照してください。

関連トピック

Firepower システムの NetFlow データ，（1441 ページ）

接続の概要（グラフ用集約データ）

Firepower システムは 5 分間隔で収集された接続データを集約し、接続の概要を作成します。この概要を使用して、接続グラフとトラフィック プロファイルがシステムで生成されます。必要に応じて、接続の概要データに基づいてカスタム ワークフローを作成できます。これは、個々の接続イベントに基づいたワークフローと同じように使用できます。

セキュリティインテリジェンスイベント専用の接続の概要はないことに注意してください。ただし、対応する接続終了イベントは接続の概要データに集約できます。

集約するには、複数の接続が以下の状態である必要があります。

- 接続終了を表している
- 送信元と宛先の IP アドレスが同じで、レスポンダ（宛先）のホストで同じポートを使用している
- 同じプロトコルを使用している（TCP または UDP）
- 同じアプリケーション プロトコルを使用している

- 同じ Firepower システム管理対象デバイスまたは同じ NetFlow エクスポータによって検出される

各接続の概要には、接続数など全トラフィック統計情報が含まれています。NetFlow エクスポータは単一方向接続を生成するので、接続の概要では、NetFlow データに基づく接続ごとに接続数が 2 ずつ増えます。

接続の概要には、概要内の集約された接続に関するすべての情報が含まれているわけではありませんので注意してください。たとえば、接続の概要に集約される接続にはクライアント情報が使用されないため、概要にクライアント情報は含まれません。

長時間接続

接続データを集約する 5 分間隔の 2 回以上に監視対象のセッションがまたがる場合、その接続は長時間接続と見なされます。接続サマリーで接続数を計算する際には、長時間接続が開始された 5 分間隔の回のみカウントします。

また、長時間接続において発信側と応答側が送信したパケット数とバイト数を計算する際は、システムは 5 分間隔の各回で実際に送信されたパケット数とバイト数を報告しません。代わりにシステムは、送信された合計パケット数と合計バイト数、接続の長さ、5 分間隔の各回で接続のどの部分が行われたかに基づいて、一定の送信速度を仮定し、値を推定します。

外部応答側からの統合接続サマリ

接続データの保存に必要なスペースを減らし、接続グラフのレンダリングを高速化するために、システムは次の場合に接続サマリを統合します。

- 接続に関連するホストの 1 つが監視対象のネットワーク上にない場合
- 外部ホストの IP アドレス以外で、サマリ内の接続がサマリ集約条件を満たす場合

イベント ビューアで接続サマリを表示する場合や、接続グラフを使用する場合、システムは非監視対象ホストの IP アドレスの代わりに [外部（`external`）] と表示します。

この集約の結果として、外部応答側を含む接続サマリまたはグラフから接続データのテーブル ビューにドリル ダウンしようとすると（つまり、個別の接続データへのアクセス）、テーブル ビューには情報が何も表示されません。

接続およびセキュリティ インテリジェンス イベント フィールド

表形式およびグラフィカル ワークフローを使用して表示や検索ができる接続およびセキュリティ インテリジェンス イベントには、次に示すフィールドがあります。個別のイベントで利用可能な情報は、システムがいつ、なぜ、どのようにして接続を記録したかによって異なることに注意してください。

（注） 各セキュリティ インテリジェンス イベントには、同一の、個別に保存された接続イベントがあります。すべてのセキュリティ インテリジェンス イベントに、入力済みの [セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）] フィールドがあります。

接続グラフは接続サマリーに基づいているため、接続サマリーを制約しているのと同じ条件が接続グラフを制約します。検索ページのアスタリスク（*）が付いたフィールドは、接続グラフおよび接続サマリーを制約します。無効な検索条件を使用して接続サマリーを検索し、カスタム ワークフローの接続サマリー ページを使用して結果を見る場合、無効な条件には適用不可（N/A）としてラベルが付けられ、取り消し線が引かれます。

全般情報（General Information）

アクセス コントロール ポリシー（Access Control Policy）

接続をモニタしたアクセス コントロール ポリシー。

アクセス コントロール ルール（Access Control Rule）

接続を処理したアクセス コントロール ルールまたはデフォルト アクションと、その接続に一致した最大 8 つのモニタ ルール。

接続が 1 つのモニタ ルールに一致した場合、Firepower Management Center は接続を処理したルールの名前を表示し、その後にモニタ ルール名を表示します。接続が複数のモニタ ルールに一致したときは、イベント ビューアは一致したモニタ ルールの数を `Default Action + 2 Monitor Rules` などと表示します。

接続に一致した最初の 8 つのモニタ ルールのリストをポップアップ ウィンドウに表示するには、[N モニタ ルール（*N*Monitor Rules）] をクリックします。

アクション（**Action**）

接続をロギングした設定に関連付けられているアクション。

セキュリティ インテリジェンスによってモニタされている接続の場合、そのアクションは、接続によってトリガーされる最初のモニタ以外のアクセス コントロール ルールのアクションであるか、またはデフォルト アクションです。同様に、モニタ ルールに一致するトラフィックは常に後続のルールまたはデフォルト アクションによって処理されるため、モニタ ルールによってロギングされた接続と関連付けられたアクションが [モニタ（Monitor）] になることはありません。ただし、モニタ ルールに一致する接続の相関ポリシー違反をトリガーする可能性があります。

アクション	説明
許可（Allow）	アクセス コントロールによって明示的に許可された、またはユーザがインタラクティブ ブロックをバイパスしたために許可された接続。
ブロック（Block）、リセットしてブロック（Block with reset）	次を含むブロックされた接続： • セキュリティ インテリジェンスによってブラックリストに載せられた接続 • SSL ポリシーによってブロックされた暗号化接続 • 侵入ポリシーによってエクスプロイトがブロックされた接続 • ファイル ポリシーによってファイル（マルウェアを含む）がブロックされた接続。 システムが侵入またはファイルをブロックする接続では、アクセス コントロールの許可ルールを使用してディープ インスペクションを呼び出す場合にも、システムはブロックを表示します。
インタラクティブ ブロック（Interactive Block）、リセット付きインタラクティブ ブロック（Interactive Block with reset）	システムがインタラクティブ ブロック ルールを使用してユーザの HTTP 要求を最初にブロックしたときにログに記録された接続。システムにより表示される警告ページでユーザがクリックスルーすると、そのセッションでログに記録されるその後の接続に許可アクションが付きます。
信頼（Trust）	アクセス コントロールによって信頼された接続。デバイスモデルに応じて、システムは信頼された TCP 接続を別にログに記録します。信頼されている接続のロギング，（1913 ページ）を参照してください。
デフォルト アクション（Default Action）	アクセス コントロール ポリシーのデフォルト アクションによって処理される接続。

接続（Connections）

接続サマリーに含まれる接続数。長時間接続（複数回の接続サマリー間隔にまたがる接続）の場合、最初の接続サマリー間隔の分だけ増加します。[接続（Connections）] 条件を使用した検索で意味のある結果を表示するには、接続サマリーページを持つカスタム ワークフローを使用する必要があります。

メンバー数（Count）

各行に表示される情報に一致する接続数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。カスタム ワークフローを作成し、ドリルダウン ページに [カウント（Count）] カラムを追加しない場合、各接続は個別に表示され、パケット数とバイト数は合計されません。

エンドポイント ロケーション（Endpoint Location）

ISE で指定された、ユーザの認証に ISE を使用したネットワーク デバイスの IP アドレス。

エンドポイント プロファイル（Endpoint Profile）

ISE で指定されたユーザのエンドポイント デバイス タイプ。

最初のパケットまたは最後のパケット（First Packet or Last Packet）

セッションの最初または最後のパケットが検出された日時。

イニシエータ/レスポンダ バイト（Initiator/Responder Bytes）

セッション イニシエータまたはセッション レスポンダが送信した合計バイト数。

イニシエータ/レスポンダ パケット（Initiator/Responder Packets）

セッション イニシエータが送信した合計パケット数。

イニシエータ ユーザ（Initiator User）（サマリーおよびグラフを制約）

セッション イニシエータにログインしていたユーザ。このフィールドに [認証なし（No Authentication）] が入力されている場合、ユーザ トラフィックは次のようになります。

- 関連付けられたアイデンティティ ポリシーがないアクセス コントロール ポリシーに一致しました。
- アイデンティティ ポリシーのいずれのルールにも一致しませんでした。

IOC

マルウェア イベントが、接続に関与したホストに対する侵入の痕跡（IOC）をトリガーしたかどうか。

ネットワーク分析ポリシー（Network Analysis Policy）

イベントの生成に関連付けられているネットワーク分析ポリシー（NAP）（ある場合）。

理由（Reason）

多くの場合に接続がロギングされた1つまたは複数の原因。完全なリストについては、接続イベントの理由，（1941 ページ）を参照してください。

IP ブロック、DNS ブロック、および URL ブロックの理由による接続には、固有のイニシエータ レスポンダ ペアごとに15秒のしきい値があります。システムがこれらのいずれかの接続をブロックした後、イベントを生成した時点から 15 秒の間、この 2 つのホスト間で接続がブロックされたとしても、ポートやプロトコルの違いに関わらず、接続イベントを生成しません。

セキュリティ コンテキスト（Security Context）

ASA FirePOWER でマルチ コンテキスト モードで処理される接続で、トラフィックが通過した仮想ファイアウォール グループを特定するメタデータ。

セキュリティ グループ タグ（Security Group Tag）

接続に関係するパケットのセキュリティ グループ タグ（SGT）属性。SGT は、信頼ネットワーク内での、トラフィックの送信元の権限を指定します。セキュリティ グループ アクセス（Cisco TrustSec と Cisco ISE の両方に共通の機能）は、パケットがネットワークに入るときに属性を適用します。

セキュリティ インテリジェンスのカテゴリ（Security Intelligence Category）

接続でブラックリストに記載された IP アドレスを表すか、もしくはそれを含む、ブラックリストに記載されたオブジェクトの名前。セキュリティ インテリジェンスのカテゴリは、ネットワーク オブジェクトまたはグループ、ブラックリスト、カスタム セキュリティ インテリジェンスのリストまたはフィード、またはインテリジェンス フィードのカテゴリのいずれかの名前にすることができます。

インテリジェンス フィードのカテゴリの詳細については、セキュリティ インテリジェンス オプション，（836 ページ）を参照してください。

TCP フラグ（TCP Flags）

NetFlowデータから生成された接続において、接続で検出されたTCPフラグ。このフィールドを検索する場合は、TCPフラグのカンマ区切りリストを入力することで、これらのフラグが *1* つ以上あるすべての接続が表示されます。

時刻（Time）

システムが接続を接続サマリーに集約するために使用した5分間隔の終了時刻。このフィールドは検索できません。

トラフィック（KB）（Traffic (KB)）（検索のみ）

接続で送信されたデータの総量（キロバイト単位）。

合計パケット（Total Packets）（検索のみ）

接続で送信された合計パケット数。

Networking

宛先ポート/ICMP コード（Destination Port/ICMP Code）（サマリーおよびグラフを制約）

セッション レスポンダが使用するポートまたは ICMP コード。

DNS クエリ（DNS Query）

ドメイン名を検索するために接続でネーム サーバに送信された DNS クエリ。

DNS レコード タイプ（DNS Record Type）

接続で送信された DNS クエリを解決するために使用された DNS リソース レコードのタイプ。

DNS レスポンス（DNS Response）

問い合わせ時に接続でネーム サーバに返された DNS レスポンス。

DNS シンクホール名（DNS Sinkhole Name）

システムが接続をリダイレクトしたシンクホール サーバの名前。

DNS TTL

DNS サーバが DNS リソース レコードをキャッシュする秒数。

HTTP 応答コード（HTTP Response Code）

クライアントからの接続経由の HTTP 要求に応じて送信される HTTP ステータス コード。

入力/出力セキュリティ ゾーン（Ingress/Egress Security Zone）

接続に関連付けられた入力または出力のセキュリティ ゾーン。

イニシエータ/レスポンダ IP（Initiator/Responder IP）（サマリーおよびグラフを制約）

セッション イニシエータまたはレスポンダの IP アドレス（および DNS 解決が有効化されている場合はホスト名）。ブラックリストに記載された接続でブラックリストに記載された IP アドレスを識別できるように、ブラックリストに記載された IP アドレスの横のアイコンは見た目が少し異なります。

クライアントのオリジナル IP（Original Client IP）

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーから抽出された元のクライアント IP アドレス。このフィールドに入力するには、ネットワーク解析ポリシーの HTTP プリプロセッサの [クライアントのオリジナル IP アドレスの抽出（Extract Original Client IP Address）] オプションを有効にする必要があります。また、ネットワーク解析ポリシーで、最大 6 つのカスタム クライアント IP 見出しを指定し、システムが [クライアントのオリジナル IP（Original Client IP）] イベント フィールドの値を選択する優先順位を設定します。

プロトコル（Protocol）（サマリーおよびグラフを制約、検索のみ）

接続に使用されるトランスポート プロトコルです。特定のプロトコルを検索するには、名前を使用するか、http://www.iana.org/assignments/protocol-numbers に記載されたプロトコルの番号を指定します。

送信元ポート/ICMP タイプ（Source Port/ICMP Type）（サマリーおよびグラフを制約）

セッション イニシエータが使用するポートまたは ICMP タイプ。

VLAN ID（Admin. VLAN ID）

接続をトリガーしたパケットに関連付けられている最内部 VLAN ID。

位置情報（GeoLocation）

イニシエータ/レスポンダ国（Initiator/Responder Country）

ルーティング可能な IP が検出された場合の、セッション イニシエータまたはレスポンダの IP アドレスに関連付けられた国。システムにより、国旗のアイコンと、国の ISO 3166-1 alpha-3 国番号が表示されます。国旗アイコンの上にポインタを移動すると、国の完全な名称が表示されます。

イニシエータ/レスポンダ大陸（Initiator/Responder Continent）

ルーティング可能な IP が検出された場合の、セッション イニシエータまたはレスポンダの IP アドレスに関連付けられた大陸。

Device

デバイス（Device）（サマリーおよびグラフを制約）

接続を検出した管理対象デバイス。または、NetFlowデータから生成された接続の場合は、データを処理した管理対象デバイス。

ドメイン（Domain）

接続を検出した管理対象デバイスのドメイン。または、NetFlowデータから生成された接続の場合は、データを処理した管理対象デバイスのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

入力/出力インターフェイス（Ingress/Egress Interface）

接続に関連付けられた入力または出力のインターフェイス。展開に非同期のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインターフェイス セットに属する場合があります。

SSL

SSL の実際の動作（SSL Actual Action）（検索のみ）

システムが SSL ポリシーの暗号化トラフィックに適用したアクション。システムにより、検索ワークフローのページの [SSL ステータス（SSL Status）] フィールドにフィールド値が表示されます。

アクション	説明
ブロック（Block）/ リセットしてブロック（Block With Reset）	ブロックされた暗号化接続を表します。
複合（再署名）（Decrypt (Resign)）	再署名サーバ証明書を使用して復号された発信接続を表します。
復号（キーの置き換え）（Decrypt (Replace Key)）	置き換えられた公開キーと自己署名サーバ証明書を使用して復号された発信接続を表します。
復号（既知のキー）（Decrypt (Known Key)）	既知の秘密キーを使用して復号された着信接続を表します。
デフォルトアクション（Default Action）	接続がデフォルト アクションによって処理されたことを示しています。
復号しない（Do Not Decrypt）	システムが復号しなかった接続を表します。

SSL 証明書ステータス（SSL Certificate Status）

これは、認証ステータスの SSL ルール条件が設定されている場合にのみ適用されます。暗号化されたトラフィックが SSL ルールに一致すると、このフィールドに次のサーバの証明書のステータス値の 1 つ以上が表示されます。

- 自署（Self Signed）
- 有効（Valid）
- 署名が無効（Invalid Signature）
- 発行元が無効（Invalid Issuer）
- 期限切れ
- 不明
- まだ有効ではない（Not Valid Yet）
- 失効（Revoked）

復号できないトラフィックが SSL ルールと一致する場合、このフィールドには [未チェック（Not Checked）] と表示されます。

SSL 証明書情報（SSL Certificate Information）（検索のみ）

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- 件名/発行元共通名（Subject/Issuer Common Name）
- 件名/発行元組織（Subject/Issuer Organization）
- 件名/発行元組織ユニット（Subject/Issuer Organization Unit）
- 有効期間の開始/終了（Not Valid Before/After）
- シリアル番号（Serial Number）
- 証明書フィンガープリント（Certificate Fingerprint）
- 公開キー フィンガープリント（Public Key Fingerprint）

SSL 暗号スイート（SSL Cipher Suite）

接続を暗号化するのに使用される暗号スイートを表すマクロ値。暗号スイート値の指定については、www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。

接続に適用された SSL 暗号化（SSL Encryption applied to the connection）（検索のみ）

yes または no を [SSL（SSL）] 検索フィールドに入力することで、SSL 暗号化された接続または暗号化されていない接続が表示されます。

SSL 予想アクション（SSL Expected Action）（検索のみ）

有効な SSL ルールで指定された、暗号化トラフィックに適用されると予想されるアクション。[SSL の実際の動作（SSL Actual Action）] にリストされている値を入力します。

SSL 失敗理由（SSL Failure Reason）

システムが暗号化されたトラフィックの復号に失敗した理由：

- 不明
- 不一致（No Match）
- Success
- キャッシュされていないセッション（Uncached Session）
- 不明な暗号スイート（Unknown Cipher Suite）
- サポートされていない暗号スイート（Unsupported Cipher Suite）
- サポートされていない SSL バージョン（Unsupported SSL Version）
- SSL 圧縮の使用（SSL Compression Used）
- パッシブ モードで復号できないセッション（Session Undecryptable in Passive Mode）
- ハンドシェイク エラー（Handshake Error）
- 復号エラー（Decryption Error）
- 保留サーバ名カテゴリ ルックアップ（Pending Server Name Category Lookup）
- 保留共通名カテゴリ ルックアップ（Pending Common Name Category Lookup）
- 内部エラー（Internal Error）
- ネットワーク パラメータを使用できません（Network Parameters Unavailable）
- 無効なサーバ証明書の処理（Invalid Server Certificate Handle）
- サーバ証明書フィンガープリントを使用できません（Server Certificate Fingerprint Unavailable）
- サブジェクト DN をキャッシュできません（Cannot Cache Subject DN）
- 発行元 DN をキャッシュできません（Cannot Cache Issuer DN）
- 不明の SSL バージョン（Unknown SSL Version）
- 外部証明書リストを使用できません（External Certificate List Unavailable）
- 外部証明書フィンガープリントを使用できません（External Certificate Fingerprint Unavailable）
- 内部証明書リストが無効です（Internal Certificate List Invalid）
- 内部証明書リストを使用できません（Internal Certificate List Unavailable）
- 内部証明書を使用できません（Internal Certificate Unavailable）
- 内部証明書フィンガープリントを使用できません（Internal Certificate Fingerprint Unavailable）
- サーバ証明書検証を使用できません（Server Certificate Fingerprint Unavailable）

- サーバ証明書検証エラー（Server Certificate Validation Failure）
- 無効なアクション（Invalid Action）

フィールド値は、検索ワークフローのページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL フロー エラー（SSL Flow Error）

エラーが SSL セッション中に発生した場合はエラー名および 16 進数コード。エラーが発生しない場合は [成功（Success）]。

SSL フロー フラグ（SSL Flow Flags）

暗号化された接続の最初の 10 個のデバッグ レベル フラグ。ワークフロー ページでは、すべてのフラグを表示するには、省略記号（...）をクリックします。

SSL フロー メッセージ（SSL Flow Messages）

次のキーワードは、暗号化トラフィックが SSL ハンドシェイク時にクライアントとサーバ間で交換される指定されたメッセージ タイプに関連付けられていることを示します。詳細については、http://tools.ietf.org/html/rfc5246を参照してください。

- HELLO_REQUEST
- CLIENT_ALERT
- SERVER_ALERT
- CLIENT_HELLO
- SERVER_HELLO
- SERVER_CERTIFICATE
- SERVER_KEY_EXCHANGE
- CERTIFICATE_REQUEST
- SERVER_HELLO_DONE
- CLIENT_CERTIFICATE
- CLIENT_KEY_EXCHANGE
- CERTIFICATE_VERIFY
- CLIENT_CHANGE_CIPHER_SPEC
- CLIENT_FINISHED
- SERVER_CHANGE_CIPHER_SPEC
- SERVER_FINISHED
- NEW_SESSION_TICKET
- HANDSHAKE_OTHER
- APP_DATA_FROM_CLIENT
- APP_DATA_FROM_SERVER

SSL ポリシー（SSL Policy）

接続を処理した SSL ポリシー。

SSL ルール（SSL Rule）

接続を処理した SSL ルールまたはデフォルト アクションと、その接続に一致した最初のモニタ ルール。接続が 1 つのモニタ ルールに一致した場合、Firepower Management Center は接続を処理したルールの名前を表示し、その後にモニタ ルール名を表示します。

SSL セッション ID（SSL Session ID）

SSL ハンドシェイク時にクライアントとサーバ間でネゴシエートされた 16 進数セッション ID。

SSL ステータス（SSL Status）

暗号化された接続を記録した、[SSL の実際の動作（SSL Actual Action）]（SSL ルール、デフォルト アクション、または復号できないトラフィック アクション）に関連したアクション。ロック アイコン（  ）は、SSL 証明書の詳細にリンクしています。証明書を利用できない場合（たとえば、SSL ハンドシェイク エラーにより接続がブロックされる場合）、ロック アイコンはグレー表示になります。

システムが暗号化接続を復号できなかった場合は、[SSL の実際の動作（SSL Actual Action）]（実行された復号不能のトラフィック アクション）と、[SSL 失敗理由（SSL Failure Reason）] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [Do Not Decrypt (Unknown Cipher Suite)] が表示されます。

このフィールドを検索する場合は、[SSL の実際の動作（SSL Actual Action）] と [SSL 失敗理由（SSL Failure Reason）] の 1 つ以上の値を入力することで、システムが処理した、または復号に失敗した暗号化トラフィックが表示されます。

SSL 件名/発行元国（SSL Subject/Issuer Country）（検索のみ）

暗号化証明書に関連付けられた件名または発行元国の 2 文字の ISO 3166-1 alpha-2 国番号。

SSL チケット ID（SSL Ticket ID）

SSL ハンドシェイク時に送信されたセッション チケット情報の 16 進数のハッシュ値。

SSL バージョン（SSL Version）

接続の暗号化に使用された SSL または TLS プロトコル バージョン。

- 不明
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TSLv1.2

Application

アプリケーション プロトコル（Application Protocol）（サマリーおよびグラフを制約）

接続で検出された、ホスト間の通信を表すアプリケーション プロトコル。

アプリケーション プロトコル カテゴリとタグ（Application Protocol Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

アプリケーションのリスク（Application Risk）

接続で検出されたアプリケーション トラフィックに関連付けられたリスク。「非常に高い（Very High）」、「高（High）」、「中（Medium）」、「低（Low）」、「非常に低い（Very Low）」のいずれかとなります。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

ビジネスとの関連性（Business Relevance）

接続で検出されたアプリケーション トラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネス関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

クライアントおよびクライアント バージョン（Client and Client Version）

接続で検出されたクライアントのクライアント アプリケーションとバージョン。

接続に使用されている特定のクライアントをシステムが特定できなかった場合、このフィールドは汎用的な名称としてアプリケーション プロトコル名の後に「client」という語を付加して FTP client などと表示します。

クライアント カテゴリとタグ（Client Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

HTTP リファラ（HTTP Referrer）

接続で検出された HTTP トラフィックの要求 URL のリファラを示す HTTP リファラ（他の URL へのリンクを提供した Web サイト、他の URL からリンクをインポートした Web サイトなど）。

参照ホスト（Referenced Host）

接続のプロトコルが HTTP または HTTPS の場合、このフィールドにはそれぞれのプロトコルが使用していたホスト名が表示されます。

ユーザ エージェント（User Agent）

接続で検出された HTTP トラフィックから取得したユーザ エージェント文字列アプリケーションの情報。

Web アプリケーション（Web Application）

接続で検出された HTTP トラフィックの内容または要求された URL を表す Web アプリケーション。

Web アプリケーションがイベントの URL に一致しない場合、そのトラフィックは通常、参照先のトラフィックです（アドバタイズメントのトラフィックなど）。システムは、参照先のトラフィックを検出すると、参照元のアプリケーションを保存し（可能な場合）、そのアプリケーションを Web アプリケーションとして表示します。

HTTP トラフィックに含まれる特定の Web アプリケーションをシステムが特定できなかった場合、このフィールドには [Web ブランジング（Web Browsing）] と表示されます。

Web アプリケーションのカテゴリとタグ（Web Application Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

URL

URL、URL カテゴリ、および URL レピュテーション（URL, URL Category, and URL Reputation）

セッション中に監視対象のホストによって要求された URL と、関連付けられたカテゴリおよびレピュテーション（利用できる場合）。

システムが SSL アプリケーションを識別またはブロックする場合、要求された URL は暗号化トラフィック内にあるため、システムは、SSL 証明書に基づいてトラフィックを識別します。したがって SSL アプリケーションの場合、このフィールドは証明書に含まれる一般名を表示します。

NetFlow

NetBIOS ドメイン（NetBIOS Domain）

セッションで使用された NetBIOS ドメイン。

NetFlow 送信元/宛先の自律システム（NetFlow Source/Destination Autonomous System）

NetFlowデータから生成された接続の場合、接続のトラフィックの送信元または宛先に対する、Border Gateway Protocol の自律システム番号。

NetFlow 送信元/宛先のプレフィックス（NetFlow Source/Destination Prefix）

NetFlow データから生成された接続の場合、送信元または宛先の IP アドレスに、送信元と宛先のプレフィックス マスクが追加されたもの。

NetFlow 送信元/宛先 TOS（NetFlow Source/Destination TOS）

NetFlow データから生成された接続の場合、接続トラフィックが NetFlow 対応デバイスに入ったか、NetFlow エクスポータから出たときの Type of Service（TOS）バイトの設定。

NetFlow SNMP 入出力（NetFlow SNMP Input/Output）

NetFlow データから生成された接続の場合、接続トラフィックが NetFlow 対応デバイスに入ったか、NetFlow エクスポータから出た際のインターフェイスのインターフェイス インデックス。

ソース デバイス（Source Device）（サマリーおよびグラフを制約）

接続の生成に使用されたデータをブロードキャストする NetFlow エクスポータの IP アドレス。管理対象デバイスによって接続が検出された場合、このフィールドには`Firepower`と表示されます。

関連イベント（Associated Events）

接続に関連付けられたイベントの検索に、接続やセキュリティ インテリジェンスのイベントの検索ページは使用できません。

ファイル（Files）

接続に関連付けられたファイル イベント（ある場合）。ファイルの表示アイコン（  ）は、ファイルのリストにリンクしています。アイコンの数字は、その接続で検出またはブロックされたファイル数（マルウェア ファイルを含む）を示します。

侵入イベント（Intrusion Events）

接続に関連付けられた侵入イベント（ある場合）。侵入イベントの表示アイコン（  ）は、イベントのリストにリンクしています。

接続イベントの理由

接続イベントの [理由（Reason）] フィールドには、次の状況で接続がロギングされた理由が表示されます。

理由（Reason）	説明
DNS ブロック（DNS Block）	ドメイン名とセキュリティ インテリジェンス データに基づいて、インスペクションなしで接続が拒否されました。DNS ブロックの理由は、DNS ルール アクションに応じて、[ブロック（Block）]、[ドメインが見つかりません（Domain not found）]、[シンクホール（Sinkhole）] のアクションと対として組み合わされます。
DNS モニタ（DNS Monitor）	システムはドメイン名とセキュリティ インテリジェンス データに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニタするように設定されています。

理由（**Reason**）	説明
ファイル ブロック（File Block）	ファイルまたはマルウェア ファイルが接続に含まれており、システムがその送信を防いでいます。[ファイルブロック（File Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
ファイル カスタム検出（File Custom Detection）	カスタム検出リストにあるファイルが接続に含まれており、システムがその送信を防いでいます。
ファイル モニタ（File Monitor）	システムが接続において特定のファイルの種類を検出しました。
ファイル復帰許可（File Resume Allow）	ファイル送信がはじめに [ファイル ブロック（Block Files）] ルールまたは [マルウェア ブロック（Block Malware）] ファイル ルールによってブロックされました。ファイルを許可する新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に再開しました。この理由はインライン展開のみで表示されます。
ファイル復帰ブロック（File Resume Block）	ファイル送信がはじめに [ファイル検出（Detect Files）] ルールまたは [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] ファイル ルールによって許可されました。ファイルをブロックする新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に停止しました。この理由はインライン展開のみで表示されます。
インテリジェント アプリケーション バイパス（Intelligent App Bypass）	インテリジェント アプリケーション バイパス（IAB）モード： • アクションが [信頼（Trust）] の場合、IAB はバイパス モードでした。一致するトラフィックは、追加のインスペクションなしで通過しました。 • アクションが [許可（Allow）] の場合、IAB はテスト モードでした。一致するトラフィックは、追加のインスペクションに使用できました。
侵入ブロック（Intrusion Block）	接続で検出されたエクスプロイト（侵入ポリシー違反）をシステムがブロックしたか、ブロックするはずでした。[侵入ブロック（Intrusion Block）] の原因は、ブロックされたエクスプロイトの場合は [ブロック（Block）]、ブロックされるはずだったエクスプロイトの場合は [許可（Allow）] のアクションと対として組み合わされます。
侵入モニタ（Intrusion Monitor）	接続で検出されたエクスプロイトをシステムが検出したものの、ブロックしなかったことを示します。これは、トリガーされた侵入ルールの状態が [イベントを生成する（Generate Events）] に設定されている場合に発生します。

理由（**Reason**）	説明
IP ブロック（IP Block）	IP アドレスとセキュリティインテリジェンスデータに基づいて、インスペクションなしで接続が拒否されました。[IP ブロック（IP Block）] の原因は必ず [ブロック（Block）] のアクションと対として組み合わされます。
IP モニタ（IP Monitor）	システムは IP アドレスとセキュリティ インテリジェンス データに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニタするように設定されています。
SSL ブロック（SSL Block）	システムが SSL インスペクション設定に基づいて暗号化接続をブロックしました。[SSL ブロック（SSL Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
URL ブロック（URL Block）	URL とセキュリティ インテリジェンス データに基づいて、インスペクションなしで接続が拒否されました。[URL ブロック（URL Block）] の原因は必ず [ブロック（Block）] のアクションと対として組み合わされます。
URL モニタ（URL Monitor）	システムは URL とセキュリティ インテリジェンス データに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニタするように設定されています。
ユーザ バイパス（User Bypass）	最初にユーザの HTTP 要求をブロックしましたが、ユーザのクリックによって警告ページからサイトを表示しました。[ユーザ バイパス（User Bypass）] の理由は必ず [許可（Allow）] のアクションと対として組み合わされます。

接続イベント フィールドの入力の要件

接続イベント、セキュリティインテリジェンスイベント、接続サマリーで利用可能な情報は、いくつかの要因によって異なります。

アプライアンス モデルおよびライセンス

多くの機能は、ターゲット デバイスで特定のライセンス付与対象の機能を有効にしなければ使用できません。また、一部のモデルでしか使用できない機能も多くあります。

たとえば、NGIPSv デバイスは SSL インスペクションをサポートしません。これらのデバイスは暗号化されたトラフィックを検査できないため、記録される接続イベントには暗号化された接続に関する情報は含まれていません。

トラフィックの特性

システムは、ネットワーク トラフィック内に存在する（および検出可能な）情報だけを報告します。たとえば、イニシエータ ホストに関連付けられているユーザがいない、またはプロトコルが DNS、HTTP、または HTTPS ではない接続で検出される参照先ホストがいない可能性があります。

発信元/検出方法：トラフィック ベースの検出と NetFlow

NetFlow 専用フィールドを除き、NetFlow レコードで利用可能な情報は、トラフィック ベースの検出によって生成される情報よりも限定されます。NetFlow データと管理対象デバイス データの違い，（1442 ページ）を参照してください。

評価ステージ

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。

たとえば、システムは、さらなるリソース集中型評価を行う前に、セキュリティ インテリジェンスを強制します。接続がセキュリティ インテリジェンスによってブロックされた場合、結果として生成されるイベントには、その後の評価によってシステムで収集されることになっていた情報（ユーザ ID など）が含まれません。

ロギング方法：接続の開始または終了

システムが接続の検出時にその接続の開始または終了（またはその両方）をログに記録できるかどうかは、システムがその接続をどのように検出して処理するように設定されているかによって異なります。

接続開始イベントには、セッション期間にわたってトラフィックを調査して判別しなければならない情報が伴ってません（送信されたデータの合計量や、接続の最終パケットのタイムスタンプなど）。また、接続開始イベントにセッションのアプリケーションやURL トラフィックに関する情報が伴っている保証もなく、セッションの暗号化に関する詳細は含まれていません。通常、ブロックされる接続については、接続開始イベントのログへの記録が唯一のオプションになります。

接続イベント タイプ：個々またはサマリー

接続サマリーには、集約された接続に関連付けられたすべての情報が含まれているわけではありません。たとえば、接続の概要に集約される接続にはクライアント情報が使用されないため、概要にはクライアント情報は含まれません。

接続グラフは、接続終了ログのみを使用する接続サマリーのデータに基づいていることに注意してください。接続開始データだけをロギングするようにシステムが設定されている場合、接続グラフと接続サマリーのイベント ビューにはデータが表示されません。

その他の設定

接続のロギングに影響するその他の設定には以下のものが含まれますが、これらに限定されるわけではありません。

- Active Directory ドメイン コントローラで認証するユーザに関連付けられている接続では、ISE が設定されている場合にのみ、ISE 関連のフィールドにデータが入力されます。接続イベントには、LDAP、RADIUS、RSA ドメイン コントローラで認証するユーザの ISE データは含まれません。
- SSL 関連のフィールドには、SSL ポリシーで処理される暗号化接続の場合にのみ、データが入力されます。

- ファイル情報フィールドには、ファイル ポリシーと関連付けられたアクセス コントロール ルールによってログに記録される接続の場合にのみ、データが入力されます。
- 侵入情報フィールドには、侵入ポリシーに関連付けられているアクセス コントロール ルールあるいはデフォルト アクションによってログに記録される接続の場合にのみ、データが入力されます。
- [理由（Reason）] フィールドには、特定の場合にのみデータが入力されます（ユーザがインタラクティブ ブロック設定をバイパスしている場合など）。
- [ドメイン（Domain）] フィールドが表示されるのは、マルチテナンシー用に Firepower Management Center を設定した場合のみです。
- アクセス コントロール ポリシーの詳細設定では、HTTP セッションのモニタ対象ホストによって要求された URL ごとにシステムが接続ログに保存する文字数を制御できます。この設定を使用して URL のロギングを無効化する場合、システムは接続ログで個々の URL を表示しませんが、カテゴリとレピュテーション データは参照できます（存在する場合）。

関連トピック

NetFlow データと管理対象デバイス データの違い, （1442 ページ）

接続イベント フィールドで利用可能な情報

このトピックの表に、システムが接続およびセキュリティ インテリジェンスのフィールドに値を読み込むことができるタイミングを示します。表の列は、次のイベント タイプを示しています。

- [発信元：直接（Origin: Direct）]：Firepower システムの管理対象デバイスで検出および処理される接続を表すイベント。
- [発信元：NetFlow（Origin: NetFlow）]：NetFlow エクスポータでエクスポートされる接続を表すイベント。
- [ロギング：開始（Logging: Start）]：開始時にログに記録される接続を表すイベント。
- [ロギング：終了（Logging: End）]：終了時にログに記録される接続を表すイベント。

表内の「はい（yes）」は、システムが接続イベント フィールドに値を読み込む必要があることを意味するものではなく、読み込むことができることを意味します。システムは、ネットワーク トラフィック内に存在する（および検出可能な）情報だけを報告します。たとえば、SSL 関連のフィールドには、SSL ポリシーによって処理される暗号化された接続のレコードについてのみ値が読み込まれます。

接続イベント フィールド	[発信元：直接（Origin: Direct）]	[発信元：NetFlow（Origin: NetFlow）]	[ロギング：開始（Logging: Start）]	[ロギング：終了（Logging: End）]
アクセス コントロール ポリシー（Access Control Policy）	Yes	No	Yes	Yes

接続イベント フィールド	[発信元：直接（**Origin: Direct**）]	[発信元：**NetFlow**（**Origin: NetFlow**）]	[ロギング：開始（**Logging: Start**）]	[ロギング：終了（**Logging: End**）]
アクセス コントロール ルール（Access Control Rule）	Yes	No	Yes	Yes
操作	Yes	No	Yes	Yes
アプリケーション プロトコル	Yes	Yes	利用可能な場合	Yes
アプリケーション プロトコル カテゴリとタグ（Application Protocol Category & Tag）	Yes	No	利用可能な場合	Yes
アプリケーションのリスク（Application Risk）	Yes	No	利用可能な場合	Yes
ビジネスとの関連性（Business Relevance）	Yes	No	利用可能な場合	Yes
クライアント	Yes	No	利用可能な場合	Yes
クライアント カテゴリとタグ（Client Category & Tag）	Yes	No	利用可能な場合	Yes
クライアント バージョン（Client Version）	Yes	No	利用可能な場合	Yes
接続（Connections）	Yes	Yes	No	Yes
メンバー数（Count）	Yes	Yes	Yes	Yes
宛先ポート/ICMP タイプ（Destination Port/ICMP Type）	Yes	Yes	Yes	Yes
Device	Yes	Yes	Yes	Yes
ドメイン（Domain）	Yes	Yes	Yes	Yes
DNS クエリ（DNS Query）	Yes	No	Yes	Yes
DNS レコード タイプ（DNS Record Type）	Yes	No	Yes	Yes

接続イベント フィールド	[発信元：直接（**Origin: Direct**）]	[発信元：**NetFlow**（**Origin: NetFlow**）]	[ロギング：開始（**Logging: Start**）]	[ロギング：終了（**Logging: End**）]
DNS レスポンス（DNS Response）	Yes	No	Yes	Yes
DNS シンクホール名（DNS Sinkhole Name）	Yes	No	Yes	Yes
DNS TTL	Yes	No	Yes	Yes
出力インターフェイス（Egress Interface）	Yes	No	Yes	Yes
出力セキュリティ ゾーン（Egress Security Zone）	Yes	No	Yes	Yes
エンドポイント ロケーション（Endpoint Location）	Yes	No	Yes	Yes
エンドポイント プロファイル（Endpoint Profile）	Yes	No	Yes	Yes
ファイル	Yes	No	No	Yes
最初のパケット（First Packet）	Yes	Yes	Yes	Yes
HTTP リファラ（HTTP Referrer）	Yes	No	No	Yes
HTTP 応答コード（HTTP Response Code）	Yes	No	Yes	Yes
入力インターフェイス（Ingress Interface）	Yes	No	Yes	Yes
入力セキュリティ ゾーン（Ingress Security Zone）	Yes	No	Yes	Yes
イニシエータ バイト数（Initiator Bytes）	Yes	Yes	有用でない	Yes
イニシエータの国（Initiator Country）	Yes	No	Yes	Yes

接続イベント フィールド	[発信元：直接（**Origin: Direct**）]	[発信元：**NetFlow**（**Origin: NetFlow**）]	[ロギング：開始（**Logging: Start**）]	[ロギング：終了（**Logging: End**）]
イニシエータ IP（Initiator IP）	Yes	Yes	Yes	Yes
イニシエータ パケット（Initiator Packets）	Yes	Yes	有用でない	Yes
イニシエータ ユーザ（Initiator User）	Yes	Yes	Yes	Yes
侵入イベント	Yes	No	No	Yes
侵入ポリシー（Intrusion Policy）	Yes	No	Yes	Yes
IOC（侵害の兆候）（IOC (Indication of Compromise)）	Yes	No	Yes	Yes
最後のパケット（Last Packet）	Yes	Yes	No	Yes
NetBIOS ドメイン（NetBIOS Domain）	Yes	No	Yes	Yes
NetFlow 送信元/宛先の自律システム（NetFlow Source/Destination Autonomous System）	No	Yes	No	Yes
NetFlow 送信元/宛先のプレフィックス（NetFlow Source/Destination Prefix）	No	Yes	No	Yes
NetFlow 送信元/宛先 TOS（NetFlow Source/Destination TOS）	No	Yes	No	Yes
NetFlow SNMP 入出力（NetFlow SNMP Input/Output）	No	Yes	No	Yes
ネットワーク分析ポリシー（Network Analysis Policy）	Yes	No	Yes	Yes
理由（Reason）	Yes	No	Yes	Yes

接続イベント フィールド	[発信元：直接（**Origin: Direct**）]	[発信元：**NetFlow**（**Origin: NetFlow**）]	[ロギング：開始（**Logging: Start**）]	[ロギング：終了（**Logging: End**）]
参照ホスト（Referenced Host）	Yes	No	No	Yes
レスポンダ バイト数（Responder Bytes）	Yes	Yes	有用でない	Yes
レスポンダの国（Responder Country）	Yes	No	Yes	Yes
レスポンダ IP（Responder IP）	Yes	Yes	Yes	Yes
レスポンダ パケット（Responder Packets）	Yes	Yes	有用でない	Yes
セキュリティ コンテキスト（ASA のみ）（Security Context (ASA only)）	Yes	No	Yes	Yes
セキュリティ グループ タグ（SGT）（Security Group Tag (SGT)）	Yes	No	Yes	Yes
セキュリティ インテリジェンスのカテゴリ（Security Intelligence Category）	Yes	No	Yes	Yes
送信元デバイス（Source Device）	Yes	Yes	Yes	Yes
送信元ポート/ICMP タイプ（Source Port/ICMP Type）	Yes	Yes	Yes	Yes
SSL 証明書ステータス（SSL Certificate Status）	Yes	No	No	Yes
SSL 暗号スイート（SSL Cipher Suite）	Yes	No	No	Yes
SSL フロー エラー（SSL Flow Error）	Yes	No	No	Yes

接続イベント フィールド	[発信元：直接（**Origin: Direct**）]	[発信元：**NetFlow**（**Origin: NetFlow**）]	[ロギング：開始（**Logging: Start**）]	[ロギング：終了（**Logging: End**）]
SSL フロー フラグ（SSL Flow Flags）	Yes	No	No	Yes
SSL フロー メッセージ（SSL Flow Messages）	Yes	No	No	Yes
SSL ポリシー（SSL Policy）	Yes	No	No	Yes
SSL ルール（SSL Rule）	Yes	No	No	Yes
SSL セッション ID（SSL Session ID）	Yes	No	No	Yes
SSL ステータス（SSL Status）	Yes	No	No	Yes
SSL バージョン（SSL Version）	Yes	No	No	Yes
TCP フラグ（TCP Flags）	No	Yes	No	Yes
時刻（Time）	Yes	Yes	No	Yes
URL	Yes	No	利用可能な場合	Yes
URL Category	Yes	No	利用可能な場合	Yes
URL レピュテーション（URL Reputation）	Yes	No	利用可能な場合	Yes
ユーザ エージェント（User Agent）	Yes	No	No	Yes
VLAN ID（Admin. VLAN ID）	Yes	No	Yes	Yes
Web アプリケーション（Web Application）	Yes	No	利用可能な場合	Yes
Web アプリケーションのカテゴリとタグ（Web Application Category & Tag）	Yes	No	利用可能な場合	Yes

接続およびセキュリティ インテリジェンス イベント テーブルの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、接続イベントまたはセキュリティ インテリジェンス イベントのテーブルを表示することができます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

接続グラフにアクセスしたときに表示されるページは、使用するワークフローによって異なります。イベントのテーブル ビューで終わる事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

接続またはセキュリティ インテリジェンス ワークフロー テーブルを使用すると、たくさんの一般的なアクションを実行できます。

ドリルダウン ページで接続イベントを制約する場合、同一のイベントからのパケット数とバイト数が合計されることに注意してください。ただし、カスタム ワークフローを使用しており、ドリルダウン ページに [カウント（Count）] カラムを追加していない場合、イベントは個別に表示され、パケット数とバイト数は合計されません。

手順

ステップ 1 次のいずれかを選択します。

- [分析（Analysis）] > [接続（Connections）] > [イベント（Events）]（接続イベントの場合）
- [分析（Analysis）] > [接続（Connections）] > [セキュリティ インテリジェンス イベント（Security Intelligence Events）]

（注） テーブルの代わりに接続グラフが表示された場合、ワークフロータイトルで [(ワークフローの切り替え)（(switch workflow)）] をクリックし、事前定義された [接続イベント（Connection Events）] ワークフローまたはカスタム ワークフローを選択します。事前定義されたすべての接続イベント（接続グラフを含む）は、接続のテーブル ビューで終了することに注意してください。

ステップ 2 次の選択肢があります。

- 時間範囲：時間範囲を調整（イベントが表示されない場合に役立ちます）する方法については、時間枠の変更, （1859 ページ）を参照してください。

- フィールド名：テーブルのカラムの内容について詳しく調べるには、接続およびセキュリティ インテリジェンス イベント フィールド, （1923 ページ）を参照してください。

  ヒント イベントのテーブル ビューでは、各アプリケーション タイプの [カテゴリ（Category）] および [タグ（Tag）] フィールド、NetFlow 関連のフィールド、SSL 関連のフィールドなど、いくつかのフィールドがデフォルトで非表示です。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のフィールド名をクリックします。

- ホスト プロファイル：IP アドレスのホスト プロファイルを表示するには、ホスト プロファイルのアイコン（  ）をクリックします。アクティブな侵害の兆候（IOC）タグのあるホストの場合は、IP アドレスの横に表示される侵害されたホストのアイコン（  ）をクリックします。

- ユーザ プロファイル：ユーザ ID 情報を表示するには、ユーザ ID の横に表示されるユーザ アイコン（  ）をクリックします。

- ファイルおよびマルウェア：接続で検出されたまたはブロックされたマルウェアを含むファイルを表示するには、ファイルの表示アイコン（  ）をクリックし、接続で検出されたファイルとマルウェアの表示, （1953 ページ）の説明に従って続行します。

- 侵入イベント：接続に関連付けられている侵入イベントを優先順位や影響とともに表示するには、[侵入イベント（Intrusion Events）] カラムの侵入イベント アイコン（  ）をクリックして、接続に関連付けられた侵入イベントの表示, （1954 ページ）の説明に従って続行します。

  ヒント 1 つまたは複数の接続に関連付けられた侵入、ファイル、マルウェア イベントをすばやく表示するには、イベント ビューアのチェック ボックスを使用して接続を選択し、[ジャンプ（Jump to）] ドロップダウン リストから該当するオプションを選択します。セキュリティ インテリジェンスによりブラックリストに載せられている接続に関連するファイルまたは侵入が、アクセス コントロール ルールの評価の前にブロックされることによって、1 つも存在しない可能性があることに注意してください。ブラックリストではなく、接続をモニタするようにセキュリティ インテリジェンスを設定した場合に限り、セキュリティ インテリジェンス イベントに関するこの情報が表示されます。

- 証明書：接続を暗号化するために使用される利用可能な証明書についての詳細を表示するには、[SSL ステータス（SSL Status）] カラムの有効なロック アイコン（  ）をクリックします。

- 制約：表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン（  ）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効になったカラムをビューに再び追加するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- イベントの削除：現在の制約されたビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。
- ドリル ダウン：ドリルダウン ページの使用，（1844 ページ）を参照してください。

  ヒント ロギングされた接続に一致した複数のモニタ ルールのうち 1 つにドリル ダウンするには、[*N* モニタ ルール（N Monitor Rules）] の値をクリックします。表示されるポップアップ ウィンドウで、接続イベントを抑制するために使用するモニタ ルールをクリックします。
- このページに移動する：ワークフロー ページのトラバーサル ツール，（1840 ページ）を参照してください。
- ページ間で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- イベント ビュー間で移動する：関連するイベントを表示するためその他のイベント ビューに移動するには、[ジャンプ（Jump to）] をクリックし、ドロップダウン リストからイベント ビューを選択します。
- ソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。

関連トピック

概要：ワークフロー，（1823 ページ）
イベント ビュー設定の設定，（38 ページ）

接続で検出されたファイルとマルウェアの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威またはマルウェア	保護またはマルウェア	任意（Any）	任意（Any）	Admin/Any Security Analyst

1 つまたは複数のアクセス コントロール ルールにファイル ポリシーを関連付けると、システムは一致するトラフィックのファイル（マルウェアを含む）を検出できます。これらのルールによってロギングされた接続に関連付けられたファイル イベントがある場合は、イベント ビューアを使用して確認できます。ファイル リストの代わりに、Firepower Management Center はファイル表示アイコン（  ）を [ファイル（Files）] カラムに表示します。アイコンの数字は、その接続で検出またはブロックされたファイル数（マルウェア ファイルを含む）を示します。

すべてのファイルおよびマルウェア イベントが接続に関連付けられるわけではありません。具体的には次のとおりです。

- エンドポイントベースのマルウェア イベントは、接続に関連付けられていません。これらのイベントは AMP for Endpoints 展開からインポートされます。
- IMAP に対応した電子メール クライアントの多くは単一 IMAP セッションを使用し、それはユーザがアプリケーションを終了したときに終了します。長時間接続はシステムによってロギングされますが、セッションでダウンロードされたファイルは、そのセッションが終了するまで接続に関連付けられません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 接続イベント テーブルを使用している場合、ファイル表示アイコン（  ）をクリックします。ポップアップ ウィンドウが表示され、接続で検出されたファイルのリストとともに、そのタイプと、該当する場合はマルウェア処理が示されます。

ステップ 2 次の選択肢があります。

- 表示：ファイルイベントのテーブル ビューを表示するには、ファイルの表示アイコン（  ）をクリックします。
- 表示：マルウェア イベントのテーブル ビューに詳細を表示するには、マルウェア ファイルの表示アイコン（  ）をクリックします。
- 追跡：ネットワークを経由するファイルの伝送を追跡するには、ファイルのトラジェクトリアイコン（  ）をクリックします。
- 表示：接続で検出されたファイルまたはネットワーク ベースのマルウェア イベントすべての詳細を表示するには、[ファイル イベントの表示（View File Events）] または [マルウェア イベントの表示（View Malware Events）] をクリックします。

接続に関連付けられた侵入イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Any Security Analyst

アクセス コントロール ルールまたはデフォルト アクションに侵入ポリシーを関連付けると、システムは一致するトラフィックのエクスプロイトを検出できます。イベント ビューアを使用して、ロギングされた接続に関連付けられた侵入イベント（ある場合）と、その優先順位や影響について確認できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 接続イベント テーブルを使用する場合、[侵入イベント（Intrusion Events）] カラムの侵入イベント アイコン（  ）をクリックします。

ステップ 2 表示されるポップアップ ウィンドウで、以下のオプションを選択できます。

- パケット ビューで詳細を表示するには、リストされたイベントの表示アイコン（  ）をクリックします。
- [侵入イベントの表示（View Intrusion Events）] をクリックして、接続に関連付けられた侵入イベントすべての詳細を表示します。

暗号化接続の証明書の詳細

イベント ビューアを使用して、システムで処理される接続を暗号化するために使用される公開キー証明書（使用可能な場合）を表示できます。証明書には次の情報が含まれています。

表 *267*：暗号化接続の証明書の詳細

属性（**Attribute**）	説明
サブジェクト/発行元共通名（Subject/Issuer Common Name）	証明書のサブジェクトまたは証明書発行元のホストおよびドメイン名。
サブジェクト/発行元組織（Subject/Issuer Organization）	証明書のサブジェクトまたは証明書発行元の組織。
サブジェクト/発行元組織単位（Subject/Issuer Organization Unit）	証明書のサブジェクトまたは証明書発行元の組織単位。
有効期間（Not Valid Before/After）	証明書の有効期間。

属性（Attribute）	説明
シリアル番号（Serial Number）	発行元 CA によって割り当てられたシリアル番号。
証明書フィンガープリント（Certificate Fingerprint）	証明書の認証に使用する SHA ハッシュ値。
公開キーフィンガープリント（Public Key Fingerprint）	証明書に含まれる公開キーの認証に使用する SHA ハッシュ値。

デバイス サマリー ページの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	カスタム（Custom）

[接続サマリー（Connection Summary）]ページは、接続イベントの検索によって制限されたカスタム ロールを持ち、[接続サマリー（Connection Summary）] ページへのメニュー ベースの明示的なアクセスを許可されたユーザにのみ表示されます。このページは、監視対象ネットワーク上のアクティビティをさまざまな条件で整理したグラフを表示します。たとえば [一定期間の接続数（Connections over Time）] グラフでは、選択した間隔における監視対象ネットワーク上の接続の合計数が表示されます。

接続グラフでできる操作と同じことが、接続サマリーのグラフでも、ほぼすべてできます。ただし、[接続サマリー（Connection Summary）]ページのグラフは集約データに基づいているため、グラフの基になっている個々の接続イベントを調べることはできません。つまり、接続サマリーのグラフから接続データのテーブル ビューにドリルダウンすることはできません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [概要（Overview）] > [概要（Summary）] > [接続の概要（Connection Summary）]を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、サマリーを表示したいデバイスを選択するか、もしくはすべてのデバイスのサマリーを表示するために [すべて（All）] を選択します。

ステップ 3 グラフ接続の操作および分析を行うには、接続イベント グラフの使用方法, （1848 ページ）の説明に従って続行します。

ヒント デフォルトの時間範囲に影響を与えずにさらに分析を行えるように接続グラフ分離するには、[表示（View）] をクリックします。

関連トピック

ユーザ ロールのエスカレーション, （74 ページ）

第 85 章

侵入イベントの操作

以下のトピックでは、侵入イベントを操作する方法について説明します。

侵入イベントについて

Firepower システムは、ホストとそのデータの可用性、整合性、および機密性に影響する可能性のあるトラフィックがないかどうか、ネットワークをモニタするのに役立ちます。主要なネットワーク セグメントに管理対象デバイスを配置すると、悪意のあるアクティビティを目的としてネットワークを通過するパケットを検査できます。このシステムには、攻撃者が開発したさまざまなエクスプロイトを検索するのに使用できるいくつかのメカニズムがあります。

システムは、潜在的な侵入を特定すると侵入イベントを生成します。これは、エクスプロイトの日付、時間、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報のデータです。パケットベースのイベントの場合、イベントをトリガーとして使用したパケットのコピーも記録されます。管理対象デバイスは、Firepower Management Center にイベントを送信します。ここで、集約データを確認し、ネットワーク アセットに対する攻撃を的確に把握できます。

管理対象デバイスをインライン、スイッチド、またはルーテッドの侵入システムとして展開することもできます。これにより、危険だと認識したパケットをドロップまたは置換するようデバイスを設定できます。

Firepower システムは、ユーザが侵入イベントを確認し、ネットワーク環境とセキュリティ ポリシーのコンテキストでそのイベントが重要であるかどうかを評価するために必要なツールも提供します。これらのツールは次のとおりです。

- 管理対象デバイスでの現在のアクティビティの概要について説明するイベント要約ページ
- 選択した任意の期間に生成できるテキストベースおよびグラフィカルなレポート。独自のレポートを設計し、スケジュールされた間隔で実行されるよう設定することもできます
- 攻撃に関連したイベントデータの収集に使用できるインシデント処理ツール。調査や応答のトラッキングに役立つ注記を追加することもできます
- SNMP、電子メール、および syslog で設定できる自動アラート
- 特定の侵入イベントに対する応答や修復に使用できる自動化された相関ポリシー
- データをドリルダウンして、さらに調査したいイベントを特定するのに使用できる定義済みカスタム ワークフロー

侵入イベントの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

侵入イベントは、ネットワーク セキュリティに対する脅威があるかどうかを判断するために表示します。

初期の侵入イベント ビューは、ページにアクセスするために使用するワークフローによって異なります。1 つ以上のドリルダウン ページ、侵入イベントのテーブル ビュー、および終了パケット ビューを含む、定義済みワークフローの1つを使用するか、独自のワークフローを作成できます。カスタム テーブルに基づいてワークフローを表示することもできます。これには、侵入イベントを含めることができます。

大量の IP アドレスが含まれている状態で、[IP アドレスの解決（Resolve IP Addresses）] イベント ビュー設定が有効になっていると、イベント ビューの表示が遅くなる場合があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）]を選択します。

ステップ 2 次の選択肢があります。

- 時間範囲の調整：時間枠の変更，（1859ページ）の説明に従って、イベント ビューの時間範囲を調整します。
- ワークフローの変更：侵入イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合、ワークフローのタイトルの横にある [(ワークフローの切り替え)（(switch workflow)）] をクリックして、システム提供のワークフローのいずれかを選択します。
- 制約：表示する対象を分析において重要な侵入イベントに狭めるには、侵入イベント ワークフローの使用，（1980 ページ）を参照してください。
- イベントの削除：データベースからイベントを削除するには、[削除（Delete）] をクリックして表示しているパケットのイベントを削除するか、[すべて削除（Delete All）] をクリックして以前に選択したパケットのすべてのイベントを削除します。
- 確認済みのマークを付ける：侵入イベントに確認済みのマークを付けるには、侵入イベントを確認済みとしてマーク，（1974 ページ）を参照してください。
- 接続データの表示：侵入イベントに関連付けられた接続データを表示するには、侵入イベントと関連付けられた接続データの表示，（1973 ページ）を参照してください。
- 内容の表示：侵入イベント フィールド，（1961ページ）の説明に従ってテーブルのカラムの内容を表示します。

関連トピック

侵入イベント パケット ビューの使用，（1983 ページ）

侵入イベント フィールド

システムは、潜在的な侵入を特定すると侵入イベントを生成します。これは、エクスプロイトの日付、時間、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報のデータです。パケットベースのイベントの場合、イベントをトリガーとして使用したパケットのコピーも記録されます。

侵入イベントを検索するときは、個別のイベントで利用可能な情報は、システムがいつ、なぜ、どのようにしてイベントを記録したかによって異なることに注意してください。たとえば、復号化されたトラフィックでトリガーされた侵入イベントだけが SSL 情報を含んでいます。

（注） デフォルトでは、侵入イベントのテーブル ビューにいくつかのフィールドが表示されます。セッション中にフィールドを有効にするには、検索制約を拡張してから、[無効の列（Disabled Columns）] の下の列名をクリックします。

アクセス コントロール ポリシー（Access Control Policy）

イベントを生成した侵入ルール、プリプロセッサルール、またはデコーダルールが有効になっている侵入ポリシーに関連付けられているアクセス コントロール ポリシー。

アクセス コントロール ルール（Access Control Rule）

イベントを生成した侵入ルールを呼び出したアクセスコントロールルール。[デフォルトアクション（Default Action）] は、ルールが有効化されている侵入ポリシーが特定のアクセス コントロール ルールに関連付けられておらず、代わりに、アクセス コントロール ポリシーのデフォルト アクションとして設定されていることを示しています。

侵入インスペクションがアクセス コントロール ルールにもデフォルト アクションにも関連付けられていない場合、このフィールドは空欄になります。たとえば、パケットがデフォルトの侵入ポリシーによって検査された場合などです。

アプリケーション プロトコル（Application Protocol）

（使用可能な場合）侵入イベントをトリガーとして使用したトラフィックで検出されたホスト間の通信を表す、アプリケーション プロトコル。

アプリケーション プロトコル カテゴリおよびタグ（Application Protocol Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

アプリケーションのリスク（Application Risk）

侵入イベントをトリガーしたトラフィックで検出されたアプリケーションに関連付けられているリスク。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、および [非常に低い（Very Low）]。接続で検出されるアプリケーションのタイプごとに関連するリスクがあります。このフィールドは、それらのうち最も高いリスクを表示します。

ビジネスとの関連性（Business Relevance）

侵入イベントをトリガーしたトラフィックで検出されたアプリケーションに関連付けられているビジネスとの関連性。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、および [非常に低い（Very Low）]。接続で検出されるアプリケーションのタイプごとに関連するビジネスとの関連性があります。このフィールドは、それらのうち最も低い（関連性が最も低い）ものを表示します。

分類（Classification）

イベントを生成したルールが属する分類。

このフィールドを検索するときは、表示するイベントを生成したルールの分類番号を入力するか、分類名または説明のすべてまたは一部を入力します。また、番号、名前、または説明のコンマ区切りリストを入力することもできます。最後に、カスタム分類を追加した場合、その名前または説明のすべてまたは一部を使用して検索することもできます。

クライアント（Client）

（使用可能な場合）侵入イベントをトリガーとして使用したトラフィックで検出されたモニタ対象のホストで実行されているソフトウェアを表す、クライアント アプリケーション。

クライアント カテゴリおよびタグ（Client Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

メンバー数（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

送信先の大陸（Destination Continent）

侵入イベントに関連する受信ホストの大陸。

送信先の国（Destination Country）

侵入イベントに関連する受信ホストの国。

宛先 IP（Destination IP）

侵入イベントに関連する受信ホストが使用する IP アドレス。

送信先ポートまたは ICMP コード（Destination Port / ICMP Code）

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、このフィールドには ICMP コードが表示されます。

宛先ユーザ（Destination User）

宛先ホストにログインしている既知のユーザのユーザ ID。

Device

アクセス コントロール ポリシーが展開された管理対象デバイス。

スタック構成設定では、プライマリ デバイスとセカンダリ デバイスは、別々のデバイスであるかのように侵入イベントをレポートすることに注意してください。

ドメイン

侵入を検出したデバイスのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

出力インターフェイス（Egress Interface）

イベントをトリガーとして使用したパケットの出力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列には入力されません。

出力セキュリティ ゾーン（Egress Security Zone）

イベントをトリガーとして使用したパケットの出力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーンのフィールドには入力されません。

電子メールの添付ファイル（Email Attachments）

[MIME コンテンツ - 傾向（MIME Content-Disposition）] 見出しから取得された MIME 添付ファイル名。添付ファイルの名前を表示するには、SMTP プリプロセッサの [MIME 添付ファイル名のログ（Log MIME Attachment Names）] オプションを有効にする必要があります。複数の添付ファイル名がサポートされます。

電子メール ヘッダー（Email Headers）（検索のみ）

電子メールのヘッダーから取得したデータ。

電子メールのヘッダーを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [ヘッダーのログ（Log Headers）] オプションを有効にする必要があります。

メール受信者（Email Recipient）

SMTP RCPT TO コマンドから取得された電子メール受信者のアドレス。このフィールドの値を表示するには、SMTP プリプロセッサの [受信者アドレスのログ（Log To Addresses）] オプションを有効にする必要があります。複数の受信者アドレスがサポートされます。

メール送信者（Email Sender）

SMTP MAIL FROM コマンドから取得された電子メール送信者のアドレス。このフィールドの値を表示するには、SMTP プリプロセッサの [送信者アドレスのログ（Log From Address）] オプションを有効にする必要があります。複数の送信者アドレスがサポートされます。

ジェネレータ（Generator）

イベントを生成したコンポーネント。

HTTP ホスト名（HTTP Hostname）

HTTP 要求のホスト ヘッダーから取得されたホスト名（存在する場合）。要求パケットにホスト名が常に含まれているわけではないことに注意してください。

ホスト名を HTTP クライアント トラフィックの侵入イベントと関連付けるには、HTTP 検査プリプロセッサの [ホスト名のログ（Log Headers）] オプションを有効にする必要があります。

テーブル ビューで、この列には、取得されたホスト名の最初の 50 文字が表示されます。ホストの省略名の表示部分にポインタを合わせると、最大 256 バイトまでの完全な名前を表示することができます。また、最大 256 バイトまでの完全なホスト名をパケット ビューに表示することもできます。

HTTP 応答コード（HTTP Response Code）

イベントをトリガーした接続を介してクライアントの HTTP 要求に応答して送信される HTTP ステータス コード。

HTTP URI

（存在する場合）侵入イベントをトリガーした HTTP 要求パケットに関連付けられた raw URI。要求パケットに URI が常に含まれているわけではないことに注意してください。

URI を HTTP クライアント トラフィックの侵入イベントと関連付けるには、HTTP 検査プリプロセッサの [URI のログ（Log URI）] オプションを有効にする必要があります。

HTTP 応答によってトリガーとして使用された侵入イベントの関連 HTTP URI を参照するには、[両方のポートでのストリーム再構成の実行（Perform Stream Reassembly on Both Ports）] オプションに HTTP サーバのポートを設定する必要があります。ただし、これにより、トラフィックのリアセンブル用のリソース要求が増加することに注意してください。

この列には、取得された URI の最初の 50 文字が表示されます。省略 URI の表示部分にポインタを合わせると、最大 2048 バイトまでの完全な URI を表示することができます。また、最大 2048 バイトまでの完全な URI をパケット ビューに表示することもできます。

影響（Impact）

このフィールドの影響レベルは、侵入データ、ネットワーク検出データ、脆弱性情報との関係を示します。

このフィールドを検索するときは、影響アイコンの色または一部の文字列を指定しないでください。たとえば、blue、level 1、または 0 を使用しないでください。有効な大文字と小文字を区別しない値は次のとおりです。

- Impact 0、Impact Level 0
- Impact 1、Impact Level 1
- Impact 2、Impact Level 2
- Impact 3、Impact Level 3
- Impact 4、Impact Level 4

NetFlow データからネットワーク マップに追加されたホストに使用可能なオペレーティング システムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクト レベル 1：赤）インパクト レベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティング システム ID を手動で設定します。

入力インターフェイス（Ingress Interface）

イベントをトリガーしたパケットの入力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列だけに入力されます。

入力セキュリティ ゾーン（Ingress Security Zone）

イベントをトリガーとして使用したパケットの入力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。

インライン結果（Inline Result）

ワークフローとテーブル ビューでは、このフィールドには次のいずれかが表示されます。

- 黒い下矢印：ルールをトリガーとして使用したパケットをシステムがドロップしたことを示します
- 灰色の下矢印：[インライン時にドロップ（Drop when Inline）] 侵入ポリシー オプション（インライン展開環境）を有効にした場合、またはシステムがプルーニングしている間に [ドロップしてイベントを生成する（Drop and Generate）] ルールがイベントを生成した場合、IPS がパケットをドロップしたことを示します
- 空白：トリガーとして使用されたルールが [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていないことを示します

侵入ポリシーのルールの状態またはインライン ドロップ動作にかかわらず、インライン インターフェイスがタップ モードになっている場合を含め、パッシブ展開環境ではシステムはパケットをドロップしません。

このフィールドを検索するときは、次のいずれかを入力します。

- dropped：パケットがインライン展開環境でパケットをドロップするかどうかを指定します
- would have dropped：インライン展開環境でパケットをドロップするように侵入ポリシーが設定されている場合に、パケットをドロップするかどうかを指定します

侵入ポリシー（Intrusion Policy）

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。

IOC

侵入イベントをトリガーとして使用したトラフィックが、接続に関係するホストに対する侵入の痕跡（IOC）もトリガーとして使用したかどうか。このフィールドを検索するときは、triggered または n/a を指定します。

メッセージ（Message）

イベントを説明するテキスト。ルールベースの侵入イベントの場合、イベント メッセージはルールから取得されます。デコーダベースおよびプリプロセッサベースのイベントの場合は、イベント メッセージはハード コーディングされています。

MPLSラベル（MPLS Label）

侵入イベントをトリガーしたパケットと関連付けられているマルチプロトコルラベルスイッチング ラベル。

ネットワーク分析ポリシー（Network Analysis Policy）

イベントの生成に関連付けられているネットワーク分析ポリシー（ある場合）。

この列には、取得された URI の最初の 50 文字が表示されます。省略 URI の表示部分にポインタを合わせると、最大 2048 バイトまでの完全な URI を表示することができます。また、最大 2048 バイトまでの完全な URI をパケット ビューに表示することもできます。

クライアントのオリジナル IP（Original Client IP）

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーから取得された、元のクライアント IP アドレス。

このフィールドの値を表示するには、ネットワーク解析ポリシーで HTTP プリプロセッサ [元のクライアント IP アドレスの抽出（Extract Original Client IP Address）] オプションを有効にする必要があります。オプションで、ネットワーク解析ポリシーの同じエリアで、最大 6 つのカスタム クライアント IP 見出しを指定し、システムが [クライアントのオリジナル IP（Original Client IP）] イベント フィールドの値を選択する優先順位を設定します。

[プライオリティ（Priority）]

Cisco Talos Security Intelligence and Research Group（Talos） で指定されたイベントの優先度。優先度は、`priority` キーワードの値または `classtype` キーワードの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。有効な値は、[高（high）]、[中（medium）]、および [低（low）] です。

プロトコル（Protocol）（検索のみ）

http://www.iana.org/assignments/protocol-numbers に一覧表示されている、接続で使用するトランスポート プロトコルの名前または番号。これは、送信元および宛先ポート/ICMP の列と関連付けられたプロトコルです。

確認者（Reviewed By）

イベントを確認したユーザの名前。このフィールドを検索するときは、unreviewed と入力すると、まだ確認されていないイベントを検索できます。

セキュリティ コンテキスト（Security Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチ コンテキスト モードの ASA FirePOWER だけです。

Snort ID（Snort ID）（検索のみ）

イベントを生成したルールの Snort ID（SID）を指定するか、オプションで、ルールの複合ジェネレータ ID（GID）および SID を指定します。ここで、GID および SID は、コロン（:）で区切られ、GID:SID の形式になります。次の表の任意の値を指定できます。

表 *268*：*Snort ID* 検索値

値	例
単一の SID	10000
SID の範囲	10000 ～ 11000
SID より大きい	>10000
SID 以上	>=10000
SID 未満	<10000
SID 以下	<=10000
SID のカンマ区切りリスト	10000,11000,12000
単一の GID:SID の組み合わせ	1:10000
GID:SID の組み合わせのカンマ区切りリスト	1:10000,1:11000,1:12000
SID および GID:SID の組み合わせのカンマ区切りリスト	10000,1:11000,12000

表示しているイベントの SID が [メッセージ（Message）] 列に表示されます。

ソースの大陸（Source Continent）

侵入イベントに関連する送信ホストのある大陸。

ソースの国（Source Country）

侵入イベントに関連する送信ホストのある国。

ソース IP

侵入イベントに関連する送信ホストが使用する IP アドレス。

送信元ポート/ICMP タイプ（Source Port / ICMP Type）

送信元ホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、このフィールドには ICMP タイプが表示されます。

送信元ユーザ（Source User）

送信元ホストにログインしている既知のユーザのユーザ ID。

SSL の実際のアクション（SSL Actual Action）（検索のみ）

システムが暗号化トラフィックに適用したアクション。

ブロック（Block）/リセットしてブロック（Block With Reset）

ブロックされた暗号化接続を表します。

複合（再署名）（Decrypt (Resign)）

再署名サーバ証明書を使用して復号された発信接続を表します。

復号（キーの置き換え）（Decrypt (Replace Key)）

置き換えられた公開キーと自己署名サーバ証明書を使用して復号された発信接続を表します。

復号（既知のキー）（Decrypt (Known Key)）

既知の秘密キーを使用して復号された着信接続を表します。

デフォルト アクション（Default Action）

接続がデフォルト アクションによって処理されたことを示しています。

復号しない（Do Not Decrypt）

システムが復号しなかった接続を表します。

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL 証明書情報（SSL Certificate Information）（検索のみ）

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- 件名/発行元共通名（Subject/Issuer Common Name）
- 件名/発行元組織（Subject/Issuer Organization）
- 件名/発行元組織ユニット（Subject/Issuer Organization Unit）
- 有効期間の開始/終了（Not Valid Before/After）
- シリアル番号（Serial Number）
- 証明書フィンガープリント（Certificate Fingerprint）
- 公開キー フィンガープリント（Public Key Fingerprint）

SSL 失敗理由（SSL Failure Reason）（検索のみ）

システムが暗号化されたトラフィックの復号に失敗した理由：

- 不明
- 不一致（No Match）
- Success
- キャッシュされていないセッション（Uncached Session）
- 不明な暗号スイート（Unknown Cipher Suite）
- サポートされていない暗号スイート（Unsupported Cipher Suite）
- サポートされていない SSL バージョン（Unsupported SSL Version）
- SSL 圧縮の使用（SSL Compression Used）
- パッシブ モードで復号できないセッション（Session Undecryptable in Passive Mode）
- ハンドシェイク エラー（Handshake Error）
- 復号エラー（Decryption Error）
- 保留サーバ名カテゴリ ルックアップ（Pending Server Name Category Lookup）
- 保留共通名カテゴリ ルックアップ（Pending Common Name Category Lookup）
- 内部エラー（Internal Error）
- ネットワーク パラメータを使用できません（Network Parameters Unavailable）
- 無効なサーバ証明書の処理（Invalid Server Certificate Handle）
- サーバ証明書フィンガープリントを使用できません（Server Certificate Fingerprint Unavailable）
- サブジェクト DN をキャッシュできません（Cannot Cache Subject DN）
- 発行元 DN をキャッシュできません（Cannot Cache Issuer DN）
- 不明の SSL バージョン（Unknown SSL Version）
- 外部証明書リストを使用できません（External Certificate List Unavailable）
- 外部証明書フィンガープリントを使用できません（External Certificate Fingerprint Unavailable）
- 内部証明書リストが無効です（Internal Certificate List Invalid）
- 内部証明書リストを使用できません（Internal Certificate List Unavailable）
- 内部証明書を使用できません（Internal Certificate Unavailable）
- 内部証明書フィンガープリントを使用できません（Internal Certificate Fingerprint Unavailable）
- サーバ証明書検証を使用できません（Server Certificate Fingerprint Unavailable）
- サーバ証明書検証エラー（Server Certificate Validation Failure）
- 無効なアクション（Invalid Action）

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL ステータス（SSL Status）

暗号化接続をログに記録した [SSL の実際のアクション（SSL Actual Action）]（SSL ルール、デフォルトのアクション、または復号化できないトラフィック アクション）に関連付けられているアクション。

システムが暗号化された接続の復号化に失敗した場合、実行された [SSL の実際のアクション（SSL Actual Action）]（復号化できないトラフィック アクション）と [SSL 障害の理由（SSL Failure Reason）] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [復号しない（不明な暗号スイート）（Do Not Decrypt (Unknown Cipher Suite)）] が表示されます。

証明書の詳細を表示するにはロック アイコン（  ）をクリックします。

このフィールドを検索するときは、[SSL の実際のアクション（SSL Actual Action）] および [SSL 障害の理由（SSL Failure Reason）] の値を 1 つ以上を入力して、システムが処理した暗号化されたトラフィック、または復号化に失敗したトラフィックを表示します。

SSL 件名/発行元国（SSL Subject/Issuer Country）（検索のみ）

暗号化証明書に関連付けられている件名または発行者の国に関する 2 文字の ISO 3166-1 アルファ 2 国コード。

時刻（Time）

イベントの日付と時刻。このフィールドは検索できません。

VLAN ID（Admin. VLAN ID）

侵入イベントをトリガーとして使用したパケットと関連付けられた最内部 VLAN ID。

Web アプリケーション（Web Application）

侵入イベントをトリガーとして使用したトラフィックで検出された HTTP トラフィックの内容または要求された URL を表す、Web アプリケーション。

システムが HTTP のアプリケーション プロトコルを検出し、特定の Web アプリケーションを検出できなかった場合、システムはここで一般的な Web ブラウジング指定を提供します。

Web アプリケーション カテゴリおよびタグ（Web Application Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

関連トピック

イベントの検索, （1871 ページ）

侵入イベント影響レベル

イベントがネットワークに与える影響を評価するために、Firepower Management Center は侵入イベントのテーブル ビューに影響レベルを表示します。イベントごとに、システムは影響レベルアイコンを追加し、侵入データ、ネットワーク検出データ、脆弱性情報との関係を色で示します。

（注） NetFlow データからネットワーク マップに追加されたホストに使用可能なオペレーティング システムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクト レベル 1：赤）インパクト レベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティング システム ID を手動で設定します。

次の表に、影響レベルで使用可能な値を示します。

表 *269*：影響レベル

影響レベル	脆弱性	カラー	説明
0	不明	グレー	送信元ホストと宛先ホストは両方ともネットワーク検出によってモニタされているネットワーク上に存在しません。
1	脆弱	赤色	次のいずれかを行います。 • 送信元ホストまたは宛先ホストはネットワーク マップ内にあり、脆弱性はホストにマッピングされます • 送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵害される可能性があります。
2	潜在的に脆弱	オレンジ	送信元ホストまたは宛先ホストはネットワーク マップ内にあり、次のいずれかに当てはまります。 • ポート指向のトラフィックの場合、ポートはサーバ アプリケーション プロトコルを実行しています • ポート指向ではないトラフィックの場合、ホストはプロトコルを使用します

影響レベル	脆弱性	カラー	説明
3	現在は脆弱ではない	黄色	送信元ホストまたは宛先ホストはネットワーク マップ内にあり、次のいずれかに当てはまります。 • ポート指向のトラフィック（たとえば、TCP または UDP）の場合、ポートが開いていません • ポート指向ではないトラフィック（たとえば、ICMP）の場合、ホストはプロトコルを使用しません
4	ターゲット不明	青	送信元ホストまたは宛先ホストがモニタ対象のネットワークにありますが、ネットワーク マップ内にそのホストのエントリがありません。

侵入イベントと関連付けられた接続データの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

システムは、侵入イベントが検出された接続を記録できます。このロギングは、アクセス コントロール ルールに関連付けられている侵入ポリシーに対して自動的に行われますが、デフォルト アクションに関連する接続データを参照するには、接続ロギングを手動で有効にする必要があります。

関連データの表示は、イベントのテーブル ビュー間を移動する場合に非常に役立ちます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）]を選択します。

ステップ 2 イベント ビューアのチェック ボックスを使用して侵入イベントを選択してから、[ジャンプ（Jump to）] ドロップダウン リストから [接続（Connections）] を選択します。

ヒント 同じ方法で、特定の接続に関連した侵入イベントを表示できます。詳細については、ワークフロー間のナビゲーション，（1866 ページ）を参照してください。

関連トピック

許可された接続のロギング, （1915 ページ）
侵入イベント ワークフローの使用, （1980 ページ）
接続およびセキュリティ インテリジェンス イベント テーブルの使用, （1951 ページ）

侵入イベントを確認済みとしてマーク

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

侵入イベントが悪意のあるものではないことがわかったら、そのイベントを確認済みとしてマークできます。

侵入イベントを調べて、そのイベントがネットワーク セキュリティに対して脅威ではないことがわかったら（たとえば、ネットワーク上のどのホストも検出されたエクスプロイトに対して脆弱でないことがわかっているなど）、そのイベントを確認済みとしてマークできます。確認済みのイベントはイベント データベースに保存され、イベント要約統計に含まれますが、デフォルトの侵入イベント ページには表示されなくなります。自分の名前がレビューアとして表示されます。

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

バックアップを実行してから確認済みの侵入イベントビューを削除した場合、バックアップを復元すると、削除された侵入イベント ビューは復元されますが、確認済みのステータスは復元されません。こうして復元された侵入イベントは、[確認済みイベント（Reviewed Events）] の下ではなく [侵入イベント（Intrusion Events）] の下に表示されます。

手順

侵入イベントが表示されるページで、次の 2 つの方法を選択できます。

- イベントのリストから 1 つまたは複数の侵入イベントにマークを付けるには、イベントの横にあるチェックボックスをオンにして、[レビュー（Review）] をクリックします。
- イベントのリストからすべての侵入イベントにマークを付けるには、[すべて確認（Review All）] をクリックします。

関連トピック

侵入イベント ワークフローの使用, （1980 ページ）

以前に確認された侵入イベントの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

手順

ステップ 1 [分析（Analysis）] > [侵入（Intrusions）] > [見直されたイベント（Reviewed Events）]を選択します。

ステップ 2 次の選択肢があります。

- 時間枠の変更, （1859 ページ）の説明に従って、時間範囲を調整します。
- 侵入イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合、ワークフローのタイトルの横にある [(ワークフローの切り替え)（(switch workflow)）] をクリックして、システム提供のワークフローのいずれかを選択します。
- 表示されるイベントの詳細については、侵入イベント フィールド, （1961 ページ）を参照してください。

関連トピック

侵入イベント ワークフローの使用, （1980 ページ）

侵入イベントへの未確認としてマーク

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

イベントに未確認のマークを付けることで、確認済みイベントをデフォルトの侵入イベント ビューに戻すことができます。

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

手順

確認済みイベントが表示されるページで、次の 2 つの方法を選択できます。

- 確認済みイベントリストから個別の侵入イベントを削除するには、特定のイベントの横にあるチェックボックスをオンにして、[未確認（Unreview）] をクリックします。
- 確認済みイベントリストからすべての侵入イベントを削除するには、[すべて未確認（Unreview All）] をクリックします。

プロプロセッサ イベント

プリプロセッサが提供する機能は 2 つあります。1 つは、パケットに対して指定されたアクション（HTTP トラフィックを復号して正規化するなど）を実行する機能、もう 1 つは、パケットが特定のプリプロセッサオプションをトリガーしたときに関連するプリプロセッサルールが有効にされている場合は常にイベントを生成することで、指定のプリプロセッサ オプションの実行を報告するという機能です。たとえば、プリプロセッサが IIS の二重にエンコードされたトラフィックを検出した場合にイベントが生成されるようにするには、HTTP Inspect の [二重エンコード（Double Encoding）] オプションと、HTTP Inspect Generator（GID）119 および Snort ID（SID）2 が設定された関連するプリプロセッサ ルールを有効にします。

プリプロセッサの実行を報告するイベントを生成すると、異常なプロトコル エクスプロイトを検出するのに役立ちます。たとえば、攻撃者は重複している IP フラグメントを作成して、ホスト上で DoS 攻撃を引き起こす可能性があります。IP 最適化プリプロセッサはこのタイプの攻撃を検出し、それに関する侵入イベントを生成できます。

プリプロセッサイベントは、パケットディスプレイにイベントの詳細なルールの説明が表示されないという点で、ルールイベントとは異なります。代わりに、パケットディスプレイには、イベント メッセージ、GID、SID、パケット ヘッダー データおよびパケット ペイロードが表示されます。これにより、パケットのヘッダー情報を分析し、そのヘッダー オプションが使用中であるかをどうか判断して、それがシステムをエクスプロイトする可能性がある場合は、パケット ペイロードを検査できます。プリプロセッサによる各パケットの分析が完了すると、ルール エンジンは、その結果に応じて適切なルールを実行し（プリプロセッサが各パケットを最適化し、有効なセッションの一部として確立できた場合）、潜在的なコンテンツ レベルの脅威についてさらに分析を行い、それらのパケットについて報告します。

プリプロセッサのジェネレータ ID

各プリプロセッサには、独自のジェネレータ ID 番号（GID）があり、これはパケットによってトリガーとして使用されたプリプロセッサを示します。一部のプリプロセッサは関連した SID もあり、これは潜在的攻撃を分類する ID 番号です。ルールの Snort ID（SID）が、ルールをトリガーとして使用するパケットのコンテキストを提供できる方法とほぼ同じで、この ID 番号によりイベントのタイプを分類することによって、イベントをより効率的に分析するのに役立ちます。侵入

ポリシー ルールのページのプリプロセッサ フィルター グループのプリプロセッサごとにプリプロセッサ ルールをリストできます。また、プリプロセッサのプリプロセッサ ルールとカテゴリ フィルター グループのパケット デコーダ サブグループをリストできます。

（注） 標準テキスト ルールによって生成されるイベントのジェネレータ ID は 1 です。共有オブジェクト ルールの場合、イベントのジェネレータ ID は 3 です。どちらの場合も、トリガーした特定のルールがイベントの SID に示されます。

次の表では、各 GID を生成するイベントのタイプについて説明します。

表 *270*：ジェネレータ *ID*

ID	コンポーネント	説明
1	標準的なテキストルール	パケットが標準テキストルールをトリガーとして使用したときにイベントが生成されました。
2	タグ付きパケット	タグ付きセッションからパケットを生成するタグ ジェネレータによって、イベントが生成されました。これは、`tag` ルール オプションが使用される場合に発生します。
3	共有オブジェクト ルール	パケットが共有オブジェクトルールをトリガーとして使用したときにイベントが生成されました。
102	HTTP デコーダ	デコーダ エンジンが、パケット内の HTTP データを復号化しました。
105	Back Orifice ディテクタ	Back Orifice ディテクタが、パケットに関連付けられた Back Orifice 攻撃を特定しました。
106	RPC デコーダ	RPC デコーダがパケットを復号化しました。
116	パケット デコーダ	パケット デコーダによってイベントが生成されました。
119、120	HTTP Inspect プリプロセッサ	HTTP Inspect プリプロセッサによってイベントが生成されました。GID 120 ルールは、サーバ固有の HTTP トラフィックに関するルールです。
122	ポートスキャンディテクタ	ポートスキャン フロー ディテクタによってイベントが生成されました。
123	IP デフラグメンタ	断片化された IP データグラムを適切に再構成できなかったときに、イベントが生成されました。
124	SMTP デコーダ	SMTP プリプロセッサが SMTP バーブに対するエクスプロイトを検出したときに、イベントが生成されました。
125	FTP デコーダ	FTP/Telnet デコーダが FTP トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。

ID	コンポーネント	説明
126	Telnet デコーダ	FTP/Telnet デコーダが Telnet トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。
128	SSH プリプロセッサ	SSH プリプロセッサが SSH トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。
129	ストリームプリプロセッサ	ストリームプリプロセッサによるストリームの前処理中に、イベントが生成されました。
131	DNSプリプロセッサ	DNS プリプロセッサによってイベントが生成されました。
133	DCE/RPC プリプロセッサ	このイベントは、DCE/RPC プリプロセッサにより生成されました。
134	ルール遅延 パケット遅延	ルール遅延によって侵入ルールのグループが中断された（134:1）または再有効化された（134:2）とき、あるいはパケット遅延しきい値が超過したために、システムがパケットの検査を停止したとき（134:3）に、イベントが生成されました。
135	レートベースの攻撃ディテクタ	レートベースの攻撃ディテクタがネットワークのホストに対する過度の識別したときに、イベントが生成されました。
137	SSL プリプロセッサ	このイベントは、SSL プリプロセッサによって生成されました。
138、139	機密データプリプロセッサ	機密データ プリプロセッサによってイベントが生成されました。
140	SIP プリプロセッサ	SIP プリプロセッサによってイベントが生成されました。
141	IMAP プリプロセッサ	IMAP プリプロセッサによってイベントが生成されました。
142	POP プリプロセッサ	POP プリプロセッサによってイベントが生成されました。
143	GTP プリプロセッサ	GTP プリプロセッサによってイベントが生成されました。
144	Modbus プリプロセッサ	Modbus SCADA プリプロセッサによってイベントが生成されました。
145	DNP3 プリプロセッサ	DNP3 SCADA プリプロセッサによってイベントが生成されました。

侵入イベントのワークフロー ページ

現在の侵入ポリシーで有効になっているプリプロセッサ、デコーダ、および侵入ルールは、モニタしているトラフィックがポリシーに違反するたびに、侵入イベントを生成します。

Firepowerシステムは、侵入イベントの表示および分析に使用できる、イベントデータが入力された定義済みワークフローのセットを提供します。これらのワークフローは、評価する侵入イベントの特定に役立つ一連のページを表示して手順を示します。

定義済みの侵入イベントのワークフローには、次の 3 種類のページまたはイベント ビューがあります。

- 1 つ以上のドリルダウン ページ
- 侵入イベントのテーブル ビュー
- パケット ビュー

ドリルダウン ページには通常、1 つの特定の種類の情報を表示できるように 1 つのテーブル（一部のドリルダウン ビューでは複数のテーブル）に 2 つ以上の列が含まれます。

「ドリルダウン」して 1 つ以上の宛先ポートの詳細情報を検索すると、これらのイベントは自動的に選択され、ワークフローの次のページが表示されます。このように、ドリルダウン テーブルを使用すると、一度に分析するイベントの数を減らすことができます。

侵入イベントの最初のテーブル ビューでは、各侵入イベントが独自の行にリストされます。テーブルの列には、時間、発信元 IP アドレスおよびポート、宛先 IP アドレスおよびポート、イベントの優先度、イベント メッセージなどの情報が示されます。

イベントを選択してワークフローの次のページを表示する代わりに、テーブル ビューでイベントを選択した場合、イベントはいわゆる制約に追加されます。制約とは、分析するイベントの種類に加える制限のことです。

たとえば、任意の列で列のクローズアイコン（ ）をクリックして、ドロップダウンリストから [時間（Time）] をクリアすると、[時間（Time）] を列の 1 つとして削除できます。分析内でイベントのリストを絞り込むには、テーブル ビューの行のいずれかの値のリンクをクリックします。たとえば、分析を送信元 IP アドレスの 1 つ（おそらく、潜在的な攻撃者）から生成されたイベントに制限するには、[送信元 IP アドレス（Source IP Address）] 列の IP アドレスをクリックします。

テーブル ビューの 1 つまたは複数の行を選択し、[表示（View）] をクリックすると、パケット ビューが表示されます。パケット ビューは、ルールをトリガーとして使用したパケットまたはイベントを生成したプリプロセッサに関する情報を提供します。パケット ビューの各セクションには、パケット内の特定の層についての情報が含まれます。折りたたまれたセクションを展開すると、より多くの情報を参照できます。

（注） それぞれのポートスキャン イベントは複数のパケットによってトリガーとして使用されるため、ポートスキャン イベントは特別なバージョンのパケット ビューを使用します。

事前定義済みのワークフローが特定のニーズに合致しない場合は、必要な情報だけを表示するカスタム ワークフローを作成できます。カスタム侵入イベントのワークフローには、ドリルダウン ページ、イベントのテーブル ビュー、またはその両方を含めることができます。システムはパケット ビューを最後のページとして自動的に組み込みます。イベントを調査する方法に応じて、定義済みワークフローと独自のカスタム ワークフローを簡単に切り替えることができます。

侵入イベント ワークフローの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

イベントのドリルダウン ビューとテーブル ビューは、イベントのリストを絞り込み、関連するイベントのグループに分析を集中するために使用できる共通機能を共有します。

別のワークフロー ページで同じ侵入イベントを表示しないようにするため、ページの下部にあるリンクをクリックして別のページのイベントを表示すると時間範囲は一時停止し、クリックして後続のページでその他のアクションを実行すると再開します。

ヒント プロセスの任意の時点で、制約を検索条件のセットとして保存できます。たとえば、ネットワークが数日にわたり単一の IP アドレスから攻撃者によって探られていることに気付いた場合、調査中に制約をいったん保存し、後で使用することができます。ただし、複合制約を検索条件のセットとして保存することはできません。

手順

ステップ 1 [分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）] を使用して侵入イベント ワークフローにアクセスします。

ステップ 2 オプションで、侵入イベント ドリルダウン ページの制約, （1982 ページ）または侵入イベント テーブル ビューの制約, （1982 ページ）の説明に従って、イベント ビューに表示される侵入イベントの数を制限します。

ステップ 3 次の選択肢があります。

- 表示されるカラムの詳細については、侵入イベント フィールド, （1961 ページ）を参照してください。
- ホストのプロファイルを表示するには、ホスト IP アドレスの横に表示されるホスト プロファイル アイコン（  ）をクリックします。
- 地理位置情報の詳細を表示するには、[送信元の国（Source Country）] または [宛先の国（Destination Country）] カラムに表示されるフラグ アイコンをクリックします。
- 表示されたイベントの時刻と日付の範囲を変更するには、時間枠の変更, （1859 ページ）を参照してください。

  ヒント 侵入イベントがイベント ビューに表示されない場合、指定した時間範囲を調整すると、結果が返される場合があります。古い時間範囲を指定した場合、その時間範囲内のイベントが削除されることがあります。ルールのしきい値の設定を調整すると、イベントが生成される場合があります。

（注） イベント ビューを時間によって制約している場合は、（グローバルかイベント固有かに関係なく）アプライアンスに設定されている時間枠の外で生成されたイベントがイベント ビューに表示されます。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

- 現在のワークフロー ページのイベントをソートする、または現在のワークフロー ページ内で移動するには、ワークフローの使用，（1834 ページ）を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- 後でインシデントにイベントを転送できるように、クリップボードにイベントを追加するには、[コピー（Copy）] または [すべてコピー（Copy All）] をクリックします。
- イベント データベースからイベントを削除するには、削除するイベントの横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。
- イベントに確認済みのマークを付けて、侵入イベントのページからそれらを削除し、イベント データベースからは削除しないようにするには、侵入イベントを確認済みとしてマーク，（1974 ページ）を参照してください。
- 選択したイベントをトリガーしたパケットのローカル コピー（libpcap 形式のパケット キャプチャ ファイル）をダウンロードするには、ダウンロードするパケットによってトリガーされたイベントの横にあるチェックボックスをオンにして、[パケットのダウンロード（Download Packets）] または [すべてのパケットのダウンロード（Download All Packets）] をクリックします。キャプチャされたパケットは libpcap 形式で保存されます。この形式は、複数の一般的なプロトコル アナライザで使用されます。
- 他のイベント ビューに移動して関連イベントを表示するには、ワークフロー間のナビゲーション，（1866 ページ）を参照してください。
- 別のワークフローを一時的に使用するには、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。
- [サマリー ダッシュボード（Summary Dashboard）] の [侵入イベント（Intrusion Events）] セクションを表示するには、[ダッシュボード（Dashboards）] をクリックします。
- ブックマークの管理ページに移動するには、[ブックマークの表示（View Bookmarks）] をクリックします。
- 現在のビューのデータに基づいてレポートを生成するには、イベント ビューからのレポート テンプレートの作成，（1716 ページ）を参照してください。

関連トピック

イベントの検索，（1871 ページ）

ブックマーク，（1867 ページ）

侵入イベント ドリルダウン ページの制約

次の表では、ドリルダウン ページの使用方法について説明します。

表 *271*：ドリルダウン ページでのイベントの制約

目的	操作
次のワークフロー ページのドリルダウンを特定の値に制約する	値をクリックします。 たとえば、[宛先ポート（Destination Port）] ワークフローで、イベントを宛先ポートが 80 であるものに制約するには、[DST ポート/ICMP コード（DST Port/ICMP Code）] 列で [80/tcp（80/tcp）] をクリックします。ワークフローの次のページ [イベント（Events）] が表示され、ポート 80/tcp のイベントだけが含まれます。
次のワークフロー ページのドリルダウンを選択したイベントに制約する	次のワークフロー ページで表示するイベントの横にあるチェックボックスを選択し、[表示（View）] をクリックします。 たとえば、[宛先ポート（Destination Port）] ワークフローで、イベントを宛先がポート 20/tcp および 21/tcp であるものに制約するには、それらのポートの行の横にあるチェックボックスを選択し、[表示（View）] をクリックします。ワークフローの次のページ [イベント（Events）] が表示され、ポート 20/tcp および 21/tcp のイベントだけが含まれます。 複数の行を制約し、テーブルに複数の列が存在する場合（[数（Count）] 列を含まない）は、複合制約と呼ばれるものが作成されることに注意してください。複合制約により、必要以上のイベントを制約に含めないようにすることができます。たとえば、[イベント（Event）] と [宛先（Destination）] のワークフローを使用する場合は、最初のドリルダウン ページで選択した各行により、複合制約が作成されます。宛先 IP アドレス 10.10.10.100 のイベント 1:100 を選択し、宛先 IP アドレス 192.168.10.100 のイベント 1:200 も選択した場合、複合制約により、イベント タイプとして 1:100 を含むイベントや宛先 IP アドレスとして 192.168.10.100 を含むイベント、またはイベント タイプとして 1:200 を含むイベントや宛先 IP アドレスとして 10.10.10.100 を含むイベントが選択されないようになります。
現在の制約を保持しながら、次のワークフロー ページをドリルダウンする	[すべて表示（View All）] をクリックします。

侵入イベント テーブル ビューの制約

次の表では、テーブル ビューの使用方法について説明します。

表 *272*：イベントのテーブル ビューでのイベントの制約

目的	操作
1つの属性を持つイベントにビューを制約する	属性をクリックします。 たとえば、宛先がポート 80 であるイベントにビューを制約するには、[DST ポート/ICMP コード（DST Port/ICMP Code）] 列で [80/tcp（80/tcp）] をクリックします。
テーブルから列を削除する	非表示にする列見出しのクローズ アイコン（  ）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェックボックスをオンまたはオフにします。無効になった列をビューに再追加するには、展開矢印（  ）をクリックして検索制約を拡張し、[無効の列（Disabled Columns）] の下の列名をクリックします。
1つ以上のイベントに関連付けられたパケットを表示する	次のいずれかを行います。 • パケットを表示するイベントの横にある下矢印アイコン（  ）をクリックします。 • パケットを表示する1つ以上のイベントを選択し、ページの下部にある [表示（View）] をクリックします。 • ページの下部で、[すべて表示（View All）] をクリックして、現在の制約に一致するすべてのイベントのパケットを表示します。

侵入イベント パケット ビューの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

パケット ビューは、侵入イベントを生成したルールをトリガーとして使用したパケットに関する情報を表示します。

ヒント イベントを検出するデバイスで [パケットの転送（Transfer Packet）] オプションが無効になっている場合、Firepower Management Center でのパケット ビューにはパケット情報は含まれません。

パケット ビューは、パケットがトリガーとして使用した侵入イベントに関する情報を提供することによって、イベントのタイム スタンプ、メッセージ、分類、優先度、イベントを生成したルー

ル（イベントが標準テキスト ルールによって生成された場合）など、特定のパケットがキャプチャされた理由を示します。パケット ビューは、パケットのサイズなど、パケットに関する一般情報も表示します。

さらに、パケット ビューにはパケット内の各層（データ リンク、ネットワーク、およびトランスポート）について説明したセクションと、パケットを構成するバイトについて説明したセクションがあります。システムがパケットを復号化した場合は、復号化されたバイトを表示できます。折りたたまれたセクションを展開すると、詳細情報を参照できます。

（注） それぞれのポートスキャン イベントは複数のパケットによってトリガーとして使用されるため、ポートスキャン イベントは特別なバージョンのパケット ビューを使用します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 侵入イベント テーブル ビューの制約, （1982 ページ）の説明に従って、侵入イベントのテーブル ビューで、表示するパケットを選択します。

ステップ 2 複数のイベントを選択した場合は、オプションで、ページの下部にあるページ番号を使用することによって、パケット ビューでパケットのページを切り替えることができます。

ステップ 3 次のオプションもあります。

- 調整：パケット ビューで日時範囲を変更するには、時間枠の変更, （1859 ページ）を参照してください。
- クリップボード：後でイベントをインシデントに転送するためクリップボードにそのイベントを追加するには、[コピー（Copy）] をクリックして表示しているパケットのイベントをコピーするか、[すべてコピー（Copy All）] をクリックして以前に選択したパケットのすべてのイベントをコピーします。
- 設定：イベントをトリガした侵入ルールを設定するには、[アクション（Actions）] の横にある矢印をクリックし、パケット ビュー内での侵入ルールの設定, （1989 ページ）の説明に従って操作を続けます。
- 削除：データベースからイベントを削除するには、[削除（Delete）] をクリックして表示しているパケットのイベントを削除するか、[すべて削除（Delete All）] をクリックして以前に選択したパケットのすべてのイベントを削除します。
- ダウンロード：イベントをトリガーしたパケットのローカル コピー（libpcap 形式のパケット キャプチャ ファイル）をダウンロードするには、[パケットのダウンロード（Download Packet）] をクリックして表示しているイベントに関するキャプチャしたパケットのコピーを保存するか、[すべてのパケットをダウンロード（Download All Packets）] をクリックして以前に選択したパケットのすべてのイベントのキャプチャしたパケットのコピーを保存します。キャプチャされたパケットは libpcap 形式で保存されます。この形式は、複数の一般的なプロトコル アナライザで使用されます。

（注） 単一のポートスキャン イベントは複数のパケットに基づいているため、ポートスキャン パケットをダウンロードできません。ただし、ポートスキャン ビューは使用可能なすべてのパケット情報を提供します。ダウンロードするには少なくとも 15 % の使用可能なディスク領域が必要です。

- 確認済みのマークを付ける：イベント データベースからは削除せずに、イベント ビューから削除するため確認済みのイベントにマークを付けるには、[確認（Review）] をクリックして表示しているパケットのイベントにマークを付けるか、[すべて確認（Review All）] をクリックして以前に選択したパケットのすべてのイベントにマーク付けます。 詳細については、侵入イベントを確認済みとしてマーク, （1974 ページ）を参照してください。
- 追加情報の表示：ページセクションを展開したり、折りたたんだりするには、セクションの横にある矢印をクリックします。詳細については、イベント情報のフィールド, （1985 ページ）、フレーム情報のフィールド, （1993 ページ）、データリンク層情報フィールド, （1994 ページ）を参照してください。
- ネットワーク層の情報の表示：ネットワーク層情報の表示, （1995 ページ）を参照してください。
- パケット バイト情報の表示：パケット バイト情報の表示, （2001 ページ）を参照してください。
- トランスポート層の情報の表示：次を参照してください。 トランスポート層情報の表示, （1998 ページ）

関連トピック

ポートスキャン検出, （1407 ページ）
侵入イベントのクリップボード, （2001 ページ）

イベント情報のフィールド

パケット ビューで、[イベント情報（Event Information）] セクションのパケットに関する情報を表示できます。

イベント

イベントのメッセージ。ルールベースのイベントの場合、これはルール メッセージに対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

イベントの ID は、(GID:SID:Rev) の形式でメッセージに付加されます。GID は、ルール エンジン、デコーダ、またはイベントを生成したプリプロセッサのジェネレータ ID です。SID は、ルール、デコーダ メッセージ、またはプリプロセッサ メッセージの ID です。Rev はルールのリビジョン番号です。

Timestamp

パケットがキャプチャされた時間。

分類（Classification）

イベントの分類。ルールベースのイベントの場合、これはルールの分類に対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

[プライオリティ（Priority）]

イベントの優先度。ルールベースのイベントの場合、これは `priority` キーワードの値または `classtype` キーワードの値に対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

入力セキュリティ ゾーン（Ingress Security Zone）

イベントをトリガーしたパケットの入力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。

出力セキュリティ ゾーン（Egress Security Zone）

イベントをトリガーとして使用したパケットの出力セキュリティ ゾーン。パッシブ展開では、このフィールドには入力されません。

ドメイン

管理対象デバイスが属するドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

Device

アクセス コントロール ポリシーが展開された管理対象デバイス。

スタック構成設定では、プライマリ デバイスとセカンダリ デバイスは、別々のデバイスであるかのように侵入イベントをレポートすることに注意してください。

セキュリティ コンテキスト（Security Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。マルチ コンテキスト モードの ASA FirePOWER の場合に、システムがこのフィールドにデータを設定することに注意してください。

入力インターフェイス（Ingress Interface）

イベントをトリガーしたパケットの入力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列だけに入力されます。

出力インターフェイス（Egress Interface）

インライン セットの場合、イベントをトリガーとして使用したパケットの出力インターフェイス。

送信元/宛先 IP（Source/Destination IP）

イベントをトリガーとして使用したパケットの発生元（送信元）であるホストIPアドレスまたはドメイン名、またはイベントをトリガーとして使用したトラフィックのターゲット（宛先）ホスト。

送信元ポート/ICMP タイプ（Source Port/ICMP Type）

イベントをトリガーしたパケットの送信元ポート。ICMPトラフィックの場合は、ポート番号がないため、システムはICMP タイプを表示します。

宛先ポート/ICMP コード（Destination Port/ICMP Code）

トラフィックを受信するホストのポート番号。ICMPトラフィックの場合は、ポート番号がないため、システムはICMP コードを表示します。

電子メールのヘッダー（Email Headers）

電子メールヘッダーから取得したデータ。電子メールヘッダーは侵入イベントのテーブル ビューには表示されませんが、電子メールヘッダーデータは検索条件として使用できることに注意してください。

電子メールのヘッダーを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [ヘッダーのログ（Log Headers）] オプションを有効にする必要があります。ルールベースのイベントの場合、この行は電子メール データが取得されたときに表示されます。

HTTP ホスト名（HTTP Hostname）

（存在する場合）HTTP 要求のホスト ヘッダーから取得されたホスト名。この行には、最大 256 バイトの完全なホスト名が表示されます。ホスト名が 1 行より長い場合は、完全なホスト名を展開できます。

ホスト名を表示するには、HTTP検査プリプロセッサ [ホスト名のログ（Log Hostname）] オプションを有効にする必要があります。

HTTP 要求パケットにホスト名が常に含まれているわけではないことに注意してください。ルールベースのイベントの場合、この行はパケットに HTTP ホスト名または HTTP URI が含まれる場合に表示されます。

HTTP URI

（存在する場合）侵入イベントをトリガーした HTTP 要求パケットに関連付けられた raw URI。この行には、最大2048バイトの完全なURIが表示されます。URIが1行より長い場合は、完全なURI を展開できます。

URIを表示するには、HTTP 検査プリプロセッサ [URIのログ（Log URI）] オプションを有効にする必要があります。

HTTP要求パケットにURIが常に含まれているわけではないことに注意してください。ルールベースのイベントの場合、この行はパケットに HTTP ホスト名または HTTP URI が含まれる場合に表示されます。

HTTP 応答によってトリガーとして使用された侵入イベントの関連 HTTP URI を参照するには、[両方のポートでのストリーム再構成の実行（Perform Stream Reassembly on Both Ports）] オプションに HTTP サーバのポートを設定する必要があります。ただし、これにより、トラフィックのリアセンブル用のリソース要求が増加することに注意してください。

侵入ポリシー（Intrusion Policy）

（存在する場合）侵入イベントを生成した侵入、プリプロセッサ、デコーダのルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。

アクセス コントロール ポリシー（Access Control Policy）

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効にされた侵入ポリシーが含まれるアクセス コントロール ポリシー。

アクセス コントロール ルール（Access Control Rule）

イベントを生成した侵入ルールと関連付けられたアクセス コントロール ルール。[デフォルト アクション（Default Action）] は、ルールが有効にされた侵入ポリシーがアクセス コントロール ルールに関連付けられていないことと、代わりにアクセス コントロール ポリシーのデフォルト アクションとして設定されていることを示します。

ルール（Rule）

標準テキスト ルール イベントの場合、イベントを生成したルール。

イベントが、共有オブジェクト ルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

ルール データにはネットワークに関する機密情報が含まれるため、管理者はユーザがローカル ルールの表示権限を使用してパケット ビューでルール情報を表示できる機能を、ユーザ ロール エディタで切り替えることができます。

アクション（Actions）

標準テキスト ルール イベントの場合は、[アクション（Actions）] を展開して、イベントをトリガーとして使用したルールに対して次の操作のいずれかを実行します。

- ルールを編集する
- ルールのリビジョンのドキュメンテーションを表示する
- ルールにコメントを追加する
- ルールの状態を変更する
- ルールのしきい値を設定する

- ルールを抑制する

イベントが、共有オブジェクト ルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

パケット ビュー内での侵入ルールの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

侵入イベントのパケット ビュー内で、イベントをトリガーとして使用したルールに対して複数のアクションを実行できます。イベントが、共有オブジェクト ルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

手順

ステップ 1 侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報（Event Information）] セクションの [アクション（Actions）] を展開します。

ステップ 2 次の選択肢があります。

- コメント：標準テキスト ルール イベントの場合、[ルール コメント（Rule Comment）] をクリックして、イベントを生成したルールにテキスト コメントを追加します。これにより、ルールや、特定されたエクスプロイトまたはポリシー違反に関するコンテキストおよび情報を提供できます。さらに、侵入ルール エディタでルールのコメントの追加および表示を行うこともできます。
- 無効化：[このルールを無効にする...（Disable this rule...）] をクリックして、ルールを無効にします。
  このイベントが標準テキスト ルールによって生成された場合は、必要に応じてルールを無効にできます。ローカルで編集できるすべてのポリシーにルールを設定できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

  現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、システムが提供するデフォルト ポリシーは編集できません。

  （注） パケット ビューから共有オブジェクト ルールを無効にしたり、デフォルトのポリシーでルールを無効にしたりすることは**できません**。
- パケットのドロップ：[このルールを設定してトリガー パケットをドロップ...（Set this rule to drop the triggering packet...）] をクリックして、トリガーするパケットをドロップするルールを設定します。

管理対象デバイスがネットワーク上でインライン展開されている場合、イベントをトリガーとして使用したルールを設定して、ローカルで編集できるすべてのポリシーでルールをトリガーするパケットをドロップできます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、システムが提供するデフォルト ポリシーは編集できません。このオプションは [インラインの場合ドロップ（Drop when Inline）] が現在のポリシーで有効になっている場合のみ表示されることに注意してください。

- 編集：標準テキスト ルール イベントの場合、[編集（Edit）] をクリックして、イベントを生成したルールを編集します。イベントが、共有オブジェクト ルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できません。

  （注） システムによって提供された（カスタム標準テキスト ルールではない）ルールを編集する場合、実際には新規のローカル ルールを作成していることになります。ローカル ルールを設定して、イベントを生成し、現在の侵入ポリシーで元のルールを無効にしていることを確認してください。ただし、デフォルトのポリシーのローカル ルールは有効に**できない**ことに注意してください。

- イベントの生成：[このルールを設定してイベントを生成...（Set this rule to generate events...）] をクリックして、イベントを生成するルールを設定します。
このイベントが標準テキスト ルールによって生成された場合は、ルールを設定して、ローカルで編集できるすべてのポリシーでイベントを生成できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

  現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、システムが提供するデフォルト ポリシーは編集できません。

  （注） 共有オブジェクト ルールでパケット ビューからイベントを生成したり、デフォルト ポリシーでルールを無効にしたりすることは**できません**。

- 抑制オプションの設定：パケット ビュー内での抑制オプションの設定, （1992 ページ）の説明に従って、[抑制オプションの設定（Set Suppression Options）] を展開し、続行します。
このオプションを使用して、ローカルで編集できるすべてのポリシーで、このイベントをトリガーとして使用したルールを抑制できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみでルールを制約することもできます。

  現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、シスコが提供するデフォルト ポリシーは編集できません。

- しきい値オプションの設定：パケット ビュー内でのしきい値オプションの設定, （1991 ページ）の説明に従って、[しきい値オプションの設定（Set Thresholding Options）] を展開し、続行します。

このオプションを使用して、ローカルで編集できるすべてのポリシーでも、これをトリガーとして使用したルールのしきい値を作成できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）でのみしきい値を作成することもできます。

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーは編集できますが、システムが提供するデフォルトの侵入ポリシーは編集できません。

- ドキュメントの表示：標準テキスト ルール イベントの場合、[ドキュメントの表示（View Documentation）] をクリックして、イベントを生成したルール リビジョンの説明を確認します。

パケット ビュー内でのしきい値オプションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

侵入イベントのパケット ビューでしきい値オプションを設定することによって、ルールごとに時間の経過とともに生成されるイベントの数を制御できます。ローカルで編集できるすべてのポリシーに、またはローカルで編集できる場合は現在のポリシー（つまり、イベントを生成したポリシー）のみに、しきい値オプションを設定できます。

手順

ステップ 1 侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報（Event Information）] セクションの [アクション（Actions）] を展開します。

ステップ 2 [しきい値オプションの設定（Set Thresholding Options）] を展開し、次の 2 つの有効なオプションから 1 つを選択します。

- 現在のポリシー（in the current policy）
- ローカルで作成されたすべてのポリシー（in all locally created policies）

（注） 現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されます。たとえば、カスタム ポリシーは編集できますが、システムが提供するデフォルト ポリシーは編集できません。

ステップ 3 設定するしきい値のタイプを選択します。

- 通知を期間ごとに指定したイベント インスタンスの数に制限する場合は、[制限（limit）] をクリックします。

- 期間ごとに指定したイベント インスタンス数に達するたびに通知を行う場合は、[しきい値（threshold）] をクリックします。
- 指定されたイベント インスタンス数に達した後で、期間あたり 1 回ずつ通知を行う場合は、[両方（Both）] をクリックします。

ステップ 4 該当するオプション ボタンをクリックして、イベント インスタンスを [送信元（Source）] IP アドレスと [宛先（Destination）] IP アドレスのどちらで追跡するかを指定します。

ステップ 5 [カウント（Count）] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

ステップ 6 [秒（Seconds）] フィールドに、イベント インスタンスを追跡する期間を指定する数（1 ～ 86400）を入力します。

ステップ 7 既存の侵入ポリシーでこのルールの現在のしきい値をオーバーライドする場合は、[このルールの既存の設定をオーバーライドする（Override any existing settings for this rule）] チェックボックスをオンにします。

ステップ 8 [しきい値の保存（Save Thresholding）] をクリックします。

パケット ビュー内での抑制オプションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

抑制オプションを使用して、侵入イベントをまとめて、または送信元 IP アドレスまたは宛先 IP アドレスに基づいて抑制できます。ローカルで編集できるすべてのポリシーで抑制オプションを設定できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみに抑制オプションを設定することもできます。

手順

ステップ 1 侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報（Event Information）] セクションの [アクション（Actions）] を展開します。

ステップ 2 [抑制オプションの設定（Set Suppression Options）] を展開し、次の 2 つの有効なオプションから 1 つを選択します。

- 現在のポリシー（in the current policy）
- ローカルで作成されたすべてのポリシー（in all locally created policies）

（注） 現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されます。たとえば、カスタム ポリシーを編集できますが、シスコが提供するデフォルト ポリシーは編集できません。

ステップ 3 次のいずれかの [追跡対象（Track By）] オプションを選択します。

- 指定した送信元IPアドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元（Source）] をクリックします。
- 指定した宛先IPアドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先（Destination）] をクリックします。
- このイベントをトリガーしたルールのイベントを完全に抑制する場合は、[ルール（Rule）] をクリックします。

ステップ 4 [IP アドレス（IP address）] または [CIDR ブロック（CIDR block）] フィールドに、送信元または宛先IPアドレスとして指定するIPアドレスまたはCIDRブロック/プレフィクス長を入力します。

ステップ 5 [抑制の保存（Save Suppression）] をクリックします。

関連トピック

Firepower システムの IP アドレス表記法, （16 ページ）

フレーム情報のフィールド

パケット ビューで、[フレーム（Frame）] の横にある矢印をクリックして、キャプチャされたフレームに関する情報を表示します。パケット ビューには単一フレームまたは複数フレームを表示できます。各フレームには、個々のネットワーク パケットに関する情報が表示されます。たとえば、タグ付きパケットまたは再構成された TCP ストリーム内のパケットの場合、複数のフレームが表示されます。

フレーム n（Frame n）

キャプチャされたフレーム。*n* は単一フレーム パケットの場合は 1、複数フレーム パケットの場合は差分フレーム番号です。フレーム内のキャプチャされたバイト数はフレーム番号に追加されます。

到着時間（Arrival Time）

フレームがキャプチャされた日時。

キャプチャ済みのフレームの時間デルタ（Time delta from previous captured frame）

複数フレーム パケットの場合、前のフレームがキャプチャされてからの経過時間。

表示済みのフレームの時間デルタ（Time delta from previous displayed frame）

複数フレーム パケットの場合、前のフレームが表示されてからの経過時間。

参照以降または先頭フレームからの時間（Time since reference or first frame）

複数フレーム パケットの場合、最初のフレームがキャプチャされてからの経過時間。

フレーム番号（Frame Number）

増分フレーム番号。

フレーム長（Frame Length）

フレームの長さ（バイト単位）。

キャプチャ長（Capture Length）

キャプチャされたフレームの長さ（バイト単位）。

フレームのマーク付け（Frame is marked）

フレームがマークされているかどうか（true または false）。

フレームのプロトコル（Protocols in frame）

フレームに含まれるプロトコル。

関連トピック

tag キーワード, （1224 ページ）
TCP ストリームの再構成, （1391 ページ）

データリンク層情報フィールド

パケット ビューで、データリンク層プロトコル（たとえば、[イーサネット II（Ethernet II）]）の横にある矢印をクリックして、パケットに関するデータリンク層情報を表示します。これには、送信元ホストおよび宛先ホストの 48 ビットの Media Access Control（MAC）アドレスが含まれます。ハードウェア プロトコルに応じて、パケットに関する他の情報も表示されることがあります。

（注） この例では、イーサネット リンク層情報について説明していることに注意してください。他のプロトコルも表示されることがあります。

パケット ビューはデータリンク層で使用されるプロトコルを反映します。次のリストでは、パケット ビューでイーサネット II または IEEE 802.3 イーサネット パケットについて参照できる情報について説明します。

[接続先（Destination）]

宛先ホストの MAC アドレス。

（注） イーサネットは、宛先アドレスとしてマルチキャストおよびブロードキャスト アドレスを使用することもできます。

ソース（Source）

送信元ホストの MAC アドレス。

タイプ（Type）

イーサネット II パケットの場合、イーサネット フレームでカプセル化されるパケットの種類。たとえば、IPv6 または ARP データグラム。この項目はイーサネット II パケットの場合にのみ表示されることに注意してください。

長さ（Length）

IEEE 802.3 イーサネット パケットの場合、チェックサムを含まないパケットのトータル長（バイト単位）。この項目は IEEE 802.3 イーサネット パケットの場合にのみ表示されることに注意してください。

ネットワーク層情報の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

手順

パケット ビューで、パケットにネットワーク層プロトコル（たとえば、[インターネット プロトコル（Internet Protocol）]）の横にある矢印をクリックして、パケットに関連したネットワーク層の情報の詳細情報を表示します。

（注） この例では、IP パケットについて説明していることに注意してください。他のプロトコルも表示されることがあります。

IPv4 ネットワーク層の情報フィールド

以下のリストは、IPv4 パケットで表示される可能性があるプロトコル固有の情報の説明です。

バージョン（Version）

インターネット プロトコルのバージョン番号。

ヘッダー長（Header Length）

すべての IP オプションを含む、ヘッダーのバイト数。オプションのない IP ヘッダーの長さは 20 バイトです。

差別化サービス（Differentiated Services）フィールド

送信元ホストが明示的輻輳通知（ECN）サポートする方法を示す次の差別化サービスの値。

- `0x0`：ECN-Capable Transport（ECT）をサポートしません
- `0x1` および `0x2`：ECT をサポートします
- `0x3`：Congestion Experienced（CE）

トータル長（Total Length）

IP ヘッダーを差し引いた IP パケットの長さ（バイト単位）。

ID

送信元ホストから送信されるIPデータグラムを一意に識別する値。この値は同じデータグラムフラグメントをトレースするために使用されます。

フラグ（Flags）

IP フラグメンテーションを制御する値。

[最終フラグメント（Last Fragment）] フラグの値は、データグラムに関連付けられた追加のフラグメントが存在するかどうかを次のように示します。

- `0`：データグラムに関連付けられた追加のフラグメントは存在しない
- `1`：データグラムに関連付けられた追加のフラグメントが存在する

[フラグメント化しない（Don't Fragment）] フラグの値は、データグラムをフラグメント化できるかどうかを次のように制御します。

- `0`：データグラムをフラグメント化できる
- `1`：データグラムをフラグメント化**してはならない**

フラグメント オフセット（Fragment Offset）

データグラムの先頭からのフラグメント オフセットの値。

存続時間（ttl）（Time to Live (ttl)）

データグラムが期限切れになる前にデータグラムがルータ間で作成できるホップの残数。

プロトコル

IPデータグラムにカプセル化されるトランスポートプロトコル。たとえば、ICMP、IGMP、TCP、または UDP。

ヘッダー チェックサム（Header Checksum）

IP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損したか、侵入回避の試行において使用中である可能性があります。

送信元/宛先（Source/Destination）

送信元（または宛先）ホストの IP アドレスまたはドメイン名。

ドメイン名を表示するには、IP アドレス解決を有効にする必要があることに注意してください。

アドレスまたはドメイン名をクリックしてコンテキスト メニューを表示してから、whois 検索を実行する場合は [Whois] を、ホスト情報を表示する場合は [ホストプロファイルの表示（View Host Profile）] を、アドレスをグローバル ブラックリストまたはホワイトリストに追加する場合は [今すぐブラックリスト化する（Blacklist Now）] または [今すぐホワイトリスト化する（Whitelist Now）] を選択します。

IPv6 ネットワーク層の情報フィールド

以下のリストは、IPv6 パケットで表示される可能性があるプロトコル固有の情報の説明です。

トラフィック クラス（Traffic Class）

IPv4 で提供される差別化サービス機能と同じように、IPv6 パケット クラスまたは優先度を特定する IPv6 見出し内の Experimental 8 ビットのフィールド。未使用の場合、このフィールドはゼロに設定されます。

フロー ラベル（Flow Label）

非デフォルトの QoS またはリアルタイム サービスなどの特別なフローを特定する、1 から FFFF までの、オプションの 20 ビットの IPv6 16 進数値。未使用の場合、このフィールドはゼロに設定されます。

ペイロード長（Payload Length）

IPv6 ペイロードのオクテットの数を特定する 16 ビット フィールド。これは、任意の拡張子見出しを含む、IPv6 見出しに続くすべてのパケットで構成されます。

次ヘッダー（Next Header）

IPv4 プロトコル フィールドと同じ値を使用して、IPv6 見出しのすぐ後に続く、見出しの種類を特定する 8 ビットのフィールド。

ホップ リミット（Hop Limit）

パケットを転送するノードごとに 1 つずつデクリメントする 8 ビットの 10 進整数。デクリメントした値がゼロになると、パケットは破棄されます。

ソース（Source）

送信元ホストの 128 ビットの IPv6 アドレス。

[接続先（Destination）]

宛先ホストの 128 ビットの IPv6 アドレス。

トランスポート層情報の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

手順

ステップ 1 パケット ビューで、トランスポート層プロトコル（たとえば [TCP]、[UDP]、または [ICMP]）の横にある矢印をクリックします。

ステップ 2 オプションで、存在する場合、[データ（Data）] をクリックして、パケット ビューの [パケット情報（Packet Information）] セクションで、プロトコルのすぐ上にあるペイロードの最初の 24 バイトを表示します。

ステップ 3 TCP パケット ビューのフィールド, （1998 ページ）、UDP パケット ビューのフィールド, （1999 ページ）、またはICMP パケット ビュー フィールド, （2000 ページ）の説明に従って、TCP、UDP、ICMP プロトコルのトランスポート層の内容を表示します。

（注） これらの例では、TCP、UDP、ICMP パケットについて説明していますが、他のプロトコルも表示されることがあることに注意してください。

TCP パケット ビューのフィールド

ここでは、TCP パケットのプロトコル固有の情報について説明します。

ソース ポート

発信元のアプリケーション プロトコルを識別する番号。

接続先ポート（**Destination port**）

受信側のアプリケーション プロトコルを識別する番号。

シーケンス番号（**Sequence number**）

TCP ストリームの初期シーケンス番号と連動する、現在の TCP セグメントの最初のバイトの値。

次のシーケンス番号（**Next sequence number**）

応答パケットにおける、送信する次のパケットのシーケンス番号。

確認応答番号（**Acknowledgement number**）

以前に受信されたデータのシーケンス番号に連動した TCP 確認応答。

ヘッダー長（Header Length）

ヘッダーのバイト数。

フラグ（Flags）

TCP セグメントの伝送状態を示す 6 ビット。

- `U`：緊急ポインタが有効
- `A`：確認応答番号が有効
- `P`：受信者はデータをプッシュする必要がある
- `R`：接続をリセットする
- `S`：シーケンス番号を同期して新しい接続を開始する
- `F`：送信者はデータ送信を終了した

ウィンドウ サイズ（Window size）

受信ホストが受け入れる、確認応答されていないデータの量（バイト単位）。

チェックサム（Checksum）

TCP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損したか、回避の試行において使用中である可能性があります。

緊急ポインタ（Urgent Pointer）

緊急データが終了する TCP セグメントの位置（存在する場合）。`U` フラグとともに使用します。

オプション（Options）

TCP オプションの値（存在する場合）。

UDP パケット ビューのフィールド

ここでは、UDP パケットのプロトコル固有の情報について説明します。

ソース ポート

発信元のアプリケーション プロトコルを識別する番号。

接続先ポート（Destination port）

受信側のアプリケーション プロトコルを識別する番号。

長さ（Length）

UDP ヘッダーとデータを組み合わせた長さ。

チェックサム（Checksum）

UDP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損した可能性があります。

ICMP パケット ビュー フィールド

ここでは、ICMP パケットのプロトコル固有の情報について説明します。

タイプ（Type）

ICMP メッセージのタイプ。

- 0：エコー応答
- 3：宛先到達不能
- 4：ソース クエンチ（始点抑制要求）
- 5：リダイレクト
- 8：エコー要求
- 9：ルータ アドバタイズメント
- 10：ルータ送信要求
- 11：時間超過
- 12：パラメータの問題
- 13：タイムスタンプ要求
- 14：タイムスタンプ応答
- 15：情報要求（廃止）
- 16：情報応答（廃止）
- 17：アドレス マスク要求
- 18：アドレス マスク応答

コード（Code）

ICMP メッセージ タイプに付随するコード。ICMP メッセージ タイプ 3、5、11、および 12 には、RFC 792 で説明されている対応コードがあります。

チェックサム（Checksum）

ICMPチェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損した可能性があります。

パケット バイト情報の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

手順

パケット ビューで、[パケット バイト（Packet Bytes）] の横にある矢印をクリックして、パケットを構成するバイトの 16 進数および ASCII バージョンを表示します。システムがトラフィックを復号化した場合は、復号化されたパケット バイトを表示できます。

侵入イベントのクリップボード

クリップボードは、任意の侵入イベント ビューから侵入イベントをコピーできる保存エリアです。

クリップボードの内容は、イベントが生成された日時別にソートされます。クリップボードに侵入イベントを追加した後、クリップボードからそれらを削除することも、クリップボードの内容のレポートを生成することもできます。

クリップボードの侵入イベントをインシデントに追加することもできます。インシデントとは、セキュリティ ポリシーの違反の可能性に関係していると思われるイベントのコンパイルです。

関連トピック

侵入イベント ワークフローの使用, （1980 ページ）
侵入イベント パケット ビューの使用, （1983 ページ）
インシデントの作成, （1816 ページ）

クリップボードのレポートの生成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

任意のイベント ビューで行うのと同じように、クリップボードのイベントに関するレポートを生成できます。

はじめる前に

- クリップボードに1つ以上のイベントを追加します。詳細については、侵入イベント ワークフローの使用，（1980ページ）または侵入イベント パケット ビューの使用，（1983ページ）を参照してください。

手順

ステップ1 [分析（Analysis）] > [侵入（Intrusions）] > [クリップボード（Clipboard）]を選択します。

ステップ2 次の選択肢があります。

- クリップボード上のページの特定のイベントを含めるには、そのページに移動し、イベントの横にあるチェックボックスをオンにして、[レポートの生成（Generate Report）] をクリックします。
- クリップボードのすべてのイベントを含めるには、[すべてのレポートの生成（Generate Report All）] をクリックします。

ステップ3 レポートの表示方法を指定して、[生成（Generate）] をクリックします。

ステップ4 1つ以上の出力形式を選択し、オプションで、他の設定を変更します。

ステップ5 [生成（Generate）] をクリックしてから、[はい（Yes）] をクリックします。

ステップ6 次の選択肢があります。

- レポート リンクをクリックして、新しいウィンドウにレポートを表示します。
- [OK] をクリックして、レポートのデザインを変更できる [レポート テンプレート（Report Templates）] ページに戻ります。

関連トピック

レポート テンプレート，（1712 ページ）

クリップボードからのイベントの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

インシデントに追加したくない侵入イベントがクリップボード上にある場合は、そのイベントを削除できます。

（注） クリップボードからイベントを削除しても、イベント データベースからイベントは削除**されません**。ただし、イベントデータベースからイベントを削除すると、イベントはクリップボードから削除されます。

手順

ステップ 1 [分析（Analysis）] > [侵入（Intrusions）] > [クリップボード（Clipboard）]を選択します。

ステップ 2 次の選択肢があります。

- クリップボードのページの特定の侵入イベントを削除するには、そのページに移動し、イベントの横にあるチェックボックスを選択し、[削除（Delete）] をクリックします。
- クリップボードからすべての侵入イベントを削除するには、[すべて削除（Delete All）] をクリックします。[イベント設定（Event Preferences）] で [全てのアクションを確認（Confirm All Actions）] オプションを選択した場合、最初にすべてのイベントを削除するかどうか確認するプロンプトが出されることに注意してください。

侵入イベントの統計情報の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

[侵入イベントの統計情報（Intrusion Event Statistics）] ページは、アプライアンスの現在の状態の概要と、ネットワークで生成されたすべての侵入イベントを表示します。

このページに表示されるIPアドレス、ポート、プロトコル、イベントメッセージなどはそれぞれリンクになっています。関連イベントの情報を表示するには、任意のリンクをクリックします。たとえば、上位10個の宛先ポートのいずれかが `80 (http) /tcp` である場合、そのリンクをクリックすると、デフォルトの侵入イベント ワークフローの最初のページが表示され、そのポートをターゲットとするイベントがリストされます。現在の時刻範囲で表示されるのはイベント（およびイベントを生成する管理対象デバイス）のみであることに注意してください。さらに、確認済みマークを付けた侵入イベントも統計に引き続き表示されます。たとえば、現在の時刻範囲が過去1時間であり、最初のイベントが5時間前に生成された場合、[最初のイベント（First Event）] リンクをクリックすると、そのイベントは時刻範囲を変更するまでイベント ページには表示されません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [概要（Overview）] > [概要（Summary）] > [侵入イベント統計（Intrusion Event Statistics）]を選択します。

ステップ 2 ページの上部にある 2 つの選択ボックスから、統計を表示するゾーンおよびデバイスを選択するか、[すべてのセキュリティ ゾーン（All Security Zones）] および [すべてのデバイス（All Devices）] を選択して、侵入イベントを収集するすべてのデバイスの統計を表示します。

ステップ 3 [統計の取得（Get Statistics）] をクリックします。

ヒント カスタム時刻範囲からデータを表示するには、右上のページ エリアのリンクをクリックし、時間枠の変更, （1859 ページ）にある指示に従います。

ホスト統計情報

[侵入イベント統計情報（Intrusion Event Statistics）] ページの [ホスト統計情報（Host Statistics）] セクションは、アプライアンス自体に関する情報を提供します。Firepower Management Center では、このセクションはすべての管理対象デバイスに関する情報も提供します。

この情報には、次の内容が含まれます。

時刻（Time）

アプライアンスの現在の時刻。

アップタイム（Uptime）

アプライアンス自体が再起動してから経過した日数、時間、および分数。Firepower Management Center では、[アップタイム（Uptime）] に各管理対象デバイスの最終起動時刻、ログインしたユーザの数、および負荷平均も示されます。

ディスク使用率（Disk Usage）

使用中のディスクの割合。

メモリ使用率（Memory Usage）

使用中のシステム メモリの割合。

負荷平均（Load Average）

直前の 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数。

イベントの概要

[侵入イベント統計（Intrusion Event Statistics）] ページの [イベントの概要（Event Overview）] セクションは、侵入イベント データベースにある情報の概要を示します。

これらの統計には、次の情報が含まれています。

イベント

侵入イベント データベースのイベントの数。

時間範囲内のイベント（Events in Time Range）

現在選択されている時間範囲と、時間範囲内に収まるデータベースのイベントの割合。

最初のイベント（First Event）

イベント データベース内の最初のイベントのイベント メッセージ。

最後のイベント（Last Event）

イベント データベース内の最後のイベントのイベント メッセージ。

（注） Firepower Management Center で侵入イベント データを表示中に管理対象デバイスを選択した場合は、そのデバイスの [イベントの概要（Event Overview）] セクションが代わりに表示されます。

イベント統計

[侵入イベント統計（Intrusion Event Statistics）] ページの [イベント統計（Event Statistics）] セクションでは、侵入イベント データベース内の情報に関する具体的な情報が表示されます。

この情報には、次に関する詳細が含まれます。

- 上位 10 個のイベント タイプ
- 上位 10 個の送信元 IP アドレス
- 上位 10 個の宛先 IP アドレス
- 上位 10 個の宛先ポート
- イベント数が最大であるプロトコル、イングレスとイーグレスのセキュリティ ゾーン、およびデバイス

（注） マルチドメイン展開では、システムは、各リーフ ドメインに個別のネットワーク マップを作成します。その結果、リーフ ドメインには、ネットワーク内で一意である IP アドレスを含めることができますが、別のリーフ ドメイン内の IP アドレスと同じにすることができます。先祖ドメインでイベントの統計情報を表示すると、システムで、その IP アドレスの複数のインスタンスが繰り返し表示される場合があります。一見すると、エントリが重複しているように見えることがあります。ただし、各 IP アドレスのホスト プロファイル情報までドリル ダウンすると、それらが異なるリーフ ドメインに属していることがわかります。

侵入イベントのパフォーマンス グラフの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

[侵入イベントのパフォーマンス（Intrusion Event Performance）] ページでは、Firepower Management Center または管理対象デバイスの指定された期間の侵入イベントのパフォーマンス統計情報を示すグラフを生成できます。グラフを生成することにより、1秒あたりの侵入イベントの数、1秒あたりのメガビット数、1 パケットあたりの平均バイト数、Snort によって検査されていないパケットの割合、および TCP 正規化の結果としてブロックされたパケットの数を反映できます。これらのグラフは、過去 1 時間、前日、先週、または先月の操作の統計を表示できます。

（注） 新しいデータは5分ごとに統計グラフに蓄積されます。したがって、グラフをすばやくリロードしても、次の5分の差分更新が実行されるまでデータは変更されていない場合があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [概要（Overview）] > [概要（Summary）] > [侵入イベント パフォーマンス（Intrusion Event Performance）]を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、データを表示するデバイスを選択します。

ステップ 3 侵入イベントのパフォーマンス統計情報グラフの種類, （2007ページ）で説明されているように、[グラフの選択（Select Graph(s)）] リストから、作成するグラフの種類を選択します。

ステップ 4 [時間範囲の選択（Select Time Range）] リストから、グラフに使用する時間範囲を選択します。

ステップ 5 [グラフ（Graph）] をクリックします。

ステップ 6 グラフを保存するには、グラフを右クリックし、ブラウザでイメージを保存する手順に従います。

侵入イベントのパフォーマンス統計情報グラフの種類

次の表に、表示可能なグラフの種類を示します。ネットワーク分析ポリシーの [インライン モード（Inline Mode）] 設定の影響を受けるデータを含むグラフ タイプでは、表示が異なるので注意してください。[インライン モード（Inline Mode）] が無効になっている場合、Web インターフェイスでアスタリスク（*）が付いているグラフ タイプ（下記の表では列に [はい（yes）] と記載）には、[インライン モード（Inline Mode）] が有効になっている場合に変更またはドロップされるトラフィックに関するデータが含まれています。

表 *273*：侵入イベントのパフォーマンス グラフの種類

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
平均バイト/パケット	適用対象外	各パケットに含まれる平均バイト数。	No
TCP トラフィックまたはパケットで正規化された ECN フラグ	[明示的輻輳通知（Explicit Congestion Notification）] を有効にして、[パケット（Packet）] を選択します。	ネゴシエーションに関係なく、パケット単位で ECN フラグがクリアされたパケットの数。	Yes
TCP トラフィックまたはセッションで正規化された ECN フラグ	[明示的輻輳通知（Explicit Congestion Notification）] を有効にして、[ストリーム（Stream）] を選択します。	ECN の使用がネゴシエートされなかった場合にストリーム単位で ECN フラグがクリアされた回数。	Yes
イベント/秒	適用対象外	デバイスで生成された 1 秒あたりのイベント数。	No

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
ICMPv4 エコーの正規化	[ICMPv4 の正規化（Normalize ICMPv4）] を有効にします。	エコー（要求）またはエコー応答メッセージの 8 ビット コード フィールドがクリアされた ICMPv4 パケットの数。	Yes
ICMPv6 エコーの正規化	[ICMPv6 の正規化（Normalize ICMPv6）] を有効にします。	エコー（要求）またはエコー応答メッセージの 8 ビット コード フィールドがクリアされた ICMPv6 パケットの数。	Yes
IPv4 DF フラグの正規化	[IPv4 の正規化（Normalize IPv4）] と [DF ビットの正規化（Normalize Don't Fragment Bit）] を有効にします。	[IPv4 フラグ（IPv4 Flags）] ヘッダー フィールドのシングル ビット [フラグメント禁止（Don't Fragment）] サブフィールドがクリアされた IPv4 パケットの数。	Yes
IPv4 オプションの正規化	[IPv4 の正規化（Normalize IPv4）] を有効にします。	オプション オクテットが 1（No Operation）に設定された IPv4 パケットの数。	Yes
IPv4 予約済みフラグの正規化	[IPv4 の正規化（Normalize IPv4）] と [予約済みビットの正規化（Normalize Reserved Bit）] を有効にします。	[IPv4 フラグ（IPv4 Flags）] ヘッダー フィールドのシングル ビット [予約済み（Reserved）] サブフィールドがクリアされた IPv4 パケットの数。	Yes
IPv4 サイズ変更の正規化	[IPv4 の正規化（Normalize IPv4）] を有効にします。	超過ペイロードが IP ヘッダーで指定されたデータグラム長に切り詰められた IPv4 パケットの数。	Yes
IPv4 TOS の正規化	[IPv4 の正規化（Normalize IPv4）] と [TOS ビットの正規化（Normalize TOS Bit）] を有効にします。	1 バイトの [差別化サービス（DS）（Differentiated Services (DS)）] フィールド（旧 [タイプ オブ サービス（ToS）（Type of Service (TOS)）] フィールド）がクリアされた IPv4 パケットの数。	Yes
IPv4 TTL の正規化	[IPv4 の正規化（Normalize IPv4）]、[最大 TTL（Maximum TTL）]、および [TTL のリセット（Reset TTL）] を有効にします。	IPv4 存続時間（TTL）正規化の数。	Yes

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
IPv6 オプションの正規化	[IPv6 の正規化（Normalize IPv6）] を有効にします。	[ホップバイホップ オプション（Hop-by-Hop Options）] または [宛先オプション（Destination Options）] 拡張ヘッダーの [オプション タイプ（Option Type）] フィールドが、00（スキップして処理を続行）に設定された IPv6 パケットの数。	Yes
IPv6 TTL の正規化	[IPv6 の正規化（Normalize IPv6）]、[最小 TTL（Minimum TTL）]、および [TTL のリセット（Reset TTL）] を有効にします。	IPv6 ホップ リミット（TTL）正規化の数。	Yes
メガビット/秒	適用対象外	デバイスをパス スルーするトラフィックの 1 秒あたりのメガビット数。	No
MSS に合わせてサイズ変更されたパケットの正規化	[データを MSS にトリミング（Trim Data to MSS）] を有効にします。	ペイロードが TCP データフィールドよりも長かったために、ペイロードが最大セグメント サイズに切り詰められたパケットの数。	Yes
TCP ウィンドウに合わせてサイズ変更されたパケットの正規化	[データをウィンドウにトリミング（Trim Data to Window）] を有効にします。	受信側ホストの TCP ウィンドウに合わせて TCP データフィールドが切り詰められたパケットの数。	Yes
ドロップされたパケットの割合	適用対象外	選択されたすべてのデバイスにおける未検査のパケットの平均パーセンテージ。たとえば、2 つのデバイスを選択した場合、平均が 50 % であるというのは、1 つのデバイスのドロップ率が 90 % であり、もう 1 つのデバイスのドロップ率が 10 % であることを示している可能性があります。また、両方のデバイスのドロップ率が 50 % である可能性もあります。グラフは、1 つのデバイスを選択した場合にのみ合計ドロップ率を表します。	No
データ ストリップが適用された RST パケットの正規化	[RST に関するデータを削除（Remove Data on RST）] を有効にします。	TCP リセット（RST）パケットからデータが削除されたパケットの数。	Yes

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
データ ストリップが適用された SYN パケットの正規化	[SYN に関するデータを削除（Remove Data on SYN）] を有効にします。	TCP オペレーティング システムが Mac OS でない場合に、SYN パケットからデータが削除されたパケットの数。	Yes
TCP ヘッダー パディングの正規化	[オプション パディング バイトの正規化またはクリア（Normalize/Clear Option Padding Bytes）] を有効にします。	オプションのパディング バイトが 0 に設定された TCP パケットの数。	Yes
TCP オプションなしの正規化	[これらの TCP オプションを許可（Allow These TCP Options）] を有効にして、[任意（any）] 以外のオプションに設定します。	タイムスタンプ オプションがストリップされたパケットの数。	Yes
TCP NS フラグの正規化	[明示的輻輳通知（Explicit Congestion Notification）] を有効にして、[パケット（Packet）] を選択します。	ECN Nonce Sum（NS）オプション正規化の数。	Yes
TCP オプションの正規化	[これらの TCP オプションを許可（Allow These TCP Options）] を有効にして、[任意（any）] 以外のオプションに設定します。	オプション フィールドが No Operation（TCP オプション 1）に設定されているオプションの数（MSS、ウィンドウ スケール、タイムスタンプ、および明示的に許可されたオプションを除く）。	Yes
正規化によってブロックされた TCP パケット	[TCP ペイロードの正規化（Normalize TCP Payload）] を有効にします（セグメントのリアセンブリは失敗します）。	TCP セグメントを正常にリアセンブルできなかったためにドロップされたパケットの数。	Yes
TCP 予約済みフラグの正規化	[予約済みビットの正規化またはクリア（Normalize/Clear Reserved Bits）] を有効にします。	予約済みビットがクリアされた TCP パケットの数。	Yes

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
TCP セグメント リアセンブルの正規化	[TCP ペイロードの正規化（Normalize TCP Payload）] を有効にします（セグメントのリアセンブリは成功します）。	再送信データの一貫性を確保するために TCP データフィールドが正規化されたパケットの数（正しくリアセンブルできないセグメントはすべてドロップされます）。	Yes
TCP SYN オプションの正規化	[これらの TCP オプションを許可（Allow These TCP Options）] を有効にして、[任意（any）] 以外のオプションに設定します。	SYN 制御ビットが設定されていないため、最大セグメント サイズまたはウィンドウ スケール オプションが No Operation（TCP オプション 1）に設定されたオプションの数。	Yes
TCP タイムスタンプ ECR の正規化	[これらの TCP オプションを許可（Allow These TCP Options）] を有効にして、[任意（any）] 以外のオプションに設定します。	確認応答（ACK）制御ビットが設定されていないために、タイムスタンプ エコー応答（TSecr）オプション フィールドがクリアされたパケットの数。	Yes
TCP 緊急ポインタの正規化	[緊急ポインタの正規化（Normalize Urgent Pointer）] を有効にします。	TCP ヘッダーの [緊急ポインタ（Urgent Pointer）] フィールド（2 バイト）がペイロード長を超えていたため、ペイロード長に合わせて設定されたパケットの数。	Yes
ブロックされたパケットの総数	[インライン モード（Inline Mode）] または [インライン時にドロップ（Drop when Inline）] を設定します。	ルール、デコーダ、およびプリプロセッサのドロップを含む、ドロップされたパケットの総数。	No
インジェクトされたパケットの総数	[インライン モード（Inline Mode）] を設定します。	再送信前にサイズ変更されたパケットの数。	No
TCP フィルタ適用パケットの総数	TCP ストリームの前処理を設定します。	TCP ポート フィルタリングのためにストリームによってスキップされたパケットの数。	No
UDP フィルタ適用パケットの総数	UDP ストリームの前処理を設定します。	UDP ポート フィルタリングのためにストリームによってスキップされたパケットの数。	No
緊急フラグ クリア済みの正規化	[緊急ポインタが設定されていない場合 URG をクリア（Clear URG if Urgent Pointer is Not Set）] を有効にします。	緊急ポインタが設定されていなかったために、TCP ヘッダーの URG 制御ビットがクリアされたパケットの数。	Yes

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
緊急ポインタおよび緊急フラグ クリア済みの正規化	[空のペイロードに設定された緊急ポインタまたはURGをクリア（Clear Urgent Pointer/URG on Empty Payload）]を有効にします。	ペイロードがなかったために、TCPヘッダーの緊急ポインタ フィールドと URG 制御ビットがクリアされたパケットの数。	Yes
緊急ポインタ クリア済みの正規化	[URG=0 の場合に緊急ポインタをクリア（Clear Urgent Pointer if URG=0）] を有効にします。	緊急（URG）制御ビットが設定されていなかったため、TCPヘッダーの[緊急ポインタ（Urgent Pointer）] フィールド（16 ビット）がクリアされたパケットの数。	Yes

関連トピック

インライン正規化プリプロセッサ, （1371 ページ）
インライン導入でのプリプロセッサによるトラフィックの変更, （1274 ページ）
インライン展開でのドロップ動作, （1039 ページ）

侵入イベント グラフの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

Firepower System は、経時的な侵入イベントの傾向を示すグラフを表示します。1 つまたはすべての管理対象デバイスについて、過去 1 時間から先月までの範囲の経時的な侵入イベント グラフを生成できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [概要（Overview）] > [概要（Summary）] > [侵入イベント グラフ（Intrusion Event Graphs）]を選択します。

ステップ 2 [デバイスの選択（Select Device）] で、[すべて（all）] を選択してすべてのデバイスを含めるか、グラフに含める特定のデバイスを選択します。

ステップ 3 [グラフの選択（Select Graph(s)）] で、生成するグラフの種類を選択します。

- 上位 10 個の宛先ポート
- 上位 10 個の送信元 IP アドレス
- 上位 10 個のイベント メッセージ

ステップ 4 [時間範囲の選択（Select Time Range）] で、グラフの時間範囲を選択します。

- 直近の 1 時間（Last Hour）
- 前日（Last Day）
- 先週（Last Week）
- 先月（Last Month）

ステップ 5 [グラフ（Graph）] をクリックします。

第 86 章

ファイル/マルウェアイベントとネットワーク ファイル トラジェクトリ

次のトピックでは、ファイル/マルウェア イベント、ローカル マルウェア分析、動的分析、キャプチャされたファイル、およびネットワーク ファイル トラジェクトリの概要を示します。

ファイル イベント/マルウェア イベントとネットワーク ファイル トラジェクトリについて

マルウェアの影響を特定して軽減しやすくするため、Firepower システムのファイル制御、ネットワーク ファイル トラジェクトリ、および *AMP for Firepower* の各コンポーネントによって、アーカイブ ファイルの内のマルウェア ファイルとネストされたファイルを含むファイルの伝送を検出、追跡、キャプチャ、分析、ログ記録、および必要に応じてブロックできます。

また、システムを組織の *AMP for Endpoints* の展開に統合して、スキャン、マルウェア検出、および検疫のレコードと侵害の兆候（IOC）をインポートできます。

コンテキスト エクスプローラ、およびレポート機能を使用すると、検出/キャプチャ/ブロックされたファイルとマルウェアについてより詳しく理解できます。また、イベントを使用して相関ポ

リシー違反をトリガーしたり、電子メール、SMTP、またはsyslogによるアラートを発行したりすることもできます。

（注） Firepower システムでは、Unicode（UTF-8）文字を使用するファイル名の表示および入力がサポートされます。ただし、Unicode のファイル名は PDF レポートに変換された形式で表示されます。また、SMB プロトコルによって、ファイル名の印刷不能な文字がピリオドに置き換えられます。

ファイルおよびマルウェア イベント

Firepower Management Center は、さまざまなタイプのファイルおよびマルウェア イベントをログに記録できます。個々のイベントに関する情報は、イベントの生成方法と生成理由に応じて異なります。

- ファイルイベントとは、AMP for Firepowerによって検出されたマルウェアを含むファイルを意味します。ファイルイベントには、AMP for Endpoints関連のフィールドは含まれません。
- マルウェア イベントとは、AMP for Firepower または AMP for Endpoints によって検出されたマルウェアを意味します。また、マルウェア イベントは、スキャンや検疫など、AMP for Endpoints の導入からの脅威以外のデータを記録できます。
- レトロスペクティブ マルウェア イベントとは、性質（ファイルがマルウェアかどうか）が変更された、AMP for Firepower によって検出されたファイルを意味します。

（注） AMP for Firepower によってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。エンドポイントベースのマルウェア イベントには、対応するファイル イベントはありません。

ファイル イベントおよびマルウェア イベントの種類

ファイル イベント

システムは、現在展開されているファイル ポリシーのルールに従って、管理対象デバイスがネットワーク トラフィック内のファイルを検出またはブロックしたときに生成されたファイルイベントを記録します。

システムがファイル イベントを生成する際に、呼び出しを行うアクセス コントロール ルールのログ設定に関係なく、システムは Firepower Management Center データベースへの関連する接続の終わりも記録します。

ネットワーク ベースのマルウェア イベント（AMP for Firepower）

システムは、全体的なアクセス コントロール設定の一環として、ネットワーク トラフィックのマルウェアを検出できます。AMP for Firepower は、結果として生じたイベントの性質や、いつどこでどのようにしてマルウェアが検出されたかに関するコンテキストデータを含むマルウェア イベントを生成できます。

表 *274*：*AMP for Firepower* でのマルウェア イベントの生成シナリオ

AMP for Firepower によるファイル検出時の動作	性質
AMP クラウドにファイルの性質についてクエリを行い（マルウェア クラウド ルックアップを実行）、クエリに成功した場合	マルウェア、クリーン、または不明
AMP クライドにクエリを行ったものの、接続を確立できないか、他の理由でクライドが利用可能でない場合	応対不可 この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。
ファイルに関連付けられている脅威スコアが、ファイルを検出したファイル ポリシーで定義されたマルウェアしきい値の脅威スコアを超えた場合、またはローカルマルウェア分析でマルウェアが識別された場合	マルウェア
ファイルがカスタム検出リストに設定されている場合（手動でマルウェアとしてマークされている場合）	カスタム検出
ファイルがクリーン リストに設定されている場合（手動でクリーンとしてマークされている場合）	クリーン

遡及的マルウェア イベント（AMP for Firepower）

ネットワーク トラフィックで検出されたマルウェアの場合、性質が変わることがあります。たとえば、AMP クラウドによる判定の結果、以前はクリーンであると考えられていたファイルが今はマルウェアとして識別されるようになったり、その逆、つまりマルウェアと識別されたファイルが実際にはクリーンであったりする可能性があります。先週クエリしたファイルの性質が変わると、AMP クラウドがシステムに通知します。その場合、以下の 2 つが行われます。

- Firepower Management Center が新しい遡及的マルウェア イベントを生成します。

  この新しい遡及的マルウェア イベントは、前の週に検出された、同じ SHA-256 ハッシュ値を持つすべてのファイルの性質変更を表します。そのため、これらのイベントに含まれる情報は、Firepower Management Center に性質変更が通知された日時、新しい性質、ファイルの SHA-256 ハッシュ値、脅威名に限定されています。IP アドレスや他のコンテキスト情報は含まれません。

- Firepower Management Center は遡及的イベントに関連付けられた SHA-256 ハッシュ値を持つ、検出済みのファイルのファイル性質を変更します。

  ファイルの性質が [マルウェア（Malware）] に変更されると、Firepower Management Center は新しいマルウェアイベントをデータベースに記録します。新しい性質を除き、この新しいマルウェア イベントの情報は、ファイルが最初に検出されたときに生成されたファイル イベントのものと同じです。

  ファイルの性質が [クリーン（Clean）] に変更された場合、Firepower Management Center はそのマルウェアイベントを削除しません。代わりに、イベントに性質の変更が反映されます。つまり、マルウェア テーブルには性質が [クリーン（Clean）] のファイルが含められることがありますが、それはそのファイルが最初マルウェアと識別されていた場合だけです。マルウェアとして識別されたことのないファイルは、ファイルのテーブルにのみ含められます。

エンドポイントベースのマルウェア イベント（AMP for Endpoints）

組織で AMP for Endpoints を使用している場合は、個々のユーザがエンドポイントに軽量コネクタ（コンピュータおよびモバイル デバイス）を取り付けます。コネクタは、ファイルのアップロード、ダウンロード、実行、開く、コピー、移動などの操作を行う際にファイルを検査します。コネクタはAMPクラウドと通信して、検査対象のファイルにマルウェアが含まれるかどうかを判断します。

ファイルがマルウェアとして特定された場合、AMP クラウドは特定した脅威の情報を Firepower Management Centerに送ります。さらにAMPクラウドは、スキャン、検疫、実行のブロッキング、クラウド リコールなど、他の種類のデータを Firepower Management Center に送信することもできます。Firepower Management Center はこれらの情報をマルウェア イベントとしてログに記録します。

（注） エンドポイントベースのマルウェア イベントで報告される IP アドレスは、ネットワーク マップに（そして、モニタ対象ネットワークにも）含まれない場合もあります。展開、コンプライアンスのレベル、およびその他の要因によっては、AMP for Endpointsによってモニタされる組織内のエンドポイントが、AMP for Firepowerによってモニタされているものと同じホストではない可能性があります。

ファイルおよびマルウェア イベントのワークフローの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

イベント ビューアでは、テーブルにファイル イベントとマルウェア イベントを表示できます。分析に関連する情報に応じてイベント ビューを操作することができます。イベントにアクセスしたときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページです。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

次のいずれかを実行します。

- [分析（Analysis）] > [ファイル（Files）] > [ファイル イベント（File Events）]
- [分析（Analysis）] > [ファイル（Files）] > [マルウェア イベント（Malware Events）]

ヒント イベントのテーブル ビューでは、一部のフィールドがデフォルトで非表示にされています。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のフィールド名をクリックします。

ヒント 特定のファイルが検出された接続をすぐに表示するには、イベント ビューアーでチェック ボックスを使用してファイルを選択してから、[ジャンプ（Jump to）] ドロップダウン リストで [接続イベント（Connections Events）] を選択します。

関連トピック

ファイルおよびマルウェア イベント フィールド, （2019 ページ）
定義済みファイルのワークフロー, （1826 ページ）
定義済みマルウェアのワークフロー, （1825 ページ）
イベント ビュー設定の設定, （38 ページ）

ファイルおよびマルウェア イベント フィールド

ワークフローを使用して表示および検索できるマルウェア イベントには、このセクションにリストするフィールドがあります。個別のイベントで利用可能な情報は、いつ、どのように生成されたかによって異なることに注意してください。

（注） AMP for Firepower によってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。エンドポイントベースのマルウェア イベントには、対応するファイル イベントはありません。また、ファイル イベントには AMP for Endpoints 関連のフィールドはありません。

アクション（Action）

ファイルを検出したファイル ポリシー ルールに関連したアクション、および関連するファイル アクション オプション。

AMP クラウド（AMP Cloud）

AMP for Endpoints イベントが発信された AMP クラウドの名前。

アプリケーション ファイル名（Application File Name）

AMP for Endpoints 検出が行われたときに、マルウェア ファイルにアクセスしていたクライアント アプリケーション。これらのアプリケーションはネットワーク検出またはアプリケーション制御とは関係**ありません**。

アプリケーション ファイル SHA256（Application File SHA256）

検出が行われたときに、AMP for Endpoints で検出された、または隔離されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。

アプリケーション プロトコル（Application Protocol）

管理対象デバイスがファイルを検出したトラフィックで使用されるアプリケーション プロトコル。

アプリケーション プロトコル カテゴリまたはタグ（Application Protocol Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

アプリケーションのリスク（Application Risk）

接続で検出されたアプリケーション トラフィックに関連付けられたリスク。「非常に高い（Very High）」、「高（High）」、「中（Medium）」、「低（Low）」、「非常に低い（Very Low）」のいずれかとなります。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

アーカイブ深度（Archive Depth）

アーカイブ ファイル内でファイルがネストされたレベル（存在する場合）。

アーカイブ名（Archive Name）

マルウェア ファイルが関連付けられているアーカイブ ファイル（存在する場合）の名前。アーカイブ ファイルの内容を表示するには、アーカイブ ファイルのイベント ビューア行を右クリックしてコンテキスト メニューを開き、[アーカイブ コンテンツの表示（View Archive Contents）] をクリックします。

アーカイブ SHA256（Archive SHA256）

マルウェア ファイルが関連付けられているアーカイブ ファイル（存在する場合）の SHA-256 ハッシュ値。アーカイブ ファイルの内容を表示するには、アーカイブ ファイルのイベント ビューア

行を右クリックしてコンテキスト メニューを開き、[アーカイブ コンテンツの表示（View Archive Contents）] をクリックします。

ビジネスとの関連性（Business Relevance）

接続で検出されたアプリケーション トラフィックに関連するビジネス関連性：Very High、High、Medium、Low、またはVery Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネス関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

カテゴリ（Category）/ファイル タイプ カテゴリ（File Type Category）

ファイル タイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイルなど）。

クライアント（Client）

1 つのホストで実行され、ファイルを送信するためにサーバに依存するクライアント アプリケーション。

クライアント カテゴリまたはタグ（Client Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

メンバー数（Count）

複数の同じ行を作成する制約を適用した後の、各行の情報に一致するイベントの数。

検出名（Detection Name）

検出されたマルウェアの名前。

ディテクタ（Detector）

マルウェアを識別した AMP for Endpoints ディテクタ（ClamAV、Spero、SHA など）。

Device

ファイルイベントおよびネットワークベースのマルウェア イベントの場合、ファイルを検出したデバイスの名前。

エンドポイントベースのマルウェア イベントおよび AMP クラウドによって生成される遡及的マルウェア イベントの場合、Firepower Management Center の名前。

傾向（Disposition）/ファイル性質（File Disposition）

ファイルの性質：

マルウェア（Malware）

AMP クラウドでそのファイルがマルウェアとして分類された、ローカル マルウェア分析でマルウェアとして識別された、またはファイル ポリシーで定義されたマルウェアしきい値をファイルの脅威スコアが超えたことを示します。

クリーン（Clean）

AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。クリーンのファイルがマルウェア テーブルに含められるのは、そのファイルがクリーンに変更された場合だけです。

不明

システムが AMP クラウドに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、AMP クラウドがファイルを正しく分類していませんでした。

カスタム検出（Custom Detection）

ユーザがカスタム検出リストにファイルを追加したことを示します。

応対不可（Unavailable）

システムがAMPクラウドに問い合わせできなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。

該当なし

[ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] ルールがファイルを処理し、Firepower Management Center が AMP クラウドに問い合わせなかったことを示します。

ファイル性質は、システムが AMP クラウドに問い合わせたファイルでのみ表示されます。

ドメイン（Domain）

ファイルイベントおよびネットワークベースのマルウェアイベントの場合、ファイルを検出したデバイスのドメイン。エンドポイント ベースのマルウェア イベントおよび AMP クラウドによって生成される遡及的マルウェア イベントの場合、イベントを報告した AMP クラウド接続に関連付けられたドメイン。

このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

イベント サブタイプ（Event Subtype）

マルウェア検出につながった AMP for Endpoints アクション（[作成（Create）]、[実行（Execute）]、[移動（Move）]、[スキャン（Scan）] など）。

イベント タイプ（Event Type）

マルウェア イベントのサブタイプ。

ファイル名（File Name）

マルウェア ファイルの名前。

ファイル パス（File Path）

AMP for Endpointsによって検出されたマルウェア ファイルのファイル パス（ファイル名を含まない）。

ファイル ポリシー（File Policy）

ファイルを検出したファイル ポリシー。

ファイル ストレージ（File Storage）/保存（Stored）（検索のみ）

イベントに関連付けられたファイルのストレージ ステータス：

保存（Stored）

関連するファイルが現在保存されているすべてのイベントを返します。

関連保存（Stored in connection）

関連するファイルが現在保存されているかどうかに関係なく、関連するファイルをシステムがキャプチャおよび保存したすべてのイベントを返します。

失敗しました（Failed）

関連するファイルをシステムが保存できなかったすべてのイベントを返します。

ファイルのタイムスタンプ（File Timestamp）

AMP for Endpoints が検出したマルウェア ファイルが作成された日時。

HTTP 応答コード（HTTP Response Code）

ファイルの転送時にクライアントの HTTP 要求に応じて送信される HTTP ステータス コード。

IOC

マルウェア イベントが、接続に関与したホストに対する侵入の痕跡（IOC）をトリガーしたかどうか。AMP for Endpoints データが IOC ルールをトリガーした場合、タイプ AMP IOC で、完全なマルウェア イベントが生成されます。

メッセージ（Message）

マルウェア イベントに関連付けられる追加情報。ファイル イベントおよびネットワーク ベースのマルウェア イベントでは、このフィールドは、性質が変更された、つまり関連付けられた遡及的イベントがあるファイルに対してのみ入力されます。

受信側の大陸（Receiving Continent）

ファイルを受信するホストの大陸。

受信側の国（Receiving Country）

ファイルを受信するホストの国。

受信側 IP（Receiving IP）

ファイルイベントおよびネットワークベースのマルウェアイベントの場合、ファイルを受信するホストのIPアドレス。エンドポイントベースのマルウェアのイベントの場合、コネクタがイベントを報告したエンドポイントの IP アドレス。

受信側のポート（Receiving Port）

ファイルが検出されたトラフィックによって使用される宛先ポート。

セキュリティ コンテキスト（Security Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチコンテキスト モードの ASA FirePOWER だけです。

送信側の大陸（Sending Continent）

ファイルを送信するホストの大陸。

送信側の国（Sending Country）

ファイルを送信するホストの国。

送信側 IP（Sending IP）

ファイルを送信するホストの IP アドレス。

送信側のポート（Sending Port）

ファイルが検出されたトラフィックによって使用される送信元ポート。

SHA256/ファイル SHA256（File SHA256）

ファイルのSHA-256ハッシュ値と、最後に検出されたファイルイベントおよびファイル性質を表すネットワーク ファイル トラジェクトリ アイコン、およびネットワーク ファイル トラジェクトリにリンクするネットワーク ファイル トラジェクトリ アイコン。SHA256 値を得るには、ファイルが次のいずれかによって処理されている必要があります。

- [ファイルの保存（Store files）] が有効になっているファイル検出ファイル ルール。
- [ファイルの保存（Store files）] が有効になっているファイル ブロック ファイル ルール。
- マルウェア クラウド ルックアップ ファイル ルール
- マルウェア ブロック ファイル ルール
- AMP for Endpoints

サイズ（KB）（Size (KB)）/ファイル サイズ（KB）（ファイル サイズ（KB））

ファイルのサイズ（KB単位）。ファイルが完全に受信される前にシステムがファイルのタイプを判別すると、ファイル サイズが計算されずに、このフィールドがブランクになる場合があるので注意してください。

SSL の実際の動作（SSL Actual Action）（検索のみ）

システムが暗号化トラフィックに適用したアクション。

ブロック（Block）/リセットしてブロック（Block With Reset）

ブロックされた暗号化接続を表します。

複合（再署名）（Decrypt (Resign)）

再署名サーバ証明書を使用して復号された発信接続を表します。

復号（キーの置き換え）（Decrypt (Replace Key)）

置き換えられた公開キーと自己署名サーバ証明書を使用して復号された発信接続を表します。

復号（既知のキー）（Decrypt (Known Key)）

既知の秘密キーを使用して復号された着信接続を表します。

デフォルト アクション（Default Action）

接続がデフォルト アクションによって処理されたことを示しています。

復号しない（Do Not Decrypt）

システムが復号しなかった接続を表します。

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL 証明書情報（SSL Certificate Information）（検索のみ）

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- 件名/発行元共通名（Subject/Issuer Common Name）

- 件名/発行元組織（Subject/Issuer Organization）
- 件名/発行元組織ユニット（Subject/Issuer Organization Unit）
- 有効期間の開始/終了（Not Valid Before/After）
- シリアル番号（Serial Number）、証明書フィンガープリント（Certificate Fingerprint）
- 公開キー フィンガープリント（Public Key Fingerprint）

SSL 失敗理由（SSL Failure Reason）（検索のみ）

システムが暗号化されたトラフィックの復号に失敗した理由：

- 不明
- 不一致（No Match）
- Success
- キャッシュされていないセッション（Uncached Session）
- 不明な暗号スイート（Unknown Cipher Suite）
- サポートされていない暗号スイート（Unsupported Cipher Suite）
- サポートされていない SSL バージョン（Unsupported SSL Version）
- SSL 圧縮の使用（SSL Compression Used）
- パッシブ モードで復号できないセッション（Session Undecryptable in Passive Mode）
- ハンドシェイク エラー（Handshake Error）
- 復号エラー（Decryption Error）
- 保留サーバ名カテゴリ ルックアップ（Pending Server Name Category Lookup）
- 保留共通名カテゴリ ルックアップ（Pending Common Name Category Lookup）
- 内部エラー（Internal Error）
- ネットワーク パラメータを使用できません（Network Parameters Unavailable）
- 無効なサーバ証明書の処理（Invalid Server Certificate Handle）
- サーバ証明書フィンガープリントを使用できません（Server Certificate Fingerprint Unavailable）
- サブジェクト DN をキャッシュできません（Cannot Cache Subject DN）
- 発行元 DN をキャッシュできません（Cannot Cache Issuer DN）
- 不明の SSL バージョン（Unknown SSL Version）
- 外部証明書リストを使用できません（External Certificate List Unavailable）
- 外部証明書フィンガープリントを使用できません（External Certificate Fingerprint Unavailable）
- 内部証明書リストが無効です（Internal Certificate List Invalid）

- 内部証明書リストを使用できません（Internal Certificate List Unavailable）
- 内部証明書を使用できません（Internal Certificate Unavailable）
- 内部証明書フィンガープリントを使用できません（Internal Certificate Fingerprint Unavailable）
- サーバ証明書検証を使用できません（Server Certificate Fingerprint Unavailable）
- サーバ証明書検証エラー（Server Certificate Validation Failure）
- 無効なアクション（Invalid Action）

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL ステータス（SSL Status）

暗号化された接続を記録した、[SSL の実際の動作（SSL Actual Action）]（SSL ルール、デフォルト アクション、または復号できないトラフィック アクション）に関連したアクション。ロック アイコン（  ）は、SSL 証明書の詳細にリンクしています。証明書を利用できない場合（たとえば、SSL ハンドシェイク エラーにより接続がブロックされる場合）、ロック アイコンはグレー表示になります。

システムが暗号化接続を復号できなかった場合は、[SSL の実際の動作（SSL Actual Action）]（実行された復号不能のトラフィック アクション）と、[SSL 失敗理由（SSL Failure Reason）] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [Do Not Decrypt (Unknown Cipher Suite)] が表示されます。

このフィールドを検索する場合は、[SSL の実際の動作（SSL Actual Action）] と [SSL 失敗理由（SSL Failure Reason）] の 1 つ以上の値を入力し、システムが処理した、または復号に失敗した暗号化トラフィックを表示します。

SSL 件名/発行元国（SSL Subject/Issuer Country）（検索のみ）

暗号化証明書に関連付けられた件名または発行元国の 2 文字の ISO 3166-1 alpha-2 国番号。

脅威名（Threat Name）

検出されたマルウェアの名前。

脅威スコア（Threat Score）

そのファイルに関連する最新の脅威スコア。脅威スコア アイコンは、[動的分析要約（Dynamic Analysis Summary）] レポートにリンクされています。

時刻（Time）

イベントが生成された日時。このフィールドは検索できません。

タイプ（Type）/ファイル タイプ（File Type）

ファイルのタイプ（HTML や MSEXE など）。

URI（URI）/ファイル URI（File URI）

ファイルの送信元の URI（ファイルをダウンロードした URL など）。

ユーザ（User）

イベントが発生したホスト（受信 IP）のユーザ

ファイルイベントおよびネットワークベースのマルウェアイベントの場合、このユーザはネットワーク検出によって判別されます。ユーザは宛先ホストに関連付けられているため、ユーザがマルウェア ファイルをアップロードしたマルウェア イベントに、ユーザは関連付けられていません。

エンドポイントベースのマルウェア イベントの場合、AMP for Endpoints がユーザ名を判別します。これらのユーザをユーザ検出または制御に関連付けることは**できません**。それらは [ユーザ（Users）] テーブルに含まれず、それらのユーザの詳細を表示することもできません。

Web アプリケーション（Web Application）

接続で検出された HTTP トラフィックについて、内容を表すまたは URL を要求したアプリケーション。

Web アプリケーションのカテゴリまたはタグ（Web Application Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

マルウェア イベントのサブタイプ

次の表に、マルウェア イベントのサブタイプと、ネットワークベースまたはエンドポイントベースのマルウェア イベントにそのサブタイプを指定できるかどうか、そのサブタイプを使用してネットワーク ファイル トラジェクトリが構築されるかどうかを一覧で示します。

表 *275*：マルウェア イベントのタイプ

マルウェア イベントのサブタイプ/検索値	AMP for Firepower	エンドポイント向け AMP	ファイル トラジェクトリ
ネットワーク ファイル転送時に検出された脅威（Threat Detected in Network File Transfer）	Yes	No	Yes
ネットワーク ファイル転送時に検出された脅威（遡及的）（Threat Detected in Network File Transfer (retrospective)）	Yes	No	Yes
検出された脅威（Threat Detected）	No	Yes	Yes

マルウェア イベントのサブタイプ/検索値	AMP for Firepower	エンドポイント向け AMP	ファイル トラジェクトリ
除外項目内で検出された脅威（Threat Detected in Exclusion）	No	Yes	Yes
検疫された脅威（Threat Quarantined）	No	Yes	Yes
AMP IOC（侵害の兆候）（AMP IOC (Indications of compromise)）	No	Yes	No
ブロックされた実行（Blocked Execution）	No	Yes	No
隔離のクラウド リコール（Cloud Recall Quarantine）	No	Yes	No
隔離のクラウドリコールの試行に失敗（Cloud Recall Quarantine Attempt Failed）	No	Yes	No
隔離のクラウド リコールの開始（Cloud Recall Quarantine Started）	No	Yes	No
隔離からのクラウド リコールの復元（Cloud Recall Restore from Quarantine）	No	Yes	No
隔離からのクラウドリコールの復元に失敗（Cloud Recall Restore from Quarantine Failed）	No	Yes	No
隔離からのクラウドリコールの復元の開始（Cloud Recall Restore from Quarantine Started）	No	Yes	No
隔離エラー（Quarantine Failure）	No	Yes	No
隔離されたアイテムの復元（Quarantined Item Restored）	No	Yes	No
隔離の復元に失敗（Quarantine Restore Failed）	No	Yes	No
隔離の復元の開始（Quarantine Restore Started）	No	Yes	No
スキャン完了、検出なし（Scan Completed, No Detections）	No	Yes	No
スキャンが検出ありで完了（Scan Completed With Detections）	No	Yes	No
スキャンに失敗（Scan Failed）	No	Yes	No

マルウェア イベントのサブタイプ/検索値	AMP for Firepower	エンドポイント向け AMP	ファイル トラジェクトリ
スキャン開始（Scan Started）	No	Yes	No

ファイルおよびマルウェア イベント フィールドで利用可能な情報

次の表に、システムが各ファイルおよびマルウェアイベントフィールドの情報を表示するかどうかを示します。すべてのフィールドがすべてのイベントに読み込まれるわけではないことに留意してください。次に例を示します。

- AMP for Firepower はネットワーク トラフィックでマルウェア ファイルを検出することから、ファイル イベントおよびネットワーク ベースのマルウェア イベントには、ファイルの送信に使用された接続に関する、ポート、アプリケーション プロトコル、および送信元 IP アドレスの情報が含まれます。
- エンドポイント向け AMP の展開からインポートされたマルウェア イベントと侵害の兆候（IOC）には、コンテキスト接続情報は含まれていませんが、ダウンロード時または実行時に取得された情報（ファイル パス、呼び出し元クライアント アプリケーションなど）が含まれています。
- ファイル イベント テーブル ビューには、エンドポイント向け AMP 関連のフィールドは表示されません。

表 *276*：ファイルおよびマルウェア イベント フィールドで利用可能な情報

フィールド	ファイルイベント	AMP for Firepower マルウェアイベント	AMP for Firepower レトロスペクティブ イベント	エンドポイント向け AMP マルウェア イベント
操作（Action）	Yes	Yes	Yes	No
AMP クラウド（AMP Cloud）	No	No	No	Yes
アプリケーション ファイル名（Application File Name）	No	No	No	Yes
アプリケーション ファイル SHA256（Application File SHA256）	No	No	No	Yes
アプリケーション プロトコル	Yes	Yes	No	No
アプリケーション プロトコル カテゴリまたはタグ（Application Protocol Category or Tag）	Yes	Yes	Yes	No

フィールド	ファイルイベント	AMP for Firepower マルウェアイベント	AMP for Firepower レトロスペクティブ イベント	エンドポイント向け AMP マルウェア イベント
アプリケーションのリスク（Application Risk）	Yes	Yes	Yes	No
アーカイブ深度（Archive Depth）	Yes	Yes	No	Yes
アーカイブ名（Archive Name）	Yes	Yes	No	Yes
アーカイブ SHA256（Archive SHA256）	Yes	Yes	No	Yes
ビジネスとの関連性（Business Relevance）	Yes	Yes	Yes	No
カテゴリ/ファイル タイプ カテゴリ（Category / File Type Category）	Yes	Yes	No	Yes
クライアント	Yes	Yes	Yes	No
クライアント カテゴリまたはタグ（Client Category or Tag）	Yes	Yes	Yes	No
メンバー数（Count）	Yes	Yes	Yes	Yes
検出名（Detection Name）	No	Yes	No	No
ディテクタ（Detector）	No	No	No	Yes
Device	Yes	Yes	Yes	Yes
処理/ファイルの処理（Disposition / File Disposition）	Yes	Yes	Yes	No
ドメイン（Domain）	Yes	Yes	Yes	Yes
イベント サブタイプ（Event Subtype）	No	No	No	Yes
イベント タイプ（Event Type）	No	Yes	Yes	Yes
ファイル名（File Name）	Yes	Yes	No	Yes
ファイル パス（File Path）	No	No	No	Yes
ファイル ポリシー（File Policy）	Yes	No	No	No

フィールド	ファイルイベント	AMP for Firepower マルウェアイベント	AMP for Firepower レトロスペクティブ イベント	エンドポイント向け AMP マルウェア イベント
ファイルのタイムスタンプ（File Timestamp）	No	No	No	Yes
HTTP 応答コード（HTTP Response Code）	Yes	Yes	No	No
IOC（侵害の兆候）（IOC (Indication of Compromise)）	No	Yes	Yes	Yes
メッセージ（Message）	Yes	Yes	No	Yes
受信側の大陸（Receiving Continent）	Yes	Yes	Yes	No
受信側の国（Receiving Country）	Yes	Yes	No	No
受信側 IP（Receiving IP）	Yes	Yes	No	Yes
受信側のポート（Receiving Port）	Yes	Yes	No	No
セキュリティ コンテキスト（Security Context）	Yes	Yes	Yes	Yes
送信側の大陸（Sending Continent）	Yes	Yes	Yes	No
送信側の国（Sending Country）	Yes	Yes	No	No
送信側 IP（Sending IP）	Yes	Yes	No	No
送信側のポート（Sending Port）	Yes	Yes	No	No
SHA256/ファイル SHA256（SHA256 / File SHA256）	Yes	Yes	Yes	Yes
サイズ（KB）/ファイルサイズ（KB）（Size (KB) / File Size (KB)）	Yes	Yes	No	Yes
SSL の実際のアクション（SSL Actual Action）（検索のみ）	Yes	Yes	No	No
SSL 証明書情報（SSL Certificate Information）（検索のみ）	Yes	Yes	No	No

フィールド	ファイルイベント	AMP for Firepower マルウェアイベント	AMP for Firepower レトロスペクティブイベント	エンドポイント向け AMP マルウェア イベント
SSL 障害の理由（SSL Failure Reason）（検索のみ）	Yes	Yes	No	No
SSL ステータス（SSL Status）	Yes	Yes	No	No
SSL 件名/発行者の国（SSL Subject/Issuer Country）（検索のみ）	Yes	Yes	No	No
ファイル ストレージ/保存済み（File Storage / Stored）（検索のみ）	Yes	Yes	No	No
脅威名（Threat Name）	No	Yes	Yes	Yes
脅威スコア（Threat Score）	Yes	Yes	No	No
時刻（Time）	Yes	Yes	Yes	Yes
タイプ/ファイル タイプ（Type / File Type）	Yes	Yes	No	Yes
URI/ファイル URI（URI / File URI）	Yes	Yes	No	No
ユーザ（User）	Yes	Yes	No	Yes
Web アプリケーション（Web Application）	Yes	Yes	Yes	No
Web アプリケーション カテゴリまたはタグ（Web Application Category or Tag）	Yes	Yes	Yes	No

ローカル マルウェア分析（Local Malware Analysis）

ローカル マルウェア分析では、管理対象デバイスで Cisco Talos Security Intelligence and Research Group（Talos）から提供される検出ルールを使用して、実行可能ファイル、PDF、Office 文書、およびその他のタイプのファイルで最も一般的なタイプのマルウェアの有無をローカルで検査することができます。ローカルマルウェア分析ではファイルを AMP クラウドに送信する必要はなく、ファイルを実行することもしないので、時間とシステム リソースを節約できます。

システムはローカル マルウェアによってマルウェアを識別すると、その既存のファイルの性質を [不明（Unknown）] から [マルウェア（Malware）] に更新します。その上で、システムは新しいマ

ルウェア イベントを生成します。システムはマルウェアを識別しなかったとしても、ファイルの性質を [不明（Unknown）] から [正常（Clean）] に更新することはしません。ローカル マルウェア分析を実行した後、システムはファイル情報（SHA-256 ハッシュ値、タイムスタンプ、ファイルの性質など）をキャッシュに入れて、特定の期間内にそのファイルを再度検出した場合に再び分析を行わなくてもマルウェアを識別できるようにします。

イベント ビューアで、コンテキスト メニューを使用してローカル マルウェア分析用にファイルを 1 つずつ手動で送信することも、最大 25 個のキャプチャ済みフィルを同時に送信することもできます。システムはローカル分析を実行してから、それらのファイルをダイナミック分析対象としてクラウドに送信します。

ローカル マルウェア分析では、AMP Threat Grid クラウドとの通信を確立する必要はありません。ただし、マルウェアとして事前に分類したファイルをダイナミック分析用にクラウドに送信するため、また、アップデートをローカル マルウェア分析ルールセットにダウンロードするために、クラウドとの通信を設定する必要があります。

ファイル構成

ローカル マルウェアの分析または動的分析を設定すると、ファイルの分析後にファイル構成レポートが生成されます。このレポートを使用して、ファイルをさらに分析し、ファイルにマルウェアが組み込まれているかどうかを判断することができます。

ファイル構成レポートでは、ファイルのプロパティ、ファイルに組み込まれているオブジェクト、および検出されたウイルスが示されます。また、ファイル構成レポートでは、そのファイル タイプに固有の追加情報が示される場合があります。保存されているファイルのプルーニング時に、関連ファイル構成レポートもプルーニングされます。

動的分析（Dynamic Analysis）

AMP クラウドの精度を改善し、追加のマルウェア分析および脅威の特定を提供するには、AMP Threat Grid クラウドまたはオンプレミスの AMP Threat Grid アプライアンスに、キャプチャされた適格なファイルを動的分析用に送信します。AMP クラウドでは、ファイルがサンドボックス環境で実行され、ファイルにマルウェアが含まれているかどうかが判別されます。

動的分析用にファイルを送信できるかどうかは、次によって異なります。

- ファイル タイプ
- ファイル サイズ
- ファイル ルールのアクション
- 自動送信用にマルウェアとしてシステムで事前に分類されたファイル

マルウェアをブロックするか、マルウェア クラウド ルックアップを実行するようにルールが設定されている場合は、不明または使用不可の性質を持つ一致するファイルのみが送信されます。

AMP Threat Grid クラウドでは、動的分析用にファイルがキューに登録され、各ファイルがサンドボックス環境で実行されます。クラウドは、ファイルにマルウェアが含まれている確率の詳細を

示す脅威スコアを返します。脅威スコアが定義されているしきい値を超えるファイルを自動的にブロックできます。

イベント ビューア、キャプチャされたファイル ビュー、またはネットワーク ファイル トラジェクトリから、ファイルが動的分析用に送信されたかどうかの特定、ローカル マルウェアおよびファイルの動的分析用の手動送信、またはクラウドに脅威スコアが割り当てられている理由のサマリーの表示を行うことができます。また、動的分析のサマリー レポートも取得できます。これには、全体的な脅威スコアを構成する各種評価、およびクラウドによるファイル実行の試行時に開始されたその他のプロセスが示されます。

自動ダイナミック分析と Spero 分析

ファイル ポリシーは、マルウェアとして事前分類されたファイルを自動的にダイナミック分析に提出するように設定できます。

クエリ対象にするファイルを自動的に Spero 分析に提出することで、ダイナミック分析を補足することができます。Spero 分析は SHA-256 ハッシュ値の分析を補うもので、実行可能ファイル内のマルウェアをより正確に識別できます。

Spero分析では、ファイル構造の特性（メタデータやヘッダー情報など）を調べます。この情報に基づいて Spero シグネチャを生成した後、デバイスはそれを AMP クラウド内の Spero ヒューリスティック エンジンに送信します。Spero シグネチャに基づいて、そのファイルがマルウェアかどうかを Spero エンジンが返します。現時点のファイル処理が [不明（Unknown）] であれば、システムは [マルウェア（Malware）] のファイル処理を割り当てます。

Spero分析のために実行可能ファイルを送信できるのは、検出時だけなので注意してください。後から手動で送信することはできません。ダイナミック分析にはファイルを送信せずに、Spero分析にのみファイルを送信することもできます。

手動によるダイナミック分析

イベント ビューア、コンテキスト メニュー、ネットワーク ファイル トラジェクトリから、保管されたファイルをダイナミック分析の対象として手動で送信できます。キャプチャ ファイル ビューからは、一度に最大 25 個の保存済みファイルを手動で送信できます。

実行可能ファイルの他に、自動送信に適格ではないファイル タイプ（.swf、.jar など）も送信できます。これにより、ファイルの性質に関わらず、さまざまなファイルをより迅速に分析し、問題の正確な原因を突き止めることができます。

（注） 動的分析に適格なファイル タイプのリストと送信可能な最小および最大のファイル サイズに関して更新がないか、システムは AMP クラウドを検査します（この検査は、一日に 1 回だけ行われます）。

動的分析とキャパシティ処理

容量処理によって、現在、ファイルを動的分析のためにクラウドに送信できない場合に一時的にデバイスでファイルを保存できます。デバイスでは、そのハードドライブまたはマルウェア ストレージ パックにファイルが保存されます。

システムでは、動的分析を有効にして、マルウェア クラウドルックアップを実行する任意のファイルを一時的に保存できます。ファイルがマルウェアとして事前に分類されており、デバイスがクラウドへの最大送信数に到達したか、クラウドと通信できない場合に、システムはこのファイルを保存します。

デバイスでは、次のいずれかの場合に保存されているファイルがクラウドに再送信されます。

- デバイスがクラウドと通信できず、クラウド コミュニケーションを再確立する場合
- デバイスがクラウドへの最大送信数に到達し、十分な時間が経過した場合

脅威スコアと動的分析のサマリ レポート

脅威スコア

表 *277*：脅威スコア レーティング

脅威スコア	アイコン
Low	
Medium	
High	
Very High	

Firepower Management Center は、ファイルの性質と同じ期間だけ、ファイルの脅威スコアをキャッシュに入れます。これらのファイルが後から検出されると、AMP Threat Grid クラウドまたは AMP Threat Grid オンプレミス アプライアンスが再クエリされる代わりに、キャッシュされた脅威スコアが表示されます。ファイルの脅威スコアが、定義済みのマルウェアしきい値の脅威スコアを超える場合は、そのファイルにマルウェアの性質を自動的に割り当てることができます。

動的分析のサマリ

動的分析のサマリが生成可能な場合、脅威スコア アイコンをクリックすると、サマリが表示されます。複数のレポートが存在する場合、このサマリは、脅威スコアと完全に一致する最新のレポートに基づいて生成されます。完全に一致する脅威スコアがない場合、最も高い脅威スコアに関するレポートが表示されます。複数のレポートがある場合は、脅威スコアを選択して、それぞれのレポートを表示することができます。

サマリには、脅威スコアを構成する各コンポーネントの脅威がリストされます。各コンポーネントの脅威を展開すると、そのコンポーネントの脅威に関連するプロセスだけでなく、AMP クラウドの調査結果もリストされます。

プロセス ツリーには、AMP Threat Grid クラウドがファイルを実行しようとしたときに開始されたプロセスが示されています。これは、マルウェアを含むファイルが、想定外のプロセスやシステム リソースへアクセスしようとしているかどうか（たとえば、Word ドキュメントを実行すると、Microsoft Word が開き、次に Internet Explorer が起動し、さらに Java Runtime Environment が実行されるなど）を識別するのに役立ちます。

リストされる各プロセスには、実際のプロセスを検査するのに使用できるプロセス ID が含まれます。プロセス ツリー内の子ノードは、親プロセスの結果として開始されたプロセスを表します。

動的分析のサマリから [完全なレポートを表示（View Full Report）] をクリックすることにより、AMP クラウドの完全な分析を詳述する完全版分析レポートを表示できます。レポートには、ファイルの一般情報、検出されたすべてのプロセスの詳細な説明、ファイル分析の概要、およびその他の関連情報が含まれます。

ファイル分析評価

Spero 分析とローカル マルウェア分析、動的分析、またはこれらの組み合わせの結果に基づいて、システムはファイルの性質を更新することがあります。

システムは、ファイルに対して最初に Spero 分析、次にローカル マルウェア分析、動的分析の順に実行します。システムがマルウェアを特定した場合でも、ファイルがマルウェアとして事前分類されていれば、ファイルは AMP Threat Grid クラウドに送信されます。

ファイル ルールでローカル マルウェア分析または動的分析を設定すると、システムによってルールに一致するファイルが事前分類され、ファイル構成レポートが生成されます。事前分類の結果としてファイルの性質が変更されることはありません。

次の表に、ファイル分析の各タイプの利点と欠点、および分析に基づいたファイルの性質の変更方法について説明します。

表 *278*：ファイル分析のタイプの比較

分析タイプ	利点	制限事項	マルウェアの特定
Spero 分析	実行可能ファイルの構造分析。Spero シグネチャを分析のために AMP クラウドに送信します。	ローカル マルウェア分析または動的分析よりも詳細度が低くなります。実行可能ファイル専用です。	マルウェアの特定がポジティブの場合にのみ、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
ローカル マルウェア分析	動的分析より消費するリソースが少なく、特に検出されたマルウェアが一般的な場合は結果がより迅速に返されます。	動的分析よりも結果の詳細度が低くなります。	マルウェアの特定がポジティブの場合にのみ、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
動的分析	AMP Threat Grid クラウドを使用してサンドボックス環境でファイルを実行することで、結果の詳細度がより高くなります。	ローカル マルウェア分析単独の場合よりも消費するリソースが多くなります。	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ファイル ポリシーに設定されている脅威スコアしきい値に基づいて性質が変更されます。
Spero 分析とローカル マルウェア分析	AMP クラウドのリソースを使用してマルウェアを特定しながら、ローカル マルウェア分析と動的分析を設定するよりも少ないリソースを消費します。	動的分析、Spero 分析よりも詳細度が低くなります。実行可能ファイル専用です。	マルウェアの特定がポジティブの場合にのみ、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。

分析タイプ	利点	制限事項	マルウェアの特定
Spero 分析と動的分析	ファイルおよびSpero シグネチャの送信時にAMP クラウドの全機能を使用します。	ローカル マルウェア分析を使用する場合よりも結果の取得に時間がかかります。	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ファイル ポリシーで設定されている脅威スコアしきい値に基づいて、およびSpero 分析でマルウェアが特定された場合は、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
ローカル マルウェア分析と動的分析	両方のタイプのファイル分析を使用することで詳細な結果が得られます。	どちらか一方の場合よりも消費するリソースが多くなります。	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ローカル マルウェア分析でマルウェアが特定された場合、またはファイル ポリシーで設定されている脅威スコアしきい値に基づいて、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
Spero 分析、ローカル マルウェア分析、および動的分析	最も詳細な結果になります。	3 つすべてのタイプのファイル分析を実行するため消費するリソースが最も多くなります。	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。Spero 分析またはローカル マルウェア分析でマルウェアが特定された場合、またはファイル ポリシーで設定されている脅威スコアしきい値に基づいて、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。

キャプチャ ファイルとファイル ストレージ

ファイル ポリシーの設定に基づき、ファイル制御機能を使用して、ファイルの検出およびブロックを行えます。ただし、疑わしいホストまたはネットワークからのファイルや、ネットワーク上の監視対象ホストに送信された大量のファイルについては、さらに分析が必要になる場合があります。ファイル ストレージ機能を使用することにより、選択したファイル（トラフィックで検出された）をキャプチャして、それらをデバイスのハードドライブかマルウェア ストレージ パック（インストールされている場合）に自動的に保存できます。

デバイスがトラフィックでファイルを検出すると、そのファイルをキャプチャできます。このようにして作成されたコピーは、ダイナミック分析のために、システムが保存したり送信したりできます。デバイスがファイルをキャプチャした後に、以下の選択肢があります。

- 後で分析するために、キャプチャしたファイルをデバイスのハードドライブに保存する。
- さらに手動で分析したりアーカイブしたりするために、保存したファイルをローカル コンピュータにダウンロードする。
- ダイナミック分析用に、AMP クラウドにファイルを送信します。

注意すべき点として、デバイスがファイルを保存した後は、以後それを検出しても、デバイスが引き続きそれを保存していれば、そのファイルを再度キャプチャすることはありません。

（注） ファイルがネットワーク上で初めて検出された際には、ファイルの検出を表すファイル イベントを生成できます。ただし、ファイル ルールがマルウェア クラウド ルックアップを行う場合は、システムが AMP クラウドにクエリを行い、判定結果が返るまで、より多く時間を要します。この遅延により、システムはネットワークでこのファイルが2回目に検出され、ファイルの判定結果を即座に判断できるまでは、このファイルを保存できません。

システムがファイルをキャプチャするか保存するかに関わらず、以下が可能です。

- イベント ビューアからのキャプチャされたファイルに関する情報（ダイナミック分析のためにファイルが保存されたのか送信されたかどうか、ファイル判定結果、脅威スコアなど）を確認することにより、ネットワーク上で検出されたマルウェアの潜在的な脅威について迅速に検討する。
- ファイルのトラジェクトリを表示して、ネットワークのトラバースの仕方およびコピーを保持しているホストを判別する。
- ファイルをクリーン リストまたはカスタム検出リストに追加することで、以後の検出時には常に、クリーンまたはマルウェアの判定結果を持つファイルとして扱う。

ファイル ポリシーでファイル ルールを設定して、特定のタイプまたは特定のファイル判定結果（使用できる場合）のファイルをキャプチャして保存します。ファイル ポリシーをアクセス コントロール ポリシーと関連付けて、それをデバイスに展開した後、トラフィック内の一致ファイルが検出され、保存されます。また、保存するファイル サイズの最小値と最大値を設定できます。保存したファイルは、システム バックアップ ファイルには含まれません。

マルウェア ストレージ パック

ファイル ポリシー構成によっては、デバイスがハード ドライブにかなりの量のファイル データを保存することがあります。デバイスにマルウェア ストレージ パックを設置すると、システムはファイルをマルウェア ストレージ パックに保存して、プライマリ ハード ドライブでイベントおよび設定ファイルの保存用スペースをより多く確保できます。システムは定期的に古いファイルを削除します。デバイスのプライマリ ハード ドライブに使用可能な領域が十分でなく、マルウェア ストレージ パックも設置されていない場合、ファイルを保存することはできません。

注意 Cisco から供給されたハード ドライブ以外はデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、シスコから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パックのサポートが必要な場合は、サポートにお問い合わせください。詳細については、*Firepower System Malware Storage Pack Guide*を参照してください。

マルウェアストレージパックが設置されていない場合、ファイルを保存するデバイスを設定すると、プライマリ ハード ドライブのスペースの特定の部分がキャプチャ ファイル ストレージに割り当てられます。ダイナミック分析用に一時的にファイルに保存するよう容量処理を設定すると、システムはファイルをクラウドに再送信できるようになるまで、同じハード ドライブ割り当てを使用してそれらのファイルを保存します。

デバイスにマルウェア ストレージ パックを設置してファイル ストレージまたは容量処理を設定すると、デバイスはマルウェアストレージパック全体をこれらのファイルの保存用として割り当てます。デバイスは、マルウェア ストレージ パックに他の情報を保存することはできません。

キャプチャ ファイル ストレージに割り当てられたスペースがいっぱいになると、システムは割り当てられたスペースがシステム定義しきい値に達するまで、保管されている古いファイルを削除します。保存されていたファイルの数によっては、システムがファイルを削除した後、ディスク使用率がかなり減る場合があります。

マルウェア ストレージ パックを設置する時点で、デバイスがすでにファイルを保存している場合、次にデバイスを再起動したときに、プライマリ ハード ドライブに保存されていたキャプチャ ファイルまたは容量処理ファイルはすべて、マルウェアストレージパックに移動します。それ以降デバイスが保存するファイルはすべて、マルウェア ストレージ パックに保存されます。

保存されているファイルのダウンロード

デバイスによって保存されたファイルは、Firepower Management Center がそのデバイスと通信可能であり、ファイルが削除されていない限り、長期間保存し分析するためにローカル ホストにダウンロードし、手動でファイルを分析できます。関連ファイル イベント、マルウェア イベント、キャプチャ ファイル ビュー、またはファイルのトラジェクトリからファイルをダウンロードできます。

マルウェアによる被害を防ぐため、デフォルトでは、ファイルのダウンロードのたびに確認を行う必要があります。ただし、この確認は [ユーザ設定（User Preferences）] で無効にすることもできます。

性質が使用不可のファイルにはマルウェアが含まれている可能性があるため、ファイルをダウンロードすると、システムはまずそのファイルを `.zip` パッケージにアーカイブします。`.zip` ファイル名には、ファイルの性質とファイル タイプ（存在する場合）さらに SHA-256 ハッシュ値が含まれます。誤って解凍してしまわないように、`.zip` ファイルをパスワードで保護できます。`.zip` ファイルのデフォルト パスワードは、[ユーザ設定（User Preferences）] で編集または削除できます。

注意 有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先をセキュアにするために必要な予防措置を行っていることを確認します。

キャプチャされたファイル ワークフローの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

管理対象デバイスは、ネットワーク トラフィックで検出されたファイルをキャプチャすると、イベントをログに記録します。

（注） デバイスがマルウェアを含むファイルをキャプチャすると、デバイスは、ファイルを検出した場合はファイル イベント、マルウェアを識別した場合はマルウェア イベントの 2 種類のイベントを生成します。

イベント ビューアでは、テーブルにキャプチャ ファイルを表示できます。また、分析に関連する情報に応じてイベント ビューを操作することができます。キャプチャ ファイルにアクセスしたときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページです。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

ファイル ポリシーの更新など設定を変更した後に、システムがファイルを再キャプチャする場合、そのファイルの既存の情報が更新されます。

たとえば、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）] アクションを使用してファイルをキャプチャするようにファイル ポリシーを設定した場合、システムはそのファイルと一緒にファイル処理と脅威スコアを保存します。その後、ファイル ポリシーを更新し、新しい

[ファイルの検出（Detect Files）] アクションのためにシステムが同じファイルを再キャプチャすると、システムはファイルの [最終変更時刻（Last Changed）] の値を更新します。ただし、別のマルウェア クラウド ルックアップを実行しなかったとしても、システムは既存の処理や脅威スコアを削除しません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

[分析（Analysis）]>[ファイル（Files）]>[キャプチャ ファイル（Captured Files）]を選択します。

ヒント イベントのテーブル ビューでは、一部のフィールドがデフォルトで非表示にされています。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のフィールド名をクリックします。

関連トピック

キャプチャされたファイルのフィールド, （2043 ページ）
定義済みキャプチャ ファイルのワークフロー, （1826 ページ）
イベント ビュー設定の設定, （38 ページ）

キャプチャされたファイルのフィールド

キャプチャされたファイルのテーブル ビューは、定義済みファイル イベントのワークフローの最後のページであり、カスタム ワークフローに追加できます。このテーブル ビューには、ファイル テーブルの各フィールドの列が含まれます。

このテーブルを検索する場合、検索結果は、検索対象のイベントで使用可能なデータによって決まることに留意してください。使用可能なデータによって、検索の制約が適用されないことがあります。たとえば、ダイナミック分析のためにファイルが送信されていない場合は、関連する脅威スコアがない可能性があります。

表 *279*：キャプチャされたファイルのフィールド

フィールド	説明
アーカイブ検査ステータス（Archive Inspection Status）	アーカイブ ファイルのアーカイブ検査ステータスであり、次のいずれかになります。 • [保留中（Pending）] は、システムがアーカイブ ファイルとその内容をまだ検査していることを示します。ファイルが再びシステムを通過すると、完全な情報が使用可能になります。 • [抽出済み（Extracted）] は、アーカイブの内容を抽出し、検査できたことを示します。 • [失敗（Failed）] は、まれなケースですが、システムが抽出を処理できない場合に発生します。 • [深さ超過（Depth Exceeded）] は、許可されている最大深さを超えるネストされたアーカイブ ファイルがアーカイブに含まれていることを示します。 • [暗号化（Encrypted）] は、アーカイブ ファイルの内容が暗号化されていて、検査できなかったことを示します。 • [検査不可（Not Inspectable）] は、システムがアーカイブの内容を抽出して検査しなかったことを示しています。このステータスの主な理由としては、ポリシー ルール アクション、ポリシー設定、破損ファイルの 3 つがあります。 アーカイブ ファイルの内容を表示するには、イベント ビューアで該当の行を右クリックしてコンテキスト メニューを開いてから、[アーカイブの内容の表示（View Archive Contents）] を選択します。
カテゴリ（Category）	ファイル タイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイルなど）。
検出名（Detection Name）	検出されたマルウェアの名前。

フィールド	説明
傾向（Disposition）	Firepower の傾向に関するファイルの AMP であり、次のいずれかになります。 • [マルウェア（Malware）] は、ファイルがローカルのマルウェア分析でマルウェアとして認識され、クラウドでマルウェアとして分類されていること、または、ファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。 • [クリーン（Clean）] は、ファイルが AMP クラウドでクリーンとして分類されていること、または、ファイルをユーザがクリーン リストに追加したことを示します。 • [不明（Unknown）] は、システムが AMP クラウドに問い合わせましたが、ファイルの傾向が割り当てられていないこと、つまり、ファイルが AMP クラウドで正しく分類されていないことを示します。 • [カスタム検出（Custom Detection）] は、ファイルをユーザがカスタム検出リストに追加したことを示します。 • [使用不可（Unavailable）] は、システムが AMP クラウドに問い合わせできなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。 • [N/A] は、[ファイルを検出する（Detect Files）] または [ファイルをブロックする（Block Files）] ルールによってファイルが処理され、Firepower Management Center が AMP クラウドに問い合わせなかったことを示します。
ドメイン	キャプチャされたファイルが検出されたドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

フィールド	説明
ダイナミック分析ステータス（Dynamic Analysis Status）	ファイルが AMP for Firepower によるダイナミック分析のために送信されたかどうかを示すものであり、次のうちの 1 つ以上が表示されます。 • [分析完了（Analysis Complete）]：ファイルがダイナミック分析のために送信され、脅威スコアおよびダイナミック分析のサマリー レポートを受け取りました。 • [処理予定の容量（Capacity Handled）]：送信できなかったため、ファイルが保存されました。 • [処理予定の容量（ネットワークの問題）（Capacity Handled (Network Issue)）]：ネットワーク接続の問題が原因で送信できなかったため、ファイルが保存されました。 • [処理予定の容量（レート制限）（Capacity Handled (Rate Limit)）]：最大数に達したことが原因で送信できなかったため、ファイルが保存されました。 • [非アクティブなデバイス（Device Not Activated）]：デバイスがオンプレミスの AMP Threat Grid アプライアンスでアクティブになっていないため、ファイルが送信されません。このステータスが表示された場合は、サポート担当に連絡してください。 • [失敗（分析タイムアウト）（Failure (Analysis Timeout)）]：ファイルが送信されましたが、まだ AMP から結果が返されていません。 • [失敗（ファイル実行不可）（Failure (Cannot Run File)）]：ファイルが送信されましたが、AMP クラウドがテスト環境でファイルを実行できませんでした。 • [失敗（ネットワークの問題）（Failure (Network Issue)）]：ネットワーク接続の問題のため、ファイルが送信されませんでした。 • [分析のための送信なし（Not Sent for Analysis）]：ファイルが送信されませんでした。 • [疑わしくないファイル（分析のための送信なし）（Not Suspicious (Not Sent For Analysis)）]：ファイルがマルウェアではないものとして事前に分類されています。 • [以前に分析済み（Previously Analyzed）]：キャッシュされた脅威スコアがあるファイルをユーザが再び送信しようとしました。 • [分析のために送信（Sent for Analysis）]：ファイルがマルウェアとして事前に分類されており、ダイナミック分析のためにキューに入れられました。
ダイナミック分析ステータスの変更（Dynamic Analysis Status Changed）	前回、ファイルのダイナミック分析のステータスが変更された日時。
ファイル名	ファイルの SHA-256 ハッシュ値に関連付けられているものとして最後に検出されたファイル名。
前回の変更（Last Changed）	このファイルに関連する情報が最後に更新された時刻。

フィールド	説明
最終送信日時（Last Sent）	ファイルがダイナミック分析のために AMP for Firepower によって AMP クラウドに最後に送信された日時。
ローカル マルウェア分析ステータス（Local Malware Analysis Status）	ローカルマルウェア分析が実行されたかどうかを示すものであり、次のいずれかになります。 • [分析完了（Analysis Complete）]：ローカル マルウェア分析を使用してファイルが検査され、事前に分類されました。 • [分析失敗（Analysis Failed）]：ローカル マルウェア分析を使用してファイルを検査しようとし、失敗しました。 • [手動による要求の送信（Manual Request Submitted）]：ユーがローカル マルウェア分析のためにファイルを送信しました。 • [分析なし（Not Analyzed）]：システムでローカル マルウェア分析を使用してファイルが検査されませんでした。
SHA256	ファイルの SHA-256 ハッシュ値と、最後に検出されたファイル イベントおよびファイルの性質を表すネットワーク ファイル トラジェクトリ アイコン。ネットワーク ファイル トラジェクトリを表示するには、トラジェクトリ アイコンをクリックします。
ストレージ ステータス（Storage Status）	ファイルが管理対象デバイスに保存されているかどうかを示し、次のいずれかになります。 • ファイル保存済み（File Stored） • 保存なし（性質分析の保留）（Not Stored (Disposition Was Pending)）
脅威スコア（Threat Score）	このファイルに関連付けられている最新の脅威スコア。 ダイナミック分析のサマリー レポートを表示するには、脅威スコア アイコンをクリックします。
タイプ（Type）	ファイルのタイプ（HTML や MSEXE など）。

ネットワーク ファイル トラジェクトリ

ネットワーク ファイルのトラジェクトリ機能は、ネットワーク全体でホストがどのようにファイル（マルウェア ファイルを含む）を転送したかをマッピングします。トラジェクトリは、ファイル転送データ、ファイルの性質、ファイル転送がブロックされたかどうか、ファイルが隔離されたかどうかをグラフに示します。これにより、マルウェアを転送したおそれのあるホストやリスクがあるホストがどれであるかを判定したり、ファイル転送の傾向を観測したりできます。

AMP クラウドで性質が割り当てられているファイルであれば、どのファイルの送信でも追跡できます。システムは、AMP for Firepower と AMP for Endpoints の両方によるマルウェアの検出およびブロック情報を使用して、トラジェクトリを作成します。

最近検出されたマルウェアおよび分析済みトラジェクトリ

[ネットワーク ファイル トラジェクトリ リスト（Network File Trajectory List）] ページには、ネットワークで最近検出されたマルウェアと最後に表示したトラジェクトリ マップのファイルが表示されます。これらのリストから、ネットワークで各ファイルが最後に発見されたのはいつか、ファイルのSHA-256のハッシュ値、名前、タイプ、現在のファイルの性質、内容（アーカイブ ファイルの場合）、ファイルに関連付けられたイベント数を確認できます。

また、このページに含まれる検索ボックスを使用して、SHA-256 ハッシュ値またはファイル名を基準に、あるいはファイルを送信または受信するホストのIPアドレスによってファイルを見つけることができます。ファイルを見つけた後、[ファイル SHA256（File SHA256）] 値をクリックすると詳細なトラジェクトリ マップが表示されます。

ネットワーク ファイル トラジェクトリの詳細ビュー

詳細なネットワークファイルトラジェクトリを表示して、ネットワーク全体でファイルを追跡できます。ファイルのSHA 256値を検索するか、[ネットワーク ファイル トラジェクトリ（Network File Trajectory）] リスト内の [ファイルの SHA 256（File SHA 256）] リンクをクリックして、そのファイルに関する詳細を表示します。

ネットワーク ファイル トラジェクトリの詳細ページには、3 つの部分があります。

- サマリー情報：ファイルのトラジェクトリページには、ファイルに関するサマリー情報（ファイル識別情報、ネットワーク上でファイルが最初に表示された時間および最後に表示された時間、ファイルに関連したイベントおよびホストの数、ファイルの現在の性質など）が表示されます。このセクションから、管理対象デバイスがファイルを保存した場合に、そのファイルをローカルにダウンロードしたり、ファイルを動的分析用に送信したり、ファイルをファイル リストに追加したりできます。
- トラジェクトリー マップ：ファイルのトラジェクトリ マップは、ネットワークで最初に検出された時点から直近までファイルを視覚的に追跡します。このマップは、ホストがファイルを転送または受信した時点、ファイルを転送した頻度、ファイルがブロックまたは隔離された時点を示します。データ ポイント間の縦線は、ホスト間のファイル転送を表します。データ ポイントをつなぐ横棒は、時間の経過に応じたホストのファイル アクティビティを示します。

  また、そのファイルでファイルイベントが発生した頻度や、システムがファイルに性質または遡及的性質を割り当てた時点についても示します。マップでデータ ポイントを選択し、ホストがそのファイルを転送した最初のインスタンスに遡るパスを強調表示できます。また、このパスは、ファイルの送信側または受信側としてホストが関与する各オカレンスと交差します。
- 関連イベント：[イベント（Events）] テーブルに、マップ内の各データ ポイントに関するイベント情報がリストされます。テーブルおよびマップを使用して、特定のファイル イベント、このファイルを転送または受信したネットワーク上のホスト、マップ内の関連するイベント、選択した値で制限されたテーブル内の他の関連するイベントを特定することができます。

ネットワーク ファイル トラジェクトリのサマリー情報

次の概要情報は、ネットワーク ファイル トラジェクトリのリストに表示されるファイルの詳細ページの上部に表示されます。

ヒント　関連するファイル イベントを表示するには、フィールド値のリンクをクリックします。ファイル イベントのデフォルトのワークフローの最初のページが新しいウィンドウで開き、選択した値を含むすべてのファイル イベントも表示されます。

表 *280*：ネットワーク ファイル トラジェクトリのサマリー情報フィールド

[名前（Name）]	説明
コンテンツのアーカイブ（Archive Contents）	検査されたアーカイブ ファイルで、アーカイブに含まれているファイルの数。
現在の傾向（Current Disposition）	次のいずれかの AMP for Firepower ファイルの性質です。 • マルウェア（Malware）：ファイルが AMP クラウドでマルウェアと分類されていること、ローカル マルウェア分析でマルウェアとして識別されたこと、またはファイルの脅威スコアがファイル ポリシーに定義されたマルウェアのしきい値を超えたこと示します。 • [クリーン（Clean）]：AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。 • [不明（Unknown）]：システムが AMP クラウドに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、AMP クラウドがファイルを正しく分類していませんでした。 • カスタム検出（Custom Detection）：ユーザがカスタム検出リストにファイルを追加したことを示します。 • 利用不可（Unavailable）：システムが AMP クラウドでクエリを行えなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。 • [該当なし（N/A）]：[ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] ルールがファイルを処理し、Firepower Management Center が AMP クラウドに問い合わせなかったことを示します。
検出名（Detection Name）	ローカル マルウェア分析によって検出されたマルウェアの名前。
イベント カウント（Event Count）	ファイルに関連付けられたネットワークで発見されたイベントの数、検出されたイベントの数が 250 を超える場合は、マップに表示されるイベントの数。

[名前（Name）]	説明
ファイル カテゴリ（File Category）	ファイル タイプの一般的なカテゴリ（`Office Documents` や `System Files` など）。
ファイル名（File Names）	ネットワーク上で発見された、イベントに関連したファイルの名前。 複数のファイル名がSHA-256ハッシュ値に関連付けられている場合、最後に検出されたファイル名がリストされます。[詳細（more）] をクリックすると、これが展開されて、残りのファイル名が表示されます。
ファイル SHA256（File SHA256）	ファイルの SHA-256 ハッシュ値。 デフォルトで、ハッシュは簡略化された形式で表示されます。完全なハッシュ値を表示するには、その上にポインタを移動させます。複数の SHA-256 ハッシュ値がファイル名に関連付けられている場合、リンクの上にポインタを移動されると、すべてのハッシュ値が表示されます。
ファイル サイズ（File Size）（KB）	ファイルのサイズ（KB 単位）。
ファイル タイプ（File Type）	ファイルのタイプ（`HTML` や `MSEXE` など）。
最初の確認日時（First Seen）	AMP for Firepower またはエンドポイント向け AMP による初めてのファイル検出に加えて、ファイルを初めてアップロードしたホストの IP アドレス、。
前回の検出（Last Seen）	AMP for Firepower またはエンドポイント向け AMP による最新のファイル検出に加えて、ファイルを最後にダウンロードしたホストの IP アドレス、。
親アプリケーション（Parent Application）	エンドポイント向け AMP による検出が行われたときに、マルウェア ファイルにアクセスしていたクライアント アプリケーション。これらのアプリケーションはネットワーク検出またはアプリケーション制御とは関係**ありません**。
表示日（Seen On）	ファイルを送信または受信したホストの数。1 つのホストが 1 つのファイルのアップロードおよびダウンロードを時を異にして行う場合があるため、ホストの合計数が、[明細の表示日（Seen On Breakdown）] フィールドの送信側の総数と受信側の総数の合計と一致しないことがあります。
分析（Seen On Breakdown）	ファイルを送信したホストの数とファイルを受信したホストの数。
脅威名（Threat Name）	エンドポイント向け AMP によって検出されたマルウェアに関連付けられている脅威の名前。
脅威スコア（Threat Score）	ファイルの脅威スコア。

ネットワーク ファイル トラジェクトリ マップと関連イベント リスト

ファイル トラジェクトリ マップの Y 軸には、ファイルと対話したすべてのホストの IP アドレスがリストされます。IP アドレスは、システムがそのホストでファイルを最初に検出した時点に基づいて降順でリストされます。各行には、その IP アドレスに関連付けられたすべてのイベント（単一のファイル イベント、ファイル転送、遡及的イベント）が含まれます。X 軸には、システムが各イベントを検出した日時が含まれます。タイムスタンプは時間順にリストされます。複数のイベントが 1 分以内に発生する場合、すべてが同じ列内にリストされます。マップを左右および上下にスクロールして、イベントおよび IP アドレスをさらに表示できます。

マップには、ファイルの SHA-256 ハッシュに関連した最大 250 のイベントが表示されます。イベントが 250 を超える場合、マップには最初の 10 個が表示され、余分のイベントは省略されて矢印アイコン（）が示されます。その後ろに、マップは残りの 240 個のイベントを表示します。

デフォルトの [File Events（ファイル イベント）] ワークフローの最初のページが新しいウィンドウで開き、ファイル タイプに基づいて制限されて、すべての余分のイベントが表示されます。エンドポイントベースのマルウェア イベントが表示されない場合、[マルウェア イベント（Malware Events）] テーブルに切り替えて、それらを表示する必要があります。

各データ ポイントは、イベントの他にファイル性質を表しています。マップの下の凡例を参照してください。たとえば、[マルウェア ブロック（Malware Block）] イベント アイコンは、[悪意のある性質（Malicious Disposition）] アイコンと [ブロック イベント（Block Event）] アイコンを結合したものです。

エンドポイントベースのマルウェア イベントには 1 つアイコンが含まれます。遡及的イベントでは、ファイルで検出された各ホストのコラムにアイコンが表示されます。ファイル転送イベントでは、縦線でつながれた 2 つのアイコン（ファイル送信アイコンとファイル受信アイコン）が常に含まれます。矢印は、送信側から受信側へのファイル転送方向を示します。

ネットワークを介したファイルの進行状況を追跡するために、データ ポイントをクリックして、選択したデータ ポイントに関連するすべてのデータ ポイントを含むパスを強調表示できます。これには、次のタイプのイベントに関連付けられたデータ ポイントが含まれます。

- 関連付けられている IP アドレスが送信側または受信側だったファイル転送
- 関連付けられている IP アドレスが関係するエンドポイントベースのマルウェア イベント
- 別の IP アドレスが関係する場合、その関連する IP アドレスが送信側または受信側であったすべてのファイル転送
- 別の IP アドレスが関係する場合、その他方の IP アドレスが関係するエンドポイントベースのマルウェア イベント

強調表示されたデータ ポイントに関連付けられたすべての IP アドレスとタイムスタンプも強調表示されます。[イベント（Events）] テーブルの対応するイベントも強調表示されます。省略されたイベントがパスに含まれている場合、そのパス自体が点線で強調表示されます。省略されたイベントがパスを交差している場合がありますが、マップに表示されません。

ネットワーク ファイル トラジェクトリの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
マルウェア（AMP for Firepower） 任意（AMP for Endpoints）	マルウェア（AMP for Firepower） 任意（AMP for Endpoints）	任意（Any）	任意（Any）	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [ファイル（Files）] > [ネットワーク ファイル トラジェクトリ（Network File Trajectory）]を選択します。

ヒント また、ファイル情報を使用して、コンテキスト エクスプローラ、ダッシュボード、またはイベント ビューからファイルのトラジェクトリにアクセスできます。

ステップ 2 リストの [ファイル SHA 256（File SHA 256）] リンクをクリックします。

ステップ 3 オプションで、追跡するファイルの完全なSHA-256ハッシュ値、ホストIPアドレス、またはファイル名を検索フィールドに入力して、Enter を押します。

ヒント 1 つの結果だけが一致する場合、そのファイルの [ネットワーク ファイル トラジェクトリ（Network File Trajectory）] ページが表示されます。

ステップ 4 [サマリー情報（Summary Information）] セクションでは、以下を実行できます。

- ファイル リストにファイルを追加する：クリーン リストまたはカスタム検出リストにファイルを追加したり、ファイルを削除したりするには、編集アイコン（  ）をクリックします。
- ファイルをダウンロードする：ファイルをダウンロードするには、ファイルのダウンロードアイコン（  ）をクリックし、プロンプトが表示されたら、ファイルをダウンロードすることを確認します。ファイルをダウンロードできない場合、このアイコンは淡色表示されます。
- レポートする：脅威スコア アイコンをクリックすると、動的分析サマリー レポートが表示されます。
- 動的分析のために送信する：AMP クラウド アイコン（  ）をクリックすると、動的分析のためにファイルを送信できます。ファイルを送信できない場合、または AMP クラウドに接続できない場合は、このアイコンは淡色表示されます。
- アーカイブの内容を表示する：アーカイブ ファイルの内容に関する情報を表示するには、表示アイコン（  ）をクリックします。

- ファイル構成を表示する：ファイルの構成を表示するには、ファイル リストアイコン（  ）をクリックします。システムがファイル構成レポートを生成していなければ、このアイコンは淡色表示されます。
- 同じ脅威スコアでキャプチャされたファイルを表示する：脅威スコア リンクをクリックすると、その脅威スコアでキャプチャされたすべてのファイルが表示されます。

（注） シスコでは、有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先を保護するために必要な予防措置を行っていることを確認します。

ステップ 5 トラジェクトリ マップでは、以下を実行できます。

- 最初のインスタンスを見つける：IPアドレスをクリックして、IPアドレスが含まれる、最初に発生したファイル イベントを見つけます。これにより、そのデータ ポイントへのパスが強調表示され、その最初のファイル イベントに関連した仲介ファイル イベントと IP アドレスがあればそれも強調表示されます。[イベント（Events）] テーブルの対応するイベントも強調表示されます。そのデータ ポイントが現在表示されていない場合、表示されるまでマップがスクロールされます。
- 追跡する：データ ポイントをクリックすると、選択したデータ ポイントに関連するすべてのデータ ポイントが含まれるパスが強調表示されます。これにより、ネットワークを介してファイルの進捗を追跡できます。
- 非表示のイベントを表示する：矢印アイコンをクリックすると、[ファイル サマリー（File Summary）] イベント ビューに表示されていないすべてのイベントが表示されます。
- ファイルの一致イベントを表示する：イベント アイコン（  ）の上にポインタを合わせると、イベントのサマリー情報が表示されます。いずれかのイベント サマリー情報リンクをクリックすると、デフォルトの [ファイル イベント（File Events）] ワークフローの最初のページが新しいウィンドウで開き、そのファイル タイプのすべての余分のイベントが表示されます。[ファイル サマリー（File Summary）] イベント ビューが新しいウィンドウで表示され、クリックした条件値に一致するすべてのファイル イベントが表示されます。

ステップ 6 [イベント（Events）] テーブルでは、以下を実行できます。

- 強調表示：テーブル行を選択すると、マップ上のデータ ポイントが強調表示されます。選択したファイルイベントが現在表示されていない場合、表示されるまでマップがスクロールされます。
- ソート：カラム見出しをクリックすると、昇順または降順で情報をソートできます。

第 87 章

ホスト プロファイルの使用

ここでは、ホスト プロファイルの使用方法について説明します。

ホスト プロファイル

ホスト プロファイルは、システムが 1 つのホストについて収集したすべての情報の完全なビューを提供します。ホスト プロファイルにアクセスするには、以下のいずれかを実行します。

- 任意のネットワーク マップ ビューから選択します。

- モニタ対象ネットワークでホストの IP アドレスを含む任意のイベント ビューから選択します。

ホスト プロファイルは、ホスト名や MAC アドレスなど、検出されたホストやデバイスに関する基本的な情報を提供します。ライセンスやシステム設定によっては、ホスト プロファイルは次の情報を提供することもできます。

- ホスト上で実行中のオペレーティング システム
- ホスト上で実行中のサーバ
- ホスト上で実行中のクライアントと Web アプリケーション
- ホスト上で実行中のプロトコル
- ホスト上の侵害の兆候（IOC）タグ
- ホスト上の VLAN タグ
- ネットワーク上での過去 24 時間のユーザ アクティビティ
- ホストに関連付けられているホワイト リスト違反
- ホストの最新のマルウェア イベント
- ホストに関連付けられている脆弱性
- ホストの Nmap スキャン結果

プロファイルには、ホスト属性もリストされます。ホスト属性を使用して、ネットワーク環境にとって重要な方法でホストを分類することができます。例えば、以下を行うことができます。

- ホストが存在する建物を示すホスト属性を割り当てる
- ホストの重要度の属性を使用して、特定のホストのビジネス重要度を指定し、ホストの重要度に基づいて相関ポリシーとアラートを作成する

ホスト プロファイルで、そのホストに適用されている既存のホスト属性を表示し、そのホスト属性値を変更できます。

パッシブ侵入防御展開の一部としてアダプティブ プロファイルを使用している場合、ホスト上のオペレーティング システム、およびホストが実行しているサーバとクライアントのタイプに最も適合するように、システムがトラフィックを処理する方法を調整することができます。

オプションで、ホスト プロファイルから Nmap スキャンを実行し、ホスト プロファイルのサーバ情報とオペレーティング システムの情報を増やすことができます。Nmap スキャナはホストをアクティブに調査し、ホストを実行しているオペレーティング システムおよびサーバの情報を取得します。スキャンの結果は、ホストのオペレーティング システムおよびサーバアイデンティティのリストに追加されます。

ホスト プロファイルには、次の制限事項があります。

利用できないホスト

ホスト プロファイルは、ネットワーク上のすべてのホストでは使用できない可能性があります。考えられる原因は次のとおりです。

- タイムアウトしたため、ネットワーク マップからホストが削除された。
- ホスト ライセンスの制限に達した。
- ネットワーク検出ポリシーでモニタリングされないネットワーク セグメントに、ホストが存在している。

利用できない情報

ホスト プロファイルに表示される情報は、ホストのタイプ、および利用可能なホストの情報によって異なる可能性があります。

次に例を示します。

- 非 IP ベースのプロトコル（STP、SNAP、IPX など）を使用してシステムでホストを検出した場合、そのホストは MAC ホストとしてネットワーク マップに追加され、IP ホストに比べて使用できる情報はかなり少なくなります。
- システムは、ホストをエクスポートされた NetFlow レコードからネットワーク マップに追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違い，（1442 ページ） を参照）。

関連トピック

ホスト プロファイルの表示，（2057 ページ）

ホスト プロファイルの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

次の 2 つの選択肢があります。

- ネットワーク マップで、プロファイルを表示するホストの IP アドレスをドリル ダウンします。

- 任意のイベント ビューで、ホスト プロファイル アイコン（  ）をクリックするか、またはプロファイルを表示するホストのIPアドレスの隣にある、侵害されたホストアイコン（  ）をクリックします。

ホスト プロファイルの基本ホスト情報

各ホスト プロファイルは、検出されたホストまたは他のデバイスに関する基本情報を提供します。

次に、基本的なホスト プロファイルのフィールドについて説明します。

ドメイン（Domain）

ホストに関連付けられているドメイン。

IP アドレス

ホストに関連付けられているすべての IP アドレス（IPv4 と IPv6 の両方）。システムは、ホストに関連付けられている IP アドレスを検出し、サポートされている場合は、同じホストで使用される複数の IP アドレスをグループ化します。多くの場合、IPv6 ホストには、少なくとも 2 つの IPv6 アドレス（ローカルのみでルーティング可能なものと、グローバルにルーティング可能なもの）があり、その他に IPv4 アドレスを持っていることがあります。IPv4 専用ホストは、複数の IPv4 アドレスを持っていることがあります。

ホストプロファイルは、そのホストに関連付けられている、検出されたすべてのIPアドレスを一覧で示します。可能な場合は、ルーティング可能なホストIPアドレスに、フラグアイコン、およびアドレスに関連付けられている地理情報データを表す国コードも含まれています。

デフォルトでは最初の 3 つのアドレスだけが表示されることに注意してください。[すべて表示（Show All）] をクリックすると、ホストのすべてのアドレスが表示されます。

ホストネーム

ホストの完全修飾ドメイン名（わかる場合）。

NetBIOS 名（NetBIOS Name）

ホストの NetBIOS 名（使用できる場合）。Microsoft Windows ホストだけでなく、Macintosh、Linux、または NetBIOS を使用するように設定されているその他のプラットフォームに NetBIOS 名を指定できます。たとえば、Samba サーバとして設定されている Linux ホストに NetBIOS 名を指定します。

デバイス (ホップ数)（Device (Hops)）

次のいずれかを行います。

- ホストが存在しているネットワークの報告元のデバイス（ネットワーク検出ポリシーで定義）、または
- ホストをネットワーク マップへ追加する NetFlow データを処理したデバイス

デバイス名の後に、ホストを検出したデバイスとホスト自身の間のネットワーク ホップの数が丸括弧で囲まれて表示されます。複数のデバイスで対象のホストを参照できる場合は、報告元のデバイスが太字で表示されます。

このフィールドが空白の場合は、次のいずれかです。

- ホストがデバイスによってネットワーク マップに追加されたが、このデバイスは、ホストが存在しているネットワークに対してネットワーク検出ポリシーに定義されているとおりに明示的に監視していない。または、
- ホストの入力機能を使用してホストが追加されたが、Firepower システムによって検出されていない。

MAC アドレス（TTL）（MAC Addresses (TTL)）

ホストについて検出された 1 つ以上の MAC アドレスおよび関連付けられている NIC ベンダー。NIC のハードウェア ベンダーと現在の存続可能時間（TTL）値が括弧で囲まれて表示されます。MAC アドレスが太字で表示されている場合、その MAC アドレスは、ARP および DHCP トラフィックで検出されたホストの実際の MAC アドレスです。複数のデバイスが同じホストを検出した場合、Firepower Management Center には、どのデバイスがホストを報告したかに関係なく、ホストに関連付けられているすべての MAC アドレスと TTL 値が表示されます。

ルータのホストプロファイルは、通常、このリスト内でルーティングしているネットワーク セグメント内のホスト（IP アドレス）を示します。モニタリング対象のルータの IP アドレスは、多くの場合、モニタリングされるワークステーションとサーバのリストに表示されます。MAC アドレスの実際の IP アドレスは太字で表示されます。

ホスト タイプ（Host Type）

システムで検出されたデバイスのタイプ（ホスト、モバイル デバイス、ジェイルブレイクされたモバイル デバイス、ルータ、ブリッジ、NAT デバイス、またはロード バランサ）。

ネットワーク デバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol（CDP）メッセージの分析。ネットワークのデバイスおよびそれらのタイプ（シスコ デバイスのみ）を特定できます。
- スパニング ツリー プロトコル（STP）の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。
- モバイル デバイスを区別するためにシステムでは次の方法を使用します。

- モバイル デバイスのモバイル ブラウザからの HTTP トラフィックのユーザ エージェント文字列の分析
- 特定のモバイル アプリケーションの HTTP トラフィックのモニタリング

デバイスがネットワーク デバイスまたはモバイルデバイスとして識別されない場合は、ホストとして分類されます。

前回の検出（Last Seen）

ホストのいずれかの IP アドレスが最後に検出された日時。

現在のユーザ（Current User）

このホストに最後にログインしたユーザ。

既存の現在のユーザが権限のあるユーザでない場合、ホストにログインしている権限を持たないユーザは、現在のユーザとして登録されるだけであることに注意してください。

表示（View）

接続、検出、マルウェア、および侵入イベント データのビューへのリンク。このリンクは、そのイベントタイプのデフォルト ワークフローを使用し、ホストに関連するイベントを表示するように制限されています。可能な場合は、これらのイベントには、ホストに関連付けられているすべての IP アドレスが含まれます。

ホスト プロファイルのオペレーティング システム

システムは、ホストで生成されたトラフィック内のネットワークおよびアプリケーション スタックを分析したり、User Agent でレポートされたホスト データを分析することによって、ホスト上で稼動しているオペレーティング システムのアイデンティティをパッシブに検出します。システムでは、他のソース（Nmap スキャナ、ホストの入力機能によりインポートされたアプリケーションデータ）のオペレーティング システムの情報も照合します。どのアイデンティティを使用するかを判断する場合、システムは、各アイデンティティのソース（発生源）に割り当てられている優先度を考慮します。デフォルトでは、ユーザ入力が最も高い優先度を持ち、以降は高い順にアプリケーションまたはスキャナ ソース、検出されたアイデンティティ、となります。

システムでは、オペレーティング システムの具体的な定義ではなく、全般的な定義を提供することがあります。これは、トラフィックおよび他のアイデンティティ ソースで、対象のアイデンティティを詳しく調べるための十分な情報が提供されないためです。システムは、できるだけ詳しい定義を使用するために、ソースの情報を照合します。

オペレーティング システムは、ホストの脆弱性リスト、およびホストを対象とするイベントの影響の相関関係に影響するため、オペレーティング システムの特定の情報を手動で入力することもできます。また、オペレーティング システムに対して、サービス パックやアップデートなどの修正ファイルが適用されたことを示すことも、修正ファイルによって対処された脆弱性を無効にすることもできます。

たとえば、システムでホストのオペレーティング システムが Microsoft Windows 2003 であると特定されたが、実際にはホストが Microsoft Windows XP Professional および Service Pack 2 を実行していることがわかっている場合、オペレーティング システムのアイデンティティを実際のとおりに設定することができます。より具体的なオペレーティング システムのアイデンティティを設定すると、ホストの脆弱性のリストの精度が向上するため、対象のホストに対する影響の相関関係が、より限定的かつ正確になります。

システムでホストに対するオペレーティング システム情報が検出され、その情報が、アクティブなソースによって提供されている現行のオペレーティング システムのアイデンティティと競合している場合、アイデンティティの競合が発生します。実際にアイデンティティの競合が発生している場合、システムは脆弱性と影響の相関関係の両方のアイデンティティを使用します。

ネットワーク検出ポリシーを設定して、NetFlowエクスポータによってモニタされるホストのネットワークマップに検出データを追加することができます。ただし、オペレーティングシステムの ID を設定するためにホスト入力機能の使用を設定しない限り、これらのホストで使用可能なオペレーティング システム データはありません。

オペレーティング システムを実行しているホストが、有効なネットワーク検出ポリシーのコンプライアンスのホワイト リストに違反している場合、Firepower Management Center はオペレーティング システムの情報にホワイトリストの違反アイコン（）のマークを付けます。また、ジェイルブレイクされたモバイルデバイスが有効なホワイトリストに違反している場合、そのデバイスのオペレーティング システムの隣にアイコンが表示されます。

ホストのオペレーティング システムのアイデンティティに対して、カスタム表示文字列を設定できます。この表示文字列は、ホスト プロファイルで使用されます。

（注） あるホストについてオペレーティング システムの情報を変更すると、ホストのコンプライアンス、およびコンプライアンスのホワイト リストが変わる可能性があります。

ネットワーク デバイスに対するホストプロファイルでは、[オペレーティング システム（Operating Systems）] セクションのラベルが [システム（Systems）] に変わり、[ハードウェア（Hardware）] カラムが新しく表示されます。[システム（Systems）] の下にハードウェア プラットフォームの値が表示され場合、システムは、ネットワーク デバイスの背後で 1 つ以上のモバイル デバイスが検出されたことを示しています。モバイルデバイスはハードウェアプラットフォームの情報を持っていることも、持っていないこともありますが、モバイル デバイスではないシステムではハードウェア プラットフォーム情報は検出されないことに注意してください。

次に、ホストプロファイルで表示されるオペレーティング システムの情報フィールドについて説明します。

ハードウェア（Hardware）

モバイル デバイスのハードウェア プラットフォーム。

OS ベンダー/ベンダー（OS Vendor/Vendor）

オペレーティング システムのベンダー。

OS 製品/製品（OS Product/Product）

次の値のいずれかを指定します。

- すべてのソースから収集されたアイデンティティ データに基づいて、実行されている可能性が最も高いと判断されたオペレーティング システム。
- [Pending]：システムがオペレーティング システムをまだ識別しておらず、他に使用可能なアイデンティティ データがない場合。
- [unknown]：システムがオペレーティング システムを識別できず、オペレーティング システムに関して他に使用可能なアイデンティティ データがない場合。

（注） ホストのオペレーティング システムをシステムで検出できない場合には、ホスト オペレーティング システムの識別, （1454 ページ）を参照してください。

OS バージョン/バージョン（OS Version/Version）

オペレーティング システムのバージョン。ホストがジェイルブレイクされたモバイル デバイスの場合、バージョンの後に括弧で囲まれて `Jailbroken` と示されます。

ソース（Source）

次の値のいずれかを指定します。

- [ユーザ（User）]：user_name
- [アプリケーション（Application）]：app_name
- [スキャナ（Scanner）]：scanner_type（Nmap またはその他のスキャナ）
- Firepower

システムでは、オペレーティング システムのアイデンティティを判断するために、複数のソースのデータを統合することができます。

オペレーティング システム アイデンティティの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

検出された、またはホストに追加された特定のオペレーティング システムのアイデンティティを表示することができます。システムはソースの優先度を使用して、ホストに対する現行のアイデ

ンティティを判断します。アイデンティティのリストでは、現行のアイデンティティが太字で強調されます。

1 つのホストに対して複数のオペレーティング システムのアイデンティティが存在している場合のみ、[表示（View）] ボタンが有効になっていることに注意してください。

手順

ステップ 1 ホスト プロファイルの [オペレーティング システム（Operating System）] または [オペレーティング システムの競合（Operating System Conflicts）] セクションで [表示（View）] をクリックします。

ステップ 2 ホスト プロファイルのオペレーティング システム, （2060 ページ）の説明に従って情報を入力します。

ステップ 3 必要に応じて、オペレーティング システムのアイデンティティの横にある削除アイコン（）をクリックします。

（注） シスコが検出したオペレーティング システムのアイデンティティは削除できません。

該当する場合は、このシステムは [オペレーティング システムのアイデンティティ情報（Operating System Identity Information）] ポップアップ ウィンドウからアイデンティティを削除し、ホスト プロファイルのオペレーティング システムの現在のアイデンティティを更新します。

現在のオペレーティング システムのアイデンティティの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

Firepower システム Web インターフェイスを使用して、ホストに対する現行のオペレーティング システムのアイデンティティを設定できます。Web インターフェイスを介してアイデンティティを設定すると、他のすべてのアイデンティティ ソースが上書きされるため、このアイデンティティが、脆弱性の評価および影響の相関関係で使用されます。ただし、オペレーティング システムを編集した後で、ホストに対するオペレーティング システムのアイデンティティの競合がシステムで検出されると、オペレーティング システムの競合が発生します。競合が解決されるまで、両方のオペレーティング システムが現行のものであるとみなされます。

手順

ステップ 1 ホスト プロファイルの [オペレーティング システム（Operating System）] セクションで [編集（Edit）] をクリックします。

ステップ 2 ここでは次のオプションがあります。

- [OS 定義（OS Definition）] ドロップダウンリストから [現在の定義（Current Definition）] を選択して、ホスト入力によって現行のオペレーティング システムのアイデンティティを確認して、手順 6 に進みます。
- [OS 定義（OS Definition）] ドロップダウン リストから現行のオペレーティング システムのアイデンティティのバリエーションを選択し、手順 6 に進みます。
- [OS 定義（OS Definition）] ドロップダウンリストから [ユーザ定義（User-Defined）] を選択して、手順 3 に進みます。

ステップ 3 必要に応じて、[カスタム表示文字列を使用する（Use Custom Display String）] を選択し、[ベンダー文字列（Vendor String）]、[製品文字列（Product String）]、および [バージョン文字列（Version String）] フィールドに表示するカスタム文字列を変更します。

ステップ 4 必要に応じて、別のベンダーからのオペレーティング システムに変更するには、[ベンダー（Vendor）] と [製品（Product）] のドロップダウンリストから選択します。

ステップ 5 必要に応じて、オペレーティング システムの製品リリース レベルを設定するには、[メジャー（Major）]、[マイナー（Minor）]、[リビジョン（Revision）]、[ビルド（Build）]、[パッチ（Patch）]、および [拡張（Extension）] ドロップダウン リストから選択します。

ステップ 6 必要に応じて、オペレーティング システムに対して修正ファイルが適用されたことを示す場合は、[修正の設定（Configure Fixes）] をクリックします。

ステップ 7 ドロップダウン リストから適用可能な修正を選択し、[追加（Add）] をクリックします。

ステップ 8 必要に応じて、[パッチ（Patch）] および [拡張（Extension）] ドロップダウン リストを使用して、対象のパッチと拡張機能を追加します。

ステップ 9 [終了（Finish）] をクリックします。

関連トピック

オペレーティング システムのアイデンティティの競合, （2064 ページ）

オペレーティング システムのアイデンティティの競合

システムで検出された新しいアイデンティティと現行のアイデンティティが競合しており、そのアイデンティティが、スキャナやアプリケーション、ユーザなどのアクティブなソースによって提供されていた場合、オペレーティング システムのアイデンティティで競合が発生します。

ホストプロファイルでは、競合状態のオペレーティングシステムのアイデンティティのリストは太字で表示されます。

システムの Web インターフェイスを介して、アイデンティティの競合を解決し、ホストに対する現行のオペレーティング システムのアイデンティティを設定することができます。Web インターフェイスを介してアイデンティティを設定すると、他のすべてのアイデンティティ ソースが上書きされるため、このアイデンティティが、脆弱性の評価および影響の相関関係で使用されます。

関連トピック

ネットワーク検出アイデンティティ競合の解決の設定, （1568 ページ）

競合しているオペレーティング システムのアイデンティティの現行化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 ホスト プロファイルの [オペレーティング システム（Operating System）] セクションに移動します。

ステップ 2 次の 2 つの選択肢があります。

- ホストのオペレーティング システムとして設定するオペレーティング システムのアイデンティティの隣にある、[現行にする（Make Current）] をクリックします。
- アクティブなソースで、現行のアイデンティティとして使用しないアイデンティティが表示された場合は、使用しないアイデンティティを削除します。

オペレーティング システムのアイデンティティ競合の解決

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 ホストプロファイルの [オペレーティング システムの競合（Operating System Conflicts）] セクションにある [解決（Resolve）] をクリックします。

ステップ 2 次の選択肢があります。

- [OS 定義（OS Definition）] ドロップダウンリストから [現在の定義（Current Definition）] を選択して、ホスト入力によって現行のオペレーティング システムのアイデンティティを確認して、手順 6 に進みます。
- [OS 定義（OS Definition）] ドロップダウンリストから、競合しているオペレーティング システムのアイデンティティのいずれかのバリエーションを選択して、手順 6 に進みます。
- [OS 定義（OS Definition）] ドロップダウンリストから [ユーザ定義（User-Defined）] を選択して、手順 3 に進みます。

ステップ 3 必要に応じて、[カスタム表示文字列の使用（Use Custom Display String）] を選択して、表示するカスタム文字列を [ベンダー文字列（Vendor String）]、[製品文字列（Product String）]、および [バージョン文字列（Version String）] フィールドに入力します。

ステップ 4 必要に応じて、別のベンダーからのオペレーティング システムに変更するには、[ベンダー（Vendor）] と [製品（Product）] のドロップダウンリストから選択します。

ステップ 5 必要に応じて、オペレーティング システムの製品リリース レベルを設定するには、[メジャー（Major）]、[マイナー（Minor）]、[リビジョン（Revision）]、[ビルド（Build）]、[パッチ（Patch）] および [拡張（Extension）] ドロップダウンリストから選択します。

ステップ 6 必要に応じて、オペレーティング システムに対して修正ファイルが適用されたことを示す場合は、[修正の設定（Configure Fixes）] をクリックします。

ステップ 7 適用した修正ファイルを、修正ファイル リストに追加します。

ステップ 8 [終了（Finish）] をクリックします。

関連トピック

ネットワーク検出アイデンティティ競合の解決の設定, （1568 ページ）

ホスト プロファイルのサーバ

ホスト プロファイルのサーバ セクションでは、監視対象ネットワーク上のホストで検出されるか、エクスポートされた NetFlow レコードから追加されるか、スキャナまたはホスト入力機能のようなアクティブなソースを介して追加されるサーバを列挙します。

リストは 1 つのホストにつき最大 100 台のサーバを表示します。100 個の制限に達すると、ホストからサーバを削除するか、またはサーバがタイムアウトになるまで、いずれかのソースの新しいサーバ情報は、アクティブであってもパッシブであっても廃棄されます。

Nmap を使用してホストをスキャンすると、オープンな TCP ポート上で稼動している、以前に検出されなかったサーバの結果が Nmap によって Servers リストに追加されます。Nmap スキャンを実行した場合、またはNmapの結果をインポートした場合、ホストプロファイルに拡張可能な[スキャン結果（Scan Results）]セクションも表示され、Nmap スキャンによってホスト上で検出されたサーバ情報が示されます。さらに、ネットワーク マップからホストが削除されると、ホストのそのサーバに対する Nmap スキャンの結果は廃棄されます。

（注） システムは、ホストをエクスポートされた NetFlow レコードからネットワーク マップに追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違い, （1442 ページ） を参照）。

ホスト プロファイルでサーバを使用するためのプロセスは、ユーザがプロファイルにアクセスする方法によって異なります。

- ネットワーク マップを介したドリル ダウンによりホスト プロファイルにアクセスする場合は、サーバの名前が太字で強調されて、サーバの詳細が表示されます。ホストの他のサーバについて詳細を表示する場合は、対象のサーバ名の隣にある表示アイコン（[]）をクリックします。
- 他の方法でホスト プロファイルにアクセスする場合は、[サーバ（Servers）]セクションを展開し、詳細を表示するサーバの隣にある表示アイコン（[]）をクリックします。

（注） ホストが、有効な相関ポリシーにおけるコンプライアンスのホワイトリストに違反しているサーバを実行している場合、Firepower Management Center は非準拠サーバに、ホワイト リストの違反アイコン（[]）のマークを付けます。

次に、[Servers リスト（Servers list）] の列について説明します。

プロトコル

サーバが使用するプロトコルの名前。

[ポート（Port）]

サーバが実行されているポート。

アプリケーション プロトコル（Application Protocol）

次のいずれかになります。

- アプリケーション プロトコルの名前
- [保留中（pending）]：システムで、いずれかの理由のでアプリケーション プロトコルをポジティブまたはネガティブに識別できない場合

- [未知（unknown）]：既知のアプリケーション プロトコルのフィンガープリントに基づいてシステムでアプリケーションプロトコルを識別できない場合、または（対応するサーバは追加せずに、ポート情報での脆弱性を追加することにより）ホストの入力を介してサーバが追加された場合

アプリケーション プロトコルの名前にマウスを重ねると、タグが表示されます。

ベンダーおよびバージョン（Vendor and Version）

Firepowerシステム、Nmap、または他のアクティブなソースで識別されたベンダーとバージョン、またはホストの入力機能を介して取得したベンダーとバージョン。有効なソースで識別が行われなかった場合、フィールドは空白になります。

関連トピック

ホスト制限と検出イベント ロギング，（1511 ページ）
NetFlow データと管理対象デバイス データの違い，（1442 ページ）
アプリケーション ディテクタの基本，（1509 ページ）

ホスト プロファイルのサーバの詳細

Firepower Management Centerは、1つのサーバについてパッシブに検出されるアイデンティティを最大16個表示します。パッシブな検出ソースには、ネットワーク検出データおよびNetFlowレコードが含まれます。システムで、このサーバの複数のベンダーまたはバージョンを検出した場合、サーバは複数のパッシブなアイデンティティを持つことができます。たとえば、Webサーバが、サーバ ソフトウェアと同じバージョンを実行していない場合、管理対象デバイスとWebサーバ ファーム間にロード バランサがあると、HTTPに対してシステムが複数のパッシブ アイデンティティを識別することがあります。Firepower Management Centerは、ユーザ入力、スキャナ、その他のアプリケーションなど、アクティブなソースからのサーバ アイデンティティの数を制限することはありません。

Firepower Management Centerは現行のアイデンティティを太字で表示します。システムでは、1つのホストに対する脆弱性の割り当て、影響の評価、ホスト プロファイルの証明書およびコンプライアンス ホワイトリストに対して記載された相関ルールの評価など、いくつかの目的のためにサーバの現行のアイデンティティを使用します。

サーバの詳細には、選択されたサーバについて知られている、更新済みのサブサーバ情報が表示されることもあります。

サーバの詳細にサーバのバナーが表示されることもあります。これは、ホスト プロファイルからサーバを表示したときに、サーバの詳細の下に表示されます。サーバのバナーは、サーバを識別するのに役立つサーバに関する追加情報を提供します。攻撃者がサーバのバナー文字列を意図的に変更した場合、システムは誤ったアイデンティティが示されたサーバを識別または検出できません。サーバのバナーには、そのサーバについて検出された最初のパケットの最初の256文字が表示されます。この情報は、サーバがシステムによって最初に検出されたときに一度だけ収集されます。バナーの内容は2列で表示されます。左側の列は16進表記で示され、右側の列は対応するASCII表記で示されます。

（注） サーバのバナーを表示するには、ネットワーク検出ポリシーで [バナーのキャプチャ（Capture Banners）] チェックボックスを有効にする必要があります。このオプションはデフォルトでは無効になっています。

ホスト プロファイルのサーバの詳細セクションには、次の情報が含まれています。

プロトコル

サーバが使用するプロトコルの名前。

[ポート（Port）]

サーバが実行されているポート。

ヒット数（Hits）

Firepower システムの管理対象デバイスまたは Nmap スキャナによってサーバが検出された回数。ホストの入力によってインポートされたサーバについては、システムがそのサーバについてトラフィックを検出しない場合、検出回数は 0 になります。

前回の使用（Last Used）

サーバが最後に検出された日時。システムで対象のサーバについて新しいトラフィックを検出しない場合、ホスト入力のデータが最後に使用された時間は、データの最初のインポート時間を反映しています。ホストの入力機能を介してインポートされたスキャナおよびアプリケーションのデータは、Firepower Management Center の設定に応じてタイム アウトしますが、Management Center の Web インターフェイスを介したユーザ入力の場合はタイム アウトしません。

アプリケーション プロトコル（Application Protocol）

既知の場合、サーバが使用するアプリケーション プロトコルの名前。

ベンダー（Vendor）

サーバのベンダー。ベンダーがわからない場合、このフィールドは表示されません。

バージョン（Version）

サーバのバージョン。バージョンがわからない場合、このフィールドは表示されません。

ソース（Source）

次の値のいずれかを指定します。

- [ユーザ（User）]：user_name
- [アプリケーション（Application）]：app_name
- [スキャナ（Scanner）]：scanner_type（Nmap またはその他のスキャナ）
- Firepower システムで検出されたアプリケーションの場合、`Firepower`、`Firepower Port Match`、または `Firepower Pattern Match`
- NetFlow レコードからネットワーク マップに追加されたサーバの場合、`NetFlow`

システムでは、サーバのアイデンティティを判断するために、複数のソースのデータを統合することができます。

関連トピック

アプリケーションおよびオペレーティング システムの現在の ID, （1438 ページ）

サーバに関する詳細情報の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ホストプロファイルの[サーバ（Servers）]セクションで、サーバの横にある表示アイコン（  ）をクリックします。

サーバのアイデンティティの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

ホスト上のサーバのアイデンティティ設定を手動で更新し、修正ファイルによって対処された脆弱性を削除するために、ホストに適用した何らかの修正ファイルを設定することができます。サーバのアイデンティティを削除することもできます。

アイデンティティを削除した場合、削除したアイデンティティが唯一のアイデンティティであっても、サーバは削除されません。アイデンティティを削除すると、[サーバの詳細（Server Detail）] ポップアップ ウィンドウからアイデンティティが削除されます。可能な場合は、ホストプロファイルでそのサーバの現行のアイデンティティを更新します。

シスコ管理対象デバイスによって追加されたサーバのアイデンティティは、編集または削除できません。

手順

ステップ 1 ホスト プロファイルの [サーバ（Servers）] セクションに移動します。

ステップ 2 [表示（View）] をクリックし、[サーバの詳細（Server Detail）] ポップアップ ウィンドウを開きます。

ステップ 3 サーバのアイデンティティを削除するには、削除するサーバのアイデンティティの横にある削除アイコン（）をクリックします。

ステップ 4 サーバのアイデンティティを変更するには、サーバリストでサーバの横にある編集アイコン（）をクリックします。

ステップ 5 次の 2 つの選択肢があります。

- [サーバ タイプの選択（Select Server Type）] ドロップダウン リストから現行の定義を選択します。
- [サーバ タイプの選択（Select Server Type）] ドロップダウン リストからサーバのタイプを選択します。

ステップ 6 オプションで対象のサーバ タイプのベンダーと製品のみを表示するには、[サーバ タイプで制限（Restrict by Server Type）] チェックボックスをオンにします。

ステップ 7 オプションでサーバの名前とバージョンをカスタマイズするには、[カスタム表示文字列の使用（Use Custom Display String）] を選択し、[ベンダー文字列（Vendor String）] と [バージョン文字列（Version String）] に入力します。

ステップ 8 [製品マッピング（Product Mappings）] セクションで、使用するオペレーティング システム、製品、およびバージョンを選択します。

例：
たとえば、サーバを Red Hat Linux 9 にマップする場合は、ベンダーとして [Redhat, Inc.] を、製品として [Redhat Linux] を選択し、バージョンとして [9] を選択します。

ステップ 9 サーバの修正が適用されていることを示す場合は、[修正の設定（Configure Fixes）] をクリックして、そのサーバに適用するパッチを修正リストに追加します。

ステップ 10 [終了（Finish）] をクリックします。

サーバ アイデンティティの競合の解決

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

アプリケーションやスキャナなどのアクティブなソースが、サーバのアイデンティティ データをホストへ追加したときに、サーバ アイデンティティの競合が発生します。その後で、システムはサーバ アイデンティティの競合を示しているポートのトラフィックを検出します。

手順

ステップ 1 ホスト プロファイルで、[サーバ（Servers）] セクションに移動します。

ステップ 2 サーバの横にある解決アイコンをクリックします。

ステップ 3 [サーバ タイプの選択（Select Server Type）] ドロップダウンリストからサーバのタイプを選択します。

ステップ 4 必要に応じて、対象のサーバ タイプのベンダーと製品のみを表示する場合は、[サーバ タイプ別に制限（Restrict by Server Type）] チェックボックスをオンにします。

ステップ 5 必要に応じて、サーバの名前とバージョンをカスタマイズする場合は、[カスタム表示文字列の使用（Use Custom Display String）] を選択して、[ベンダー文字列（Vendor String）] と [バージョン文字列（Version String）] を入力します。

ステップ 6 [製品マッピング（Product Mappings）] セクションで、使用するオペレーティング システム、製品、およびバージョンを選択します。

例：
たとえば、サーバを Red Hat Linux 9 にマップする場合は、ベンダーとして [Redhat, Inc.] を、製品として [Redhat Linux] を選択し、バージョンとして [9] を選択します。

ステップ 7 サーバの修正が適用されていることを示す場合は、[修正の設定（Configure Fixes）] をクリックして、そのサーバに適用するパッチを修正リストに追加します。

ステップ 8 [終了（Finish）] をクリックします。

関連トピック

ネットワーク検出アイデンティティ競合の解決の設定, （1568 ページ）

ホスト プロファイルの Web アプリケーション

ホスト プロファイルの [Web アプリケーション（Web Application）] セクションには、ネットワーク内のホスト上で動作していることをシステムが識別したクライアントと Web アプリケーションが表示されます。システムでは、パッシブ検出ソースとアクティブ検出ソースの両方から取得されるクライアントと Web アプリケーションの情報を識別できます。ただし、NetFlow レコードから追加されたホストに関する情報は一部しか取得することができません。

このセクションには、ホスト上で検出されたアプリケーションの製品とバージョン、使用できるクライアントまたは Web アプリケーションの情報、アプリケーションが最後に使用中であると検出された時間などの詳細情報が表示されます。

ホスト上で稼動している最大 16 個のクライアントが、このセクションに表示されます。16 個の制限に達すると、ユーザがホストからクライアント アプリケーションを削除するか、または非アクティブである（クライアントがタイムアウトしている）ためにシステムによってホスト プロファイルからクライアントが削除されるまで、新しいクライアント情報は、どのソースのものであるか、アクティブかパッシブかにかかわらず、廃棄されます。

また、検出されたそれぞれの Web ブラウザについては、アクセスされた最初の 100 個の Web アプリケーションが表示されます。この制限に達すると、ブラウザに関連付けられている新しい Web アプリケーションは、どのソースのものであるか、アクティブかパッシブかにかかわらず、次の条件を満たすまで廃棄されます。

- Web ブラウザのクライアント アプリケーションがタイムアウトになる、または
- ユーザが、Web アプリケーションに関連付けられているアプリケーション情報をホスト プロファイルから削除する

ホストが、有効な相関ポリシーにおけるコンプライアンスのホワイト リストに違反しているアプリケーションを実行している場合、Firepower Management Center は非準拠アプリケーションに、ホワイト リストの違反アイコン（  ）のマークを付けます。

ヒント ホスト上の特定のアプリケーションに関連付けられている接続イベントを分析するには、アプリケーションの隣にあるイベント アイコン（  ）をクリックします。接続イベントに対する優先ワークフロー最初のページが表示され、ホストの IP アドレスの他、アプリケーションのタイプ、プロトコル、およびバージョンで制約されて接続イベントが示されます。接続イベントに対する優先ワークフローがない場合、ワークフローを選択する必要があります。

次に、ホスト プロファイルに表示されるアプリケーション情報について説明します。

アプリケーション プロトコル

アプリケーション（HTTP ブラウザ、DNS クライアントなど）で使用されるアプリケーション プロトコルを表示します。

クライアント（Client）

ペイロードから派生したクライアント情報。この情報は、Firepowerシステムが識別するか、Nmapがキャプチャするか、またはホスト入力機能によって取得されます。有効なソースで識別が行われなかった場合、フィールドは空白になります。

バージョン（Version）

クライアントのバージョンが表示されます。

Web アプリケーション

Web ブラウザの場合は、http トラフィックでシステムによって検出されたコンテンツ。Web アプリケーションの情報は、Firepower システムによって識別された、Nmap によってキャプチャされた、他のアクティブなソースによって取得された、またはホストの入力機能を介して取得された特定のタイプのコンテンツ（WMV や QuickTime など）を表します。有効なソースで識別が行われなかった場合、フィールドは空白になります。

ホスト プロファイルからの Web アプリケーションの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

ホストプロファイルからアプリケーションを削除して、ホスト上で稼動していないことがわかっているアプリケーションを削除することができます。ホストからアプリケーションを削除すると、そのホストにホワイト リストのコンプライアンスが適用されることがあります。

（注） システムでアプリケーションが再検出されると、アプリケーションはネットワーク マップおよびホスト プロファイルに再度追加されます。

手順

ステップ 1 ホスト プロファイルで、[アプリケーション（Applications）] セクションに移動します。

ステップ 2 削除するアプリケーションの横にある削除アイコン（）をクリックします。

ホスト プロファイルのホスト プロトコル

各ホストプロファイルには、ホストに関連付けられているネットワーク トラフィックで検出されたプロトコルに関する情報が含まれています。この情報には次のものが含まれます。

プロトコル

ホストが使用するプロトコルの名前。

層（Layer）

プロトコルを実行しているネットワーク層（ネットワークまたはトランスポート）。

ホストプロファイルに表示されているプロトコルが、有効な相関ポリシーのコンプライアンス ホワイト リストに違反する場合、Firepower Management Center は非準拠プロトコルに、ホワイト リストの違反アイコン（）のマークを付けます。

ホスト プロファイルに、ホスト上で実行していないことがわかっているプロトコルがリストされている場合は、これらのプロトコルを削除できます。ホストからプロトコルを削除すると、ホストがコンプライアンス ホワイト リストに準拠する可能性があります。

（注） システムでプロトコルが再検出されると、プロトコルはネットワーク マップおよびホスト プロファイルに再度追加されます。

ホスト プロファイルからのプロトコルの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 ホスト プロファイルの [プロトコル（Protocols）] セクションに移動します。

ステップ 2 削除するプロトコルの横にある削除アイコン（）をクリックします。

ホスト プロファイル内の侵害の兆候

Firepowerシステムは、さまざまなタイプのデータ（侵入イベント、セキュリティインテリジェンス、接続イベントおよびファイルまたはマルウェア イベント）を関連付け、モニタ対象ネットワーク上のホストが悪意のある手段によって侵害された可能性があるかどうかを判断します。イベント データの特定の組み合わせと頻度が、影響を受けるホストの侵害の兆候（IOC）タグをトリガーします。

ホスト プロファイルの [侵害の兆候（Indications of Compromise）] セクションには、ホストのすべての侵害の兆候のタグが表示されます。

侵害の兆候にタグを付けるようにシステムを構成するには、侵害の兆候ルールの有効化, （1570 ページ）を参照してください。

侵害の兆候についての作業の詳細については、侵害の兆候データ, （2119 ページ）とそのトピックのサブトピックを参照してください。

関連トピック

侵害の兆候, （1569 ページ）

ホスト プロファイルの VLAN タグ

ホストが仮想 LAN（VLAN）のメンバである場合、ホスト プロファイルの [VLAN タグ（VLAN Tag）] セクションが表示されます。

物理ネットワーク機器は、多くの場合にVLANを使用して、さまざまなネットワーク ブロックから論理ネットワーク セグメントを作成します。システムは802.1q VLANタグを検出し、それぞれに対して以下の情報を表示します。

- [VLAN ID] は、ホストがメンバである VLAN を表します。これは、802.1q VLAN の場合、0 ～ 4095 の任意の整数となります。
- [タイプ（Type）] は、VLAN タグが含まれている、カプセル化されたパケットを表します。値は [イーサネット（Ethernet）] または [トークン リング（Token Ring）] となります。
- [優先順位（Priority）] は、VLAN タグの優先度を表します。これは 0～7 の任意の整数で、7 が最も高い優先度です。

VLAN タグがパケット内でネスト構造になっている場合、システムは最も内側の VLAN タグを処理し、Firepower Management Center は最も内側の VLAN タグを表示します。システムは、ARP および DHCP トラフィックを通じて識別される MAC アドレスのみの VLAN タグ情報を収集し、これらのタグを表示します。

たとえば全体がプリンタで構成されている VLAN があり、システムがこの VLAN で Microsoft Windows 2000 のオペレーティング システムを検出した場合などは、VLAN タグ情報が有用です。VLAN 情報により、システムは正確性の高いネットワーク マップを生成できるようになります。

ホスト プロファイル内のユーザ履歴

ホストプロファイルのユーザ履歴の部分には、過去24時間のユーザアクティビティがグラフィック表示されます。一般的なユーザは夕方にログオフし、また他のユーザとホストのリソースを共有することがあります。電子メールのチェックなどの目的で行われる定期的なログインの要求は、短い標準の棒で示されます。ユーザのアイデンティティリストは棒グラフで提示され、ユーザログインが検出されたタイミングを示します。権限のないログインの場合は、棒グラフがグレーになっていることに注意してください。

システムは、ホストに対する権限のないユーザログインを、そのホストのIPアドレスに関連付けるため、そのユーザはそのホストのユーザ履歴に表示されます。ただし、権限のあるユーザ ログインが同じホストで検出された場合、その権限のあるユーザ ログインに関連付けられているユーザが、そのホストのIPアドレスとの関連付けを引き継ぐため、新しい権限のないユーザログインがそのホストのIPアドレスとのそのユーザの関連付けを壊すことはありません。ネットワーク検出ポリシーで、失敗したログインのキャプチャを設定した場合、リストにはこのホストへのログインに失敗したユーザが含まれます。

ホスト プロファイル内のホスト属性

ホスト属性を使用して、ネットワーク環境にとって重要な方法でホストを分類することができます。Firepower システムには以下の 3 つのタイプの属性があります。

- 定義済みホスト属性
- ホワイトリスト ホスト属性
- ユーザ定義ホスト属性

定義済みホスト属性を設定後、またはユーザ定義ホスト属性を作成後は、ホスト属性の値を割り当てる必要があります。

（注） ホスト属性は、どのドメイン レベルでも定義できます。現在のドメインと先祖ドメインで作成されたホスト属性を割り当てることができます。

定義済みホスト属性

Firepower Management Center には、2 つの定義済みホスト変数が用意されています。

ホストの重要度（Host Criticality）

特定のホストの業務の重要性を指定し、ホストの重要性に応じて相関ポリシーの応答を調整するには、この属性を使用します。たとえば、業務にとって組織のメール サーバが一般的なユーザ ワークステーションよりも重要であるとみなしている場合は、メール サーバと業務に重要なその他のデバイスに[高（High）]の値を割り当て、他のホストには[中（Medium）]または[低（Low）]の値を割り当てることができます。その上で、影響を受けるホストの重要度に基づいて異なるアラートを起動する相関ポリシーを作成できます。

注記（Notes）

他のアナリストに確認してもらいたいホストに関する情報を記録するには、このホスト固有の属性を使用します。たとえば、ネットワーク上のコンピュータに、パッチが適用されていない古いバージョンのテスト用オペレーティング システムが搭載されている場合、[注記（Notes）]属性を使用して、システムは意図的にパッチを適用していないことを明示できます。

ホワイト リストのホスト属性

ユーザが作成するそれぞれのコンプライアンス ホワイト リストによって、そのホワイト リストと同じ名前でホスト属性が自動的に作成されます。ホワイト リストのホスト属性に設定可能な値は、次のとおりです。

- 準拠（Compliant）：ホワイト リストに準拠しているホストを識別します。
- 非準拠（Non-Compliant）：ホワイト リストに違反しているホストを識別します。
- 未評価（Not Evaluated）：ホワイトリストの有効な対象ではないホスト、または何らかの理由で評価されていないホストを識別します。

ホワイトリストのホスト属性の値を編集したり、ホワイトリストのホスト属性を削除したりすることはできません。

ユーザ定義のホスト属性

定義済みのホスト属性またはホワイトリストのホスト属性で使用されている基準と異なる基準を使用してホストを識別する場合、ユーザ定義のホスト属性を作成することができます。例えば、以下を行うことができます。

- ホストに対してファシリティ コード、市町村、部屋番号などの物理的なロケーション ID を割り当てます。
- 特定のホストを担当するシステム管理者を示す担当者 ID を割り当てます。ホストに関連する問題が検出された場合、相関ルールとポリシーを作成して、適切なシステム管理者にアラートを送信することができます。

- ホストのIPアドレスに基づいて、事前定義されたリストからホストへ自動的に値を割り当てます。この機能は、ネットワーク上にホストが初めて表示されたときに、その新しいホストへ値を割り当てるために役立ちます。

ユーザ定義のホスト属性は、ホスト プロファイルのページに表示されます。ここでホストごとに値を割り当てることができます。次のことも実行できます。

- 相関ポリシーと検索でホスト属性を使用します。
- イベントのホスト属性テーブル ビューで属性を表示して、それに基づいてレポートを生成します。

ユーザ定義のホスト属性として、次のタイプのいずれか 1 つを使用できます。

テキスト（Text）

ホストに対してテキスト文字列を手動で割り当てることができます。

整数（Integer）

正の整数の範囲の最初の数と最後の数を指定してから、ホストに対してこれらの数の 1 つを手動で割り当てることができます。

リスト（List）

文字列値のリストを作成してから、ホストに対してこの値のいずれかを割り当てることができます。また、ホストの IP アドレスに基づいて、ホストに対して値を自動的に割り当てることもできます。

複数の IP アドレスを持つホストの 1 つの IP アドレスに基づいて値を自動的に割り当てると、これらの値は、ホストに関連付けられているすべてのアドレスに適用されます。[ホスト属性（Host Attributes）] テーブルを表示する場合は、このことに留意してください。

リストの値を自動的に割り当てる場合は、リテラルの IP アドレスではなくネットワーク オブジェクトの使用を検討してください。このアプローチによって保守容易性を向上でき、特にマルチドメイン展開で有効です。これは、マルチドメイン展開でオーバーライドが有効になったオブジェクトを使用すると、子孫ドメインの管理者が先祖ドメインの設定を自分のローカル環境に合わせて調整できるためです。マルチドメイン展開では、子孫ドメインで重複した IP アドレスを使用している場合に意図しないホストに一致するのを避けるために、先祖ドメイン レベルで自動割り当てリストを定義する場合は注意してください。

URL

ホストに対して手動で URL の値を割り当てることができます。

ユーザ定義のホスト属性を削除すると、その属性が使用されているすべてのホスト プロファイルから削除されます。

テキストまたは URL ベースのホスト属性の作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 [分析（Analysis）] > [ホスト（Hosts）] > [ホスト属性（Host Attributes）]を選択します。
ステップ 2 [ホスト属性管理（Host Attribute Management）] をクリックします。
ステップ 3 [属性の作成（Create Attribute）] をクリックします。
ステップ 4 名前を入力します。
ステップ 5 作成する属性の [タイプ（Type）] を選択します。 ユーザ定義のホスト属性, （2078 ページ）
ステップ 6 [保存（Save）] をクリックします。

整数ベースのホスト属性の作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

整数ベースのホスト属性を定義する場合は、その属性が受け入れる数値の範囲を指定する必要があります。

手順

ステップ 1 [分析（Analysis）] > [ホスト（Hosts）] > [ホスト属性（Host Attributes）]を選択します。

ステップ 2 [ホスト属性管理（Host Attribute Management）] をクリックします。

ステップ 3 [属性の作成（Create Attribute）] をクリックします。

ステップ 4 名前を入力します。

ステップ 5 ユーザ定義のホスト属性, （2078 ページ）の説明に従って、作成する属性の [タイプ（Type）] を選択します。

ステップ 6 [最小（Min）] フィールドに、ホストに対して割り当てることができる範囲の最小の整数値を入力します。

ステップ 7 [最大（Max）] フィールドに、ホストに対して割り当てることができる範囲の最大の整数値を入力します。

ステップ 8 [保存（Save）] をクリックします。

リストベースのホスト属性の作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

リストベースのホストの属性を定義する場合は、リストに対してそれぞれの値を提供する必要があります。これらの値には、英数字、スペース、および記号を含めることができます。

手順

ステップ 1 [分析（Analysis）] > [ホスト（Hosts）] > [ホスト属性（Host Attributes）]を選択します。

ステップ 2 [ホスト属性管理（Host Attribute Management）] をクリックします。

ステップ 3 [属性の作成（Create Attribute）] をクリックします。

ステップ 4 名前を入力します。

ステップ 5 ユーザ定義のホスト属性, （2078 ページ）の説明に従って、作成する属性の [タイプ（Type）] を選択します。

ステップ 6 リストに値を追加するには、[値の追加（Add Value）] をクリックします。

ステップ 7 [名前（Name）] フィールドに、追加する最初の値を入力します。

ステップ 8 オプションで、ホストに追加した属性値を自動で割り当てるには、[ネットワークを追加（Add Networks）] をクリックします。

ステップ 9 [値（Value）] ドロップダウン リストから、追加した値を選択します。

ステップ 10 [IP アドレス（IP Address）] および [ネットマスク（Netmask）] フィールドに、この値を自動的に割り当てる IP アドレスのブロックを表す IP アドレスとネットワーク マスク（IPv4）を入力します。

ステップ 11 リストにさらに値を追加して、IP アドレス ブロックの範囲内の新しいホストにこれらの値を自動的に割り当てるには、手順 6 ～ 10 を繰り返します。

ステップ 12 [保存（Save）] をクリックします。

ホスト属性値の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

事前定義またはユーザ定義のホスト属性に値を設定できます。システムによって生成されたホワイト リストのホスト属性値は設定できません。

手順

ステップ 1 変更するホスト プロファイルを開きます。

ステップ 2 [属性（Attributes）] セクションで、[属性の編集（Edit Attributes）] をクリックします。

ステップ 3 必要に応じて、属性を更新します。

ステップ 4 [保存（Save）] をクリックします。

ホスト プロファイル内のホワイト リスト違反

コンプライアンス ホワイト リスト（またはホワイト リスト）は一連の基準であり、ユーザはこれを使用して、特定のサブネット上での実行が許可されるオペレーティング システム、アプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルを指定することができます。

ホワイトリストをアクティブな相関ポリシーに追加した場合に、システムでホワイトリストに違反しているホストが検出されると、Firepower Management Center はホワイトリストのイベント（相関イベントの特別な種類）をデータベースに記録します。これらのホワイトリストイベントはそれぞれホワイト リスト違反に関連付けられます。これには、特定のホストがどのようにホワイト リストに違反しているか、および違反している理由が含まれています。あるホストが 1 つ以上のホワイト リストに違反している場合、ホスト プロファイルにおいて、2 つの方法でこれらの違反を参照することができます。

最初に、ホストに関連付けられている個々のホワイトリストのすべての違反が、ホストプロファイルに一覧表示されます。

ホストプロファイルに一覧表示されるホワイトリストの違反に関する情報は、次のとおりです。

タイプ（Type）

違反のタイプ（つまり、違反がオペレーティング システム、アプリケーション、サーバ、またはプロトコルの非準拠の結果として生じたかどうか）。

理由（Reason）

違反についての特別な理由。たとえば、Microsoft Windows のホストのみを許可するホワイトリストがある場合、ホストプロファイルには、ホストで稼動している現行のオペレーティング システム（`Linux Linux 2.4、2.6` など）が表示されます。

ホワイト リスト（White List）

違反に関連付けられているホワイト リストの名前。

次に、オペレーティング システム、アプリケーション、プロトコル、およびサーバに関連付けられているセクションで、Firepower Management Center が、非準拠の要素にホワイト リスト違反のアイコン（❗）のマークを付けます。たとえば、Microsoft Windows ホストのみを許可するホワイ

トリストでは、ホスト プロファイルで、ホストのオペレーティング システム情報の隣にホワイトリスト違反のアイコンが表示されます。

（注） ホストのプロファイルを使用すると、コンプライアンス ホワイト リストの共有ホスト プロファイルを作成することができます。

共有ホワイト リスト ホスト プロファイルの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

コンプライアンス ホワイト リストに対する共有ホスト プロファイルは、複数のホワイト リストをまたがるターゲットホスト上で実行を許可されるオペレーティングシステム、アプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルを指定します。つまり、複数のホワイト リストを作成するが、同じホスト プロファイルを使用して複数のホワイト リストで特定のオペレーティングシステムを実行するホストを評価する場合は、共有のホストプロファイルを使用します。

既知の IP アドレスを持つ任意のホストのホスト プロファイルを使用して、コンプライアンス ホワイトリストで使用できる共有ホストプロファイルを作成することができます。ただし、システムでホストのオペレーティングシステムをまだ特定していない場合は、個々のホストのホストプロファイルに基づいて共有ホスト プロファイルを作成することはできないことに注意してください。

手順

ステップ 1 ホスト プロファイルで、[ホワイト リスト プロファイルの生成（Generate White List Profile）] をクリックします。

ステップ 2 特別なニーズに応じて、共有ホスト プロファイルを変更し、保存します。

関連トピック

ホワイト リスト ホスト プロファイルの作成, （1622 ページ）

ホスト プロファイルでのマルウェア検出

[最後に検出されたマルウェア（Most Recent Malware Detections）] セクションには、ホストがマルウェア ファイルを送信または受信した、最近のマルウェア イベントが最大 100 個表示されます。

ホスト プロファイルは、ネットワークベース（AMP for Firepower）とエンドポイントベース（エンドポイント向け AMP）のマルウェア イベントを一覧で示します。

ファイルが遡ってマルウェアと識別されたファイル イベントにホストが関係している場合、ファイルが送信された元のイベントは、マルウェアの特定が行われた後で、マルウェアの検出リストに表示されます。マルウェアとして識別されたファイルが、マルウェアではないと遡って判断された場合、そのファイルに関連するマルウェア イベントはリストには表示されなくなります。たとえば、ファイルに `Malware` の性質が含まれており、その処理が `Clean` に変わった場合、そのファイルのイベントは、ホスト プロファイル上のマルウェア検出リストから削除されます。

ホストプロファイルでマルウェアの検出を表示する場合は、イベント ビューアで、そのホストのマルウェアイベントを表示できます。イベントを表示するには、マルウェアのアイコン（  ）をクリックします。

次に、ホスト プロファイルの [最後に検出されたマルウェア（Most Recent Malware Detections）] セクションのカラムについて説明します。

時刻（Time）

イベントが生成された日時。

ファイルがマルウェアであると遡って特定されたイベントでは、これはマルウェアが特定された時刻ではなく、元のイベントの時刻であることに注意してください。

ホストの役割（Host Role）

検出されたマルウェアの伝送におけるホストの役割（送信者または受信者）。エンドポイントベースのマルウェア イベントの場合は、ホストは常に受信者であることに注意してください。

脅威名（Threat Name）

検出されたマルウェアの名前。

ファイル名（File Name）

マルウェア ファイルの名前。

ファイル タイプ（File Type）

ファイルのタイプ（`PDF` や `MSEXE` など）。

ホスト プロファイルの脆弱性

ホスト プロファイルの [脆弱性（Vulnerabilities）] セクションには、ホストに影響を与える脆弱性が示されます。これらの脆弱性は、システムがホスト上で検出したオペレーティング システム、サーバ、およびアプリケーションに基づきます。

ホストのオペレーティング システムのアイデンティティ、またはホスト上のアプリケーション プロトコルのアイデンティティのいずれかで、アイデンティティの競合が発生している場合、システムは、競合が解決するまで両方のアイデンティティに対して脆弱性を表示します。

NetFlow データからネットワーク マップに追加されたホストに使用可能なオペレーティング システムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクト レベル 1：赤）インパクト レベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティング システム ID を手動で設定します。

サーバのベンダーおよびバージョンの情報は、ほとんどの場合はトラフィックに含まれていません。デフォルトでは、システムはこのようなトラフィックの送信側および受信側に対して、関連付けられている脆弱性をマップしません。ただし、ベンダーまたはバージョンの情報を持たない特定のアプリケーション プロトコルに対して脆弱性をマップするよう、システムを設定することができます。

ホストの入力機能を使用して、ネットワーク上のホストにサードパーティの脆弱性情報を追加すると、追加の [脆弱性（Vulnerabilities）] セクションが表示されます。たとえば QualysGuard Scanner から脆弱性をインポートすると、ホスト プロファイルには [QualysGuard 脆弱性（QualysGuard Vulnerabilities）] セクションが含まれます。サードパーティの脆弱性の場合は、ホスト プロファイルの対応する [脆弱性（Vulnerabilities）] セクションの情報は、ホストの入力機能を使用して脆弱性データをインポートしたときに提供した情報に制限されます。

サードパーティの脆弱性をオペレーティング システムおよびアプリケーション プロトコルと関連付けることはできますが、クライアントに関連付けることはできません。サードパーティの脆弱性のインポートについては、『*Firepower System Host Input API Guide*』を参照してください。

次に、ホスト プロファイルの [脆弱性（Vulnerabilities）] セクションのカラムについて説明します。

[名前（Name）]

脆弱性の名前。

[リモート（Remote）]

脆弱性がリモートで不正利用される可能性があるかどうかを示します。この列が空白の場合、脆弱性の定義にはこの情報は含まれていません。

コンポーネント

脆弱性に関連付けられているオペレーティング システム、アプリケーション プロトコル、またはクライアントの名前。

[ポート（Port）]

ポート番号（脆弱性が、特定のポート上で実行されているアプリケーション プロトコルに関連付けられている場合）。

関連トピック

脆弱性データのフィールド, （2135 ページ）
脆弱性の非アクティブ化, （2138 ページ）

脆弱性に対するパッチのダウンロード

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

ネットワーク上のホストで検出された脆弱性を軽減するためのパッチをダウンロードできます。

手順

ステップ 1 パッチをダウンロードするホストのホスト プロファイルにアクセスします。
ステップ 2 [脆弱性（Vulnerabilities）] セクションを展開します。
ステップ 3 パッチを適用する脆弱性の名前をクリックします。
ステップ 4 [修正（Fixes）] セクションを展開して、脆弱性に対するパッチの一覧を表示します。
ステップ 5 ダウンロードするパッチの隣の [ダウンロード（Download）] をクリックします。
ステップ 6 パッチをダウンロードして、影響を受けるシステムに適用します。

個々のホストに対する脆弱性の非アクティブ化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

ホストの脆弱性エディタを使用して、ホストごとに脆弱性を非アクティブにすることができます。ホストの脆弱性を非アクティブにしても、そのホストの影響の相関に対して脆弱性は使用されますが、影響レベルは自動的に 1 レベル減少します。

手順

ステップ 1 ホスト プロファイルの [脆弱性（Vulnerabilities）] セクションに移動します。
ステップ 2 [脆弱性の編集（Edit Vulnerabilities）] をクリックします。
ステップ 3 [有効な脆弱性（Valid Vulnerabilities）] リストから脆弱性を選択し、下矢印をクリックして [無効な脆弱性（Invalid Vulnerabilities）] リストに移動します。

ヒント 隣接している複数の脆弱性を選択するには、クリックおよびドラッグを使用します。脆弱性をダブルクリックして、リスト間を移動することもできます。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 必要に応じて、ホストの脆弱性を [無効な脆弱性（Invalid Vulnerabilities）] リストから [有効な脆弱性（Valid Vulnerabilities）] リストに移動して、脆弱性をアクティブ化します。

関連トピック

個々の脆弱性の非アクティブ化, （2088 ページ）
複数の脆弱性の非アクティブ化, （2140 ページ）

個々の脆弱性の非アクティブ化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

ホストプロファイルで脆弱性を非アクティブ化すると、ネットワークマップにあるすべてのホストに対して脆弱性が非アクティブ化されます。ただし、いつでもその脆弱性を再アクティブ化することができます。

マルチドメイン展開では、先祖ドメインの脆弱性を非アクティブ化すると、すべての子孫ドメインでその脆弱性が非アクティブ化されます。先祖ドメインで脆弱性をアクティブにした場合、リーフ ドメインでは、そのドメインにあるデバイスに対して脆弱性のアクティブ化または非アクティブ化を実行できます。

手順

ステップ 1 次のようにして、脆弱性の詳細にアクセスします。

- 影響を受けるホスト プロファイルで、[脆弱性（Vulnerabilities）] セクションを展開し、有効または無効にする脆弱性の名前をクリックします。
- 事前定義されたワークフローで、[分析（Analysis）] > [脆弱性（Vulnerabilities）] > [脆弱性（Vulnerabilities）] を選択し、有効または無効にする脆弱性の横にある表示アイコン（  ）をクリックします。

ステップ 2 [影響を受ける条件（Impact Qualification）] ドロップダウン リストから [無効（Disabled）] を選択します。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ネットワーク マップ上のすべてのホストに対して、[影響を受ける条件（Impact Qualification）] の値を変更することを確認します。

ステップ 4 [完了（Done）] をクリックします。

次の作業

- オプションで、上記の手順を実行中に、[影響を受ける条件（Impact Qualification）] ドロップダウン リストから [有効（Enabled）] を選択することによって、脆弱性をアクティブにします。

関連トピック

個々のホストに対する脆弱性の非アクティブ化, （2087 ページ）
複数の脆弱性の非アクティブ化, （2140 ページ）
オペレーティング システムのアイデンティティの競合, （2064 ページ）

ホスト プロファイルのスキャン結果

Nmapを使用してホストをスキャンする場合、またはNmapのスキャンから結果をインポートする場合、これらの結果は、スキャンに含まれているすべてのホストのホスト プロファイルに表示されます。

Nmap が、ホストのオペレーティング システムについて、およびオープンでフィルタリングされていないポート上で稼動している任意のサーバについて収集した情報が、ホスト プロファイルの [オペレーティング システム（Operating System）] と [サーバ（Servers）] セクションにそれぞれ追加されます。また、Nmapは、そのホストのスキャン結果のリストを[スキャン結果（Scan Results）] セクションに追加します。プロファイルに [スキャン結果（Scan Results）] セクションが表示されるのは、スキャンでホスト上のオープン ポートが検出された場合のみであることに注意してください。

各結果には、情報のソース、スキャンしたポートの番号とタイプ、ポート上で稼動しているサーバの名前、Nmapで検出された任意の追加情報（ポートの状態やサーバのベンダー名など）が示されます。UDPポートをスキャンする場合、そのポートで検出されたサーバは[スキャン結果（Scan Results）] セクションにのみ表示されます。

ホスト プロファイルから Nmap スキャンを実行できることに注意してください。

ホスト プロファイルからのホストのスキャン

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

ホスト プロファイルから、ホストに対して Nmap スキャンを実行できます。スキャンが完了すると、そのホストのサーバおよびオペレーティング システムの情報がホスト プロファイルで更新されます。追加のスキャン結果は、すべてホスト プロファイルの [スキャン結果（Scan Results）] セクションに追加されます。

注意 Nmap 提供のサーバおよびオペレーティング システムのデータは、別の Nmap スキャンを実行するか、より優先度の高いホスト入力で上書きするまでスタティックなままになります。Nmap を使用したホストのスキャンを計画している場合は、定期的にスキャンをスケジュールします。

はじめる前に

- Nmap スキャン インスタンスを追加します。Nmap スキャン インスタンスの追加, （1493 ページ）を参照してください。

手順

ステップ 1 ホスト プロファイルで、[ホストのスキャン（Scan Host）] をクリックします。

ステップ 2 ホストのスキャンに使用するスキャン修復の横にある [スキャン（Scan）] をクリックします。システムによってホストがスキャンされ、ホスト プロファイルに結果が追加されます。

関連トピック

Nmap スキャンの自動化, （202 ページ）

第 88 章

ディスカバリ イベントの操作

以下のトピックでは、ディスカバリ イベントを操作する方法について説明します。

検出イベントの検出データとアイデンティティ データ

システムは、モニタ対象のネットワークで検出された変更を表すイベントのテーブルを生成します。このテーブルを使用して、ネットワークのユーザ アクティビティを確認し、応答方法を決定できます。ネットワーク検出およびアイデンティティ ポリシーは、収集するデータ、モニタするネットワーク セグメント、およびそのために使用する特定のハードウェア インターフェイスの種類を指定します。

検出およびアイデンティティ イベント テーブルを使用して、ネットワークのホスト、アプリケーション、およびユーザに関連付けられている脅威を特定できます。システムには事前定義のワークフロー セットが用意されており、これを使用して、システムで生成されるイベントを分析することができます。また、特定のニーズに合った情報のみを表示するカスタム ワークフローを作成することもできます。

分析用にネットワーク検出およびアイデンティティ データを収集し、保存するには、ネットワーク検出およびアイデンティティ ポリシーを設定する必要があります。アイデンティティ ポリシーを設定した後、アクセス コントロール ポリシーで呼び出して、トラフィックのモニタに使用するデバイスに展開する必要があります。

ネットワーク検出ポリシーは、ホスト、アプリケーション、および権限のないユーザ データを提供します。アイデンティティ ポリシーは、権限のあるユーザ データを提供します。

次の検出イベント テーブルは、[分析（Analysis）]>[ホスト（Hosts）]、[分析（Analysis）]>[ユーザ（Users）]、および [分析（Analysis）]>[脆弱性（Vulnerabilities）] メニューにあります。

検出イベント テーブル	検出データが入力されますか。	アイデンティティ データが入力されますか。
ホスト（Hosts）	[はい（Yes）]	[いいえ（No）]
の侵害の兆候	[はい（Yes）]	[いいえ（No）]
アプリケーション	[はい（Yes）]	[いいえ（No）]
アプリケーション詳細（Application Details）	[はい（Yes）]	[いいえ（No）]
サーバ	[はい（Yes）]	[いいえ（No）]
ホスト属性（Host Attributes）	[はい（Yes）]	[いいえ（No）]
検出イベント（Discovery Events）	○	○
ユーザ アクティビティ（User Activity）	○	○
Users	○	○
脆弱性（Vulnerabilities）	[はい（Yes）]	[いいえ（No）]
サードパーティの脆弱性（Third-Party Vulnerabilities）	[はい（Yes）]	[いいえ（No）]

ディスカバリ イベントの統計情報の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

[ディスカバリ統計情報（Discovery Statistics）] ページには、システムで検出されたホスト、イベント、プロトコル、アプリケーションプロトコル、オペレーティングシステムの概要が表示されます。

ページには、最後の 1 時間の統計情報、および累計の統計情報が示されます。特定のデバイス、またはすべてのデバイスについての統計情報を表示することができます。サマリに示されているイベント、サーバ、オペレーティングシステム、またはオペレーティングシステムのベンダーをクリックして、ページ上のエントリに一致するイベントを表示することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [概要（Overview）] > [概要（Summary）] > [検出統計（Discovery Statistics）]を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、統計情報を表示するデバイスを選択します。オプションで、Firepower Management Center で管理されるすべてのデバイスの統計情報を表示するには、[すべて（All）] を選択します。

ステップ 3 次の選択肢があります。

- [統計情報サマリ（Statistics Summary）]セクション, （2093 ページ）で説明されているように、[統計サマリー（Statistics Summary）] に一般的な統計情報を表示します。
- [イベントの中断（Event Breakdown）] で、表示するイベント タイプをクリックします。イベントが 1 つも表示されない場合は、時間枠の変更, （1859 ページ）で説明されているように、時間範囲を調整する必要があるかもしれません。
- [プロトコルの中断（Protocol Breakdown）] で、検出されたホストによって現在使用されているプロトコルを表示します。
- [アプリケーション プロトコルの中断（Application Protocol Breakdown）] で、表示するアプリケーション プロトコルの名前をクリックします。
- [OS の中断（OS Breakdown）] で、[OS 名（OS Name）] または [OS ベンダー（OS Vendor）] をクリックします。

関連トピック

[イベント分類（Event Breakdown）] セクション, （2095 ページ）
[プロトコル分類（Protocol Breakdown）] セクション, （2095 ページ）
[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクション, （2095 ページ）
[OS 分類（OS Breakdown）] セクション, （2095 ページ）

[統計情報サマリ（Statistics Summary）] セクション

[統計情報サマリ（Statistics Summary）] セクションの行の説明は次のとおりです。

合計イベント数（Total Events）

Firepower Management Center に格納されているディスカバリ イベントの合計数。

過去 1 時間のイベントの合計（Total Events Last Hour）

最後の 1 時間に生成されたディスカバリ イベントの合計数。

過去 1 日のイベントの合計（Total Events Last Day）

最後の 1 日に生成されたディスカバリ イベントの合計数。

アプリケーションプロトコル合計数（Total Application Protocols）

検出されたホストで実行されているサーバのアプリケーション プロトコルの合計数。

IP ホストの合計（Total IP Hosts）

一意の IP アドレスによって特定された検出済みホストの合計数。

MAC ホストの合計（Total MAC Hosts）

IP アドレスで特定されない検出済みホストの合計数。

すべてのデバイス、または特定のデバイスのどちらについてのディスカバリ統計情報を参照している場合でも、[MAC ホストの合計（Total MAC Hosts）] の統計情報は同じになることに注意してください。これは、管理対象デバイスが IP アドレスに基づいてホストを検出するためです。この統計情報は、他の方法によって識別され、特定の管理対象デバイスに依存しないすべてのホストの合計を表します。

ルータの合計（Total Routers）

ルータとして識別された検出ノードの合計数。

ブリッジの合計（Total Bridges）

ブリッジとして識別された検出ノードの合計数。

ホスト制限の使用（Host Limit Usage）

使用中のホスト制限のパーセンテージ合計。ホストの制限は、Firepower Management Center のモデルによって定義されます。すべての管理対象デバイスについての統計情報を表示している場合は、ホストの使用制限のみが表示されることに注意してください。

（注） ホストの制限に達してホストが削除されると、ディスカバリ データを消去するネットワーク マップ上にホストは表示されなくなります。

最後に受け取ったイベント（Last Event Received）

最後のディスカバリ イベントが行われた日付と時間。

最後に受信した接続（Last Connection Received）

最後の接続が完了した日付と時間。

[イベント分類（Event Breakdown）] セクション

[イベント分類（Event Breakdown）] セクションには、データベースに格納されている各イベントタイプの合計数のカウントの他に、ネットワーク検出の各タイプのカウント、および最後の 1 時間で発生したホスト入力イベントが示されます。

[イベント分類（Event Breakdown）] セクションを使用して、ディスカバリ イベントおよびホスト入力イベントの詳細を表示することもできます。

関連トピック

検出イベントおよびホスト入力イベント，（2099 ページ）

[プロトコル分類（Protocol Breakdown）] セクション

[プロトコル分類（Protocol Breakdown）] セクションには、検出されたホストで使用されているプロトコルが示されます。このセクションには、検出されたそれぞれのプロトコル名、プロトコルスタックの「レイヤ」、およびプロトコルを使用して通信しているホストの合計数が表示されます。

[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクション

[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクションには、検出されたホストで使用されているアプリケーション プロトコルが示されます。このセクションには、プロトコル名、最後の 1 時間にアプリケーション プロトコルを実行したホストの合計数、いずれかのポイントでプロトコルの実行が検出されたホストの合計数が表示されます。

[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクションではさらに、検出されたプロトコルを使用しているサーバの詳細を表示することもできます。

関連トピック

サーバ データ，（2124 ページ）

[OS 分類（OS Breakdown）] セクション

[OS 分類（OS Breakdown）] セクションには、監視対象ネットワーク上で稼動しているオペレーティング システム、およびオペレーティング システムのベンダー、各オペレーティング システムを実行しているホストの合計数が示されます。

オペレーティング システムの名前またはバージョンの値が `unknown` の場合は、オペレーティング システムまたはそのバージョンが、システムのフィンガープリントの内容と一致しないことを意味します。値が `pending` の場合は、オペレーティング システムまたはそのバージョンを識別するための十分な情報がシステムで収集されていないことを意味します。

[OS 分類（OS Breakdown）] セクションを使用して、検出されたオペレーティング システムの詳細を表示することができます。

関連トピック

ホスト データ，（2109 ページ）

ディスカバリ パフォーマンス グラフの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint

ディスカバリ イベントを使用して、管理対象デバイスのパフォーマンス統計情報を示すグラフを生成することができます。

新しいデータは 5 分ごとに統計グラフに蓄積されます。したがって、グラフをすばやくリロードしても、次の 5 分の差分更新が実行されるまでデータは変更されていない場合があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [概要（Overview）] > [概要（Summary）] > [検出パフォーマンス（Discovery Performance）]を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、Firepower Management Center または対象とする管理対象デバイスを選択します。

ステップ 3 ディスカバリ パフォーマンス グラフ タイプ，（2096 ページ）で説明されているように、[グラフの選択（Select Graph(s)）] リストから、作成するグラフの種類を選択します。

ステップ 4 [時間範囲の選択（Select Time Range）] リストから、グラフに使用する時間範囲を選択します。

ステップ 5 [グラフ（Graph）] をクリックして、選択した統計情報をグラフ化します。

ディスカバリ パフォーマンス グラフ タイプ

次に、使用できるグラフのタイプについて説明します。

処理されたイベント数/秒

Data Correlator が 1 秒間に処理するイベントの数を表します。

処理された接続数/秒

Data Correlator が 1 秒間に処理する接続の数を表します。

生成されたイベント数/秒

システムが 1 秒間に生成するイベントの数を表します。

メガビット/秒

ディスカバリ プロセスによって 1 秒間に分析されたトラフィック数（メガビット）を表します。

平均バイト/パケット

ディスカバリ プロセスによって分析された各パケットに含まれるバイト数の平均を表します。

キロパケット/秒

ディスカバリ プロセスで 1 秒間に分析されるパケット数を 1000 単位で表します。

ディスカバリおよびアイデンティティ ワークフローの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	タスクに依存

Firepower Management Center は、ネットワークで生成されるディスカバリおよびアイデンティティ データの分析で使用できるイベント ワークフロー セットを提供します。ワークフローはネットワーク マップとともに、ネットワーク資産に関する主要な情報源になります。

Firepower Management Center には、ディスカバリおよびアイデンティティ データ、検出されたホストとそのホストの属性、サーバ、アプリケーション、アプリケーションの詳細、脆弱性、ユーザ アクティビティ、ユーザに関する事前定義されたワークフローが用意されています。ユーザはカスタム ワークフローを作成することもできます。

手順

ステップ 1 事前定義されたワークフローにアクセスするには、以下を実行します。

- ディスカバリとホスト入力データ：ディスカバリ イベントとホスト入力イベントの表示, （2107 ページ）を参照してください。
- ホスト データ：ホスト データの表示, （2109 ページ）を参照してください。
- ホスト属性データ：ホスト属性の表示, （2117 ページ）を参照してください。

- ホストまたはユーザの侵害の兆候データ：侵害の兆候データの表示，（2120ページ）を参照してください。
- サーバ データ：サーバ データの表示，（2125 ページ）を参照してください。
- アプリケーションデータ：アプリケーションデータの表示，（2129ページ）を参照してください。
- アプリケーション詳細データ：アプリケーション詳細データの表示，（2132ページ）を参照してください。
- ユーザ データ：ユーザ データの表示，（2151 ページ）を参照してください。
- ユーザアクティビティデータ：ユーザアクティビティデータの表示，（2154ページ）を参照してください。
- ネットワーク マップ：ネットワーク マップの表示，（1803 ページ）を参照してください。

ステップ 2 カスタム ワークフローにアクセスするには、[分析（Analysis）]>[カスタム（Custom）]>[カスタム ワークフロー（Custom Workflows）] を選択します。

ステップ 3 カスタム テーブルに基づいたワークフローにアクセスするには、[分析（Analysis）]>[カスタム（Custom）]>[カスタム テーブル（Custom Tables）] を選択します。

ステップ 4 以下のいずれかのアクションを実行します。これらは、ネットワーク検出ワークフローでアクセスするすべてのページに共通です。

- カラムの制約：表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン（✖）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）]をクリックする前に、該当するチェックボックスをオンまたはオフにします。無効にしたカラムをビューに戻すには、展開の矢印をクリックして検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- 削除：現在の制約されたビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。これらのアイテムが再検出されても、システムのディスカバリ機能が再開されるまで、これらのアイテムは削除されたままになります。

  注意 [分析（Analysis）]>[ユーザ（Users）]>[ユーザ（Users）] ページでセッションを削除する前に、セッションが実際に閉じられていることを確認します。アクティブなセッションを削除すると、該当するポリシーはデバイス上のセッションを検出できなくなります。そのため、モニタしたり、ブロックしたりするようポリシーが設定されていたとしても、セッションはそれらのアクションを実行しません。

  （注） サードパーティの場合とは異なり、シスコの脆弱性は削除**できません**。ただし、確認済みとしてマークすることはできます。

- ドリル ダウン：ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用，（1844 ページ）を参照してください。

- 現在のページを移動する：現在のワークフローページ内を移動するには、ワークフローページのナビゲーション ツール，（1840 ページ）を参照してください。
- ワークフロー内で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- 他のワークフローに移動する：関連するイベントを調べるために、その他のイベント ビューに移動するには、ワークフロー間のナビゲーション，（1866 ページ）を参照してください。
- データのソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- ホスト プロファイルの表示：IP アドレスのホスト プロファイルを表示するには、ホスト プロファイルのアイコン（  ）をクリックします。アクティブな侵害の兆候（IOC）タグのあるホストの場合は、IP アドレスの横に表示される侵害されたホストのアイコン（  ）をクリックします。
- ユーザ プロファイル：ユーザ ID 情報を表示するには、ユーザ ID の横に表示されるユーザ アイコン（  ）をクリックします。 の表示

関連トピック

ワークフローの使用，（1834 ページ）
Management Center データベースからのデータの消去，（219 ページ）

検出イベントおよびホスト入力イベント

システムは検出イベントを生成します。このイベントは、監視対象ネットワーク セグメントにおける変更の詳細をやり取りします。新しく検出されたネットワーク機能に対しては、新しいイベントが生成され、以前に認識されたネットワーク アセットにおける何らかの変更に対しては、変更のイベントが生成されます。

最初のネットワーク検出のフェーズ中に、システムは各ホスト、および各ホスト上での稼動が検出された TCP または UDP サーバについて、新しいイベントを生成します。必要に応じて、エクスポートされた NetFlow レコードを使用してこれらの新しいホストおよびサーバのイベントを生成するよう、システムを設定することができます。

またシステムは、検出された各ホスト上で稼動しているネットワーク、トランスポート、およびアプリケーション プロトコルのそれぞれに対して新しいイベントを生成します。設定されている検出ルールでアプリケーション プロトコルの検出を無効にして、NetFlow エクスポータをモニタできますが、Firepower システムの管理対象デバイスをモニタするよう設定された検出ルールではできません。NetFlow 以外の検出ルールでホストまたはユーザの検出を有効にすると、アプリケーションが自動的に検出されます。

最初のネットワーク マッピングが完了すると、続けてシステムは変更イベントを生成し、ネットワークの変更を記録します。変更イベントは、以前に検出されたアセットの設定が変更されるたびに生成されます。

検出イベントが生成されると、データベースに記録されます。Firepower Management Center の Web インターフェイスを使用して、検出イベントを表示、検索、および削除できます。また、相関ルールで検出イベントを使用することもできます。ユーザが指定する他の基準だけでなく、生成される検出イベントのタイプに基づいて、相関ルールを作成することができます。相関ルールは相関ポリシーで使用され、ネットワーク トラフィックが基準を満たしたときに、修復、syslog、SNMP、および電子メール アラートの応答を起動します。

ホスト入力機能を使用して、ネットワーク マップにデータを追加することができます。オペレーティング システムの情報を追加、修正、または削除することができますが、この場合、システムは対象のホストに対する情報の更新を停止します。アプリケーション プロトコル、クライアント、サーバ、およびホストの属性を手動で追加、変更、または削除することも、脆弱性の情報を変更することもできます。この処理を行う場合、システムはホスト入力機能を生成します。

ディスカバリ イベント タイプ

ネットワーク検出ポリシーにシステムが記録するディスカバリ イベントのタイプを設定できます。ディスカバリ イベントのテーブルを表示すると、[イベント（Event）] カラムにイベント タイプが表示されます。次に、ディスカバリ イベント タイプについて説明します。

ホストの追加 MAC の検出

このイベントは、以前に検出したホストに対してシステムが新しい MAC アドレスを検出したときに生成されます。

このイベントは多くの場合、ルータを通じてトラフィックを渡すホストをシステムが検出したときに生成されます。各ホストにはそれぞれ異なる IP アドレスがありますが、これらの IP アドレスはすべて、ルータに関連付けられている MAC アドレスを持っているように見えます。システムは IP アドレスに関連付けられている実際の MAC アドレスを検出すると、ホスト プロファイル内でその MAC アドレスを太字で表示し、イベント ビューのイベント説明に「ARP/DHCP detected」のメッセージを表示します。

クライアント タイムアウト

このイベントは、非アクティブであるという理由で、システムがデータベースからクライアントをドロップしたときに生成されます。

クライアント更新

このイベントは、HTTP トラフィック内でシステムがペイロード（つまり音声やビデオ、Web メールなどの特別なタイプのコンテンツ）を検出したときに生成されます。

DHCP：IP アドレスの変更

このイベントは、DHCP アドレスの割り当てによってホスト IP アドレスが変わったことがシステムで検出された場合に生成されます。

DHCP：IP アドレスの再割り当て

このイベントは、ホストがIPアドレスを再利用するとき、つまり他の物理ホストが以前に使用したIP アドレスを、別のホストが DHCP の IP アドレス割り当てによって取得した場合に生成されます。

ホップ数の変更

このイベントは、ホストと、そのホストを検出するデバイス間でシステムがネットワーク ホップ数の変更を検出した場合に生成されます。これは次のような場合に発生します。

- デバイスがさまざまなルータを介してホストのトラフィックを監視しており、ホストの場所についてより適切な決定ができる場合。
- デバイスがホストから ARP 送信を検出し、ホストがローカル セグメント上にあることを示している場合。

ホスト削除：ホスト制限に到達

このイベントは、Firepower Management Center 上でホストの制限を超えて、のネットワーク マップから監視対象のホストが削除されたときに生成されます。

ホスト ドロップ：ホスト制限に到達

このイベントは、Firepower Management Center 上でホストの制限に達して新しいホストがドロップされたときに生成されます。このイベントとの相違点として、前述のイベントでは、ホストの制限に達したときに古いホストがネットワーク マップから削除されます。

ホストの制限に達したときに新しいホストをドロップするには、[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）] > [詳細（Advanced）] を選択し、[ホストの制限に達した場合（When Host Limit Reached）] を [ホストをドロップ（Drop hosts）] に設定します。

ホストの IOC セット

このイベントは、ホストに対して IOC（侵害の痕跡）が設定され、アラートが生成されたときに生成されます。

ホスト タイムアウト

このイベントは、ネットワーク検出ポリシーで定義された間隔内でホストがトラフィックを生成しなかったために、ネットワーク マップからホストがドロップされたときに生成されます。個々のホストのIPアドレスとMACアドレスはそれぞれタイムアウトになることに注意してください。関連付けられているアドレスがすべてタイムアウトになるまで、ホストはネットワーク マップから消えません。

ネットワーク検出ポリシーで監視するネットワークを変更する場合は、ネットワーク マップから古いホストを手動で削除して、それらのホストがホストの制限に不利に作用しないようにします。

ネットワーク デバイスへのホスト タイプの変更

このイベントは、システムが、検出されたホストが実際はネットワーク デバイスであったことを認識したときに生成されます。

アイデンティティ競合

このイベントは、システムが、新しいサーバまたはオペレーティング システムに対する現行のアクティブなアイデンティティと競合する、そのサーバまたはオペレーティング システムのアイデンティティを検出したときに生成されます。

より新しいアクティブなアイデンティティ データを取得するためにホストを再スキャンして、アイデンティティの競合を解決する場合は、Identity Conflict イベントを使用して Nmap の修復をトリガーできます。

アイデンティティ タイムアウト

このイベントは、アクティブなソースからのサーバまたはオペレーティング システムの ID データがタイムアウトしたときに生成されます。

より新しいアクティブなアイデンティティ データを取得するために、ホストを再スキャンしてアイデンティティ データをリフレッシュする場合は、Identity Conflict イベントを使用して Nmap の修復をトリガーできます。

MAC 情報の変更

このイベントは、特定の MAC アドレスまたは TTL 値に関連付けられている情報で、システムが変更を検出したときに生成されます。

このイベントは多くの場合、ルータを通じてトラフィックを渡すホストをシステムが検出したときに発生します。各ホストにはそれぞれ異なる IP アドレスがありますが、これらの IP アドレスはすべて、ルータに関連付けられている MAC アドレスを持っているように見えます。システムは IP アドレスに関連付けられている実際の MAC アドレスを検出すると、ホスト プロファイル内でその MAC アドレスを太字で表示し、イベント ビューのイベント説明に「ARP/DHCP detected」のメッセージを表示します。TTL は変わる可能性がありますが、これはトラフィックが複数のルータを通じて渡される可能性があるためです。また、システムがホストの実際の MAC アドレスを検出した場合も TTL が変わる可能性があります。

NETBIOS 名の変更

このイベントは、システムがホストの NetBIOS 名に対する変更を検出したときに生成されます。このイベントは、NetBIOS プロトコルを使用するホストに対してのみ生成されます。

新しいクライアント

このイベントは、システムが新しいクライアントを検出したときに生成されます。

（注） 分析用にクライアント データを収集および格納するには、ネットワーク検出ポリシーのディスカバリ ルールでアプリケーションの検出が有効になっていることを確認します。

新しいホスト

このイベントは、システムがネットワーク上で稼動している新しいホストを検出したときに生成されます。

このイベントは、デバイスが新しいホストを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成するには、NetFlow データを管理するネットワーク検出ルールでホストを検出するように設定します。

新しいネットワーク プロトコル

このイベントは、ホストが新しいネットワーク プロトコル（IP、ARP など）と通信していることをシステムが検出したときに生成されます。

新しい OS

このイベントは、システムがホストの新しいオペレーティング システムを検出した、またはホストのオペレーティング システムで変更を検出したときに生成されます。

新しい TCP ポート

このイベントは、ホスト上でアクティブな新しい TCP サーバ ポート（SMTP または Web サービスで使用されているポートなど）をシステムが検出したときに生成されます。このイベントは、アプリケーションプロトコル、またはアプリケーションプロトコルに関連付けられているサーバの識別には使用されません。情報は、TCP Server Information Update イベントで伝送されます。

このイベントは、デバイスがネットワーク マップにすでに存在しないモニタ対象ネットワーク上のサーバを含む NetFlow データを処理するときも生成できます。この状況でイベントを生成するには、NetFlow データを管理するネットワーク検出ルールでアプリケーションを検出するように設定します。

新しいトランスポート プロトコル

このイベントは、ホストが新しいトランスポート プロトコル（TCP、UDP など）と通信していることをシステムが検出したときに生成されます。

新しい UDP ポート

このイベントは、システムが、ホスト上で稼動している新しい UDP サーバ ポートを検出したときに生成されます。

このイベントは、デバイスがネットワーク マップにすでに存在しないモニタ対象ネットワーク上のサーバを含む NetFlow データを処理するときも生成できます。この状況でイベントを生成するには、NetFlow データを管理するネットワーク検出ルールでアプリケーションを検出するように設定します。

TCP ポート クローズ

このイベントは、システムが、ホスト上で TCP ポートがクローズしたことを検出したときに生成されます。

TCP ポート タイムアウト

このイベントは、システムのネットワーク検出ポリシーに定義された間隔内で、システムが TCP ポートからアクティビティを検出しなかったときに生成されます。

TCP サーバ情報の更新

このイベントは、ホスト上で稼動しており、すでに検出されている TCP サーバでシステムが変更を検出したときに生成されます。

このイベントは、TCP サーバが更新されたときに生成される場合があります。

UDP ポート クローズ

このイベントは、システムが、ホスト上でUDPポートがクローズしたことを検出したときに生成されます。

UDP ポート タイムアウト

このイベントは、ネットワーク検出ポリシーに定義された間隔内で、システムがUDPポートからアクティビティを検出しなかったときに生成されます。

UDP サーバ情報の更新

このイベントは、ホスト上で稼動しており、すでに検出されているUDPサーバでシステムが変更を検出したときに生成されます。

このイベントは、UDP サーバが更新されたときに生成される場合があります。

VLAN タグ情報の更新

このイベントは、システムが、VLAN タグ内でホストに起因する変更を検出したときに生成されます。

関連トピック

ホスト入力イベント タイプ, （2104 ページ）
ネットワーク検出のデータ ストレージ設定, （1572 ページ）
アプリケーションおよびオペレーティング システムの ID の競合, （1440 ページ）
ネットワーク検出アイデンティティ競合の設定, （1567 ページ）

ホスト入力イベント タイプ

ディスカバリ イベントのテーブルを表示すると、[イベント（Event）] カラムにイベント タイプが表示されます。

ユーザが（手動でホストを追加するなどの）特定のアクションを実行したときに生成されるホスト入力イベントとは異なり、ディスカバリ イベントは、システムが、監視対象ネットワークで変更を検出したとき（以前は検出されなかったホストでトラフィックを検出した場合など）に生成されます。

ネットワーク検出ポリシーを変更して、システムが記録するホスト入力イベントのタイプを設定できます。

さまざまなタイプのホスト入力イベントが提示する情報を理解すると、どのイベントを記録およびアラートの対象にするか、相関ポリシーでこれらのアラートをどのように使用するかを効率よく判断できるようになります。また、イベント タイプの名前がわかると、より効率のよいイベント検索を作成するうえで役に立ちます。次に、ホスト入力イベントのさまざまなタイプについて説明します。

クライアントの追加（Add Client）

このイベントは、ユーザがクライアントを追加したときに生成されます。

ホストの追加（Add Host）

このイベントは、ユーザがホストを追加したときに生成されます。

プロトコルの追加（Add Protocol）

このイベントは、ユーザがプロトコルを追加したときに生成されます。

スキャン結果の追加（Add Scan Result）

このイベントは、システムが Nmap スキャンの結果をホストに追加したときに生成されます。

ポートの追加（Add Port）

このイベントは、ユーザがサーバ ポートを追加したときに生成されます。

クライアントの削除（Delete Client）

このイベントは、ユーザがシステムからクライアントを削除したときに生成されます。

ホスト/ネットワークの削除（Delete Host/Network）

このイベントは、ユーザがシステムから IP アドレスまたはサブネットを削除したときに生成されます。

プロトコルの削除（Delete Protocol）

このイベントは、ユーザがシステムからプロトコルを削除したときに生成されます。

ポートの削除（Delete Port）

このイベントは、ユーザがシステムからサーバポートまたはサーバポートのグループを削除したときに生成されます。

ホスト属性の追加（Host Attribute Add）

このイベントは、ユーザが新しいホスト属性を作成したときに生成されます。

ホスト属性の削除（Host Attribute Delete）

このイベントは、ユーザが、ユーザ定義のホスト属性を削除したときに生成されます。

ホスト属性値の削除（Host Attribute Delete Value）

このイベントは、ユーザが、ホスト属性に割り当てられている値を削除したときに生成されます。

ホスト属性値の設定（Host Attribute Set Value）

このイベントは、ユーザがホストに対してホスト属性値を設定したときに生成されます。

ホスト属性の更新（Host Attribute Update）

このイベントは、ユーザが、ユーザ定義のホスト属性の定義を変更したときに生成されます。

ホスト重要度の設定（Set Host Criticality）

このイベントは、ユーザがホストに対してホストの重要度の値を設定した、または変更したときに生成されます。

オペレーティング システム定義の設定（Set Operating System Definition）

このイベントは、ユーザがホストに対してオペレーティング システムを設定したときに生成されます。

サーバ定義の設定（Set Server Definition）

このイベントは、ユーザがサーバに対してベンダーおよびバージョンの定義を設定したときに生成されます。

脆弱性影響認定の設定（Set Vulnerability Impact Qualification）

このイベントは、脆弱性の影響の認定が設定されたときに生成されます。

脆弱性が、影響の認定に対する使用でグローバル レベルで無効になったとき、または脆弱性がグローバル レベルで有効になったときに、このイベントが生成されます。

脆弱性を無効に設定（Vulnerability Set Invalid）

このイベントは、ユーザが 1 つ以上の脆弱性を無効にした（または確認した）ときに生成されます。

脆弱性を有効に設定（Vulnerability Set Valid）

このイベントは、ユーザが、以前に無効であるとマークされた脆弱性を有効にしたときに生成されます。

関連トピック

ディスカバリ イベント タイプ, （2100 ページ）

ディスカバリ イベントとホスト入力イベントの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

ディスカバリ イベント ワークフローでは、ディスカバリ イベントとホスト入力イベント両方からのデータを表示できます。ユーザは検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがイベントにアクセスするときに表示されるページは、使用するワークフローによって異なります。ユーザは事前定義のワークフローを使用できますが、これにはディスカバリ イベントのテーブル ビューと、ホスト ビューの最終ページが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 [分析（Analysis）] > [ホスト（Hosts）] > [検出イベント（Discovery Events）]を選択します。

ステップ 2 次の選択肢があります。

- 時間枠の変更, （1859 ページ）の説明に従って、時間範囲を調整します。

  （注） イベント ビューを時間によって制約している場合は、（グローバルかイベント固有かに関係なく）アプライアンスに設定されている時間枠の外で生成されたイベントが、イベント ビューに表示されます。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用, （2097 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ディスカバリ イベントのフィールド, （2108 ページ）を参照）。

関連トピック

ディスカバリおよびアイデンティティ ワークフローの使用，（2097 ページ）

ディスカバリ イベントのフィールド

以下に、ディスカバリ イベント テーブルで表示および検索できるフィールドについて説明します。

時刻（Time）

システムがイベントを生成した時間。

イベント

ディスカバリ イベント タイプまたはホスト入力イベント タイプ。

[IPアドレス（IP Address）]

イベントに関連するホストに関連付けられている IP アドレス。

ユーザ（User）

イベントが生成される前に、イベントに関係するホストに最後にログインしたユーザ。権限のあるユーザの後に、権限のないユーザのみがログインした場合、権限のある別のユーザが次にログインするまで、権限のあるユーザがそのホストの現行ユーザとして保持されます。

MAC アドレス（MAC Address）

ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックが使用する NIC の MAC アドレス。この MAC アドレスは、イベントに関連するホストの実際の MAC アドレスであるか、またはトラフィックが通過したネットワーク デバイスの MAC アドレスになります。

MAC ベンダー（MAC Vendor）

ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックが使用する NIC の MAC ハードウェア ベンダー。

このフィールドを検索する場合は、virtual_mac_vendor を入力して、仮想ホストに関係するイベントを照合します。

[ポート（Port）]

イベントをトリガーとして使用したトラフィックが使用するポート（該当する場合）。

説明

テキストによるイベントの説明。

ドメイン

ホストを検出したデバイスのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

Device

イベントを生成した管理対象デバイスの名前。NetFlow データに基づいた新しいホストおよび新しいサーバのイベントの場合、これはそのデータを処理した管理対象デバイスになります。

関連トピック

イベントの検索，（1871 ページ）

ホスト データ

システムがホストを検出し、ホスト プロファイルを作成するためにホストに関する情報を収集したときに、イベントが生成されます。Firepower Management Center Web インターフェイスを使用して、ホストを表示、検索、および削除できます。

ホストの表示中に、選択したホストに基づいてトラフィックのプロファイル、およびコンプライアンスのホワイト リストを作成できます。また、（ビジネスの重要度を設定する）ホストの重要度の値などのホスト属性をホスト グループに割り当てることもできます。そのあとで、相関ルールおよびポリシーの中でこれらの重要度の値、ホワイトリスト、およびトラフィック プロファイルを使用できます。

システムは、ホストをエクスポートされた NetFlow レコードからネットワーク マップに追加できますが、これらのホストに使用できる情報は限られます（NetFlowデータと管理対象デバイス データの違い，（1442 ページ） を参照）。

関連トピック

NetFlow データと管理対象デバイス データの違い，（1442 ページ）

ホスト データの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、システムが検出したホストのテーブルを表示することができます。その後、探している情報に応じて表示方法を操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがホストにアクセスするときに表示されるページは、使用するワークフローによって異なります。両方の事前定義ワークフローが、制限を満たすすべてのホストのホスト プロファイルを

含むホストビューで終わります。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

手順

ステップ 1 次のように、ホスト データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析（Analysis）] > [ホスト（Hosts）] > [ホスト（Hosts）] を選択します。
- ホストのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ホスト（Hosts）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用, （2097 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ホストデータ フィールド, （2110ページ）を参照）。
- ホスト属性を特定のホストに割り当てます（選択したホストのホスト属性の設定, （2119ページ）を参照）。
- 特定のホストのトラフィック プロファイルを作成します（選択したホストのトラフィック プロファイルの作成, （2115 ページ）を参照）。
- 特定のホストに基づいて、コンプライアンスのホワイトリストを作成します（選択したホストに基づいたコンプライアンスのホワイト リストの作成, （2116 ページ）を参照）。

ホスト データ フィールド

システムはホストを検出したときに、そのホストに関するデータを収集します。そのデータには、ホストのIPアドレス、ホストが実行しているオペレーティング システムなどが含めることが可能です。ユーザは、ホストのテーブル ビューでこれらの情報の一部を表示することができます。

ホスト テーブルで表示および検索できるフィールドの説明が続きます。

前回の検出（Last Seen）

システムによっていずれかのホストの IP アドレスが最後に検出された日付と時間。[前回の検出（Last Seen）] の値は、ホストの IP アドレスに対してシステムが新しいホスト イベントを生成したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

ホスト入力機能を使用して、オペレーティング システムのデータを更新しているホストでは、[前回の検出（Last Seen）] の値は、そのデータが最初に追加された日付と時間を表します。

[IPアドレス（IP Address）]

ホストに関連付けられている IP アドレス。

MAC アドレス（MAC Address）

ホストが検出した NIC の MAC アドレス。

[MACアドレス（MAC Address）] フィールドは、[ホスト（Hosts）] ワークフローの [ホストのテーブル ビュー（Table View of Hosts）] に表示されます。以下のものに対して [MAC アドレス（MAC Address）] フィールドを追加できます。

- [ホスト（Hosts）] テーブルのフィールドが含まれているカスタム テーブル
- [ホスト（Hosts）] テーブルに基づいたカスタム ワークフローのドリルダウン ページ

MAC ベンダー（MAC Vendor）

ホストが検出した NIC の MAC ハードウェア ベンダー。

[MACベンダー（MAC Vendor）] フィールドは、[ホスト（Hosts）] ワークフローの [ホストのテーブル ビュー（Table View of Hosts）] に表示されます。以下のものに対して [MAC ベンダー（MAC Vendor）] フィールドを追加できます。

- [ホスト（Hosts）] テーブルのフィールドが含まれているカスタム テーブル
- [ホスト（Hosts）] テーブルに基づいたカスタム ワークフローのドリルダウン ページ

このフィールドを検索する場合は、`virtual_mac_vendor` を入力して、仮想ホストに関係するイベントを照合します。

現在のユーザ（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

ホストの重要度（Host Criticality）

ホストに割り当てられている、ユーザ指定の重要度の値。

NetBIOS 名（NetBIOS Name）

ホストのNetBIOS名。NetBIOSプロトコルを実行しているホストにのみ、NetBIOS名があります。

VLAN ID（Admin. VLAN ID）

ホストが使用する VLAN ID。

ホップ（Hops）

ホストを検出したデバイスからホストへのネットワークのホップ数。

ホスト タイプ（Host Type）

ホストのタイプ。ホスト、モバイルデバイス、jailbroken モバイルデバイス、ルータ、ブリッジ、NAT デバイス、ロード バランサのいずれかにできます。

ネットワーク デバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol（CDP）メッセージの分析。ネットワークのデバイスおよびそれらのタイプ（シスコ デバイスのみ）を特定できます。
- スパニング ツリー プロトコル（STP）の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。

デバイスがネットワーク デバイスとして識別されない場合は、ホストとして分類されます。

このフィールドを検索するときは、`!host` と入力してすべてのネットワーク デバイスを検索します。

ハードウェア（Hardware）

モバイル デバイスのハードウェア プラットフォーム。

OS

次のいずれかです。

- ホスト上で検出されたオペレーティング システム（名前、ベンダー、およびバージョン）、または Nmap かホスト入力機能を使用して更新されたオペレーティング システム。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は `unknown`
- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は `pending`

システムが複数のアイデンティティを検出した場合は、これらのアイデンティティはカンマ区切りリストで表示されます。

このフィールドは、ダッシュボード上で [カスタム分析（Custom Analysis）] ウィジェットからホスト イベント ビューを起動したときに表示されます。また、これは [ホスト（Hosts）] テーブルに基づいたカスタム テーブルのフィールド オプションです。

このフィールドを検索するときは、n/a と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

OS 競合（OS Conflict）

このフィールドは検索専用です。

OS ベンダー（OS Vendor）

次のいずれかです。

- ホストで検出されたオペレーティング システムのベンダー、または Nmap かホスト入力機能を使用して更新されたオペレーティング システムのベンダー。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は unknown
- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は pending

システムが複数のベンダーを検出した場合は、これらのベンダーはカンマ区切りリストで表示されます。

このフィールドを検索するときは、n/a と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

OS 名（OS Name）

次のいずれかです。

- ホスト上で検出されたオペレーティング システム、または Nmap かホスト入力機能を使用して更新されたオペレーティング システム。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は unknown
- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は pending

システムが複数の名前を検出した場合は、これらの名前はカンマ区切りリストで表示されます。

このフィールドを検索するときは、n/a と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

OS バージョン（OS Version）

次のいずれかです。

- ホストで検出されたオペレーティング システムのバージョン、または Nmap かホスト入力機能を使用して更新されたオペレーティング システムのバージョン。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は unknown
- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は pending

システムが複数のバージョンを検出した場合は、これらのバージョンはカンマ区切りリストで表示されます。

このフィールドを検索するときは、`n/a` と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

ソース タイプ（Source Type）

ホストのオペレーティング システムのアイデンティティを確立するために使用されるソースのタイプは次のとおりです。

- [ユーザ（User）]：user_name
- [アプリケーション（Application）]：app_name
- スキャナ：scanner_type（ネットワーク検出の設定を介して追加された Nmap またはスキャナ）
- システムによって検出されたオペレーティング システムの場合は `Firepower`

システムでは、オペレーティング システムのアイデンティティを判断するために、複数のソースのデータを統合することができます。

信頼性（Confidence）

次のいずれかです。

- システムで検出されたホストについて、ホスト上で稼動しているオペレーティング システムのアイデンティティ内にシステムが保持している信頼度（パーセンテージ）。
- 100%（ホスト入力機能やNmapスキャナなどのアクティブなソースによって識別されたオペレーティング システムの場合）。
- `unknown`（システムがオペレーティング システムのアイデンティティを特定できないホスト、および NetFlow データに基づいてネットワーク マップに追加されたホストの場合）。

このフィールドを検索するときは、`n/a` と入力して、NetFlowデータに基づいてネットワーク マップに追加されたホストを含めます。

注記（Notes）

[注記（Notes）] ホスト属性の、ユーザ定義のコンテンツ。

ドメイン

ホストに関連付けられているドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

Device

トラフィックを検出した管理対象デバイスか、NetFlow またはホスト入力データを処理したデバイスのいずれか。

このフィールドが空白の場合は、次のいずれかの条件を満たします。

- ホストがデバイスによってネットワーク マップに追加されたが、このデバイスは、ホストが存在しているネットワークに対してネットワーク検出ポリシーに定義されているとおりに明示的に監視していない。
- ホストの入力機能を使用してホストが追加されたが、システムによって検出されていない。

メンバー数（Count）

各行に表示される情報と一致するイベントの数。このフィールドが表示されるのは、2 つ以上の同一の行を作成する制限を適用した後のみです。

関連トピック

イベントの検索，（1871 ページ）
オペレーティング システムのアイデンティティの競合，（2064 ページ）

選択したホストのトラフィック プロファイルの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

トラフィック プロファイルは、指定した期間に収集された接続データに基づいた、ネットワーク上のトラフィックのプロファイルです。トラフィック プロファイルを作成した後、正常なネットワーク トラフィックを表すと想定されるプロファイルに照らして新しいトラフィックを評価することにより、異常なネットワーク トラフィックを検出できます。

[ホスト（Hosts）]ページを使用して、指定するホスト グループのトラフィック プロファイルを作成できます。トラフィック プロファイルは、指定したホストのいずれかが発信元ホストである、検出された接続に基づいています。ソートおよび検索機能を使用して、プロファイルを作成するホストを分離することができます。

手順

ステップ 1 ホスト ワークフローのテーブル ビューで、トラフィック プロファイルを作成するホストの隣にあるチェック ボックスをオンにします。

ステップ 2 ページの下部で [トラフィック プロファイルの作成（Create Traffic Profile）] をクリックします。

ステップ 3 特別なニーズに応じて、トラフィック プロファイルを変更し、保存します。

関連トピック

トラフィック プロファイルの概要，（1679 ページ）

選択したホストに基づいたコンプライアンスのホワイト リストの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

コンプライアンスのホワイトリストでは、ネットワーク上で許可されるオペレーティング システム、クライアント、ネットワーク、トランスポート、またはアプリケーション プロトコルを指定することができます。

[ホスト（Hosts）]ページを使用して、ユーザが指定するホスト グループのホスト プロファイルに基づいて、コンプライアンスのホワイト リストを作成することができます。ソートおよび検索機能を使用して、ホワイト リストの作成に使用するホストを分離することができます。

手順

ステップ 1 ホスト ワークフローのテーブル ビューで、ホワイト リストを作成するホストの隣にあるチェック ボックスをオンにします。

ステップ 2 ページの下部で [ホワイト リストの作成（Create White List）] をクリックします。

ステップ 3 特別なニーズに応じて、ホワイト リストを変更し、保存します。

関連トピック

コンプライアンス ホワイトリストの概要, （1613 ページ）

ホスト属性データ

Firepower システムは、検出したホストに関する情報を収集し、その情報を使用してホスト プロファイルを作成します。ただし、ネットワーク上のホストについて、アナリストに提供する追加情報が存在する場合があります。ユーザは、ホスト プロファイルにメモを追加する、ホストのビジネス重要度を設定する、選択する他の情報を提供する、といったことが可能です。それぞれの情報は、ホスト属性と呼ばれます。

ホスト プロファイルの認定でホスト属性を使用することができます。これにより、トラフィック プロファイルの作成中に収集するデータを制約し、相関ルールをトリガーする条件を制限することができます。相関ルールに応じて属性値を設定することもできます。

関連トピック

ホスト属性の表示, （2117 ページ）
セット属性修復の設定, （1703 ページ）

ホスト属性の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、システムで検出されたホストのテーブル、およびそのホスト属性を表示することができます。その後、探している情報に応じて表示方法を操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがホスト属性にアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフロー（検出されたすべてのホスト、およびそのホストの属性が記載されているホスト属性のテーブル ビューが含まれており、ホスト ビュー ページで終了するワークフロー）を使用することができます。このワークフローには、制約を満たすすべてのホストについて 1 つのホスト プロファイルが含まれています。

また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のように、ホスト属性データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析（Analysis）] > [ホスト（Hosts）] > [ホスト属性（Host Attributes）] を選択します。
- ホスト属性のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [属性（Attributes）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用, （2097 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ホスト属性データ フィールド, （2118 ページ）を参照）。

- ホスト属性を特定のホストに割り当てます（選択したホストのホスト属性の設定, （2119ページ）を参照）。

ホスト属性データ フィールド

ホスト属性テーブルには、MACアドレスでのみ識別されるホストは表示されないことに注意してください。

ホスト属性テーブルで表示および検索できるフィールドの説明が続きます。

[IPアドレス（IP Address）]

ホストに関連付けられている IP アドレス。

現在のユーザ（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

ホストの重要度（Host Criticality）

ユーザが割り当てた、企業にとってのホストの重要度。ホストの重要度を相関ルールおよびポリシーで使用して、イベントに関するホストの重要度に対して、ポリシー違反および違反の応答を作成することができます。ホストの重要度に[低（Low）]、[中（Medium）]、[高（High）]、または [なし（None）] を割り当てることができます。

注記（Notes）

他のアナリストに提示する、ホストに関する情報。

コンプライアンス ホワイトリストの属性を含む、ユーザ定義のホスト属性（Any user-defined host attribute, including those for compliance white lists）

ユーザ定義のホスト属性の値。ホスト属性テーブルには、ユーザ定義のそれぞれのホスト属性のフィールドが含まれています。

ドメイン

ホストに関連付けられているドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

メンバー数（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索，（1871 ページ）

選択したホストのホスト属性の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

ホスト ワークフローから、事前定義済のホスト属性とユーザ定義のホスト属性を設定できます。

手順

ステップ 1 ホスト ワークフローで、ホスト属性を追加するホストの横にあるチェックボックスをオンにします。

ヒント ソート機能と検索機能を使用して、特別な属性を割り当てるホストを分離することができます。

ステップ 2 ページの下部にある [属性の設定（Set Attributes）] をクリックします。

ステップ 3 必要に応じて、選択したホストに対してホストの重要度を設定します。[なし（None）]、[低（Low）]、[中（Medium）]、または [高（High）] を選択できます。

ステップ 4 必要に応じて、テキスト ボックスで、選択したホストのホスト プロファイルにメモを追加します。

ステップ 5 必要に応じて、自分で設定したユーザ定義のホストの属性を設定します。

ステップ 6 [保存（Save）] をクリックします。

侵害の兆候データ

Firepowerシステムは、さまざまなタイプのデータ（侵入イベント、セキュリティ インテリジェンス、接続イベントおよびファイルまたはマルウェア イベント）を関連付け、モニタ対象ネットワーク上のホストが悪意のある手段によって侵害された可能性があるかどうかを判断します。イベント データの特定の組み合わせと頻度が、影響を受けるホストの侵害の兆候（IOC）タグをトリガーします。このようなホストのIPアドレスは侵害を受けているホストの赤いアイコン（  ）でイベント ビューに表示されます。

IOC データは、Firepower システムの Web インターフェイスの数箇所で表示、操作を行えます。

- イベント ビューア：接続、セキュリティ インテリジェンス、侵入、マルウェアや IOC 検出のイベントビューでそのイベントが IOC をトリガーしたかどうかを表示します。IOC ルールをトリガーするエンドポイント ベースのマルウェア イベントは、イベント タイプが `AMP IOC` であり、侵害を指定するイベント サブタイプと一緒に表示されることに注意してください。イベント ビューは、[分析（Analysis）] タブ内のさまざまなタブから使用できます。
- ダッシュボード：ダッシュボードでは、サマリー ダッシュボードの [脅威（Threats）] タブに、ホスト別の IOC タグと一定期間にトリガーされた新しい IOC ルールがデフォルトで表示されます。カスタム分析ウィジェットは IOC データに基づくプリセットを提供します。
- コンテキスト エクスプローラ：コンテキスト エクスプローラの [侵害の兆候（Indications of Compromise）] セクションに、IOC カテゴリ別のホストとホスト別の IOC カテゴリのグラフが表示されます。
- [ネットワーク マップ（Network Map）] ページ：[分析（Analysis）] > [ホスト（Hosts）] > [ネットワーク マップ（Network Map）] にある [侵害の兆候（Indications of Compromise）] タブには、侵害されている可能性があるネットワーク上のホストが侵害のタイプと IP アドレス別にグループ分けして示されます。
- [ネットワーク ファイル トラジェクトリ（Network File Trajectory）] 詳細ページ：[分析（Analysis）] > [ファイル（Files）] > [ネットワーク ファイル トラジェクトリ（Network File Trajectory）] の下に一覧表示されているファイルの詳細ページでは、ネットワークの侵害の兆候を追跡できます。
- [侵害の兆候（Host Indications of Compromise）] ページ：[分析（Analysis）] > [ホスト（Hosts）] メニューの下の [侵害の兆候（Host Indications of Compromise）] ページには、モニタ対象ホストの一覧が IOC タグ別にグループ分けされて表示されます。このページのワークフローを使ってデータをドリルダウンできます。
- ホスト プロファイル ページ：侵害されている可能性があるホストのホスト プロファイルには、そのホストに関連付けられているすべての IOC タグが表示され、IOC タグの解決と IOC ルール状態の設定ができます。

侵害の兆候としてイベントにタグを付けるように設定するには、侵害の兆候ルールの有効化, （1570 ページ）を参照してください。

関連トピック

侵害の兆候ルールの有効化, （1570 ページ）

侵害の兆候データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、侵害の兆候（IOC）を示すテーブルを表示できます。検索する情報に応じてイベント ビューを操作します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

表示されるページは、使用するワークフローによって異なります。事前定義の IOC ワークフローはプロファイル ビューで終了しますが、これには、制約を満たすすべてのホストまたはユーザのホストプロファイルまたはユーザプロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

はじめる前に

- システムで侵害の兆候（IOC）を検出してタグを付けるには、ネットワーク検出ポリシーの IOC 機能をアクティブにして、少なくとも 1 つの IOC ルールを有効にする必要があります。侵害の兆候ルールの有効化，（1570 ページ）を参照してください。

手順

ステップ 1 事前定義されたワークフローを使用する場合、[分析（Analysis）]>[ホスト（Hosts）]>[侵害の兆候（Indications of Compromise）] を選択します。
ホスト IOC のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [侵害の兆候（Indications of Compromise）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用，（2097 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（侵害の兆候データ フィールド，（2122 ページ）を参照）。
- [ホストの侵害の兆候（Host Indications of Compromise）] ページ：[IP アドレス（IP Address）] カラムにある侵害されたホストのアイコン（  ）をクリックして、侵害されたホストのホスト プロファイルを表示します。
- IOC イベントに解決済みとマークして、リストに表示されないようにします。これを実行するには、編集する IOC イベントの横にあるチェック ボックスをオンにして、[解決済みとマークを付ける（Mark Resolved）] をクリックします。
- [最初の確認日時（First Seen）] または [前回の検出（Last Seen）] カラムにある表示アイコン（  ）をクリックして、IOC をトリガーしたイベントの詳細を表示します。

侵害の兆候データ フィールド

以下は、の IOC（侵害の兆候）テーブル内のフィールドです。すべての IOC 関連のテーブルにすべてのフィールドが含まれているわけではありません。

IP アドレス（IP Address）

IOC をトリガーとして使用したホストに関連付けられている IP アドレス。

カテゴリ（Category）

[マルウェアが実行されました（Malware Executed）] や [影響 1 の攻撃（Impact 1 Attack）] など、示された侵害のタイプの簡単な説明。

イベント タイプ（Event Type）

特定の IOC に関連付けられている識別子で、トリガーとして使用したイベントを参照します。

説明

侵害される可能性のあるホストへの影響の説明（[このホストはリモート制御下にある可能性があります（This host may be under remote control）] や [このホスト上でマルウェアが実行されました（Malware has been executed on this host）] など）。

最初の確認日時/最新の確認日時（First Seen/Last Seen）

IOC をトリガーとして使用したイベントが発生した最初（または最新）の日付と時刻。

ドメイン（Domain）

IOC をトリガーとして使用したホストのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

関連トピック

イベントの検索, （1871 ページ）

単一ホストにおける侵害の兆候のルール状態の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst（読み取り専用を除く）

ネットワーク検出ポリシーで有効になっている場合、侵害の兆候ルールは監視対象ネットワーク内のすべてのホストに適用されます。個々のホストのルールを無効にして、無用な IOC タグを回避できます（たとえば、DNS サーバに対する IOC タグが表示されないようにできます）。適用可能なネットワーク検出ポリシーでルールを無効にすると、特定のホストに対して有効にすることができません。

手順

ステップ 1 ホスト プロファイルの [侵害の兆候（Indications of Compromise）] セクションに移動します。

ステップ 2 [ルール状態の編集（Edit Rule States）] をクリックします。

ステップ 3 ルールの [有効（Enabled）] 列で、スライダをクリックしてこれを有効または無効にします。

ステップ 4 [保存（Save）] をクリックします。

侵害の兆候のタグのソース イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

ホスト プロファイルの [侵害の兆候（Indications of Compromise）] セクションを使用して、IOC タグをトリガーしたイベントにすばやく移動することができます。これらのイベントを分析すると、侵害される脅威に対処するのに必要なアクション、およびアクションが必要かどうかを判断するための情報が提供されます。

IOC タグのタイムスタンプの隣の表示アイコン（  ）をクリックすると、関連するイベント タイプのイベントのテーブル ビューにナビゲートします。ここでは、IOC タグをトリガーとして使用したイベントのみが表示されます。

手順

ステップ 1 ホスト プロファイルで、[侵害の兆候（Indications of Compromise）] セクションに移動します。

ステップ 2 調べたい IOC タグの [最初の痕跡（First Seen）] または [最後の痕跡（Last Seen）] カラムにある表示アイコン（）をクリックします。

侵害の兆候タグの解決

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

侵害の兆候（IOC）タグで示された脅威が分析および対処された後、またはIOCタグが誤検出を示していると判断した場合、イベントに解決済みのマークを付けることができます。イベントに解決済みのマークを付けると、そのイベントはホストプロファイルから削除されます。プロファイル上のアクティブなIOCタグがすべて解決されると、侵害されたホストアイコン（  ）は表示されなくなります。解決したIOCについても、IOCのトリガー元であるイベントは引き続き表示できます。

IOCタグをトリガーしたイベントが繰り返された場合、ホストに対するIOCルールが無効にされていない限り、このタグが再び設定されます。

手順

ステップ1 ホストプロファイルで、[侵害の兆候（Indications of Compromise）] セクションに移動します。

ステップ2 次の2つの選択肢があります。

- 個別のIOCタグに解決済みのマークを付けるには、解決するタグの右にある削除アイコン（）をクリックします。
- プロファイル上のすべてのIOCタグに解決済みのマークを付けるには、[すべてに解決済みのマークを付ける（Mark All Resolved）] をクリックします。

サーバ データ

Firepowerシステムは、モニタ対象ネットワーク セグメント上のホストで稼動しているすべてのサーバに関する情報を収集します。この情報には次のものが含まれます。

- サーバの名前
- サーバが使用するアプリケーションとネットワーク プロトコル
- サーバのベンダーとバージョン
- サーバを実行しているホストに関連付けられているIPアドレス
- サーバが通信するポート

システムはサーバを検出すると、関連するホストがまだサーバの最大数に達していない場合は、ディスカバリ イベントを生成します。Firepower Management Center の Web インターフェイスを使用して、サーバ イベントを表示、検索、削除できます。

また、サーバ イベントを相関ルールのベースにすることもできます。たとえばシステムが、いずれかのホスト上で稼動している ircd などのチャット サーバを検出したときに相関ルールをトリガーできます。

システムは、ホストをエクスポートされた NetFlow レコードからネットワーク マップに追加できますが、これらのホストに使用できる情報は限られます（NetFlowデータと管理対象デバイス データの違い，（1442 ページ） を参照）。

関連トピック

ホスト制限と検出イベント ロギング，（1511 ページ）
NetFlow データと管理対象デバイス データの違い，（1442 ページ）

サーバ データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、検出されたサーバのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがサーバにアクセスしたときに表示されるページは、使用するワークフローによって異なります。事前定義されたすべてのワークフローはホスト ビューで終了しますが、このホスト ビューには、制約を満たすすべてのホストに対して 1 つずつホスト プロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のように、サーバ データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析（Analysis）]>[ホスト（Hosts）]>[サーバ（Servers）] を選択します。

- サーバのテーブル ビューが含まれていないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [サーバ（Servers）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用, （2097 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（サーバデータ フィールド, （2126ページ）を参照）。
- 編集するサーバのイベントの横にあるチェック ボックスをオンにし、[サーバ アイデンティティの設定（Set Server Identity）] をクリックすることによって、サーバのアイデンティティを編集します。

関連トピック

サーバのアイデンティティの編集, （2070 ページ）

サーバ データ フィールド

サーバ テーブルで表示および検索できるフィールドの説明は次のとおりです。

前回の使用（Last Used）

ネットワーク上でサーバが最後に使用された日付と時間、またはホスト入力機能を使用してサーバが最初に更新された日付と時間。[前回の使用（Last Used）] の値は、システムがサーバ情報の更新を検出したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

[IPアドレス（IP Address）]

サーバを実行しているホストに関連付けられている IP アドレス。

[ポート（Port）]

サーバが稼動しているポート。

プロトコル

サーバが使用するネットワークまたはトランスポート プロトコル。

アプリケーション プロトコル（Application Protocol）

次のいずれかです。

- サーバのアプリケーション プロトコルの名前
- `pending`：システムで、いずれかの理由でサーバをポジティブまたはネガティブに識別できない場合
- `unknown`：既知のサーバ フィンガープリントに基づいてシステムでサーバを識別できない場合、またはホストの入力を介してサーバが追加され、アプリケーションプロトコルが含まれていなかった場合

アプリケーション プロトコルのカテゴリ、タグ、リスク、またはビジネスとの関連性（Category, Tags, Risk, or Business Relevance for Application Protocols）

アプリケーションプロトコルに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネスとの関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。

ベンダー（Vendor）

次のいずれかです。

- サーバのベンダー：システム、Nmap、その他のアクティブなソースで識別された、またはホスト入力機能を使用して指定されたサーバのベンダー
- 空白：システムが既知のサーバ フィンガープリントに基づいてベンダーを識別できなかった場合、または NetFlow データを使用してサーバがネットワーク マップに追加された場合

バージョン（Version）

次のいずれかです。

- サーバのバージョン：システム、Nmap、その他のアクティブなソースで識別された、またはホスト入力機能を使用して指定されたサーバのバージョン
- 空白：システムが既知のサーバ フィンガープリントに基づいてバージョンを識別できなかった場合、または NetFlow データを使用してサーバがネットワーク マップに追加された場合

Web アプリケーション（Web Application）

HTTP トラフィックでシステムが検出したペイロード コンテンツに基づいた Web アプリケーション。システムが `HTTP` のアプリケーション プロトコルを検出したものの、特定の Web アプリケーションを検出できない場合は、一般的な Web ブラウジングの指定が提示されるので注意してください。

Web アプリケーションのカテゴリ、タグ、リスク、またはビジネスとの関連性（Category, Tags, Risk, or Business Relevance for Web Applications）

Web アプリケーションに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネスとの関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。

ヒット数（Hits）

サーバがアクセスされた回数。ホスト入力機能を使用して追加されたサーバの場合、この値は必ず 0 になります。

ソース タイプ（Source Type）

次の値のいずれかを指定します。

- [ユーザ（User）]：user_name
- [アプリケーション（Application）]：app_name
- スキャナ：scanner_type（ネットワーク検出の設定を介して追加された Nmap またはスキャナ）
- Firepower システムによって検出されたサーバの `Firepower`、`Firepower Port Match`、または `Firepower Pattern Match`
- NetFlow データを使用して追加されたサーバの `NetFlow`

ドメイン

サーバを実行しているホストのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

Device

トラフィックを検出した管理対象デバイスか、NetFlow またはホスト入力データを処理したデバイスのいずれか。

現在のユーザ（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されます。権限のあるユーザがそのホストに関連付けられていない場合、権限のないユーザがそのホストの現行（現在の）ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

メンバー数（Count）

各行に表示される情報と一致するイベントの数。このフィールドが表示されるのは、2 つ以上の同一の行を作成する制限を適用した後のみです。

関連トピック

イベントの検索, （1871 ページ）
ネットワーク検出のデータ ストレージ設定, （1572 ページ）

アプリケーション データとアプリケーション詳細データ

監視対象ホストが別のホストに接続すると、システムは多くの場合、どのアプリケーションが使用されたかを判断することができます。Firepower システムは、電子メール、インスタント メッセージ、ピアツーピア、Web アプリケーション、およびその他のタイプのアプリケーションが多用されると検出します。

検出されたそれぞれのアプリケーションに対してシステムは、アプリケーションを使用した IP アドレス、製品、バージョン、および使用が検出された回数を記録します。Web インターフェイスを使用して、アプリケーション イベントを表示、検索、および削除できます。ホスト入力機能を使用して、1 つ以上のホスト上のアプリケーション データを更新することもできます。

どのアプリケーションがどのホストで稼動しているかがわかっている場合は、その情報をもとにホストプロファイルの認定を作成し、この認定によって、トラフィック プロファイルの作成中に収集するデータを制約することができます。また、相関ルールをトリガーする条件を制約することもできます。また、アプリケーションの検出を相関ルールのベースにすることもできます。たとえば、従業員に特定のメール クライアントを使用させたい場合は、システムが、いずれかの対象ホストで別のメール クライアントが稼動していることを検出したときに相関ルールをトリガーすることができます。

Firepower のアプリケーション ディテクタに関する最新情報は、各 Firepower システム更新のリリース ノート、各 VDB 更新のアドバイザリをよくご確認ください。

分析用にアプリケーション データを収集および保存するには、ネットワーク検出ポリシーでアプリケーションの検出が有効になっていることを確認します。

アプリケーション データの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、検出されたアプリケーションのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがアプリケーションにアクセスするときに表示されるページは、使用するワークフローによって異なります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のようにして、アプリケーション データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析（Analysis）] > [ホスト（Hosts）] > [アプリケーション詳細（Application Details）] を選択します。
- アプリケーションの詳細のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [クライアント（Clients）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用, （2097 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（アプリケーション データ フィールド, （2130 ページ）を参照）。
- クライアント、アプリケーション プロトコル、Web アプリケーションの横にあるアプリケーション詳細ビューのアイコン（  ）をクリックすることによって、特定のアプリケーションの [アプリケーション詳細ビュー（Application Detail View）] を開きます。

アプリケーション データ フィールド

システムは、既知のクライアント、アプリケーション プロトコル、または Web アプリケーションについてトラフィックを検出すると、アプリケーションおよびそのアプリケーションを実行しているホストに関する情報をログに記録します。

次に、アプリケーション テーブルで表示および検索できるフィールドについて説明します。

Application

検出されたアプリケーションの名前。

[IPアドレス（IP Address）]

アプリケーションを使用しているホストに関連付けられている IP アドレス。

タイプ（Type）

アプリケーションのタイプであり、次のものがあります。

アプリケーション プロトコル（Application Protocols）

ホスト間の通信を意味します。

クライアント アプリケーション

ホスト上で動作しているソフトウェアを意味します。

Web アプリケーション（Web Applications）

HTTP トラフィックの内容や要求された URL を意味します。

カテゴリ（Category）

アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。

タグ

アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。

リスク（Risk）

アプリケーションが組織のセキュリティ ポリシーに違反することがある目的で使用される可能性。アプリケーションのリスクの範囲は、[極めて低（Very Low）] から [極めて高（Very High）] までです。

侵入イベントをトリガーしたトラフィックで検出される Application Protocol Risk、Client Risk、Web Application Risk の 3 つ（存在する場合）の中で最も高いものとなります。

ビジネスとの関連性（Business Relevance）

アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。アプリケーションのビジネスとの関連性の範囲は、[極めて低（Very Low）] から [極めて高（Very High）] までです。

侵入イベントをトリガーしたトラフィックで検出される Application Protocol Business Relevance、Client Business Relevance、Web Application Business Relevance の 3 つ（存在する場合）の中で最も低いものとなります。

現在のユーザ（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

ドメイン

アプリケーションを使用しているホストのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

メンバー数（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索, （1871 ページ）

アプリケーション詳細データの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、検出されたアプリケーションの詳細テーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがアプリケーションの詳細にアクセスするときに表示されるページは、使用するワークフローによって異なります。2 つの事前定義されたワークフローがあります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のようにして、アプリケーション詳細データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析（Analysis）] > [ホスト（Hosts）] > [アプリケーション詳細（Application Details）] を選択します。
- アプリケーションの詳細のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [クライアント（Clients）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。

- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用, （2097 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（アプリケーションの詳細データ フィールド, （2133 ページ）を参照）。
- クライアントの横にあるアプリケーション詳細ビューのアイコン（  ）をクリックして、特定のアプリケーションの [アプリケーション詳細ビュー（Application Detail View）] を開きます。

アプリケーションの詳細データ フィールド

システムは、既知のクライアント、アプリケーションプロトコル、またはWebアプリケーションについてトラフィックを検出すると、アプリケーションおよびそのアプリケーションを実行しているホストに関する情報をログに記録します。

次に、アプリケーションの詳細テーブルで表示および検索できるフィールドについて説明します。

前回の使用（Last Used）

アプリケーションが前回使用された時間、またはホスト入力機能を使用してアプリケーションデータが更新された時間。[前回の使用（Last Used）] の値は、システムがアプリケーション情報の更新を検出したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

[IPアドレス（IP Address）]

アプリケーションを使用しているホストに関連付けられている IP アドレス。

クライアント（Client）

アプリケーションの名前。ただし、システムがアプリケーション プロトコルを検出したにも関わらず特定のクライアントを検出できなかった場合は、アプリケーション プロトコル名に `client` が付加されて一般名が表示されます。

バージョン（Version）

アプリケーションのバージョン。

クライアント、アプリケーションプロトコル、およびWebアプリケーションのカテゴリ、タグ、リスク、またはビジネスとの関係性（Category, Tags, Risk, or Business Relevance for Clients, Application Protocols, and Web Applications）

アプリケーションに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネスとの関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。

アプリケーション プロトコル（Application Protocol）

アプリケーションで使用されるアプリケーション プロトコル。ただし、システムがアプリケーション プロトコルを検出したにも関わらず特定のクライアントを検出できなかった場合は、アプリケーション プロトコル名に `client` が付加されて一般名が表示されます。

Web アプリケーション（Web Application）

HTTP トラフィックでシステムが検出したペイロード コンテンツまたは URL に基づく Web アプリケーション。ただし、HTTP のアプリケーション プロトコルが検出されたにも関わらず特定の Web アプリケーションを検出できない場合、ここには、標準の Web 閲覧先が表示されます。

ヒット数（Hits）

システムが使用中のアプリケーションを検出した回数。ホスト入力機能を使用して追加されたアプリケーションの場合、この値は常に `0` になります。

ドメイン

アプリケーションを使用しているホストのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

Device

アプリケーションの詳細が含まれている検出イベントを生成したデバイス。

現在のユーザ（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

メンバー数（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索, （1871 ページ）
ネットワーク検出のデータ ストレージ設定, （1572 ページ）

脆弱性データ

Firepowerシステムには、それ独自の脆弱性追跡データベースが含まれています。そのデータベースは、このシステムのフィンガープリンティング機能と組み合わせて使用されて、ネットワーク上のホストに関連付けられている脆弱性が特定されます。ホストで稼動しているオペレーティング システム、サーバ、およびクライアントには、関連付けられている異なる脆弱性一式があります。

Firepower Management Center を使用して次のことを行えます。

- ホストごとの脆弱性を追跡および確認できます。
- ホストにパッチを適用した後、またはホストが脆弱性に影響されないと判断した場合は、そのホストの脆弱性を非アクティブにすることができます。

サーバで使用されるアプリケーション プロトコルが Firepower Management Center 構成内でマップされない限り、ベンダーレスおよびバージョンレスのサーバの脆弱性はマップされません。ベンダーレスおよびバージョンレスのクライアントの脆弱性はマップできません。

関連トピック

サーバの脆弱性のマッピング, （611 ページ）

脆弱性データのフィールド

以下に説明する脆弱性データのフィールドは、脆弱性のテーブル ビューと脆弱性の詳細表示で次のように表示されます。

表 *281*：表示場所別の脆弱性データ フィールド

フィールド	テーブル ビュー	詳細の表示
その他の情報	No	Yes
使用可能なエクスプロイト（Available Exploits）	Yes	Yes
Bugtraq ID	Yes	Yes
CVE ID	No	Yes
メンバー数（Count）	Yes	No
発行日（Date Published）	Yes	Yes
説明	Yes	Yes
修正（Fixes）	No	Yes

フィールド	テーブル ビュー	詳細の表示
影響修飾子（Impact Qualification）	No	Yes
[リモート（Remote）]	Yes	Yes
Snort ID	Yes	Yes
ソリューション	Yes	Yes
SVID	Yes	Yes
技術的説明（Technical Description）	Yes	Yes
役職（Title）	Yes	Yes
脆弱性の影響（Vulnerability Impact）	Yes	Yes

その他の情報

既知の不正利用や可用性、不正利用のシナリオ、脆弱性を軽減する方針など、脆弱性に関する追加情報を（利用可能な場合に）表示するには、矢印をクリックします。

使用可能なエクスプロイト（Available Exploits）

脆弱性に対して既知の不正利用があるかどうかを示します（TRUE/FALSE）。

Bugtraq ID

Bugtraq データベースにおいて脆弱性に関連付けられている識別番号。（http://www.securityfocus.com/bid/）

メンバー数（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

CVE ID

MITRE の Common Vulnerabilities and Exposures（CVE）データベースで、脆弱性に関連付けられている識別番号（http://www.cve.mitre.org/）。

発行日（Date Published）

脆弱性が公開された日付。

説明

脆弱性についての簡単な説明。

修正（Fixes）

選択した脆弱性に対して、ダウンロード可能なパッチへのリンクを提供します。

ヒント　修正ファイルまたはパッチのダウンロードに対する直接リンクが表示されている場合は、リンクを右クリックして、自分のローカル コンピュータへ保存します。

影響修飾子（Impact Qualification）

ドロップダウン リストを使用して、脆弱性を有効または無効にします。Firepower Management Center は、影響の相関関係において、無効な脆弱性を無視します。

ユーザがここで指定する設定によって、システム全体で脆弱性がどのように処理されるか、およびユーザが値を選択するホスト プロファイルに脆弱性が限定されないかが決まります。

[リモート（Remote）]

脆弱性がリモートで不正利用されるかどうかを示します（TRUE/FALSE）。

Snort ID

Snort ID（SID）データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トラフィックを検出できる場合、その脆弱性は、侵入ルールの SID に関連付けられます。

脆弱性は複数の SID に関連付けることが可能（または SID に関連付けないことも可能）であることに注意してください。脆弱性が複数の SID に関連付けられている場合、脆弱性テーブルには、各 SID に対して 1 つのローが含まれています。

ソリューション

脆弱性の修復に関する情報。

SVID

脆弱性を追跡するためにシステムで使用する Cisco の脆弱性識別番号。

SVID について脆弱性の詳細にアクセスするには、表示アイコン（）をクリックします。

技術的説明（Technical Description）

脆弱性に関する詳細な技術的説明。

役職（Title）

脆弱性のタイトル。

脆弱性の影響（Vulnerability Impact）

Bugtraq データベースにおいて脆弱性に割り当てられている重大度を示します。0 ～ 10 の値で、10 が最も重大です。脆弱性の影響は、Bugtraq エントリの作成者によって決定されます。この作成者は、自身の判断および SANS Critical Vulnerability Analysis（CVA）の基準に従って脆弱性の影響を決定します。

関連トピック

イベントの検索, （1871 ページ）

脆弱性の非アクティブ化

脆弱性を非アクティブ化すると、システムでこの脆弱性を使用して侵入の影響の関連付けを評価することができなくなります。ネットワーク上のホストにパッチを適用した後、またはホストが脆弱性の影響を受けないと判断した後に、脆弱性を非アクティブ化できます。システムが、この脆弱性から影響を受けている新しいホストを検出すると、この脆弱性はこのホストに対して有効であると見なされます（自動的には非アクティブ化されません）。

IP アドレスによって制約されて**いない**脆弱性ワークフロー内である 1 つの脆弱性を非アクティブ化すると、ネットワーク上の検出されたすべてのホストに対してその脆弱性が非アクティブ化されます。脆弱性ワークフロー内の脆弱性を非アクティブ化できるのは、次の各ページだけです。

- デフォルトの脆弱性ワークフローの 2 ページ目の [ネットワーク上の脆弱性（Vulnerabilities on the Network）]。これには、ネットワーク上のホストに適用される脆弱性のみが表示されます。
- 脆弱性ワークフロー（カスタムまたは事前定義）のページ。このワークフローは、検索を使用して IP アドレスに基づいて制約されます。

1 台のホストに対して 1 つの脆弱性を非アクティブ化できます。この非アクティブ化は、ネットワークマップの使用、ホストのホストプロファイルの使用、または脆弱性を非アクティブ化する対象の 1 つ以上のホストの IP アドレスに基づいて脆弱性ワークフローを制約することによって行えます。関連付けられた複数の IP アドレスを持つホストの場合、この機能はそのホストの選択された 1 つの IP アドレスのみに適用されます。

マルチドメイン展開では、先祖ドメインで脆弱性を非アクティブ化すると、すべての子孫ドメインでその脆弱性が非アクティブ化されます。先祖ドメインで脆弱性をアクティブにした場合、リーフ ドメインでは、そのドメインにあるデバイスに対して脆弱性のアクティブ化または非アクティブ化を実行できます。

関連トピック

個々のホストに対する脆弱性の非アクティブ化, （2087 ページ）
個々の脆弱性の非アクティブ化, （2088 ページ）
複数の脆弱性の非アクティブ化, （2140 ページ）

脆弱性データの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、脆弱性のテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

脆弱性にアクセスするときに表示されるページは、使用するワークフローによって異なります。ユーザは事前定義のワークフローを使用できますが、これには脆弱性のテーブル ビューが含まれています。検出されたいずれかのホストが脆弱性を示しているかどうかに関係なく、テーブル ビューにはデータベース内の各脆弱性に対して 1 つのローが含まれています。事前定義のワークフローの2ページ目には、ネットワーク上で検出されたホストに適用されるそれぞれの脆弱性（まだユーザが非アクティブにしていないもの）に対して1つの行が含まれています。事前定義のワークフローは脆弱性の詳細ビューで終了しますが、このビューには、制約を満たすすべての脆弱性について詳細な説明が含まれています。

ヒント 単一のホストまたはホストのセットに適用される脆弱性を表示する場合は、ホストの IP アドレスまたは IP アドレスの範囲を指定して、脆弱性の検索を実行します。

また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

脆弱性のテーブルは、マルチドメイン展開のドメインによって制限されません。

手順

ステップ 1 次のように、脆弱性のテーブルにアクセスします。

- 事前定義された脆弱性ワークフローを使用する場合、[分析（Analysis）] > [脆弱性（Vulnerabilities）] > [脆弱性（Vulnerabilities）] を選択します。
- 脆弱性テーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [脆弱性（Vulnerabilities）] を選択します。

ステップ 2 次の選択肢があります。

- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用, （2097 ページ）を参照）。
- 脆弱性を非アクティブにして、現在脆弱な状態にあるホストについて、侵入の影響の相関に使用しないようにします（複数の脆弱性の非アクティブ化, （2140 ページ）を参照）。

- SVID カラムの表示アイコン（）をクリックして、脆弱性に関する詳細を表示します。または、脆弱性 ID を制約して脆弱性の詳細ページへドリルダウンします。
- タイトルを右クリックして [フルテキストの表示（Show Full Text）] を選択することによって、脆弱性タイトルのフルテキストを表示します。

脆弱性の詳細の表示

手順

脆弱性の詳細は、次の方法のいずれかで表示できます。

- [分析（Analysis）] > [脆弱性（Vulnerabilities）] > [脆弱性（Vulnerabilities）] を選択し、SVID の横にある表示アイコン（）をクリックします。
- [分析（Analysis）] > [脆弱性（Vulnerabilities）] > [サードパーティの脆弱性（Third Party Vulnerabilities）] を選択し、SVID の横にある表示アイコン（）をクリックします。
- [分析（Analysis）] > [ホスト（Hosts）] > [ネットワーク マップ（Network Map）] を選択し、[脆弱性（Vulnerabilities）] タブをクリックします。
- 脆弱性の影響を受けるホストのプロファイルを表示し、そのプロファイルの [脆弱性（Vulnerabilities）] セクションを展開します。

複数の脆弱性の非アクティブ化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

IP アドレスで制約されて**いない**脆弱性ワークフロー内で脆弱性を非アクティブにすると、ネットワーク上で検出されたすべてのホストに対する脆弱性が非アクティブ化されます。

マルチドメイン導入では、先祖ドメインで脆弱性を非アクティブ化すると、すべての子孫ドメインでも脆弱性が非アクティブ化されます。リーフ ドメインは、先祖ドメインで脆弱性がアクティブ化されていれば、自分のデバイスの脆弱性をアクティブ化または非アクティブ化できます。

手順

ステップ 1 次のように、脆弱性のテーブルにアクセスします。

- 事前定義された脆弱性ワークフローを使用する場合、[分析（Analysis）] > [脆弱性（Vulnerabilities）] > [脆弱性（Vulnerabilities）] を選択します。
- 脆弱性テーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [脆弱性（Vulnerabilities）] を選択します。

ステップ 2 [ネットワークの脆弱性（Vulnerabilities on the Network）] をクリックします。

ステップ 3 非アクティブにする脆弱性の横にあるチェックボックスをオンにします。

ステップ 4 ページ下部の [レビュー（Review）] をクリックします。

関連トピック

個々のホストに対する脆弱性の非アクティブ化, （2087 ページ）
個々の脆弱性の非アクティブ化, （2088 ページ）

サードパーティの脆弱性データ

Firepower システムには、それ独自の脆弱性追跡データベースが含まれています。そのデータベースは、このシステムのフィンガープリンティング機能と組み合わせて使用されて、ネットワーク上のホストに関連付けられている脆弱性が特定されます。

システムの脆弱性データは、サードパーティ製のアプリケーションからインポートしたネットワーク マップデータで補完できます。これを行うには、組織で、このデータをインポートするためのスクリプトを記述できるか、コマンド ラインでファイルのインポートを作成できなければなりません。詳細については、*Firepower System Host Input API Guide*を参照してください。

インポートしたデータを影響の相関に含めるには、サードパーティの脆弱性情報を、データベース内のオペレーティング システムおよびアプリケーションの定義にマップする必要があります。サードパーティの脆弱性情報は、クライアントの定義にマップすることはできません。

サードパーティの脆弱性データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

ホスト入力機能を使用してサードパーティの脆弱性データをインポートした後で、Firepower Management Center を使用してサードパーティの脆弱性のテーブルを表示することができます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

サードパーティの脆弱性にアクセスするときに表示されるページは、使用するワークフローによって異なります。2 つの事前定義されたワークフローがあります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のようにして、サードパーティの脆弱性データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析（Analysis）]>[脆弱性（Vulnerabilities）]>[サード パーティの脆弱性（Third Party Vulnerabilities）] を選択します。
- サードパーティの脆弱性のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [送信元別の脆弱性（Vulnerabilities by Source）] または [IP アドレス別の脆弱性（Vulnerabilities by IP Address）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用, （2097 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（サードパーティの脆弱性データのフィールド, （2142 ページ）を参照）。
- SVID カラムの表示アイコン（  ）をクリックして、サードパーティの脆弱性に関する詳細を表示します。または、脆弱性 ID を制約して脆弱性の詳細ページへドリルダウンします。

サードパーティの脆弱性データのフィールド

サードパーティの脆弱性テーブルで表示および検索できるフィールドの詳細は以下のとおりです。

脆弱性ソース（Vulnerability Source）

サードパーティの脆弱性のソース（QualysGuard、NeXpose など）。

脆弱性 ID（Vulnerability ID）

ソースの脆弱性に関連付けられている ID 番号。

[IPアドレス（IP Address）]

脆弱性の影響を受けるホストに関連付けられている IP アドレス。

[ポート（Port）]

ポート番号（脆弱性が、特定のポート上で実行されているサーバに関連付けられている場合）。

Bugtraq ID

Bugtraq データベースにおいて脆弱性に関連付けられている識別番号。（http://www.securityfocus.com/bid/）

CVE ID

MITRE の Common Vulnerabilities and Exposures（CVE）データベースで、脆弱性に関連付けられている識別番号（http://www.cve.mitre.org/）。

SVID

脆弱性を追跡するためにシステムで使用する従来の脆弱性識別番号。

SVID について脆弱性の詳細にアクセスするには、表示アイコン（）をクリックします。

Snort ID

Snort ID（SID）データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トラフィックを検出できる場合、その脆弱性は、侵入ルールの SID に関連付けられます。

脆弱性は複数の SID に関連付けることが可能（または SID に関連付けないことも可能）であることに注意してください。脆弱性が複数の SID に関連付けられている場合、脆弱性テーブルには、各 SID に対して 1 つのローが含まれています。

役職（Title）

脆弱性のタイトル。

説明

脆弱性についての簡単な説明。

ドメイン

この脆弱性を持つホストのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

メンバー数（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索，（1871 ページ）

ユーザおよびユーザ アクティビティ データ

ユーザおよびユーザ アクティビティ データは、個々のユーザ関連のワークフローに表示されます。

- ユーザ：このワークフローは、ネットワークで認識されるすべてのユーザを表示します。この表では 1 ユーザが 1 つの行を占めます。詳細については、ユーザ データ（User Data），（2149 ページ）を参照してください。
- ユーザ アクティビティ：このワークフローは、ネットワークで認識されるすべてのユーザ アクティビティを表示します。この表では、複数のユーザ アクティビティ インスタンスを持つ1ユーザが複数の行を占めます。詳細については、ユーザアクティビティデータ，（2152 ページ）を参照してください。

これらのワークフローの入力元であるアイデンティティ ソースの詳細については、ユーザアイデンティティ ソースについて，（1531 ページ）を参照してください。

ユーザ関連フィールド

ユーザ関連データは、ユーザおよびユーザ アクティビティのテーブルに表示されます。

表 *282*：ユーザおよびユーザ アクティビティのフィールドの説明

フィールド	説明	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
認証タイプ（Authentication Type）	認証のタイプ：[認証なし（No Authentication）]、[パッシブ認証（Passive Authentication）]、[アクティブ認証（Active Authentication）]、[ゲスト認証（Guest Authentication）]、または [失敗した認証（Failed Authentication）]。	なし	○
メンバー数（Count）	（注） [カウント（Count）]フィールドは、制約を適用した結果、同じ行が複数作成された場合にのみ表示されます。 特定の行に表示される情報と一致するユーザまたはイベントの数。	○	○

フィールド	説明	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
現在の IP（Current IP）	ユーザがログインしたホストに関連付けられている IP アドレス。ユーザがログインした後で、権限を持っている他のユーザが同じ IP アドレスでホストにログインすると、このフィールドは空白になります。ただし、あるユーザが権限を持っており、新しいユーザが権限を持っていない場合は除きます。（システムは、IP アドレスと、最後にホストにログインした権限のあるユーザを関連付けます。）	[はい（Yes）]	[いいえ（No）]
部署名（Department）	ユーザの部署（レルムが取得）。サーバ上のユーザに明示的に関連付けられている部門がない場合、この部門は、サーバが割り当てるいずれかのデフォルト グループとして示されます。たとえば、Active Directory では、これは `Users (ad)` となります。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Firepower Management Center が、Management Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。	[はい（Yes）]	[いいえ（No）]
説明	ユーザまたはユーザ アクティビティについての詳細情報（利用可能な場合）。	なし	○
Device	トラフィックベースの検出によって検出されたユーザ アクティビティの場合、ユーザを検出したデバイスの名前。他のタイプのユーザ アクティビティの場合は、管理している側の Firepower Management Center になります。	なし	○
ドメイン	[ユーザ（Users）] テーブルでは、ユーザのレルムに関連付けられたドメイン。 [ユーザ アクティビティ（User Activity）] テーブルでは、ユーザ アクティビティが検出されたドメイン。 このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。	○	○

フィールド	説明	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
電子メール（E-Mail）	ユーザのメール アドレス。以下の場合、このフィールドは空白になります。 • AIM ログインによってユーザがデータベースに追加された。 • LDAP ログインによってユーザがデータベースに追加されており、LDAP サーバ上にユーザと関連付けられている電子メール アドレスが存在しない。	[はい（Yes）]	[いいえ（No）]
イベント	ユーザ アクティビティのタイプ。	なし	○
名	ユーザの名（レルムが取得）。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Firepower Management Center が、Management Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。 • サーバに、対象のユーザと関連付けられている名がない。	[はい（Yes）]	[いいえ（No）]

フィールド	説明	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
[IPアドレス（IP Address）]	「ユーザ ログイン（User Login）」アクティビティの場合はログインに関連する IP アドレスです。ユーザのホストの IP アドレス（LDAP、POP3、IMAP、FTP、HTTP、MDNS、および AIM ログインの場合）、サーバの IP アドレス（SMTP および Oracle ログインの場合）、またはセッションの開始者の IP アドレス（SIP ログインの場合）のいずれかになります。 関連付けられている IP アドレスは、そのユーザが IP アドレスの現行のユーザであることを意味するわけではないので注意してください。権限を持たないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されます。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。 他のタイプのユーザ アクティビティの場合、このフィールドは空白です。	なし	○
姓	ユーザの姓（レルムが取得）。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Firepower Management Center が、Management Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。 • サーバに、対象のユーザと関連付けられている姓がない。	[はい（Yes）]	[いいえ（No）]

フィールド	説明	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
電話	ユーザの電話番号（レルムが取得）。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Firepower Management Center が、Management Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。 • サーバに、対象のユーザと関連付けられている電話番号が存在しない。	[はい（Yes）]	[いいえ（No）]
レルム	ユーザに関連付けられているアイデンティティ レルム。	○	○
時刻（Time）	システムがユーザ アクティビティを検出した時間。	なし	○
タイプ（Type）	ユーザの検出に使用されるプロトコル。これは、ldap、pop3、imap、oracle、sip、http、ftp、mdns、aim のいずれかです。ユーザは SMTP ログインに基づいてデータベースに追加されることはないため、このフィールドには smtp は表示されません。	○	○
ユーザ（User）	このフィールドには少なくとも、ユーザのレルムとユーザ名が表示されます。たとえば、`Lobby\jsmith` と表示された場合は、Lobby がレルム、jsmith がユーザ名です。 レルムが LDAP サーバから追加のユーザ データをダウンロードし、システムがそれをユーザに関連付けた場合は、このフィールドにユーザの名、姓、タイプも表示されます。たとえば、`John Smith (Lobby\jsmith, LDAP)` と表示された場合は、John Smith がユーザの名前、LDAP がそのタイプです。 （注） トラフィックベースの検出では失敗した AIM ログインが記録される可能性があるため（たとえば、ユーザが正しくないユーザ名を入力した場合など）、Firepower Management Center は無効な AIM ユーザを保存する可能性があります。	[はい（Yes）]	[いいえ（No）]
[ユーザ名（Username）]	ユーザに関連付けられているユーザ名。	○	○

ユーザ データ（User Data）

アイデンティティ ソースが、データベースに存在しないユーザのユーザ ログインを報告した場合、そのログイン タイプが特に制限されていない限り、そのユーザはデータベースに追加されます。

次のいずれかが発生すると、システムはユーザ データベースを更新します。

- Firepower Management Center のユーザが、[ユーザ（Users）] テーブルから権限のないユーザを手動で削除する。
- アイデンティティ ソースが、そのユーザによるログオフを報告する。
- レルムがレルムの [ユーザ セッションのタイムアウト：認証されたユーザ（User Session Timeout: Authenticated Users）] 設定、[ユーザ セッションのタイムアウト：認証に失敗したユーザ（User Session Timeout: Failed Authentication Users）] 設定、または [ユーザ セッションのタイムアウト：ゲスト ユーザ（User Session Timeout: Guest Users）] 設定で指定されているユーザ セッションを終了した。

（注） ISEが設定されている場合は、ユーザテーブルにホストデータが表示されることがあります。ISE によるホスト検出は完全にはサポートされていないため、ISE が報告したホスト データを使用してユーザ制御を実行することはできません。

システムによって検出されたユーザ ログインのタイプに応じて、新しいユーザのどの情報が保存されるかが決まります。

ID ソース	ログイン タイプ	格納されるユーザ データ
ISE	Active Directory LDAP RADIUS RSA	• ユーザ名 • 現行の IP アドレス • セキュリティ グループ タグ（SGT） • エンドポイントのプロファイル/デバイス タイプ • エンドポイントの場所/場所 IP • タイプ（LDAP）
ユーザ エージェント	Active Directory	• ユーザ名 • 現行の IP アドレス • タイプ（LDAP）

ID ソース	ログイン タイプ	格納されるユーザ データ
キャプティブ ポータル	Active Directory LDAP	• ユーザ名 • 現行の IP アドレス • タイプ（LDAP）
トラフィック ベースの検出	LDAP AIM Oracle SIP HTTP FTP MDNS	• ユーザ名 • 現行の IP アドレス • タイプ（AD）
	POP3 IMAP	• ユーザ名 • 現行の IP アドレス • 電子メール アドレス • タイプ（`pop3` または `imap`）

ユーザを自動的にダウンロードするようにレルムを設定すると、Firepower Management Center は指定した間隔に基づいてサーバに対するクエリを実行します。システムが新しいユーザのログインを検出してから、Firepower Management Center データベースがユーザのメタデータを更新するまでに、5～10 分かかることがあります。Firepower Management Centerは、ユーザごとに次の情報とメタデータを取得します。

- ユーザ名
- 姓と名
- 電子メール アドレス
- 部署
- 電話番号
- 現行の IP アドレス
- セキュリティ グループ タグ（SGT）（使用可能な場合）
- エンドポイントのプロファイル（使用可能な場合）
- エンドポイントの場所（使用可能な場合）

Firepower Management Center がデータベースに格納できるユーザの数は、Firepower Management Center のモデルによって異なります。ホストに対して権限を持たないユーザがログインしていることが検出された場合、そのログインはユーザおよびホストの履歴に記録されます。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、ホストに対して権限を持つユーザのログインが検出された後は、権限を持つ別のユーザがログインした場合にのみ、現行ユーザが変わります。

AIM、Oracle、およびSIPのログインがトラフィックベースで検出された場合は、システムがLDAPサーバから取得したどのユーザ メタデータにも関連付けられないため、これらのログインにより重複したユーザ レコードが作成されることに注意してください。これらのプロトコルから重複したユーザ レコードを取得することに起因するユーザカウントの過度な使用を回避するには、これらのプロトコルを無視するようにトラフィックベースの検出を設定します。

データベースからユーザを検索、表示、削除することができます。また、データベースからすべてのユーザを消去することもできます。

一般的なユーザ関連のイベント トラブルシューティングについては、レルムとユーザのダウンロードのトラブルシューティング, （1583 ページ） を参照してください。

ユーザ データの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

ユーザのテーブルを表示して、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができますが、これには、検出されたすべてのユーザが記載されているユーザのテーブル ビューが含まれています。このワークフローは、ユーザの詳細ページで終了します。ユーザの詳細ページは、制約を満たす各ユーザについての情報を提供します。

手順

ステップ 1 次のように、ユーザ データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析（Analysis）]>[ユーザ（Users）]>[ユーザ（Users）] を選択します。

- ユーザのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ユーザ（Users）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用, （2097 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ユーザ関連フィールド, （2144 ページ）を参照）。

ユーザ アクティビティ データ

Firepower システムでは、ネットワーク上のユーザ アクティビティの詳細を伝達するイベントを生成します。システムがユーザ アクティビティを検出すると、そのユーザ アクティビティ データはデータベースに記録されます。ユーザ アクティビティは、表示、検索、および削除することも、すべてのユーザ アクティビティをデータベースから消去することもできます。

あるユーザがネットワーク上で初めて確認されると、システムはそのユーザアクティビティイベントをログに記録します。そのユーザがその後に確認された場合、新しいユーザ アクティビティイベントはログに記録されません。ただし、そのユーザの IP アドレスが変わった場合、システムは新しいユーザ アクティビティ イベントをログに記録します。

Firepower システムでは、ユーザ アクティビティと他のタイプのイベントとの関連付けも行います。たとえば、侵入イベントは、そのイベントの発生時に送信元ホストと宛先ホストにログインしていたユーザを通知することができます。この関連付けにより、攻撃の対象になったホストにログインしていたユーザ、または内部攻撃やポートスキャンを開始したユーザがわかります。

ユーザ アクティビティは、相関ルールで使用することもできます。相関ルールは、ユーザ アクティビティのタイプだけでなく、指定した他の条件に基づいて作成することができます。相関ルールが相関ポリシーで使用される場合、ネットワーク トラフィックが条件を満たしたときは、相関ルールが修復およびアラートの応答を起動します。

（注） ISE を設定していた場合、ホスト データがユーザ テーブルに表示されることがあります。ISE によるホスト検出は完全にはサポートされていないため、ISEが報告したホストデータを使用してユーザ制御を実行することはできません。

次に、4 つのタイプのユーザ アクティビティ データについて説明します。

新しいユーザのアイデンティティ（New User Identity）

このタイプのイベントは、システムがデータベースに存在しない不明なユーザによるログインを検出したときに生成されます。

あるユーザがネットワーク上で初めて確認されると、システムはそのユーザアクティビティイベントをログに記録します。そのユーザがその後に確認された場合、新しいユーザ アクティビティイベントはログに記録されません。ただし、そのユーザのIPアドレスが変わった場合、システムは新しいユーザ アクティビティ イベントをログに記録します。

ユーザ ログイン（User Login）

このタイプのイベントは、次のことが発生した後に生成されます。

- ユーザ エージェントまたはISE が正常なユーザ ログインを報告した。
- キャプティブ ポータルのユーザ認証の実行が成功または失敗した。
- トラフィック ベースの検出がユーザ ログインの成功または失敗を検出した。

（注） トラフィック ベースの検出で検出されたSMTP ログインは、一致する電子メール アドレスを持つユーザがデータベースにすでに存在する場合を除いて記録されません。

権限のないユーザがあるホストにログインすると、そのログインはユーザとホストの履歴に記録されます。権限のあるユーザがそのホストに関連付けられていない場合、権限のないユーザがそのホストの現行（現在の）ユーザとなることが可能です。ただし、権限のあるユーザがそのホストにログインした後は、別の権限のあるユーザによるログインだけが現行ユーザを変更します。

キャプティブ ポータルまたはトラフィック ベースの検出を使用する場合、失敗したユーザ ログインと失敗したユーザ認証データについて、次の点に注意してください。

- トラフィック ベースの検出（LDAP、IMAP、FTP、およびPOP3 トラフィック）から報告された失敗したログインは、ユーザアクティビティのテーブル ビューに表示されますが、ユーザのテーブル ビューには表示されません。既知のユーザがログインに失敗した場合、システムではそのユーザをそのユーザ名で識別します。不明なユーザがログインに失敗した場合、システムではそのユーザ名として [失敗した認証（Failed Authentication）] を使用します。
- キャプティブ ポータルから報告された失敗した認証は、ユーザ アクティビティのテーブル ビューとユーザのテーブル ビューの両方に表示されます。既知のユーザが認証に失敗した場合、システムではそのユーザをそのユーザ名で識別します。不明なユーザが認証に失敗した場合、システムではそのユーザをそのユーザが入力したユーザ名で識別します。

ユーザのアイデンティティの削除（Delete User Identity）

このタイプのイベントは、データベースからユーザを手動で削除したときに生成されます。

ドロップ（廃棄）されたユーザのアイデンティティ：ユーザ制限に到達（User Identity Dropped: User Limit Reached）

このタイプのイベントは、システムがデータベースに存在しないユーザを検出したものの、Firepower Management Center のモデルで決定されているデータベースの最大ユーザ数に達したためにユーザを追加できなかったときに生成されます。

ユーザ制限に達すると、ほとんどの場合、データベースへの新しいユーザの追加が停止されます。新しいユーザを追加するには、古いユーザまたは非アクティブなユーザをデータベースから手動で削除するか、データベースからすべてのユーザを消去する必要があります。

ただし、システムでは権限のあるユーザが優先されます。すでに制限に達しており、これまでに検出されていない権限のあるユーザのログインが検出された場合、システムは長期間非アクティブな状態が続いている権限のないユーザを削除して、権限のある新しいユーザに置き換えます。

一般的なユーザ関連のイベント トラブルシューティングについては、レルムとユーザのダウンロードのトラブルシューティング，（1583 ページ） を参照してください。

関連トピック

ユーザ アクティビティ データベース，（1447 ページ）

ユーザ アクティビティ データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザアクティビティのテーブルを表示して、検索する情報に応じてイベント ビューを操作することができます。ユーザ アクティビティにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができます。このワークフローにはユーザ アクティビティのテーブル ビューが含まれており、制約を満たすすべてのユーザの詳細が含まれている、ユーザの詳細ページで終了します。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のように、ユーザ アクティビティ データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析（Analysis）]>[ユーザ（Users）]>[ユーザ アクティビティ（User Activity）] を選択します。
- ユーザ アクティビティのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ユーザ アクティビティ（User Activity）] を選択します。

ヒント イベントが表示されない場合は、時間範囲の調整が必要な可能性があります（時間枠の変更, （1859 ページ）を参照）。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用, （2097 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ユーザ関連フィールド, （2144 ページ）を参照）。

ユーザ プロファイルとホスト履歴

特定のユーザの詳細については、[ユーザ（User）] ポップアップ ウィンドウを表示して確認することができます。表示されるページ（このマニュアルでは「ユーザ プロファイル」と呼んでいます）には、Web インターフェイスで「ユーザのアイデンティティ（User Identity）」というタイトルが付いています。

このウィンドウは、次のビューから表示できます。

- ユーザ データを他の種類のイベントに関連付けるすべてのイベント ビュー
- ユーザのテーブル ビュー

ユーザ情報は、ユーザ ワークフローの最終ページにも表示されます。

表示されるユーザ データは、ユーザのテーブル ビューで表示されるものと同じです。

[侵害の兆候（Indications of Compromise）] セクション

このセクションについては、次のセクションを参照してください。

- 侵害の兆候, （1569 ページ）
- 侵害の兆候データ フィールド, （2122 ページ）
- 単一ホストにおける侵害の兆候のルール状態の編集, （2122 ページ）
- 侵害の兆候タグの解決, （2124 ページ）
- 侵害の兆候のタグのソース イベントの表示, （2123 ページ）

[ホストの履歴（Host History）] セクション

ホストの履歴には、過去 24 時間のユーザ アクティビティがグラフィック表示されます。ユーザがログインおよびログオフしたホストの IP アドレスのリストには、ログインとログアウトの概算時間が棒グラフで示されます。一般的なユーザは、1 日の間に複数のホストに対してログオンおよびログオフする可能性があります。たとえば、メール サーバに対する定期的な自動ログインは

複数回の短時間のセッションとして示されますが、（勤務時間中などの）長時間のログインは、長時間のセッションとして示されます。

トラフィック ベースの検出またはキャプティブ ポータルを使用して失敗したログインをキャプチャした場合、ホストの履歴にはユーザがログインに失敗したホストも含まれます。

ホストの履歴を生成するために使用されるデータは、ユーザの履歴データベースに格納されます。このデータベースには、デフォルトで 1000 万のユーザ ログイン イベントが格納されます。ホストの履歴に特定のユーザに関するデータが表示されない場合、そのユーザが非アクティブであるか、またはデータベースの制限を増やさなければならないことがあります。

関連トピック

ユーザ データのフィールド

ユーザの詳細およびホスト履歴の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

次の 2 つの対処法があります。

- ユーザをリストする任意のイベント ビューで、ユーザ ID の横に表示されるユーザ アイコン（  ）をクリックします。
- いずれかのユーザ ワークフローで、[ユーザ（Users）] の最終ページをクリックします。

第 89 章

相関イベントとコンプライアンス イベント

次のトピックでは、相関イベントとコンプライアンス イベントを表示する方法について説明します。

相関イベントの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

アクティブな相関ポリシーに含まれる相関ルールがトリガーとして使用されると、システムが相関イベントを生成してデータベースにそれを記録します。

（注） アクティブな相関ポリシーに含まれるコンプライアンス ホワイトリストがトリガーとして使用されると、システムがホワイトリスト イベントを生成します。

相関イベントのテーブルを表示し、検索対象の情報に応じてイベント ビューを操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

相関イベントにアクセスしたときに表示されるページは、使用するワークフローによって異なります。相関イベントのテーブル ビューが含まれる定義済みワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 [分析（Analysis）] > [相関（Correlation）] > [相関イベント（Correlation Events）] を選択します。オプションで、カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] をクリックします。

ヒント 相関イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックし、[相関イベント（Correlation Events）] を選択します。

ステップ 2 オプションで、時間枠の変更, （1859 ページ）の説明に従って、時間範囲を調整します。

ステップ 3 次のいずれかの操作を実行します。

- 表示されるカラムの詳細については、相関イベントのフィールド, （2159 ページ）を参照してください。
- IP アドレスのホスト プロファイルを表示するには、IP アドレスの横に表示されるホスト プロファイル アイコンをクリックします。
- ユーザID情報を表示するには、ユーザIDの横に表示されるユーザアイコン（  ）をクリックします。
- 現在のワークフローページ内でイベントをソートしたり制限したり、または移動するには、ワークフローの使用, （1834 ページ）を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフローページの左上にある該当するページ リンクをクリックします。
- 特定の値に制限して、ワークフロー内の次のページにドリルダウンするには、ドリルダウンページの使用, （1844 ページ）を参照してください。
- 一部またはすべての相関イベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除（Delete）] をクリックするか、[すべて削除（Delete All）] をクリックして現在の制約されているビューにあるすべてのイベントを削除することを確認します。
- 他のイベント ビューに移動して関連イベントを表示するには、ワークフロー間のナビゲーション, （1866 ページ）を参照してください。

関連トピック

データベース イベント数の制限, （563 ページ）
ワークフローのページ, （1838 ページ）

相関イベントのフィールド

相関ルールがトリガーとして使用されると、システムは相関イベントを生成します。次の表では、表示および検索可能な相関イベント テーブルのフィールドについて説明します。

表 *283*：相関イベントのフィールド

フィールド	説明
説明	相関イベントについての説明。説明に示される情報は、ルールがどのようにトリガーとして使用されたかによって異なります。 たとえば、オペレーティング システム情報の更新イベントによってルールがトリガーとして使用された場合、新しいオペレーティング システムの名前と信頼度レベルが表示されます。
Device	ポリシー違反をトリガーとして使用したイベントを生成したデバイスの名前。
ドメイン	ポリシー違反をトリガーとして使用したモニタ対象トラフィックのデバイスのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
影響（Impact）	侵入データ、ディスカバリ データ、および脆弱性情報の間の相関に基づいて相関イベントに割り当てられた影響レベル。 このフィールドを検索する場合、大文字と小文字を区別しない有効な値は、`Impact 0`、`Impact Level 0`、`Impact 1`、`Impact Level 1`、`Impact 2`、`Impact Level 2`、`Impact 3`、`Impact Level 3`、`Impact 4`、および `Impact Level 4` です。影響アイコンの色または部分文字列は使用しないでください（たとえば、`blue`、`level 1`、または `0` を使用しないでください）。
入力インターフェイス（Ingress Interface）または出力インターフェイス（Egress Interface）	ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力インターフェイス。
入力セキュリティ ゾーン（Ingress Security Zone）または出力セキュリティ ゾーン（Egress Security Zone）	ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力セキュリティ ゾーン。

フィールド	説明
インライン結果（Inline Result）	次のいずれかになります。 • 黒の下矢印：侵入ルールをトリガーとして使用したパケットがシステムによってドロップされたことを示します • グレーの下矢印：侵入ポリシーオプション[インライン時にドロップ（Drop when Inline）]を有効にした場合、インライン型、スイッチ型、またはルーティング型展開でパケットがシステムによってドロップされたと想定されることを示します • 空白：トリガーとして使用された侵入ルールが [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていなかったことを示します 侵入イベントによってトリガーとして使用されたポリシー違反を検索するためにこのフィールドを使用する場合は、次のいずれかを入力します。 • `dropped` は、インライン型、スイッチ型、またはルーティング型展開でパケットがドロップされたかどうかを示します。 • `would have dropped` は仮定を表します。インライン型、スイッチ型、またはルーティング型展開でパケットをドロップするよう侵入ポリシーが設定されていると仮定した場合、パケットがドロップされるかどうかを示します。 侵入ポリシーのドロップ動作やルール状態とは無関係に、パッシブ展開（インラインセットがタップモードである場合を含む）ではシステムがパケットをドロップしないことに注意してください。
ポリシー	違反が発生したポリシーの名前。
[プライオリティ（Priority）]	相関イベントのプライオリティ。これは、トリガーとして使用されたルールのプライオリティまたは違反が発生した相関ポリシーのプライオリティによって決まります。このフィールドを検索するとき、プライオリティなしの場合は `none` を入力します。
ルール（Rule）	ポリシー違反をトリガーとして使用したルールの名前。
セキュリティインテリジェンス カテゴリ（Security Intelligence Category）	ブラックリスト化されたオブジェクトの名前。これは、ポリシー違反をトリガーとして使用したイベントでブラックリスト化された IP アドレスを示す（またはその IP アドレスを含む）オブジェクトです。 このフィールドを検索する場合は、ポリシー違反をトリガーとして使用した相関イベントに関連付けられたセキュリティ インテリジェンスのカテゴリを指定します。セキュリティ インテリジェンスのカテゴリとして、セキュリティ インテリジェンス オブジェクト、グローバル ブラックリスト、カスタム セキュリティ インテリジェンス リストまたはフィード、あるいはインテリジェンス フィードに含まれるいずれかのカテゴリを指定できます。

フィールド	説明
送信元の大陸（Source Continent）または宛先の大陸（Destination Continent）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストIPアドレスに関連付けられた大陸。
送信元の国（Source Country）または宛先の国（Destination Country）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先IPアドレスに関連付けられた国。
送信元ホストの重大度（Source Host Criticality）または宛先ホストの重大度（Destination Host Criticality）	相関イベントに関連する送信元または宛先ホストにユーザが割り当てたホスト重要度。`None`、`Low`、`Medium`、または `High` のいずれかです。 ディスカバリイベント、ホスト入力イベント、または接続イベントに基づくルールによって生成された相関イベントにのみ、送信元ホスト重要度が含まれることに注意してください。
送信元IP（Source IP）または宛先IP（Destination IP）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストのIPアドレス。
送信元ポート/ICMPタイプ（Source Port/ICMP Type）または宛先ポート/ICMPコード（Destination Port/ICMP Code）	ポリシー違反をトリガーとして使用したイベントに関連付けられた、送信元トラフィックの送信元ポート/ICMPタイプまたは宛先トラフィックの宛先ポート/ICMPコード。
送信元ユーザ（Source User）または宛先ユーザ（Destination User）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストにログインしたユーザの名前。
時刻（Time）	相関イベントが生成された日時。このフィールドは検索できません。
メンバー数（Count）	各行に表示される情報と一致するイベントの数。[カウント（Count）]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません

関連トピック

イベントの検索，（1871 ページ）

コンプライアンス ホワイト リスト ワークフローの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst/Discovery Admin

Firepower Management Center は、ネットワークで生成されるホワイト リスト イベントおよびホワイト リスト違反の分析で使用できるワークフロー セットを提供します。ワークフローはネットワーク マップやダッシュボードとともに、ネットワーク資産のコンプライアンスに関する主要な情報源になります。

システムは、ホワイト リスト イベントとホワイト リスト違反のために事前定義されたワークフローを提供します。ユーザはカスタム ワークフローを作成することもできます。コンプライアンス ホワイト リスト ワークフローを使用すると、多くの一般的なアクションを実行できます。

手順

ステップ 1 [分析（Analysis）] > [相関（Correlation）] メニューを使用してホワイト リスト ワークフローにアクセスします。

ステップ 2 次の選択肢があります。

- ワークフローの切り替え：カスタム ワークフローなどの別のワークフローを使用するには、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。
- 時間範囲：時間範囲を調整（イベントが表示されない場合に役立ちます）する方法については、時間枠の変更, （1859 ページ）を参照してください。
- ホスト プロファイル：IP アドレスのホスト プロファイルを表示するには、ホスト プロファイルのアイコン（  ）をクリックします。アクティブな侵害の兆候（IOC）タグのあるホストの場合は、IP アドレスの横に表示される侵害されたホストのアイコン（  ）をクリックします。
- ユーザ プロファイル（イベントのみ）：ユーザ ID 情報を表示するには、ユーザ ID の横に表示されるユーザ アイコン（  ）をクリックします。
- 制約：表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン（）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

ヒント　他のカラムを表示または非表示にするには、[適用（Apply）]をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効になったカラムをビューに再び追加するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- ドリル ダウン：ドリルダウン ページの使用，（1844 ページ）を参照してください。
- ソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- このページに移動する：ワークフロー ページのトラバーサル ツール，（1840 ページ）を参照してください。
- ページ間で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- イベント ビュー間で移動する：関連するイベントを表示するためその他のイベント ビューに移動するには、[ジャンプ（Jump to）]をクリックし、ドロップダウン リストからイベント ビューを選択します。
- イベントの削除（イベントのみ）：現在の制約されているビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。

関連トピック

ワークフローのページ，（1838 ページ）
イベント ビュー設定の設定，（38 ページ）

ホワイトリスト イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst/Discovery Admin

最初の評価が行われた後、監視対象ホストがアクティブなホワイト リストに準拠しなくなると、システムはホワイト リスト イベントを生成します。ホワイト リスト イベントは、相関イベントの特殊な形態で、Management Center 相関イベント データベースに記録されます。

Firepower Management Center を使用して、コンプライアンス ホワイト リスト イベントのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ホワイトリストイベントにアクセスしたときに表示されるページは使用しているワークフローによって異なります。イベントのテーブル ビューで終わる事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 [分析（Analysis）] > [相関（Correlation）] > [ホワイトリストイベント（White List Events）]を選択します。

ステップ 2 次の選択肢があります。

- 基本的なワークフロー操作を実行するには、コンプライアンスホワイトリストワークフローの使用, （2162 ページ）を参照してください。
- テーブルのカラムの内容について詳しく調べるには、ホワイト リスト イベントのフィールド, （2164 ページ）を参照してください。

ホワイト リスト イベントのフィールド

ワークフローを使用して表示および検索できるホワイトリストイベントには、次のフィールドがあります。

Device

ホワイト リスト違反を検出した管理対象デバイスの名前。

説明

ホワイト リスト違反の説明。次に例を示します。

```
Client “AOL Instant Messenger” is not allowed.
```

アプリケーション プロトコルに関係する違反には、アプリケーション プロトコルの名前とバージョンだけでなく、使用されているポートとプロトコル（TCP または UDP）も示されます。禁止を特定のオペレーティング システムに限定する場合は、説明にオペレーティング システム名が含まれます。次に例を示します。

```
Server "ssh / 22 TCP (OpenSSH 3.6.1p2)" is not allowed on Operating System
“Linux Linux 2.4 or 2.6”.
```

ドメイン

ホワイト リストに準拠しなくなったホストのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

ホストの重要度（Host Criticality）

ホワイト リストに準拠していないホストに対してユーザが割り当てた重要度（[なし（None）]、[低（Low）]、[中（Medium）]、または [高（High）]）。

[IPアドレス（IP Address）]

ホワイト リストに準拠しなくなったホストの IP アドレス。

ポリシー

違反した相関ポリシー、つまりホワイト リストを含む相関ポリシーの名前。

[ポート（Port）]

アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーした検出イベントに関連付けられているポート（存在する場合）。他のタイプのホワイト リスト違反の場合、このフィールドは空白です。

[プライオリティ（Priority）]

ポリシーまたはポリシー違反をトリガーしたホワイト リストに指定されている優先度。これは、相関ポリシー内のホワイト リストの優先度または相関ポリシー自体の優先度によって決まります。ホワイト リストの優先度は、そのポリシーの優先度より優先されることに注意してください。このフィールドを検索するとき、プライオリティなしの場合は `none` を入力します。

時刻（Time）

ホワイト リスト イベントが生成された日時。このフィールドは検索できません。

ユーザ（User）

ホワイトリストに準拠しなくなったホストにログインしている既知のユーザのアイデンティティ。

ホワイト リスト（White List）

ホワイト リストの名前。

メンバー数（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

ホワイトリスト違反の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst/Discovery Admin

システムは、ネットワークの現在のホワイト リスト違反のレコードを保持します。違反はそれぞれ、ホストのいずれかで実行することが禁止されている事柄を表します。ホストが準拠するようになると、システムは、修正された違反をデータベースから削除します。

Firepower Management Center を使用して、アクティブなすべてのホワイト リストに対するホワイト リスト違反のテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

ホワイト リスト違反にアクセスしたときに表示されるページは使用しているワークフローによって異なります。事前定義されたワークフローはホスト ビューで終了しますが、このホスト ビューには、制約を満たすすべてのホストに対して 1 つずつホスト プロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [相関（Correlation）] > [ホワイトリスト違反（White List Violations）]を選択します。

ステップ 2 次の選択肢があります。

- 基本的なワークフロー操作を実行するには、コンプライアンス ホワイト リスト ワークフローの使用, （2162 ページ）を参照してください。
- テーブルのカラムの内容について詳しく調べるには、ホワイト リスト違反のフィールド, （2166 ページ）を参照してください。

ホワイト リスト違反のフィールド

ワークフローを使用して表示および検索できるホワイト リスト違反には、次のフィールドがあります。

ドメイン

非準拠ホストが存在するドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

情報

ホワイト リスト違反に関連付けられたすべての利用可能なベンダー、製品、またはバージョン情報。ホワイト リストに違反するプロトコルの場合、このフィールドには、違反の原因がネットワーク プロトコルとトランスポート プロトコルのどちらであるのかも示されます。

[IPアドレス（IP Address）]

非準拠ホストの IP アドレス。

[ポート（Port）]

アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられているポート（存在する場合）。他のタイプのホワイト リスト違反の場合、このフィールドは空白です。

プロトコル

アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられているプロトコル（存在する場合）。他のタイプのホワイト リスト違反の場合、このフィールドは空白です。

時刻（Time）

ホワイト リスト違反が検出された日時。

タイプ（Type）

ホワイト リスト違反のタイプ、つまり、非準拠の結果として違反が発生したかどうか。

- オペレーティング システム（os）（このフィールドを検索する場合は、os または operating system と入力してください）。
- アプリケーション プロトコル（サーバ）
- クライアント
- プロトコル
- Web アプリケーション（web）（このフィールドを検索する場合は、web application と入力してください）。

ホワイト リスト（White List）

違反されたホワイト リストの名前。

メンバー数（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

修復ステータス イベント

修復がトリガーされると、システムは修復ステータス イベントをデータベースに記録します。これらのイベントは、[修復ステータス（Remediation Status）] ページで確認できます。修復ステータス イベントを検索、表示、削除できます。

関連トピック

修復ステータスのテーブル フィールド, （2169 ページ）

修復ステータス イベントの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

修復ステータス イベントにアクセスするときに表示されるページは、使用するワークフローにより異なります。修復のテーブル ビューを含む定義済みワークフローを使用できます。テーブル ビューには、各修復ステータス イベントの行が含まれます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [相関（Correlation）] > [ステータス（Status）]を選択します。

ステップ 2 オプションで、時間枠の変更, （1859 ページ）の説明に従って、時間範囲を調整します。

ステップ 3 オプションで、カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] をクリックします。

ヒント 修復のテーブル ビューが含まれないカスタム ワークフローを使用する場合、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] メニューをクリックし、[修復ステータス（Remediation Status）] を選択します。

ステップ 4 次の選択肢があります。

- 表示されるカラムの詳細については、修復ステータスのテーブル フィールド, （2169 ページ）を参照してください。

- イベントをソートしたり、制約したりするには、ワークフローの使用, （1834ページ）を参照してください。
- 相関イベント ビューに移動し関連するイベントを確認するには、[相関イベント（Correlation Events）] をクリックします。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。ブックマークの管理ページに移動するには、[ブックマークの表示（View Bookmarks）] をクリックします。
- テーブル ビューのデータに基づいてレポートを生成するには、イベント ビューからのレポート テンプレートの作成, （1716ページ）で説明されているように、[レポート デザイナ（Report Designer）] をクリックします。
- ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用, （1844ページ）を参照してください。
- システムから修復ステータス イベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除（Delete）] をクリックするか、[すべて削除（Delete All）] をクリックして現在の制約されているビューにあるすべてのイベントを削除することを確認します。
- 修復ステータス イベントを検索するには、[検索（Search）] をクリックします。

関連トピック

ワークフローの使用, （1834 ページ）

修復ステータスのテーブル フィールド

次の表に、表示および検索できる修復のステート テーブルのフィールドを示します。

表 *284*：修復ステータス フィールド

フィールド	説明
ドメイン（Domain）	監視対象のトラフィックがポリシー違反をトリガーとして使用し、次に修復をトリガーとして使用するデバイスのドメイン。このフィールドは、マルチテナンシーのためにFirepower Management Center を設定したことがある場合に表示されます。
ポリシー	違反し、修復をトリガーとして使用した相関ポリシーの名前。
修復名	起動された修復の名前。

フィールド	説明
結果メッセージ	修復が起動したときに発生した事象を示すメッセージ。ステータス メッセージには以下が含まれます。 • Successful completion of remediation • Error in the input provided to the remediation module • Error in the remediation module configuration • Error logging into the remote device or server • Unable to gain required privileges on remote device or server • Timeout logging into remote device or server • Timeout executing remote commands or servers • The remote device or server was unreachable • The remediation was attempted but failed • Failed to execute remediation program • Unknown/unexpected error カスタム修復モジュールがインストールされている場合、カスタム モジュールによって実装される追加のステータス メッセージが表示される場合があります。
ルール（Rule）	修復をトリガーとして使用したルールの名前。
時刻（Time）	Firepower Management Center が修復を起動した日付と時刻。
メンバー数（Count）	各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

関連トピック

イベントの検索, （1871 ページ）

修復ステータス イベント テーブルの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

イベント ビューのレイアウトを変更したり、ビュー内のイベントをフィールド値で制限したりできます。

カラムを無効にすると、そのカラムは（後で元に戻さない限り）そのセッションの期間中は無効になります。最初のカラムを無効にすると、[カウント（Count）] カラムが追加されます。

テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（次のページにはドリルダウンされません）。

ヒント テーブル ビューでは、必ずページ名に「Table View」が含まれます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [相関（Correlation）] > [ステータス（Status）]を選択します。

ヒント 修復のテーブル ビューが含まれないカスタム ワークフローを使用する場合、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] メニューをクリックし、[修復ステータス（Remediation Status）] を選択します。

ステップ 2 次の選択肢があります。

- 表示されるカラムの詳細については、修復ステータスのテーブル フィールド, （2169 ページ）を参照してください。
- イベントをソートしたり、制約したりするには、ワークフローの使用, （1834 ページ）を参照してください。

第 90 章

システムの監査

次のトピックでは、システム上のアクティビティを監査する方法について説明します。

システム監査について

システム上のアクティビティを 2 つの方法で監査できます。Firepower システムの一部であるアプライアンスによって、Web インターフェイスとユーザとの対話のそれぞれに対して監査レコードが生成され、システム ステータス メッセージがシステム ログに記録されます。

関連トピック

レポートの概要，（1711 ページ）

監査レコード

Firepower Management Center および 7000 および 8000 シリーズ管理対象デバイスは、ユーザ アクティビティに関する読み取り専用の監査情報をログに記録します。監査ログは標準イベント ビューに表示され、監査ビュー内の任意の項目に基づいて監査ログ メッセージを表示、ソート、およびフィルタリングできます。監査情報を簡単に削除したり、それに関するレポートを作成したりすることができ、ユーザが行った変更に関する詳細なレポートを表示することもできます。

監査ログには最大 100,000 のエントリが保存されます。監査ログ エントリの数が 100,000 を超えると、アプライアンスは最も古いレコードをデータベースからプルーニングして、100,000 エントリまで数を削減します。

（注） 7000 または 8000 シリーズ デバイスをリブートした直後にすばやく補助 CLI にログインした場合、そこで実行するコマンドは、ローカル Web インターフェイスが使用可能になるまでは監査ログに記録されません。

監査レコードの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

Firepower Management Center または 7000 および 8000 シリーズ デバイスで、監査レコードのテーブルを表示できます。事前定義された監査ワークフローには、イベントを示す単一のテーブル ビューが含まれます。ユーザは検索する情報に応じてテーブル ビューを操作することができます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [システム（System）]>[モニタリング（Monitoring）]>[監査（Audit）] を使用して監査ログのワークフローにアクセスします。

ステップ 2 イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。詳細については、イベント時間の制約, （1855 ページ）を参照してください。

（注） イベント ビューを時間によって制約している場合は、（グローバルかイベント固有かに関係なく）アプライアンスに設定されている時間枠の外で生成されたイベントが、イベント ビューに表示されます。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

ステップ 3 次の選択肢があります。

- テーブルのカラムの内容について詳しく調べるには、システム ログ, （2182 ページ）を参照してください。
- 現在のワークフロー ページでイベントをソートしたり、制限したりするには、テーブル ビュー ページの使用, （1845 ページ）を参照してください。
- 現在のワークフローページ内で移動するには、時間枠の進行, （1862 ページ）を参照してください。

- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフローページの左上にある該当するページ リンクをクリックします。詳細については、ワークフローの使用，（1834 ページ）を参照してください。
- ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用，（1844 ページ）を参照してください。
- 特定の値で制約するには、行内の値をクリックします。ドリルダウン ページで値をクリックすると、次のページに移動し、その値だけに制約されます。テーブル ビューの行内の値をクリックすると、テーブル ビューが制限され、次のページに**ドリルダウンされない**ことに注意してください。詳細については、イベント ビューの制約，（1863 ページ）を参照してください。

  ヒント　テーブル ビューでは、必ずページ名に「Table View」が含まれます。
- 監査レコードを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除（Delete）] をクリックするか、[すべて削除（Delete All）] をクリックして現在の制約されているビューにあるすべてのイベントを削除します。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。詳細については、ブックマーク，（1867 ページ）を参照してください。
- ブックマークの管理ページに移動するには、[ブックマークの表示（View Bookmarks）] をクリックします。詳細については、ブックマーク，（1867 ページ）を参照してください。
- 現在のビューのデータに基づいてレポートを生成するには、[レポート デザイナ（Report Designer）] をクリックします。詳細については、イベント ビューからのレポート テンプレートの作成，（1716 ページ）を参照してください。
- 監査ログに記録された変更の概要を表示するには、[メッセージ（Message）] カラムの該当するイベントの横にある比較アイコン（  ）をクリックします。詳細については、監査ログを使って変更を調査する，（2177 ページ）を参照してください。

関連トピック

イベント ビューの制約，（1863 ページ）

監査ログのワークフロー フィールド

次の表で、表示および検索できる監査ログ フィールドについて説明します。

表 *285*：監査ログのフィールド

フィールド	説明
時刻（Time）	アプライアンスが監査レコードを生成した日時。

フィールド	説明
ユーザ（User）	監査イベントをトリガーしたユーザのユーザ名。
サブシステム	監査レコードが生成されたときにユーザがたどったフル メニュー パス。たとえば、[システム（System）]>[モニタリング（Monitoring）]>[監査（Audit）]は、監査ログを表示するためのメニュー パスです。 メニュー パスが該当しない数少ないケースでは、[サブシステム（Subsystem）]フィールドにイベント タイプのみが表示されます。たとえば、Login は、ユーザがログインしようとしたことを表します。
メッセージ（Message）	ユーザが実行したアクション、またはユーザがページでクリックしたボタン。 たとえば、`Page View` は、[サブシステム（Subsystem）]に示されているページをユーザが単に表示したことを意味します。`Save` は、ユーザがページの [保存（Save）] ボタンをクリックしたことを意味します。 Firepower システムに対する変更は比較アイコン（）付きで表示され、アイコンをクリックすると変更の概要を確認することができます。
ソース IP	ユーザが使用したホストに関連付けられている IP アドレス。 注：このフィールドを検索する場合は、特定の IP アドレスを入力する必要があります。監査ログの検索で IP 範囲を使用することはできません。
ドメイン（Domain）	監査イベントがトリガーされたときのユーザの現行ドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
設定の変更（Configuration Change） （検索専用）	設定の変更の監査レコードを検索結果に表示するかどうかを指定します。(`yes` または `no`)
メンバー数（Count）	各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

関連トピック

イベントの検索, （1871 ページ）

[監査イベント（Audit Events）] テーブル ビュー

イベント ビューのレイアウトを変更したり、ビュー内のイベントをフィールド値で制限したりできます。カラムを無効にする場合は、非表示にするカラム見出しの [閉じる（Close）] アイコン（✖）をクリックした後、表示されるポップアップ ウィンドウで [適用（Apply）] をクリックします。カラムを無効にすると、そのカラムは（後で元に戻さない限り）そのセッションの期間中は無効になります。最初のカラムを無効にすると、[カウント（Count）] カラムが追加されることに注意してください。

他のカラムを表示/非表示にしたり、無効になったカラムをビューに再び追加したりするには、該当するチェックボックスを選択またはクリアしてから [適用（Apply）] をクリックします。

テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（ワークフロー内の次のページにはドリルダウンされません）。

ヒント テーブル ビューでは、必ずページ名に「テーブル ビュー（Table View）」が含まれます。

関連トピック

ワークフローの使用, （1834 ページ）

監査ログを使って変更を調査する

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

監査ログを使用して、システムの変更に関する詳細レポートを表示できます。これらのレポートは、現在のシステム設定を、特定の変更が行われる直前の設定と比較します。

[設定の比較（Compare Configurations）] ページには、変更前のシステム設定と、現在実行中の設定との違いが横並び形式で表示されます。監査イベント タイプ、最終変更時間、および変更を行ったユーザ名が、各設定の上のタイトル バーに表示されます。

2 つの設定の違いは次のように強調表示されます。

- 青は、強調表示されている設定項目が 2 つの設定間で異なっていることを示し、異なっている部分は赤のテキストで表示されます。
- グリーンは、強調表示されている設定項目が一方の設定に含まれ、もう一方の設定には含まれないことを示します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [システム（System）] > [モニタリング（Monitoring）] > [監査（Audit）]を選択します。

ステップ 2 [メッセージ（Message）]カラムの該当する監査ログイベントの横にある比較アイコン（）をクリックします。

ヒント タイトル バーの上の [前へ（Previous）] または [次へ（Next）] をクリックすると、個々の変更の間を移動できます。また、変更の概要が複数のページにまたがる場合は、右側のスクロール バーを使って追加の変更を表示できます。

監査レコードの抑制

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

監査ポリシーで、Firepower System/ユーザ間の特定のタイプのインタラクションを監査する必要がない場合は、それらのインタラクションによって、Firepower Management Center または 7000 および 8000 シリーズ デバイス上で監査レコードが生成されないように設定できます。たとえば、デフォルトでは、ユーザがオンライン ヘルプを表示するたびに、Firepower System は監査レコードを生成します。このようなインタラクションのレコードを保持する必要がない場合は、これらを自動的に抑制できます。

監査イベントの抑制を設定するには、アプライアンスの `admin` ユーザ アカウントにアクセスできる必要があり、アプライアンスのコンソールにアクセスできる（またはセキュア シェルを開くことができる）必要があります。

注意 許可された担当者だけが、アプライアンスとその `admin` アカウントにアクセスできることを確認してください。

手順

`/etc/sf` ディレクトリに、次の形式で 1 つ以上の `AuditBlock` ファイルを作成します。タイプは、監査ブロック タイプ, （2179 ページ）で説明されているいずれかのタイプになります。

`AuditBlock.type`

（注） 特定のタイプの監査メッセージに関する `AuditBlock.type` ファイルを作成した後、もはやそれらを抑制しないことを決定した場合、`AuditBlock.type` ファイルの内容を削除する必要がありますが、ファイル自体は Firepower System に残してください。

監査ブロック タイプ

それぞれの監査ブロック タイプの内容は、以下の表に記載されているように、特定の形式でなければなりません。ファイル名の大文字/小文字を必ず正しく表記してください。また、ファイルの内容でも大文字と小文字が区別されることに注意してください。

`AuditBlock` ファイルを追加した場合、サブシステム `Audit` およびメッセージ `Audit Filter`*type*`Changed` を含む監査レコードが監査イベントに追加されることに注意してください。セキュリティ上の理由から、この監査レコードを抑制することは**できません**。

表 *286*：監査ブロック タイプ

タイプ（Type）	説明
アドレス（Address）	`AuditBlock.address` という名前のファイルを作成し、監査ログから抑制する IP アドレスを 1 行に 1 つずつ含めます。部分的な IP アドレスを使用できます（ただし、アドレスの先頭から照合されます）。たとえば、部分的なアドレス `10.1.1` は、`10.1.1.0` から `10.1.1.255` までのアドレスと一致します。
メッセージ	`AuditBlock.message` という名前のファイルを作成し、抑制するメッセージ部分文字列を 1 行に 1 つずつ含めます。 たとえば、`backup` をこのファイルに含めた場合、部分文字列の照合により `backup` という語を含むすべてのメッセージが抑制されることに注意してください。
サブシステム	`AuditBlock.subsystem` という名前のファイルを作成し、抑制するサブシステムを 1 行に 1 つずつ含めます。 部分文字列は照合**されない**ことに注意してください。正確な文字列を使用する必要があります。監査対象のサブシステムのリストについては、監査対象のサブシステム，（2179 ページ）を参照してください。
ユーザ（User）	`AuditBlock.user` という名前のファイルを作成し、抑制するユーザ アカウントを 1 行に 1 つずつ含めます。部分文字列の照合を使用できます（ただし、ユーザ名の先頭から照合されます）。たとえば、部分的なユーザ名 `IPSAnalyst` はユーザ名 `IPSAnalyst1` および `IPSAnalyst2` と一致します。

監査対象のサブシステム

次の表に、監査対象のサブシステムを示します。

表 *287* : サブシステム名

[名前（Name）]	何に関するユーザ インタラクションを含んでいるか
管理	管理機能（システムとアクセス権の設定、時刻の同期、バックアップと復元、デバイス管理、ユーザ アカウントの管理、スケジュール設定など）
アラート（Alerting）	アラート機能（電子メール アラート、SNMP アラート、Syslog アラートなど）
監査ログ（Audit Log）	監査イベントの表示
監査ログ検索（Audit Log Search）	監査イベントの検索
コマンド ライン	コマンドライン インターフェイス
設定（Configuration）	電子メール アラート機能
COOP	運用の継続性に関する機能
日付（Date）	イベント ビューの日時範囲
デフォルトのサブシステム（Default Subsystem）	サブシステムが割り当てられていないオプション
検出および防止ポリシー（Detection & Prevention Policy）	侵入ポリシーのメニュー オプション
エラー（Error）	システム レベルのエラー
eStreamer	eStreamer 構成
EULA	エンド ユーザ ライセンス契約書の確認
イベント	侵入および検出イベント ビュー
イベント クリップボード（Events Clipboard）	侵入イベント クリップボード
確認済みイベント（Events Reviewed）	確認済みの侵入イベント
イベント検索（Events Search）	あらゆるイベント検索

[名前（Name）]	何に関するユーザ インタラクションを含んでいるか
ルール更新のインストールの失敗（Failed to install rule update）`rule_update_id`	ルール更新のインストール
ヘッダー	ユーザ ログイン後のユーザ インターフェイスの初回表示
状態	ヘルス モニタリング
ヘルス イベント（Health Events）	ヘルス モニタリング イベントの表示
ヘルプ	オンライン ヘルプ
高可用性	高可用性ペアでの Firepower Management Center の確立と管理
IDSインパクトフラグ（IDS Impact Flag）	インパクト フラグの設定
IDS ポリシー（IDS Policy）	侵入ポリシー
IDS ルール SID：`sig_id` リビジョン：`rev_num`	SID 別の侵入ルール
[インシデント（Incidents）]	侵入インシデント
インストール（Install）	更新のインストール
侵入イベント	侵入イベント
ログイン（Login）	Web インターフェイスのログイン/ログアウト機能
メニュー	あらゆるメニュー オプション
[設定のエクスポート（Configuration export）] > [`config_type`] > [`config_name`]	特定のタイプと名前の設定のインポート
権限のエスカレーション（Permission Escalation）	ユーザ ロールのエスカレーション
初期設定	ユーザ設定（ユーザ アカウントのタイム ゾーン、個々のイベント設定など）
ポリシー	侵入ポリシーを含む、あらゆるポリシー

[名前（Name）]	何に関するユーザ インタラクションを含んでいるか
登録	Management Center でのデバイスの登録
リモート ストレージ デバイス（RemoteStorageDevice）	リモート ストレージ デバイスの設定
レポート	レポート リスト機能およびレポート デザイナ機能
ルール（Rules）	侵入ルール（侵入ルール エディタとルールのインポート プロセスを含む）
ルール更新インポート ログ（Rule Update Import Log）	ルール更新インポート ログの表示
ルール更新インストール（Rule Update Install）	ルール更新のインストール
ステータス（Status）	Syslog およびホストとパフォーマンスの統計
システム（System）	システム全体のさまざまな設定
タスク キュー（Task Queue）	バックグラウンド プロセス ステータスの表示
Users	ユーザ アカウントとロールの作成および変更

システム ログ

[システム ログ（System Log）]（syslog）ページには、アプライアンスのシステム ログ情報が表示されます。システム ログには、システムによって生成された各メッセージが表示されます。次の項目が順にリストされます。

- メッセージが生成された日付
- メッセージが生成された時刻
- メッセージを生成したホスト
- メッセージ自体

システム ログの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバルだけ	Admin/Maint

システム ログ情報はローカルな情報です。たとえば、Firepower Management Center を使用して、管理対象デバイスのシステム ログ内のシステム ステータス メッセージを見ることは**できません**。

Firepower Management Center または 7000 & 8000 シリーズ デバイスでは、特定のコンポーネントでフィルタリングすることによって、システム ログ メッセージのビューを変更できます。

手順

ステップ 1 [システム（System）] > [モニタリング（Monitoring）] > [Syslog]を選択します。

ステップ 2 システム ログの特定のメッセージ内容を検索する場合は、システム ログ メッセージのフィルタリング, （2183 ページ）を参照してください。

システム ログ メッセージのフィルタリング

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバルだけ	Admin/Maint

Firepower Management Center または 7000 および 8000 シリーズ のデバイスで、特定のコンポーネントをフィルタリングして、システム ログ メッセージの表示を変更することができます。フィルタリングにより、メッセージ内容に基づいて特定のメッセージを検索することができます。

フィルタリング機能は、UNIX ファイル検索ユーティリティ Grep を使用しているため、Grep で使用可能なほとんどの構文を使用できます。つまり、パターン マッチング用に Grep 互換の正規表現を使用できます。単一の語をフィルタとして使用したり、Grep でサポートされる正規表現を使用したりして内容を検索できます。

手順

ステップ 1 [システム（System）] > [モニタリング（Monitoring）] > [Syslog]を選択します。

ステップ 2 システム ログ フィルタの構文, （2184 ページ）に記載されているように、フィルタのフィールドに単語またはクエリを入力します。

（注） Grep 互換の検索構文のみがサポートされています。たとえば、フィルタとして `ntp` を使ってすべての NTP 関連システム ログ メッセージを検索したり、`Nov` をフィルタとして使って11月に生成されたすべてのメッセージを検索したりできます。`Nov[[:space:]]*27` または `Nov.*27` を使用すると 11 月 27 日のメッセージを表示できますが、`Nov 27` または `Nov*27` を使ってこれらのメッセージを表示することはできません。

ステップ 3 大文字と小文字が区別されるようにするには、[大文字と小文字を区別する（Case-sensitive）] をチェックします。（デフォルトでは、フィルタで大文字/小文字は区別されません。）

ステップ 4 オプションで、[除外（Exclusion）] をチェックすると、入力した条件に一致しないすべてのシステム ログ メッセージが検索されます。

ステップ 5 [移動（Go）] をクリックします。

例

11 月 5 日に生成されたすべてのログ エントリを検索するには、`Nov[[:space:]]*5` を使用します。

ユーザ名 ”Admin” を含むすべてのログ エントリを検索するには `Admin` を使用します。

11 月 5 日のデバッグ情報の認証を含むすべてのログ エントリを検索するには、`Nov[[:space:]]*5.*AUTH.*DEBUG` を使用します。

システム ログ フィルタの構文

次の表に、システム ログ フィルタで使用できる正規表現構文を示します。

表 *288*：システム ログ フィルタ構文

構文のコンポーネント	説明	例
`.`	任意の文字またはスペースと一致します	`Admi.` は、`Admin`、`AdmiN`、`Admi1`、および `Admi&` と一致します。
`[[:alpha:]]`	任意の英文字と一致します	`[[:alpha:]]dmin` は、`Admin`、`bdmin`、および `Cdmin` と一致します
`[[:upper:]]`	任意の大文字の英文字と一致します	`[[:upper:]]dmin` は、`Admin`、`Bdmin`、および `Cdmin` と一致します
`[[:lower:]]`	任意の小文字の英文字と一致します	`[[:lower:]]dmin` は、`admin`、`bdmin`、および `cdmin` と一致します
`[[:digit:]]`	任意の数字と一致します	`[[:digit:]]dmin` は、`0dmin`、`1dmin`、および `2dmin` と一致します

構文のコンポーネント	説明	例
`[[:alnum:]]`	任意の英数字と一致します	`[[:alnum:]]dmin` は、`1dmin`、`admin`、`2dmin`、および `bdmin` と一致します
`[[:space:]]`	タブを含む、任意のスペースと一致します	`Feb[[:space:]]29` は 2 月 29 日のログと一致します
*	その前にある文字または式のゼロ個以上のインスタンスと一致します	`ab*` は、`a`、`ab`、`abb`、`ca`、`cab`、および `cabb` と一致します `[ab]*` はすべてのものと一致します
?	ゼロ個または 1 つのインスタンスと一致します	`ab?` は、`a` または `ab` と一致します
\	これを使用すると、通常は正規表現構文と解釈される文字を検索できます	alert\? は、`alert?` と一致します

付 録 A

セキュリティ、インターネット アクセス、および通信ポート

以下のトピックでは、システム セキュリティ、インターネット アクセス、および通信ポートに関する情報を提供します。

セキュリティ、インターネット アクセス、および通信ポートについて

Firepower Management Center を保護するには、保護された内部ネットワークにインストールしてください。Firepower Management Center は必要なサービスとポートだけを使用するよう設定されますが、ファイアウォール外部からの攻撃がそこまで（または管理対象デバイスまで）決して到達できないようにする必要があります。

Firepower Management Center とその管理対象デバイスが同じネットワーク上に存在する場合は、デバイス上の管理インターフェイスを、Firepower Management Center と同じ保護された内部ネットワークに接続できます。これにより、Firepower Management Center からデバイスを安全に制御することができます。また、他のネットワーク上のデバイスからのトラフィックを Firepower Management Center で管理および分離できるように、複数の管理インターフェイスを設定することもできます。

アプライアンスの展開方法とは無関係に、アプライアンス間通信は暗号化されます。それでも、分散型サービス拒否（DDoS）や中間者攻撃などの手段でシステム アプライアンス間の通信が中断、ブロック、改ざんされないよう何らかの対策を講じる必要があります。

また、Firepower システムの機能によってはインターネット接続が必要となることにも注意してください。デフォルトでは、システム アプライアンスがインターネットに直接接続するように設定

されます。加えて、システムで特定のポートを開いたままにしておく必要があります。その目的は基本的なアプライアンス間通信、セキュアなアプライアンス アクセス、および特定のシステム機能を正しく動作させるために必要なローカル/インターネット リソースへのアクセスを可能にすることです。

インターネット アクセス要件

デフォルトでは、システム アプライアンスはポート 443/tcp（HTTPS）および 80/tcp（HTTP）でインターネットに直接接続するよう設定されます。これらのポートはFirepowerシステムのすべてのアプライアンスでデフォルトで開かれています。ほとんどのシステム アプライアンスではプロキシ サーバの利用がサポートされている点に注意してください。プロキシ サーバはwhoisアクセスに使用できない点にも注意が必要です。

Firepowerシステム機能のインターネット アクセス要件

次の表に、Firepowerシステムの特定の機能におけるインターネット アクセス要件を示します。

表 *289*：*Firepower*システム機能のインターネット アクセス要件

機能	インターネット アクセスの用途	アプライアンス
AMP for Firepower	マルウェア クラウド検索を実行します。	Management Center
Cisco Advanced Malware Protection（Cisco AMP）統合	エンドポイントベース（AMP for Endpoints）のマルウェア イベントをCisco AMPクラウドから受信します。	Management Center
動的分析：照会	動的分析のために、送信済みファイルの脅威スコアをAMP Threat Gridクラウドに照会します。	Management Center
動的分析：送信	動的分析用にファイルをAMP Threat Gridクラウドに送信します。	あらゆるデバイス
侵入ルール、VDB、およびGeoDBの更新	侵入ルール、GeoDB、またはVDBの更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。	Management Center
ローカルマルウェア分析およびファイル事前分類の署名アップデート	ローカルマルウェア分析および事前分類エンジンに署名アップデートをダウンロードします。	Management Center

機能	インターネット アクセスの用途	アプライアンス
RSS フィード ダッシュボード ウィジェット	シスコを含む外部ソースから RSS フィード データをダウンロードします。	Management Center 7000 & 8000 シリーズ
セキュリティ インテリジェンス フィルタリング	シスコが提供するインテリジェンス フィードを含む、外部ソースからのセキュリティ インテリジェンス フィード データをダウンロードします。	Management Center
システム ソフトウェアの更新	システム更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。	すべて（NGIPSv を除く）
URL フィルタリング	URL カテゴリおよびレピュテーション データをアクセス コントロール用にダウンロードし、分類されていない URL に対してクエリを実行します。	Management Center
whois	外部ホストの whois 情報を要求します。	Management Center

通信ポートの要件

Firepower Management Center およびその管理対象デバイスは、（デフォルトでポート 8305/tcp を使用する）双方向 SSL 暗号化通信チャネルを使って通信します。基本的なプラットフォーム間通信用にこのポートを開いたままにする**必要があります**。他のオープン ポートの役割は次のとおりです。

- Web インターフェイスへのアクセス
- デバイスまたは Firepower Management Center へのセキュアなリモート接続
- 特定のシステム機能を正しく動作させるために必要なローカル/インターネット リソースへのアクセスを可能にする

一般に、機能関連のポートは、該当する機能を有効化または設定する時点まで、閉じたままになります。たとえば、Firepower Management Centerをユーザ エージェントに接続するまでは、エージェント通信ポート（3306/tcp）は閉じたままになります。別の例として、LOM を有効にするまでは、7000 および 8000 シリーズ デバイス上のポート 623/udp が閉じたままになります。

注意 開いたポートを閉じると展開にどのような影響が及ぶか理解するまでは、開いたポートを**閉じないでください**。

たとえば、管理対象デバイスでポート 25/tcp（SMTP）アウトバウンドを閉じると、このデバイスが個々の侵入イベントに関する電子メール通知を送信できなくなります。別の例として、ポート 443/tcp（HTTPS）を閉じることにより物理管理対象デバイスの Web インターフェイスへのアクセスを無効にできますが、それと同時に、動的分析のためにデバイスから疑わしいマルウェア ファイルを AMP Threat Grid クラウドに送信できなくなります。

次のように、システムのいくつかの通信ポートを変更できることに注意してください。

- システムと認証サーバ間の接続を設定するときに、LDAP および RADIUS 認証用のカスタム ポートを指定できます。
- 管理ポート（8305/tcp）を変更できます。ただし、シスコではデフォルト設定を維持することを**強く**推奨しています。管理ポートを変更する場合は、相互に通信する必要がある展開内のすべての Firepower Management Center およびその管理対象デバイスの管理ポートを変更する必要があります。
- ポート 32137/tcp を使用して、アップグレード対象の Management Center とシスコ AMP クラウドの通信を可能にすることができます。ただし、シスコではバージョン 5.3 以降の新規インストールのデフォルトであるポート 443 に切り替えることを推奨しています。

Firepower システムの機能と運用のためのデフォルト通信ポート

次の表は、Firepower システムの機能を最大限に活用できるように、各アプライアンス タイプで必要なオープン ポートを示しています。

表 *290*：*Firepower* システムの機能と運用のためのデフォルト通信ポート

[ポート（Port）]	説明	方向（Direction）	開いているアプライアンス	目的
22/tcp	SSH/SSL	双方向	任意（Any）	アプライアンスへのセキュアなリモート接続を許可します。
25/tcp	SMTP	発信	任意（Any）	アプライアンスから電子メール通知とアラートを送信します。
53/tcp	DNS	発信	任意（Any）	DNS を使用します。
67/udp 68/udp	DHCP	発信	任意（Any）	DHCP を使用します。これらのポートはデフォルトで**閉じられている**ことに注意してください。

[ポート（Port）]	説明	方向（Direction）	開いているアプライアンス	目的
80/tcp	HTTP	発信	Management Center 7000 & 8000 シリーズ	RSS フィード ダッシュボード ウィジェットからリモート Web サーバに接続できるようにします。
		双方向	Management Center	HTTP 経由でカスタムおよびサードパーティのセキュリティ インテリジェンス フィードを更新します。 URL カテゴリおよびレピュテーション データをダウンロードします（さらにポート 443 も必要）。
161/udp	SNMP	双方向	任意（Any）	SNMP ポーリング経由でアプライアンスの MIB にアクセスできるようにします。
162/udp	SNMP	発信	任意（Any）	リモート トラップ サーバに SNMP アラートを送信します。
389/tcp 636/tcp	LDAP	発信	すべて（NGIPSv を除く）	外部認証用に LDAP サーバと通信します。
389/tcp 636/tcp	LDAP	発信	Management Center	検出された LDAP ユーザに関するメタデータを取得します。
443/tcp	HTTPS	着信	すべて（NGIPSv を除く）	アプライアンスの Web インターフェイスにアクセスします。
443/tcp	HTTPS AMQP AMP クラウド、AMP Threat Grid クラウド、および脅威インテリジェンスの通信設定	双方向	Management Center	次のものを取得します。 • ソフトウェア、侵入ルール、VDB、および GeoDB の更新 • URL カテゴリおよびレピュテーション データ（さらにポート 80 も必要） • インテリジェンス フィードおよび他のセキュアなセキュリティ インテリジェンス フィード • エンドポイントベース（AMP for Endpoints）のマルウェア イベント • ファイルに関してネットワーク トラフィックで検出されたマルウェアの性質 • 送信されたファイルに関する動的分析情報

[ポート（Port）]	説明	方向（Direction）	開いているアプライアンス	目的
		双方向	Management Center、7000 & 8000 シリーズ	デバイスのローカル Web インターフェイスを使用してソフトウェア更新をダウンロードします。
		双方向	すべての管理対象デバイス	動的分析のためにファイルを送信します。
514/udp	syslog	発信	任意（Any）	リモート syslog サーバにアラートを送信します。
623/udp	SOL/LOM	双方向	7000 & 8000 シリーズ	Serial Over LAN（SOL）接続を使用して Lights-Out Management を実行できるようにします。
1500/tcp 2000/tcp	データベース アクセス	着信	Management Center	サードパーティ クライアントによるデータベースへの読み取り専用アクセスを可能にします。
1812/udp 1813/udp	RADIUS	双方向	すべて（NGIPSv を除く）	外部認証とアカウンティングのために RADIUS サーバと通信します。
3306/tcp	ユーザ エージェント	着信	Management Center	ユーザ エージェントと通信します。
8302/tcp	eStreamer	双方向	Management Center 、 7000 & 8000 シリーズ	eStreamer クライアントと通信します。
8305/tcp	アプライアンス通信	双方向	任意（Any）	展開におけるアプライアンス間で安全に通信します。**必須作業です。**
8307/tcp	ホスト入力クライアント	双方向	Management Center	ホスト入力クライアントと通信します。
32137/tcp	AMP クラウドおよび脅威インテリジェンスの通信設定	双方向	Management Center	アップグレード対象の Management Center と Cisco AMP クラウドの通信を可能にします。

付 録 B

のコマンド ライン リファレンス

このリファレンスでは、次のデバイスのコマンドラインインターフェイス（CLI）について説明します。

- 7000 および 8000 シリーズ
- ASA FirePOWER
- NGIPSv

（注） Firepower Management Center で CLI を使用することはできません。Firepower Management Center は、Linux シェル アクセスをサポートし、Cisco Technical Assistance Center（TAC） の監督下でのみサポートされます。

CLI について

従来型デバイスに CLI（コマンドライン インターフェイスへのログイン，（29 ページ） を参照）を使用してログインすると、この章で説明するコマンドを使用して、デバイスを表示、設定、およびトラブルシューティングすることができます。

（注） 7000 または 8000 シリーズ デバイスをリブートし、できるだけ早く CLI にログインしても、Webインターフェイスが使用できるようになるまで、実行するすべてのコマンドは監査ログに記録されません。

CLI コマンドでは大文字と小文字が区別されません。ただし、ユーザ名や検索フィルタなど、テキストが CLI フレームワークの一部ではないパラメータでは区別されるので注意してください。

CLI モード

CLI モードには `show` や `configure` など多数あり、これらのモードにはモード名で始まる一連のコマンドが含まれています。モードを開始して、そのモードで有効なコマンドを入力することも、任意のモードからフル コマンドを入力することもできます。たとえば、Analyst1 というユーザ アカウントの情報を表示するには、CLI プロンプトで次のように入力します。

show user Analyst1

すでに `show` モードを開始している場合は、CLI プロンプトで次のように入力します。

user Analyst1

CLI アクセス レベル

各モードで、ユーザが使用できるコマンドは、ユーザの CLI アクセスによって異なります。ユーザ アカウントを作成する場合は、手動で次のいずれかの CLI アクセス レベルに割り当てることができます。

- [基本（Basic）] : ユーザは読み取り専用のアクセス権を持ち、システム パフォーマンスに影響を与えるコマンドを実行することはできません。
- [設定（Configuration）] : ユーザは、読み取り/書き込みアクセス権があり、システム パフォーマンスに影響を与えるコマンドを実行することができます。
- [なし（None）] : ユーザはシェルにログインできません。

7000 および 8000 シリーズ デバイスでは、Web インターフェイスの [ユーザ管理（User Management）] ページでコマンド ラインの権限を割り当てることができます。NGIPSv と ASA FirePOWER では、CLI を使用してコマンド ラインの権限を割り当てます。

基本的な CLI コマンド

基本的な CLI コマンドを使用して、CLI とやりとりすることができます。これらのコマンドはデバイスの動作に影響しません。基本的なコマンドは、すべての CLI ユーザが使用可能です。

configure password

現行のユーザは、自身のパスワードを変更することができます。コマンドを発行すると、CLI は現在の（古い）パスワードを入力するようユーザに要求し、その後で新しいパスワードを 2 回入力するよう要求します。

アクセス（Access）

基本

構文

```
configure password
```

例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

終了

ユーザをデフォルトのモードに戻します。（ユーザは、いずれかの下位レベルの CLI コンテキストから上位のデフォルト モードへ移動します）。

アクセス（Access）

基本

構文

```
end
```

例

```
configure network ipv4> end
>
```

exit

CLI コンテキストを、次に高い CLI コンテキスト レベルへ移動します。デフォルト モードからこのコマンドを発行すると、ユーザは現行の CLI セッションからログアウトします。これは、CLI コマンドの `logout` を発行するのと同じです。

アクセス（Access）

基本

構文

```
exit
```

例

```
configure network ipv4> exit
configure network>
```

ヘルプ

CLI 構文の概要を表示します。

アクセス（Access）

基本

構文

```
help
```

例

```
> help
```

history

現行のセッションのコマンドラインの履歴を表示します。

アクセス（Access）

基本

構文

```
history limit
```

ここで`limit`は履歴リストのサイズを設定します。サイズを無制限に設定するには、0を入力します。

例

```
history 25
```

ログアウト

現行の CLI コンソール セッションから現行のユーザをログアウトします。

アクセス（Access）

基本

構文

```
logout
```

例

```
> logout
```

? （疑問符）

CLI コマンドと CLI パラメータの状況依存ヘルプを表示します。以下のように疑問符（?）コマンドを使用します。

- 現在の CLI コンテキストで使用できるコマンドのヘルプを表示するには、コマンドプロンプトに疑問符（?）を入力します。
- 特定の文字列セットで始まる使用可能なコマンドのリストを表示するには、疑問符（?）の直後に短縮コマンドを入力します。
- コマンドの法的引数のヘルプを表示するには、コマンドプロンプトの引数の代わりに疑問符（?）を入力します。

疑問符（?）は、コンソールにエコーバックすることはない点にご注意ください。

アクセス（Access）

基本

構文

```
?
abbreviated_command ?
command [arguments] ?
```

例

```
> ?
```

?? （二重の疑問符）

CLI コマンドおよびパラメータの詳細な状況依存ヘルプを表示します。

アクセス（Access）

基本

構文

```
??
abbreviated_command end??
command [arguments] ??
```

例

```
> configure manager add ??
```

show コマンド

show コマンドは、デバイスの状態に関する情報を提供します。これらのコマンドはデバイスの動作モードを変更しません。また、これらのコマンドを実行しても、システムの動作に対する影響は最小限になります。ほとんどの show コマンドはすべての CLI ユーザが利用できますが、`show user` コマンドを発行できるのは、Configuration CLI アクセス権限を持つユーザのみです。

access-control-config

現在展開されている次のようなアクセス制御設定を表示します。

- セキュリティ インテリジェンスの設定
- アクセス コントロール ポリシーで呼び出されるあらゆるサブポリシーの名前
- 侵入変数セット データ
- ロギングの設定
- ポリシー レベルのパフォーマンス、前処理、全般設定などのその他の詳細設定

また、送信元と宛先ポートのデータ（ICMPエントリのタイプとコードを含む）および各アクセス コントロール ルールに一致する接続数（ヒット数）などの、ポリシーに関連する接続情報も表示します。

アクセス（Access）

基本

構文

```
show access-control-config
```

例

```
> show access-control-config
```

alarms

デバイスで現在アクティブ（障害/停止）状態になっているハードウェアのアラームを表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス（Access）

基本

構文

```
show alarms
```

例

```
> show alarms
```

arp-tables

ネットワークに適用できる Address Resolution Protocol テーブルを表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show arp-tables
```

例

```
> show arp-tables
```

audit-log

監査ログを時系列の逆順に表示します。最も新しい監査ログ イベントが先頭になります。

アクセス（Access）

基本

構文

```
show audit-log
```

例

```
> show audit-log
```

bypass

7000 または 8000 シリーズ デバイスで、使用中のインライン セットを一覧表示し、それらのセットについて次のいずれかのバイパス モード ステータスを表示します。

- `armed`：インターフェイス ペアが、障害発生時にハードウェア バイパスになるように設定されている（[バイパス モード：バイパス（Bypass Mode: Bypass）]）か、または、configure bypass close コマンドを使用して強制的にフェールクローズされました。
- `engaged`：インターフェイス ペアが、オープンに失敗したか、または、configure bypass open コマンドを使用して強制的にハードウェア バイパスになりました。
- `off`：インターフェイス ペアがフェールクローズ（[バイパス モード：非バイパス（Bypass Mode: Non-Bypass）]）に設定されており、インターフェイス ペアで障害が発生した場合にはパケットがブロックされます。

アクセス（Access）

基本

構文

```
show bypass
```

例

```
> show bypass
s1p1 ↔ s1p2: status 'armed'
s1p1 ↔ s1p2: status 'engaged'
```

High-availability コマンド

ハイ アベイラビリティの設定、ステータス、メンバーデバイスまたはスタックの情報を表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス（Access）

基本

config

デバイスの高可用性の設定を表示します。

構文

```
show high-availability config
```

例

```
> show high-availability config
```

high-availability ha-statistics

高可用性ペアのデバイスの状態共有統計を表示します。

構文

```
show high-availability ha-statistics
```

例

```
> show high-availability ha-statistics
```

cpu

デバイス上のすべての CPU のプラットフォームに適合する現行の CPU の使用率の統計情報を表示します。7000 および 8000 シリーズ デバイスでは、次の値が表示されます。

- CPU：プロセッサ番号。
- ロード：0 ～ 100 の数値で表される CPU 使用率。0 はロードされていない状態で、100 は完全にロードされたことを表します。

NGIPSv および ASA FirePOWER では、次の値が表示されます。

- CPU：プロセッサ番号。
- %user：ユーザ レベル（アプリケーション）で実行中に生じた CPU 使用率の割合（パーセンテージ）。
- %nice：高い優先度のユーザ レベルで実行中に生じた CPU 使用率の割合（パーセンテージ）。
- %sys：システム レベル（カーネル）で実行中に生じた CPU 使用率の割合（パーセンテージ）。これには、サービスの割り込みや softirqs で経過する時間は含まれません。softirq（ソフトウェアの割り込み）は、複数の CPU で同時に実行できる最大 32 個の列挙されたソフトウェア割り込みの 1 つです。
- %iowait：システムに未処理のディスク I/O 要求があったときに、CPU がアイドル状態だった時間の割合（パーセンテージ）。
- %irq：割り込みを行うために CPU が費やした時間の割合（パーセンテージ）。
- %soft：softirqs を行うために CPU が費やした時間の割合（パーセンテージ）。

- %steal：ハイパーバイザが別の仮想プロセッサを実行しているときに、仮想 CPU が強制的な待機で費やした時間の割合（パーセンテージ）。
- %guest：仮想プロセッサを実行するために CPU が費やした時間の割合（パーセンテージ）。
- %idle：CPU がアイドル状態で、システムに未処理のディスク I/O 要求がなかった時間の割合（パーセンテージ）。

アクセス（Access）

基本

構文

```
show cpu [procnum]
```

ここで `procnum` は、使用率の情報を表示するプロセッサの数を表します。有効な値は 0 から、システム上の合計プロセッサ数から 1 引いた数までの範囲です。`procnum` が 7000 または 8000 シリーズ デバイスで使用されている場合は無視されます。このプラットフォームについては、使用率の情報はすべてのプロセッサについてのみ表示されるためです。

例

```
> show cpu
```

Database コマンド

データベースの表示（`show database`）コマンドは、デバイスの管理インターフェイスを設定します。

アクセス（Access）

基本

processes

実行中のデータベース クエリのリストを表示します。

アクセス（Access）

基本

構文

```
show database processes
```

例

```
> show database processes
```

slow-query-log

データベースのスロー クエリ ログを表示します。

アクセス（Access）

基本

構文

```
show database slow-query-log
```

例

```
> show database slow-query-log
```

device-settings

現行のデバイスに特有のアプリケーションのバイパス設定に関する情報を表示します。

アクセス（Access）

基本

構文

```
show device-settings
```

例

```
> show device-settings
```

disk

現行のディスクの使用率を表示します。

アクセス（Access）

基本

構文

```
show disk
```

例

```
> show disk
```

disk-manager

システムの各パート（サイロ、低水位、高水位など）のディスク使用率の詳細情報を表示します。

アクセス（Access）

基本

構文

```
show disk-manager
```

例

```
> show disk-manager
```

dns

現行の DNS サーバのアドレスと検索ドメインを表示します。

アクセス（Access）

基本

構文

```
show dns
```

例

```
> show dns
```

expert

シェルを起動します。

アクセス（Access）

基本

構文

```
expert
```

例

```
> expert
```

fan-status

ハードウェア ファンの現在のステータスを表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス（Access）

基本

構文

```
show fan-status
```

例

```
> show fan-status
```

fastpath-rules

現在設定されている 8000 シリーズ の fastpath ルールを表示します。このコマンドは 8000 シリーズ デバイスでは使用できません。

アクセス（Access）

基本

構文

```
show fastpath-rules
```

例

```
> show fastpath-rules
```

gui

Webインターフェイスの現在の状態を表示します。このコマンドはNGIPSvおよびASA FirePOWERでは使用できません。

アクセス（Access）

基本

構文

```
show gui
```

例

```
> show gui
```

hostname

デバイスのホスト名およびアプライアンス UUID を表示します。CLI を使用してデバイスのホスト名を編集する場合は、管理する Firepower Management Center に変更が反映されることを確認します。場合によっては、デバイス管理設定を手動で編集する必要があります。

アクセス（Access）

基本

構文

```
show hostname
```

例

```
> show hostname
```

hosts

ASA FirePOWER モジュールの /etc/hosts ファイルの内容を表示します。

アクセス（Access）

基本

構文

```
show hosts
```

例

```
> show hosts
```

hyperthreading

ハイパースレッディングが有効か無効かを表示します。このコマンドは ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show hyperthreading
```

例

```
> show hyperthreading
```

inline-sets

すべてのインライン セキュリティ ゾーンと関連するインターフェイスの設定データを表示します。このコマンドは ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show inline-sets
```

例

```
> show inline-sets
```

interfaces

パラメータが指定されていない場合は、設定されているすべてのインターフェイスのリストが表示されます。パラメータが指定されている場合は、指定されたインターフェイスの詳細情報が表示されます。

アクセス（Access）

基本

構文

```
show interfaces interface
```
ここで *interface* は詳細情報を表示する特定のインターフェイスです。

例

```
> show interfaces
```

ifconfig

ASA FirePOWER モジュールに対するインターフェイスの設定を表示します。

アクセス（Access）

基本

構文

```
show ifconfig
```

例

```
> show ifconfig
```

lcd

LCD のハードウェア ディスプレイが有効か無効かを表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show lcd
```

例

```
> show lcd
```

Link-aggregation コマンド

`show link-aggregation` コマンドは、リンク集約グループ（LAG）の設定および統計情報を表示します。このコマンドは、NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス（Access）

基本

設定：

LAG ID、インターフェイスの数、設定モード、ロードバランシング モード、LACP 情報、物理インターフェイスのタイプなど、設定された各 LAG の構成の詳細を表示します。

アクセス（Access）

基本

構文

```
show link-aggregation configuration
```

例

```
> show link-aggregation configuration
```

統計情報

ステータス、リンク ステートと速度、コンフィギュレーション モード、送受信されたパケットのカウンタ、および送受信されたバイトのカウンタなど、設定された各 LAG の統計情報をインターフェイスごとに表示します。

アクセス（Access）

基本

構文

```
show link-aggregation statistics
```

例

```
> show link-aggregation statistics
```

link-state

デバイスのポートのタイプ、リンク、スピード、速度、デュプレックスの状態およびバイパス モードを表示します。このコマンドは ASA FirePOWER デバイスでは使用できません。

アクセス（Access）

基本

構文

```
show link-state
```

例

```
> show link-state
```

log-ips-connection

記録された侵入イベントに関連付けられている接続イベントのロギングが有効か無効かを表示します。

アクセス（Access）

基本

構文

```
show log-ips-connection
```

例

```
> show log-ips-connection
```

managers

Firepower Management Center の設定および通信のステータスを表示します。登録キーおよび NAT ID は、登録が保留中の場合のみ表示されます。

デバイスが、スタック設定のセカンダリ デバイスとして設定されている場合、管理している両方の Management Center、およびプライマリ デバイスに関する情報が表示されます。

アクセス（Access）

基本

構文

```
show managers
```

例

```
> show managers
```

memory

デバイスの合計メモリ、使用中のメモリ、使用可能なメモリを表示します。

アクセス（Access）

基本

構文

```
show memory
```

例

```
> show memory
```

model

デバイスのモデル情報を表示します。

アクセス（Access）

基本

構文

```
show model
```

例

```
> show model
```

mpls-depth

管理インターフェイスに設定されている MPLS レイヤ数を 0～6 で表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show mpls-depth
```

例

```
> show mpls-depth
```

NAT コマンド

show nat コマンドは、管理インターフェイスの NAT データと設定情報を表示します。このコマンドは、NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス（Access）

基本

active-dynamic

ダイナミック ルールに従って変換されている NAT フローを表示します。これらのエントリは、フローがルールに一致している場合に、ルールがタイムアウトになるまで表示されます。したがって、リストは正確ではないことがあります。タイムアウトはプロトコルに依存します。ICMP は 5 秒、UDP は 120 秒、TCP は 3600 秒、他のすべてのプロトコルは 60 秒です。

構文

```
show nat active-dynamic
```

例

```
> show nat active-dynamic
```

active-static

スタティック ルールに従って変換されている NAT フローを表示します。これらのエントリは、デバイスにルールが展開されるとすぐに表示されます。リストは、スタティックな NAT ルールに一致しているアクティブなフローを示しているわけではありません。

構文

```
show nat active-static
```

例

```
> show nat active-static
```

allocators

すべての NAT アロケータの情報、ダイナミック ルールで使用されている変換済みアドレスのプールを表示します。

構文

```
show nat allocators
```

例

```
> show nat allocators
```

config

管理インターフェイスの現在の NAT ポリシーの設定を表示します。

構文

```
show nat config
```

例

```
> show nat config
```

dynamic-rules

指定されたアロケータ ID を使用しているダイナミックな NAT ルールを表示します。

構文

```
show nat dynamic-rules allocator_id
```
ここで `allocator_id` は有効なアロケータ ID 番号です。

例

```
> show nat dynamic-rules 9
```

flows

指定されたアロケータ ID を使用しているルールについてフローの数を表示します。

構文

```
show nat flows allocator-id
```
ここで *allocator_id* は有効なアロケータ ID 番号です。

例

```
> show nat flows 81
```

static-rules

すべてのスタティック NAT ルールを表示します。

構文

```
show nat static-rules
```

例

```
> show nat static-rules
```

netstat

ASA FirePOWER モジュールのアクティブなネットワーク接続を表示します。

アクセス（Access）

基本

構文

```
show netstat
```

例

```
> show netstat
```

network

管理インターフェイスの IPv4 および IPv6 の設定、MAC アドレス、HTTP プロキシ アドレス、ポート、ユーザ名（設定されている場合）を表示します。

アクセス（Access）

基本

構文

```
show network
```

例

```
> show network
```

network-modules

インストールされているすべてのモジュール、およびモジュールの情報（シリアル番号など）を表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show network-modules
```

例

```
> show network-modules
```

network-static-routes

インターフェイス、宛先アドレス、ネットワーク マスク、およびゲートウェイ アドレスなど、設定済みのすべてのネットワーク スタティック ルートとその情報が表示されます。

アクセス（Access）

基本

構文

```
show network-static-routes
```

例

```
> show network-static-routes
```

ntp

NTP コンフィギュレーションを表示します。

アクセス（Access）

基本

構文

```
show ntp
```

例

```
> show ntp
```

perfstats

デバイスのパフォーマンスの統計情報を表示します。

アクセス（Access）

基本

構文

```
show perfstats
```

例

```
> show perfstats
```

portstats

デバイスのすべての挿入されたポートのポート統計を表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show portstats [copper | fiber | internal | external | all]
```

銅線は、すべての銅線ポートを指定します。光ファイバはすべての光ファイバ ポートを指定します。内部はすべての内部ポートをします。外部はすべての外部（銅線および光ファイバ）ポートをします。すべてはすべてのポート（外部および内部）を指定します。

例

```
> show portstats fiber
```

power-supply-status

現在のハードウェアの電源状態を表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show power-supply-status
```

例

```
> show power-supply-status
```

process-tree

デバイスで実行中のプロセスについて、タイプごとにツリー形式でソートして表示します。

アクセス（Access）

基本

構文

```
show process-tree
```

例

```
> show process-tree
```

processes

デバイス上で現在実行中のプロセスについて、CPU 使用率の降順で表示します。

アクセス（Access）

基本

構文

```
show processes sort-flag filter
```

ここで、メモリ（の降順）でソートする場合は、*sort-flag* に `-m` を指定し、プロセス名ではなくユーザ名でソートする場合は`-u`を指定します。また、コマンドのフルネームおよびパスを表示する場合は `verbose` を指定します。*filter* パラメータは、コマンドの検索語または結果をフィルタするために使用するユーザ名を指定します。見出し行は表示されたままです。

例

```
> show processes -u user1
```

ルート

ASA FirePOWER モジュールに関するルーティング情報を表示します。

アクセス（Access）

基本

構文

```
show route
```

例

```
> show route
```

routing-table

パラメータが指定されていない場合は、すべての仮想ルータに関するルーティング情報を表示します。パラメータが指定されている場合は、指定のルータに関するルーティング情報や、該当する場合には、指定のルーティングプロトコルタイプを表示します。パラメータはすべてオプションです。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show routing-table name [ ospf | rip | static ]
```

name は、情報を必要とする特定のルータ名です。`ospf`、`rip`、`static` は、ルーティング プロトコル タイプを指定します。

例

```
> show routing-table Vrouter1 static
```

serial-number

シャーシのシリアル番号を表示します。このコマンドは NGIPSv では使用できません。

アクセス（Access）

基本

構文

```
show serial-number
```

例

```
> show serial-number
```

ssl-policy-config

現在適用されている SSL ポリシーの設定（ポリシーの説明、デフォルトのロギング設定、有効なすべての SSL ルールとルールの設定など）、信頼できる CA 証明書、および復号化不可能なトラフィックのアクションを表示します。

アクセス（Access）

基本

構文

```
show ssl-policy-config
```

例

```
> show ssl-policy-config
```

stacking

管理対象デバイスのスタッキングの設定とポジションを表示します。プライマリとして設定されているデバイスでは、すべてのセカンダリ デバイスのデータも示されます。高可用性ペアのスタックの場合、このコマンドは、スタックが高可用性ペアのメンバーであることも示します。スタッキングを有効または無効にする（大半の場合は無効にする）には、ユーザは Web インターフェイスを使用する必要があります。スタッキングが有効になっていない場合、コマンドは`Stacking not currently configured` というメッセージを返します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show stacking
```

例

```
> show stacking
```

summary

デバイスに関して最もよく使用される情報（バージョン、タイプ、UUID など）のサマリーを表示します。詳細は次の show コマンドを参照してください。version、interfaces、device-settings、および access-control-config。

アクセス（Access）

基本

構文

```
show summary
```

例

```
> show summary
```

時刻

現在の日付と時刻を、UTC および現行のユーザに設定されているローカル タイム ゾーンで表示します。

アクセス（Access）

基本

構文

```
show time
```

例

```
> show time
```

traffic-statistics

パラメータが指定されていない場合は、すべてのポートから送信された、および受信したバイトの詳細情報を表示します。ポートが指定されている場合は、指定されたポートの情報のみを表示します。ASA FirePOWER モジュールに対してポートを指定することはできません。システムはデータ プレーン インターフェイスのみを表示します。

アクセス（Access）

基本

構文

```
show traffic-statistics port
```
ここで *port* は、情報を表示させたい特定のポートです。

例

```
> show traffic-statistics s1p1
```

user

NGIPSvのみに適用できます。指定されたユーザに関する設定の詳細情報を表示します。次の値が表示されます。

- Login：ログイン名
- UID：ユーザ ID（数値）
- Auth（`Local` または `Remote`）：ユーザがどのように認証されているか
- Access（`Basic` または `Config`）：ユーザの権限レベル
- Enabled（`Enabled` または `Disabled`）：ユーザがアクティブかどうか
- Reset（`Yes` または `No`）：次のログイン時にユーザがパスワードを変更する必要があるかどうか
- Exp（`Never` または数値）：ユーザのパスワード変更が必要になるまでの日数
- Warn（`N/A` または数値）：パスワードの有効期限が切れる前に、ユーザがパスワード変更のために与えられる日数
- Str（`Yes` または `No`）：ユーザのパスワードが強度チェックの基準を満たす必要があるかどうか
- Lock（`Yes` または `No`）：ログインの失敗が多すぎる場合に、ユーザのアカウントがロックされるかどうか
- Max（`N/A` または数値）：ユーザのアカウントがロックされる前に失敗するログインの最大回数

アクセス（**Access**）

設定（Configuration）

構文

```
show user username username username ...
```
ここで *username* はユーザの名前を表します。複数の username はスペースで区切って指定します。

例

```
> show user jdoe
```

ユーザ

NGIPSv のみに適用できます。すべてのローカル ユーザの設定の詳細情報を表示します。次の値が表示されます。

- Login：ログイン名
- UID：ユーザ ID（数値）
- Auth（`Local` または `Remote`）：ユーザがどのように認証されているか
- Access（`Basic` または `Config`）：ユーザの権限レベル
- Enabled（`Enabled` または `Disabled`）：ユーザがアクティブかどうか
- Reset（`Yes` または `No`）：次のログイン時にユーザがパスワードを変更する必要があるかどうか
- Exp（`Never` または数値）：ユーザのパスワード変更が必要になるまでの日数
- Warn（`N/A` または数値）：パスワードの有効期限が切れる前に、ユーザがパスワード変更のために与えられる日数
- Str（`Yes` または `No`）：ユーザのパスワードが強度チェックの基準を満たす必要があるかどうか
- Lock（`Yes` または `No`）：ログインの失敗が多すぎる場合に、ユーザのアカウントがロックされるかどうか
- Max（`N/A` または数値）：ユーザのアカウントがロックされる前に失敗するログインの最大回数

アクセス（Access）

設定（Configuration）

構文

```
show users
```

例

```
> show users
```

version

製品のバージョンとビルドを表示します。detailパラメータが指定されている場合は、追加のコンポーネントのバージョンが表示されます。

アクセス（Access）

基本

構文

```
show version [detail]
```

例

```
> show version
```

virtual-routers

パラメータが指定されていない場合は、現在設定されているすべての仮想ルータのリスト、およびDHCP リレー、OSPF、およびRIP の情報が表示されます。パラメータが指定されている場合は、指定されたルータに関する情報が、指定されたルート タイプによって制限されて表示されます。パラメータはすべてオプションです。このコマンドはNGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show virtual-routers [ dhcprelay | ospf | rip ] name
```

ここで dhcprelay、ospf、および rip はルート タイプを表します。*name* は、情報を表示する特定のルータの名前を表します。ospf を指定した場合は、ルート タイプ、および（存在する場合は）ルート名に対して neighbors、topology、または lsadb を指定することができます。

例

```
> show virtual-routers ospf VRouter2
```

virtual-switches

パラメータが指定されていない場合は、設定されているすべての仮想スイッチのリストが表示されます。パラメータが指定されている場合は、指定されたスイッチに関する情報が表示されます。このコマンドはNGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show virtual-switches name
```

例

```
> show virtual-switches Vswitch1
```

vmware-tools

VMware Tools が、仮想デバイス上で現在有効になっているかどうかを示します。このコマンドは、NGIPSv のみで使用できます。

VMware ツールは、仮想マシンのパフォーマンスを向上させるためのユーティリティ スイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。このシステムは、すべての仮想アプライアンスで次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup

VMware ツールおよびサポートされるプラグインの詳細については、VMware の Web サイト（http://www.vmware.com）を参照してください。

アクセス（Access）

基本

構文

```
show vmware-tools
```

例

```
> show vmware-tools
```

VPN コマンド

`show VPN` コマンドは、VPN ステータス、および VPN 接続の設定情報を表示します。このコマンドは、NGIPSv デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス（Access）

基本

config

すべての VPN 接続の設定を表示します。

構文

```
show vpn config
```

例

```
> show vpn config
```

config by virtual router

仮想ルータについて、すべての VPN 接続の設定を表示します。

構文

```
show vpn config virtual router
```

例

```
> show vpn config VRouter1
```

status

VPN 接続すべてのステータスを表示します。

構文

```
show vpn status
```

例

```
> show vpn status
```

status by virtual router

仮想ルータについて、すべての VPN 接続のステータスを表示します。

構文

```
show vpn status virtual router
```

例

```
> show vpn status VRouter1
```

counters

すべての VPN 接続のカウンタを表示します。

構文

```
show vpn counters
```

例

```
> show vpn counters
```

counters by virtual router

仮想ルータについて、すべての VPN 接続のカウンタを表示します。

構文

```
show vpn counters virtual router
```

例

```
> show vpn counters VRouter1
```

コンフィギュレーション コマンド

コンフィギュレーション コマンドを使用して、システムを設定および管理することができます。これらのコマンドはシステムの動作に影響を与えます。そのため、基本（Baisc）レベルのパスワード設定（`configure password`）コマンドを除き、設定 CLI アクセス権限を持つユーザのみがこれらのコマンドを発行できます。

bypass

7000 または 8000 シリーズ デバイスで、インライン ペアをフェールオープン（ハードウェア バイパス）モードまたはフェールクローズ モードにします。このコマンドは、インライン セットの [バイパス モード（Bypass Mode）] オプションが [バイパス（Bypass）] に設定されている場合にのみ使用できます。

デバイスを再起動するとインラインセットのフェールオープンモードが解除されるということに注意してください。

アクセス（Access）

設定（Configuration）

構文

```
configure bypass {open | close} {interface}
```

ここで、`interface` はインライン ペアのいずれかのハードウェア ポートの名前です。

例

```
> configure bypass open s1p1
```

high-availability

デバイスで高可用性のバイパスを無効にしたり、設定したりします。このコマンドは、NGIPSv、ASA FirePOWER、またはセカンダリ スタック メンバとして設定されているデバイスでは使用できません。

アクセス（Access）

設定（Configuration）

構文

```
configure high-availability {disable | bypass}
```

例

```
> configure high-availability disable
```

gui

デバイスの Web インターフェイス（システムのメジャーな更新時に表示される、簡潔なアップグレード Web インターフェイスなど）を有効または無効にします。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

設定（Configuration）

構文

```
configure gui [enable | disable]
```

例

```
> configure gui disable
```

lcd

デバイスの正面の LCD ディスプレイを有効または無効にします。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

設定（Configuration）

構文

```
configure lcd {enable | disable}
```

例

```
> configure lcd disable
```

log-ips-connections

記録された侵入イベントに関連付けられている接続イベントのロギングを有効または無効にします。

アクセス（Access）

設定（Configuration）

構文

```
configure log-ips-connections {enable | disable}
```

例

```
> configure log-ips-connections disable
```

manager コマンド

`configure manager` コマンドは、管理元の Firepower Management Center へのデバイスの接続を設定します。

アクセス（Access）

設定（Configuration）

追加

管理元の Firepower Management Center からの接続を承認するようデバイスを設定します。このコマンドは、デバイスがアクティブに管理されていない場合にのみ機能します。

デバイスを Firepower Management Center に登録するには、常に一意の英数字の登録キーが必要です。ほとんどの場合は、登録キーと一緒にホスト名または IP アドレスを指定する必要があります。ただし、デバイスと Firepower Management Center が NAT デバイスによって分離されている場合は、登録キーと一緒に一意の NAT ID を入力し、ホスト名の代わりに DONTRESOLVE を指定します。

構文

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey [nat_id]
```

ここで、{hostname | IPv4_address | IPv6_address | DONTRESOLVE} は、このデバイスを管理する Firepower Management Center の DNS ホスト名、または IP アドレス（IPv4 または IPv6）を指定します。Firepower Management Center を直接アドレス指定できない場合は、DONTRESOLVE を使用します。DONTRESOLVE を使用する場合は nat_id が必要です。regkey は、デバイスを Firepower Management Center に登録するために必要な一意の英数字の登録キーです。nat_id は、Firepower Management Center とデバイス間の登録プロセスで使用される任意の英数字の文字列です。hostname が DONTRESOLVE に設定されている場合に必要です。

例

```
> configure manager add DONTRESOLVE abc123 efg456
```

削除

Firepower Management Center の接続情報をデバイスから削除します。このコマンドは、デバイスがアクティブに管理されていない場合のみ機能します。

構文

```
configure manager delete
```

例

```
> configure manager delete
```

mpls-depth

管理インターフェイスで MPLS レイヤの数を設定します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

設定（Configuration）

構文

```
configure mpls-depth depth
```
ここで *depth* は 0～6 の数値です。

例

```
> configure mpls-depth 3
```

network コマンド

`configure network` コマンドは、デバイスの管理インターフェイスを設定します。

アクセス（Access）

設定（Configuration）

dns searchdomains

DNS 検索ドメインの現行のリストを、コマンドで指定されたリストに置き換えます。

構文

```
configure network dns searchdomains {searchlist}
```
`searchlist` はカンマで区切られたドメインのリストです。

例

```
> configure network dns searchdomains foo.bar.com,bar.com
```

dns servers

DNS サーバの現行のリストを、コマンドで指定されたリストに置き換えます。

構文

```
configure nework dns servers {dnslist}
```
dnslist は、カンマで区切られた DNS サーバのリストです。

例

```
> configure network dns servers 10.123.1.10,10.124.1.10
```

hostname

デバイスのホスト名を設定します。

構文

```
configure network hostname {name}
```
name は新しいホスト名です。

例

```
> configure network hostname sfrocks
```

http-proxy

7000 & 8000 シリーズおよびNGIPSvデバイスで、HTTP プロキシを設定します。コマンドを発行した後で、CLI はユーザに対して HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかを尋ねます。認証が必要な場合はプロキシのユーザ名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

NGIPSv上でこのコマンドを使用して、HTTPプロキシサーバを設定し、仮想デバイスが動的解析のためにファイルを AMP クラウドへ送信できるようにします。

構文

```
configure network http-proxy
```

例

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address:
Enter HTTP Proxy Port:
Use Proxy Authentication? (y/n) [n]:
Enter Proxy Username:
Enter Proxy Password:
Confirm Proxy Password:
```

http-proxy-disable

7000 シリーズ、8000 シリーズ、またはNGIPSvデバイスで、任意の HTTP プロキシの設定を削除します。

構文

```
configure network http-proxy-disable
```

例

```
> configure network http-proxy-disable
Are you sure that you wish to delete the current
http-proxy configuration? (y/n):
```

ipv4 delete

デバイスの管理インターフェイスの IPv4 設定を無効にします。

構文

```
configure network ipv4 delete [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベント インターフェイスでは **eth1** です。

例

```
> configure network ipv4 delete eth1
```

ipv4 dhcp

デバイスの管理インターフェイスの IPv4 設定を DHCP に設定します。管理インターフェイスは DHCP サーバと通信して、設定情報を取得します。

構文

```
configure network ipv4 dhcp [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。DHCP はデフォルトの管理インターフェイスでのみサポートされているため、この引数を使用する必要はありません。

例

```
> configure network ipv4 dhcp
```

ipv4 manual

デバイスの管理インターフェイスの IPv4 設定を手動で設定します。

構文

```
configure network ipv4 manual ipaddr netmask [gw] [management_interface]
```

ここで *ipaddr* は IP アドレスで、*netmask* はサブネットマスク、*gw* はデフォルト ゲートウェイの IPv4 アドレスです。*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベント インターフェイスでは **eth1** です。

例

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

ipv6 delete

デバイスの管理インターフェイスの IPv6 設定を無効にします。

構文

```
configure network ipv6 delete [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベント インターフェイスでは **eth1** です。

例

```
> configure network ipv6 delete
```

ipv6 dhcp

デバイスの管理インターフェイスの IPv6 設定を DHCP に設定します。管理インターフェイスは DHCP サーバと通信して、設定情報を取得します。

構文

```
configure network ipv6 dhcp [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。DHCP はデフォルトの管理インターフェイスでのみサポートされているため、この引数を使用する必要はありません。

例

```
> configure network ipv6 dhcp
```

ipv6 manual

デバイスの管理インターフェイスの IPv6 設定を手動で設定します。

構文

```
configure network ipv6 manual ip6addr/ip6prefix [ip6gw] [management_interface]
```

ここで *ip6addr*/*ip6prefix* は IP アドレスとプレフィックス長、*ip6gw* はデフォルト ゲートウェイの IPv6 アドレスを表します。*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズデバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベント インターフェイスでは **eth1** です。

例

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

ipv6 router

デバイスの管理インターフェイスの IPv6 設定をルータに設定します。管理インターフェイスは IPv6 ルータと通信して、設定情報を取得します。

構文

```
configure network ipv6 router [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズデバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベント インターフェイスでは **eth1** です。

例

```
> configure network ipv6 router
```

management-interface disable

管理インターフェイスを無効にします。複数の管理インターフェイスは、8000 シリーズデバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface disable ethn
```

n は、設定する管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベントインターフェイスです。シスコでは、管理チャネルとイベントチャネルの両方を有効にして、eth0 デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、管理インターフェイス，（564 ページ） を参照してください。

例

```
> configure network management-interface disable eth1
```

management-interface disable-event-channel

指定された管理インターフェイスでイベントトラフィック チャネルを無効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface disable-event-channel ethn
```

n は、設定する管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベントインターフェイスです。シスコでは、管理チャネルとイベントチャネルの両方を有効にして、eth0 デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、管理インターフェイス，（564 ページ） を参照してください。

例

```
> configure network management-interface disable-event-channel eth1
```

management-interface disable-management-channel

指定された管理インターフェイスで管理トラフィック チャネルを無効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface disable-management-channel ethn
```

n は、設定する管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベントインターフェイスです。シスコでは、管理チャネルとイベントチャネルの両方を有効にして、eth0 デフォルト管理インターフェイスを有効のままにすることを推奨して

います。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、管理インターフェイス，（564 ページ） を参照してください。

例

```
> configure network management-interface disable-management-channel eth1
```

management-interface enable

指定した管理インターフェイスを有効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface enable ethn
```

n は、有効にする管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベント インターフェイスです。

デバイスを管理する場合、Firepower Management Center 管理インターフェイスには 2 つの別個のトラフィック チャネルがあります。管理トラフィック チャネルはすべての内部トラフィック（デバイスの管理に固有のデバイス間トラフィックなど）を伝送し、イベント トラフィック チャネルはすべてイベント トラフィック（Web イベントなど）を伝送します。必要に応じて、Management Center で個別のイベント専用インターフェイスを設定し、イベント トラフィックを処理することもできます（Firepower Management Center Web インタ フェースで、この設定が実行されていることを確認してください）。イベント専用インターフェイスは 1 つだけ設定できます。イベント トラフィックは大量の帯域幅を使用する可能性があるので、管理トラフィックからイベント トラフィックを分離することで、Management Center のパフォーマンスを向上させることができます。

デフォルトの eth0 インターフェイスには、デフォルトで管理とイベント チャンネルの両方が含まれています。必要に応じて、イベント専用インターフェイスとして eth0 インターフェイスを有効にできます。可能であれば、デバイス イベント インターフェイスと Firepower Management Center イベント インターフェイスの間で、イベント トラフィックが送信されます。イベント ネットワークがダウンすると、イベント トラフィックは、デフォルトの管理インターフェイスに戻ります。可能な場合には別個のイベント インターフェイスが使用されますが、管理インターフェイスが常にバックアップとなります。

管理インターフェイスを有効にすると、管理とイベント チャンネルの両方がデフォルトで有効にされます。管理チャネルとイベント チャネルの両方にデフォルト管理インターフェイスを使用することをお勧めします。その後、別個のイベント専用インターフェイスを有効にします。Firepower Management Center イベント専用インターフェイスは管理チャネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャネルを単に無効にしてください。

configure network {**ipv4** | **ipv6**} **manual** コマンドを使用して、管理インターフェイスのアドレスを設定します。

例

```
> configure network management-interface enable eth1
> configure network management-interface disable-management-channel eth1
```

management-interface enable-event-channel

指定された管理インターフェイスでイベント トラフィック チャネルを有効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface enable-event-channel ethn
```

n は、設定する管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベントインターフェイスです。シスコでは、管理チャネルとイベントチャネルの両方を有効にして、eth0 デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、管理インターフェイス，（564 ページ） を参照してください。

例

```
> configure network management-interface enable-event-channel eth1
```

management-interface enable-management-channel

指定された管理インターフェイスで管理トラフィック チャネルを有効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface enable-management-channel ethn
```

n は、設定する管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベントインターフェイスです。シスコでは、管理チャネルとイベントチャネルの両方を有効にして、eth0 デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、管理インターフェイス，（564 ページ） を参照してください。

例

```
> configure network management-interface enable-management-channel eth1
```

management-interface tcpport

管理用の TCP ポートの値を変更します。

構文

```
configure network management-interface tcpport port
```
port は設定する管理ポートの値です。

例

```
> configure network management-interface tcpport 8500
```

management-port

デバイスの TCP 管理ポートの値を設定します。

構文

```
configure network management-port number
```
number は設定する管理ポートの値を表します。

例

```
> configure network management-port 8500
```

static-routes ipv4 add

指定した管理インターフェイスの IPv4 スタティック ルートを追加します。

構文

```
configure network static-routes ipv4
add interface destination netmask gateway
```
interface は管理インターフェイス、destination は宛先 IP アドレス、netmask はネットワーク マスク アドレス、gateway は追加するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv4
add eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv4 delete

指定した管理インターフェイスの IPv4 スタティック ルートを削除します。

構文

```
configure network static-routes ipv4
delete interface destination netmask gateway
```

interface は管理インターフェイス、destination は宛先 IP アドレス、netmask はネットワーク マスク アドレス、gateway は削除するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv4
delete eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv6 add

指定した管理インターフェイスの IPv6 スタティック ルートを追加します。

構文

```
configure network static-routes ipv6
add interface destination prefix gateway
```

interface は管理インターフェイス、destination は宛先 IP アドレス、prefix は IPv6 プレフィックス長、gateway は追加するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv6
add eth1 2001:DB8:3ffe:1900:4545:3:200: f8ff:fe21:67cf 64
```

static-routes ipv6 delete

指定した管理インターフェイスの IPv6 スタティック ルートを削除します。

構文

```
configure network static-routes ipv6
delete interface destination prefix gateway
```

interface は管理インターフェイス、destination は宛先 IP アドレス、prefix は IPv6 プレフィックス長、gateway は削除するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv6
delete eth1 2001:DB8:3ffe:1900:4545:3:200:f8ff: fe21:67cf 64
```

password

現行のユーザは、自身のパスワードを変更することができます。コマンドを発行すると、CLI は現在の（古い）パスワードを入力するようユーザに要求し、その後で新しいパスワードを 2 回入力するよう要求します。

アクセス（Access）

基本

構文

```
configure password
```

例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

スタッキングの無効化

7000 および 8000 シリーズ のデバイスでは、次のデバイスに存在するスタック構成はすべて削除されます。

- プライマリとして設定されているデバイスでは、スタックは完全に削除されます。
- セカンダリとして設定されているデバイスでは、そのデバイスはスタックから削除されます。

このコマンドは、NGIPSv または ASA FirePOWER モジュールでは使用できません。また、これを使用してデバイスの高可用性ペアを解除することはできません。

スタッキング階層の上位アプライアンスとの通信を確立できない場合は、このコマンドを使用します。Firepower Management Center を通信で使用できる場合は、代わりに Firepower Management Center の Web インターフェイスを使用するよう伝えるメッセージが表示されます。同様に、プライマリ デバイスを使用できる場合に、セカンダリとして設定されているデバイス上で `stacking disable` を入力すると、プライマリ デバイスからコマンドを入力するよう伝えるメッセージが表示されます。

アクセス（Access）

設定（Configuration）

構文

```
configure stacking disable
```

例

```
> configure stacking disable
```

user コマンド

NGIPSv でのみ使用できます。`configure user` コマンドは、デバイスのローカル ユーザ データベースを管理します。

アクセス（Access）

設定（Configuration）

アクセス

指定したユーザのアクセス レベルを変更します。このコマンドは、指定されたユーザが次にログインするときに有効になります。

構文

```
configure user access username [basic | config]
```

username は、アクセスを変更するユーザの名前を表します。`basic` は basic アクセスを、`config` は configuration アクセスを表します。

例

```
> configure user access jdoe basic
```

追加

指定された名前とアクセス レベルを使用して新しいユーザを作成します。このコマンドでは、ユーザのパスワードを入力するよう要求されます。

構文

```
configure user add username [basic | config]
```

ここで、username は新しいユーザの名前を指定します。`basic` は基本アクセス、`config` は設定アクセスを表します。

例

```
> configure user add jdoe basic
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

aging

ユーザのパスワードに有効期限を設定します。

構文

```
configure user aging username max_days warn_days
```
ここで、username はユーザの名前、max_days はパスワードが有効な最大日数、warn_days は有効期限が切れる前にユーザがパスワードを変更するために確保されている日数を表します。

例

```
> configure user aging jdoe 100 3
```

削除

ユーザとユーザのホーム ディレクトリを削除します。

構文

```
configure user delete username
```
username はユーザの名前を表します。

例

```
> configure user delete jdoe
```

disable

ユーザを無効にします。無効なユーザはログインできません。

構文

```
configure user disable username
```
username はユーザの名前を表します。

例

```
> configure user disable jdoe
```

enable

ユーザを有効にします。

構文

```
configure user enable username
```
username はユーザの名前を指定します。

例

```
> configure user enable jdoe
```

forcereset

ユーザが次にログインするときに、パスワードの変更を要求します。ユーザがログインしてパスワードを変更すると、強度のチェックが自動的に有効になります。

構文

```
configure user forcereset username
```
username はユーザの名前を表します。

例

```
> configure user forcereset jdoe
```

maxfailedlogins

指定したユーザが、ログインで失敗できる最大回数を設定します。

構文

```
configure user maxfailedlogins username number
```
username はユーザの名前、*number* は、ログインで失敗できる最大回数を表します。

例

```
> configure user maxfailedlogins jdoe 3
```

password

ユーザのパスワードを設定します。このコマンドでは、ユーザのパスワードを入力するよう要求されます。

構文

```
configure user password username
```
username はユーザの名前を表します。

例

```
> configure user pasword jdoe
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

strengthcheck

ユーザのパスワードに対する強度の要件を有効または無効にします。ユーザ パスワードの有効期限が切れた場合、または configure user forcereset コマンドを使用した場合は、ユーザが次にログインしたときにこの要件が自動的に有効になります。

構文

```
configure user strengthcheck username {enable | disable}
```

username はユーザの名前を表します。`enable` は指定されたユーザのパスワードの要件を設定し、`disable` は、指定されたユーザのパスワードの要件を削除します。

例

```
> configure user strengthcheck jdoe enable
```

unlock

ログイン失敗の最大数を超過したユーザをロック解除します。

構文

```
configure user unlock username
```

username はユーザの名前を表します。

例

```
> configure user unlock jdoe
```

vmware-tools

NGIPSv での VMware Tools の機能を有効または無効にします。このコマンドは、NGIPSv のみで使用できます。

VMware ツールは、仮想マシンのパフォーマンスを向上させるためのユーティリティ スイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。このシステムは、すべての仮想アプライアンスで次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync

- vmbackup

VMware ツールおよびサポートされるプラグインの詳細については、VMware の Web サイト（http://www.vmware.com）を参照してください。

アクセス（Access）

基本

構文

```
configure vmware-tools [enable | disable]
```

例

```
> configure vmware-tools enable
```

system コマンド

system コマンドを使用して、システム全体のファイルおよびアクセス コントロールの設定を管理することができます。Configuration CLI アクセス権を持つユーザのみが、システム モードでコマンドを発行できます。

アクセス制御コマンド

`system access-control` コマンドは、ユーザがデバイス上でアクセス制御設定を管理できるようにします。

アクセス（Access）

設定（Configuration）

archive

現在展開されているアクセス コントロール ポリシーをテキスト ファイルとして `/var/common` に保存します。

構文

```
system access-control archive
```

例

```
> system access-control archive
```

clear-rule-counts

アクセス コントロール ルールのヒット数を 0 にリセットします。

構文

```
system access-control clear-rule-counts
```

例

```
> system access-control clear-rule-counts
```

rollback

これまでに導入されたアクセス制御設定に対して、システムの復帰を行います。このコマンドをスタックまたは高可用性ペアのデバイスで使用することはできません。

構文

```
system access-control rollback
```

例

```
> system access-control rollback
```

disable-http-user-cert

システム上に存在するすべての HTTP ユーザ証明書を削除します。

アクセス（Access）

設定（Configuration）

構文

```
system disable-http-user-cert
```

例

```
> system disable-http-user-cert
```

file コマンド

`system file` コマンドを使用すると、ユーザは、デバイス上の common ディレクトリにあるファイルを管理することができます。

アクセス（Access）

設定（Configuration）

copy

FTP を使用して、ログイン ユーザ名を使用しているホスト上のリモート ロケーションへファイルを転送します。ローカル ファイルは common ディレクトリに配置する必要があります。

構文

```
system file copy hostname username path filenames filenames ...
```

`hostname` はターゲットのリモート ホストの名前または IP アドレスを表します。`username` はリモート ホスト上のユーザの名前、`path` はリモート ホスト上の宛先パス、`filenames` は転送するローカル ファイルを表します。複数のファイル名はスペースで区切って指定します。

例

```
> system file copy sfrocks jdoe /pub *
```

削除

common ディレクトリから、指定したファイルを削除します。

構文

```
system file delete filenames filenames ...
```

`filenames` は削除するファイルを指定します。複数のファイル名はスペースで区切って指定します。

例

```
> system file delete *
```

list

ファイル名が指定されていない場合は、common ディレクトリ内のすべてのファイルについて変更の時刻、サイズ、およびファイル名が表示されます。ファイル名が指定されている場合は、指定されたファイル名と一致したファイルで、変更の時刻、サイズ、およびファイル名が表示されます。

構文

```
system file list filenames
```

filenames は表示するファイルを表します。複数のファイル名はスペースで区切って指定します。

例

```
> system file list
```

secure-copy

SCP を使用して、ログイン ユーザ名でホストのリモート ロケーションにファイルを転送します。ローカル ファイルは、`/var/common` ディレクトリに配置する必要があります。

構文

```
system file secure-copy hostname username path filenames filenames ...
```

hostname では、対象のリモート ホストの名前または ip アドレスを指定します。*username* では、リモート ホストのユーザ名を指定します。*path* では、リモート ホストの宛先パスを指定します。*filenames* では、転送するローカル ファイルを指定します。ファイル名はスペースで区切ります。

例

```
> system file secure-copy 10.123.31.1 jdoe /tmp *
```

generate-troubleshoot

シスコが解析に使用するトラブルシューティング データを生成します。

アクセス（Access）

設定（Configuration）

構文

```
system generate-troubleshoot
```

この構文は、どのトラブルシューティング データを表示するかを指定するための、オプションのパラメータのリストを表示します。

例

```
> system generate-troubleshoot
```

ldapsearch

ユーザが、指定された LDAP サーバのクエリを実行できるようにします。すべてのパラメータが必須であることに注意してください。

アクセス（Access）

設定（Configuration）

構文

```
system ldapsearch host port baseDN userDN basefilter
```

host は LDAP サーバのドメイン、port は LDAP サーバのポート、baseDN は検索する DN（識別名）、userDN は LDAP ディレクトリへバンドするユーザの DN、basefilter は検索するレコードを表します。

例

```
> system ldapsearch ldap.example.com 389 cn=users,
dc=example,dc=com cn=user1,cn=users,dc=example,dc=com, cn=user2
```

lockdown-sensor

`expert` コマンドを削除し、デバイス上の bash シェルへアクセスします。

注意 このコマンドは、サポートからのホットフィックスがない場合は取り消すことはできません。使用には注意が必要です。

アクセス（Access）

設定（Configuration）

構文

```
system lockdown-sensor
```

例

```
> system lockdown-sensor
```

nat rollback

以前に適用していた NAT の設定に、システムを戻します。このコマンドは NGIPSv または ASA FirePOWER では使用できません。このコマンドをスタックまたは高可用性ペアのデバイスで使用することはできません。

アクセス（Access）

設定（Configuration）

構文

```
system nat rollback
```

例

```
> system nat rollback
```

reboot

デバイスをリブートします。

アクセス（Access）

設定（Configuration）

構文

```
system reboot
```

例

```
> system reboot
```

restart

デバイスのアプリケーションを再起動します。

アクセス（Access）

設定（Configuration）

構文

```
system restart
```

例

```
> system restart
```

shutdown

デバイスをシャット ダウンします。このコマンドは ASA FirePOWER モジュールでは使用できません。

アクセス（Access）

設定（Configuration）

構文

```
system shutdown
```

例

```
> system shutdown
```